Elvin Karimli[*]

THE DEVIL IS IN THE DETAIL: CROSS-BORDER APPLICATION AND (IN)VISIBLE ISSUE OF APPLICABLE LAW IN THE GENERAL DATA PROTECTION REGULATION

Abstract

The advent of modern technologies has recently exposed the EU data protection regime to significant changes. In this vein, the General Data Protection Regulation (GDPR) has improved the previous EU data protection regime and regulated the exponentially increasing form of data processing activities – the extraterritorial data processing activities – at the required level. Accordingly, the applicability issue has played an intriguing role within the framework of the GDPR. Herewith, this article will explore the issue of determining the applicable law within the GDPR. Whereas the GDPR has uniform applicability on the EU level at first sight, a closer examination reveals that the regulation of certain substantive issues is left to the discretion of the Member States. That said, the non-existence of the rule on determining the applicable law within the GDPR puts its objective in peril.

In this article, the applicability of the GDPR will be analyzed in the context of the territorial and extraterritorial reach. Specifically, the criterion of "establishment" the criterion of "offering goods or services" and "monitoring the data subjects' behaviours" will be examined in greater detail in this regard. Furthermore, this article will delve into the (in)visible issue – the determination of applicable law – in the framework of the GDPR. As regards this issue, the possible mechanisms will be scrutinized, and viable solutions will be suggested to determine the applicable law in case of the overlapping of the Member States' laws.

Annotasiya

Müasir texnologiyaların inkişafı son zamanlarda Aİ-nin məlumatların mühafizəsi rejimində əhəmiyyətli dəyişikliklərə səbəb olmuşdur. Bu mənada, Ümumi Məlumatların Qorunması Reqlamenti ("ÜMQR") əvvəlki Aİ-nin məlumatların mühafizəsi rejimini təkmilləşdirmiş və məlumatların emalı fəaliyyətlərinin sürətlə artan formasını – məlumatların eksterritorial emalı fəaliyyətlərini lazımi səviyyədə tənzimləmişdir. Buna uyğun olaraq, tətbiqetmə məsələsi ÜMQR çərçivəsində mühüm rol oynayan məsələlərdən biridir. İlk baxışdan ÜMQR Aİ səviyyəsində vahid tətbiq olunma xüsusiyyətinə malik olsa da, daha yaxından araşdırma müəyyən mühüm məsələlərin tənzimlənməsinin Üzv Dövlətlərin ixtiyarına buraxıldığını göstərir. Beləliklə, ÜMQR daxilində tətbiq olunan qanunun müəyyən edilməsi ilə bağlı qaydanın mövcud olmaması onun məqsədini təhlükə altına qoyur.

Bu Məqalədə ÜMQR-nin tətbiqi ərazi və ekstraterritorial əhatə kontekstində təhlil ediləcəkdir. Konkret olaraq, "təsis" meyarı, "mal və ya xidmətlərin təklif edilməsi" və "məlumat subyektlərinin davranışlarının monitorinqi" meyarı bu mövzuda daha ətraflı araşdırılacaqdır. Bundan əlavə, bu Məqalə ÜMQR çərçivəsində (görünməyən) məsələni –

[*] 2nd year LL.M. student in Intellectual Property Law at Baku State University and Université Lumière Lyon-2 (double degree-program).

tətbiq olunan hüququn müəyyən edilməsini araşdıracaqdır. Bu məsələ ilə bağlı mümkün mexanizmlər müəyyən ediləcək və Üzv Dövlətlərin qanunlarının ziddiyyəti halında tətbiq olunan hüququn müəyyən edilməsi üçün məqsədəuyğun həll yolları təklif olunacaqdır.

CONTENTS

Introduction

The unprecedented expansion of modern technologies can challenge the traditional approaches in legal fields in every domain. Among them, the changes brought by the Internet are required to grab much more attention due to its importance. The Internet can provide everyone with the opportunity to cross the traditionally existing geographical boundaries between the states as freely and easily as the air we breathe. Namely, the delineation of precise boundaries does not exist in this borderless environment. Owing to such ease of online arrangements, the number of persons who utilize the advantages of the Internet is exponentially growing day by day. As a response, approximately all major companies have commenced to restructure their mode of business in accordance with the online environment. Accordingly, the companies have increased data processing activities and this has caused major concerns over privacy and security matters. To put it simply, the Big Tech – GAMAM (Google, Apple, Meta, Amazon, Microsoft) make their services accessible to the users in exchange for their data. Consequently, the raw data has started to become a major source of generating revenue for most companies through behavioural marketing or targeting advertising. It is no coincidence that the raw data is deemed a new oil in the 21st century.

The increased cross-border data processing activities raise the vexing issues on the regulation and protection of privacy and security-related matters of the data subjects. Nevertheless, in the first instance, the determination of the applicable law plays a significant role in the data processing activities. Despite the importance of this issue, there is actually no international treaty or standard for determining the applicable law for the processing of personal data. However, the regulatory initiatives can be found at the regional level. In this vein, the initiatives taken on the European Union (hereinafter EU) level, which are also at the heart of this article, should be ascribed great weight. Thus, two major legal instruments have been adopted by the EU institutions to regulate data processing activities: 1) 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 (hereinafter DPD); 2) the 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 (hereinafter GDPR). The applicability issue has played a crucial role in the frames of both these instruments. In this regard, this article will explore the applicability issue from two standpoints: 1) the applicability of the GDPR itself and 2) the issue of applicable law within the GDPR. Regarding the former, the applicability of the GPDR will be analyzed in light of the territorial and extraterritorial application. In relation to the latter, the intersection between the GDPR and the EU private international law will be addressed. In this respect, it can be understood, at first sight, that there is no room for the problem of overlapping or conflicting laws between Member States in the GDPR. However, by going much deeper, it can become apparent that the Member States' laws still maintain their importance within the GDPR and it leaves several essential issues to the discretion of the Member States to have the last say. To this end, whereas the GDPR is a Regulation in a formal way, it might have a hybrid role between the Regulation and Directive in a material form.[1] In light of this fact, the avoidance of the conflict-of-law rule raises the vexing question as to how to resolve the issue of the applicable law.

Based on the above-mentioned, the first chapter will primarily address the legislative history of the data protection regime within the EU. It will then explain the specificities of the DPD and GDPR in an orderly manner. The second chapter will further elaborate on the applicability issue within the GDPR. Especially, it will focus on the extraterritorial applicability of the GDPR in light of the newly added criteria (*"the offering of goods or services"* and *"the monitoring of the behaviours")*. The third chapter will, in turn, aim at

[1] Jiahong Chen, *How the Best-laid Plans Go Awry: The (Unsolved) Issues of Applicable Law in the General Data Protection Regulation*, 6 International Data Privacy Law 310, 312 (2016).

considering the juxtaposition between the issue of applicable law and the GDPR, and focus on finding the possible solutions for determining the applicable law within the GDPR.

I. The EU Data Protection Law and Legislative History within the EU

The formulation of data protection on the European level has approximately the same lifetime as the development of the European Union. In this context, data protection has been included as an integral part of the Treaty on the Functioning of the European Union (hereinafter TFEU), which is one of two treaties forming the constitutional basis of the EU, through Article 16 (1). Pursuant to this Article, *"everyone has the right to the protection of personal data concerning them"*.[2] Furthermore, Article 16 (2) expressly gives a mandate to the EU to legislate with respect to the protection of the individual's personal data in case of data processing activities. The advent of modern technologies and the increasing importance of personal data can bring data protection to the level of fundamental human rights. In this regard, the Charter of Fundamental Rights of the European Union (hereinafter Charter) goes a bit further and includes data protection in its composition. Under Article 8 (1), the Charter stipulates that *"everyone has the right to the protection of personal data concerning him or her"*.[3] In addition, Article 8 (2) contains the legitimate basis on which the processing of personal data is authorized. Regarding this, the Treaty of Lisbon made the Charter a legally binding instrument and incorporated the latter into the EU law.[4] By doing so, data protection as a fundamental right under the Charter is also incorporated into the integral part of the EU.

In light of this development, further initiatives have been taken to ensure the specific legislative acts regarding data protection on the EU level. These legislative acts refer to the DPD and the GDPR in a respective manner. Hence, this chapter will primarily focus on the legislative history of data protection within the EU and the specificities of the DPD and the GDPR.

A. The Legislative History of the Data Protection on the EU Level

The increasing concerns of the EU with respect to data protection were, to a certain extent, derived from the horrific experiences during World War II,

[2] European Union, Consolidated Version of the Treaty on the Functioning of the European Union, art. 16 (1) (2012).
[3] European Parliament, Charter of Fundamental Rights of the European Union, art. 8 (2000).
[4] *See* European Union, Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, art. 6 (2007).

in which personal data was used to identify Jewish individuals.[5] In its turn, the first legislative act, on both the EU and worldwide level, concerning data protection was adopted in Germany, the State of Hesse.[6] Such initiatives in data protection could further trigger the introduction of new legislative acts by other Member States. In this context, Sweden adopted the nationwide data protection legislation in 1973, which was further followed by Germany and France.[7]

As time evolved, the general legislative act was required on a European level in the context of the data protection regime. The first active role was taken by the Council of Europe instead of the EU. In the early 1970s, the Council of Europe took an initiative to strengthen the protection of personal data on a European level and two recommendations –Resolution (73) 22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector in 1973, and Resolution (79) 29 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector in 1974 – were adopted by the Committee of Ministers to the Member States.[8] As a continuation of these recommendations, the Council of Europe, at last, adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter Convention 108) in 1981. As per Article 1 of this Convention, the objective is to *"secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")"*.[9] As a result of this initiative, this Convention has been ratified approximately by 50 States, among which, all EU Member States currently exist.[10] In light of Convention 108, the European Commission sought to urge all Member States to adopt this Convention to strengthen the data protection regime. Nevertheless, the ratification of the Convention 108 lacked consistency among the EU Member States, specifically, some of which conducted the ratification process very later or some of them arrived at different conclusions through the ratification. Henceforth, the European Commission decided to take the role on its own to harmonize the national laws concerning data protection within the EU.

[5] The GDPR Is Just the Latest Example of Europe's Caution on Privacy Rights. That Outlook Has a Disturbing History (2018). Available at: https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/ (last visited Apr. 18, 2023).
[6] Dan Jerker B. Svantesson, *The Extraterritoriality of EU Data Privacy Law Its Theoretical Justification – Its Practical Effect on U.S. Businesses*, 50 Stanford Journal of International Law 53, 57 (2014).
[7] Orla Lynskey, The Foundations of EU Data Protection Law, 47 (2015).
[8] Council of Europe, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, para. 4 (1981).
[9] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, art. 1 (1981).
[10] Chart of signatures and ratifications of Treaty 108, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108 (last visited Apr. 18, 2023).

B. The Data Protection Directive

Since the adoption of Convention 108, the data has commenced becoming a valuable asset and a commodity on its own in the world market economy. Even though Facebook's motto states that *"It's free and always will be"*, it does not reflect the practical reality.[11] Notably, the raw data of the individuals has a significant commercial value for the data controllers or processors to sell them businesses for the purpose of targeting advertising. To this end, the European Commission adopted the DPD in 1995 as a response to the transforming nature of the data in the global economy.

The DPD aimed at ensuring two major objectives: firstly, the protection of the personal data of the EU individuals as a fundamental right, secondly, the prevention of blocking the free flow of the data by the Member States to improve the market economy. Herewith, the European Commission not only secured the protection of personal data at the required level but also took into consideration the indispensable role of the data for the purpose of the modern economy.[12] The further advantage of the DPD was concerned with the improvement of the functioning of the internal market by harmonizing the data protection legislations within the EU.[13]

To begin with, the scope of the DPD's applicability plays a significant role in delving much deeper into the substantive provisions of this Directive. The cases under which the DPD's applicability was triggered were enshrined under Article 4 of the DPD. As regards these cases, the primary emphasis is put on the data processing activities within the EU, but not beyond the border.[14] The reason behind this approach lies in the fact during the drafting process, the cross-border data processing activities had not received much more attention than the current period. To provide a full picture, there is a need to look into Article 4, which is specified in the following:[15]

Article 4

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

a. the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

[11] Adèle Azzi, *The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation*, 9 Journal of Intellectual Property, Information Technology and E-Commerce Law 126, 127 (2018).

[12] 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, art. 1 (1995).

[13] Lynskey, *supra* note 7, 49-50.

[14] Christopher Kuner, Transborder Data Flows and Data Privacy Law, 235 (2013).

[15] *Supra* note 12, art. 4.

b. the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

c. the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

The aforementioned Article expressly reinforced the fact that the applicability scope of the DPD was primarily confined to the territorial boundaries of the EU or required a sufficient territorial link for its applicability to non-EU data processing activities. Therefore, Article 4 (1) (a) and Article 4 (1) (c) relied specifically upon the territorial connecting factor – *"the existence of the establishment"* and *"the territorial presence of the equipment in the EU"*. The DPD's affiliation with the territoriality principle lags behind the incremental development of modern technologies. Specifically, the technological developments have led to an increased processing of individuals' personal data outside the EU, and the regulation of the data processing activities beyond the borders of the EU has started to play a much more significant role than before. In this regard, as Kuner notes, *"most of the controversies surrounding European data protection law have been caused by the fact that legal instruments designed mainly for intra-EU use have been forced by the expanding information economy to be applied to global problems on a scale for which they were not intended"*.[16] Accordingly, there is a need to adopt the novel data protection regime within the EU.

C. The General Data Protection Regulation

In light of the increased nature of the cross-border data processing activities, the territoriality principle within the DPD seems to be old-fashioned and it necessitated avoiding the straightforward approach of the territoriality principle. Herewith, the DPD was repealed by the GDPR which came into effect on May 25, 2018. By coming into force, the GDPR steps in and harmonizes the data protection regime for all Member States in the same manner. Likewise, the divergences between the data protection laws of the Member States can be brought to the minimum by adopting a uniform law.

Along with the uniform applicability, the GDPR brings about the game-changing amendments by outstretching its applicability even into the cross-border cases in which the data controller has no territorial presence in the EU, however, carries out the data processing of the persons residing in this

[16] Kuner, *supra* note 14.

Union.[17] In lieu of the old-fashioned equipment criterion, Article 3 of the GDPR has introduced new connecting factors, i.e., the offering of goods or services to data subjects in the Union[18] and the monitoring of their behaviours as far as their behaviours take place within the Union.[19] To provide a better overview, it would be insightful to put forward Article 3 in the following:[20]

Article 3

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

b. the monitoring of their behavior as far as their behavior takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

It infers that the cross-border application of the GDPR is conditioned upon two criteria, which include, on the one hand, the offering of goods or services, on the other hand, the monitoring of the EU individuals. Accordingly, the following chapter will elaborate on these aspects in detail.

II. The Issue of the Applicability within the EU Data Protection Law

Since the adoption of the GDPR, the issue of applicability has always been given great weight. Specifically, as the newly added criteria add the flavour of extraterritoriality to the GDPR, the analysis of the applicability has always been at the heart of international academia.

Accordingly, this chapter will address the in-depth analysis of the applicability issue within the GDPR. Prior to this analysis, the predecessor of this Article in the DPD will be specified, and the GDPR's counterpart will be compared in relation to the former on the basis of the newly-added criteria.

[17] Paul de Hert, Michal Czerniawski, *Expanding the European Data Protection Scope Beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context*, 6 International Data Privacy Law 230, 238 (2016).

[18] 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) (Text with EEA relevance), art. 3 (2) (a) (2016).

[19] *Id.*, art. 3 (2) (b).

[20] *Id.*, art. 3.

By doing so, it can shed much light on the better comprehension of the applicability of the GDPR.

A. The Clause on Applicable Law in Data Protection Directive

The applicability issue within the DPD had been formulated with regard to the peculiarities of its legislative form and it leaves the implementation to the discretion of Member States through their national laws as a Directive.[21] Accordingly, this situation elevated the possibility of the conflicting of Member States' laws into an evitable issue. To prevent the existence of the chaotic situation in the further application, the applicability clause under Article 4 was included in the composition of the DPD.

As it infers from this Article, three different applicability cases are identified: a) the placement of the establishment of the controller; b) the application by virtue of public international law; and c) the placement of the equipment used for processing data. Accordingly, the major connecting factor for determining the applicable law is related to the placement of the establishment and the equipment.[22] By doing so, the DPD relied on the territoriality principle by following the traditional approach of private international law.[23]

As time evolves, the advent of modern technologies has warranted a more flexible stance towards Article 4. Likewise, the advisory body of the DPD, Article 29 Data Protection Working Party (hereinafter Working Party), had pronounced its opinion on the applicable law in 2010,[24] which sought to provide a clear understanding of Article 4 to prevent any uncertainty for all stakeholders.

In the first instance, the Working Party was primarily focused on the notions of *"establishment"* and *"processing in the context of the activities of establishment"* under Article 4 (1) (a).[25] Firstly, by referring to Recital 19 of the DPD, the Working Party determined that the notion of *"establishment"* entails the effective and real exercise of activity through stable arrangements.[26] However, it took a flexible approach and interpreted the *"establishment"* in such a manner as to make the legal form of this establishment a non-determining factor.

The degree of the involvement of the establishment in the data processing activities plays a critical role in assessing the *"processing in the context of the*

[21] Directive (EU), https://uk.practicallaw.thomsonreuters.com/1-107-6116?transitionType=Default&contextData=(sc.Default)&firstPage=true (last visited Apr. 18, 2023).
[22] Lokke Moerel, *The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?*, 1 International Data Privacy Law 28, 28 (2011).
[23] *Ibid.*
[24] *See* Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law (2010).
[25] *Id.*, 11-12.
[26] *Id.*, 11.

activities of establishment". In this respect, it is necessary to delve into the question of *"who is doing what?"*.[27] Through this question, it can be identified whether the establishment is processing the personal data in the context of its own activities or the activities of another establishment. As far as the former is concerned, the law of the Member State where the establishment itself is situated is applied. Nonetheless, in case it is related to the activities of another establishment, the law of the Member State where the other establishment is located comes into play.[28]

Furthermore, the Working Party has centred on Article 4 (1) (c). The inclusion of this provision was necessitated by the higher likelihood of the processing at a distance without any presence in the EU.[29] Accordingly, this case is applicable even when there is no physical presence in the EU territory, however, there is already a close connection with this territory. In this case, the connecting factor is conditioned upon the localization of the equipment used for the processing. In the light of the flexible approach, the Working Party interpreted this criterion in the context of *"means"* instead of *"the equipment"*.[30] The reason lies in the fact that the notion of *"equipment"* would have a much narrower meaning than *"means"*, which is primarily focused on a physical apparatus rather than *"any possible means"*.[31] By this technique, the scope of this criterion is widened and even includes the cookies or JavaScript banners for the processing of personal data.

In addition, Article 4 of the DPD not only regulates the cases under which the DPD is applicable but also determines the applicable law in case of a conflict between the Member States' laws. Herewith, it seems to have a two-stage function: in the first place, it determines whether European law is applicable to the processing of personal data as opposed to the law of a non-EU country.[32] If the first stage is met, then it seeks to identify the law of which Member State is applicable to the case at hand.[33] To this end, this Article is also referred to as the *"conflict-of-law rule"*, which intends to prevent the conflicting of laws if necessary.

B. The GDPR's Applicability and Its Newly-Added Criteria

As it evolved over time, significant initiatives have been taken to enhance the lacking aspects of the DPD. That being so, the new legislative act – the

[27] *Id.*, 14.
[28] *Ibid.*
[29] Article 29 Data Protection Working Party, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, 12 (2002).
[30] *Supra* note 24, 2.
[31] Douwe Korff, EC Study on Implementation of Data Protection Directive, Comparative Summary of National Laws, 48 (2002).
[32] Maja Brkan, *Data Protection and European Private International Law*, European University Institute Schuman Center for Advanced Studies, Working Paper 2015/40, 32 (2015).
[33] *Ibid.*

GDPR – was adopted and it had introduced several significant changes to the applicability issue in the previous data protection legislation. Namely, the GDPR's applicability under Article 3 has raised very engaging issues with its newly added criteria and extraterritorial reach.[34]

As inferred from the content of Article 3, it does not completely diverge from its predecessor – Article 4 of the DPD. To put it differently, two cases triggering the applicability under Article 4 of the DPD also remain intact in Article 3 of the GDPR: a) the existence of the establishment of the controller or processor in the Union and b) the application by virtue of public international law. Along with them, the GDPR gives effect to the new criteria, which expand its territorial reach outside the EU. Pursuant to these criteria, the companies operating outside the EU can find themselves under the cloak of the GDPR when the processing is carried out in relation to the offering of goods or services[35] or to the monitoring of the behaviours[36] insofar as the data subjects are within the EU.

At first glance, the understanding of Article 3 seems to be straightforward, however, it can cause challenging issues in a practical sense. Therefore, it is much worth examining this Article in a thorough manner.

1. The Case of the Establishment in the European Union

The first case under Article 3 (1) is essentially following the traces of its counterpart under the DPD.[37] The applicability of the GDPR can be triggered in the case of the processing in the context of the activities of the establishment in the EU. Thus, the first criterion relies upon the territoriality principle by requiring physical presence within the EU, and the three-layered approach is upheld.[38]

Firstly, the central term under this Article is concerned with the notion of the *"establishment"*. As is in the DPD, the GDPR itself does not provide the definition of the *"establishment"* in the context of Article 3 (1). In this regard, this paper can recourse to Recital 22 of the GDPR and guidelines of the European Data Protection Board (hereinafter EDPB). By referring to Recital 22, the EDPB explains that the notion of *"establishment"* implies the effective and real exercise of activity through stable arrangements,[39] and the matters of the registration and legal form of the undertakings are deemed non-determining factors for evaluating the *"establishment"*. In this respect, the degree of the stability of the arrangements and the effective exercise of activities through the necessary human and technical resources should be

[34] Hert, Czerniawski, *supra* note 17, 237.
[35] *Supra* note 18.
[36] *Id.*, art. 3 (2) (b).
[37] Manuel Klar, *Binding Effects of the European General Data Protection Regulation (GDPR) on U.S. Companies*, 11 Hastings Science and Technology Law Journal 102, 106 (2020).
[38] European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Art. 3), 5 (2020).
[39] *Supra* note 18, recital 22.

taken into consideration for the determination of the *"establishment"*.[40] The current expansion of the Internet and online activities has lessened the threshold to a minimum. Accordingly, the degree of stability and the effective exercise of activities do not require the undertakings to have a complex corporate structure; instead, the presence of one representative with necessary resources might be sufficient to be considered a stable establishment.[41]

The second layer constitutes the processing in the context of the activities of the establishment. This layer sought to strike a balance in the effective interpretation of Article 3 (1). Notably, it prevents, on the one hand, the confinement of the scope of Article 3 (1) to the cases when the processing is carried out by the establishment itself.[42] On the other hand, it prevents too far-reaching applicability in cases when the operation of the establishment has the remotest connections with the data processing of the non-EU data controller or processor.[43] The EDPB has determined that there is a need, at least, for the existence of the inextricable link between the operation of the establishment and the data processing activities of non-EU data controllers or processors.[44] Further, the EDPB has recalled the fact of loosening the criterion to mere advertising or sales establishments. To put it simply, the revenue-raising activities, which are inextricably linked to the data processing, fall squarely within the context of the activities of the establishment.[45]

Such a flexible approach is also taken by the CJEU in Google Spain and Weltimmo cases consecutively. Even though these cases were handed down in the lifespan of Article 4 of the DPD, they have still been relevant with respect to Article 3 (1) of the GDPR.[46]

a. Google Spain and Google Cases

The case is primarily concerned with the dispute between, on the one hand, Google Spain SL (hereinafter Google Spain) and Google Inc., and on the other hand, the Agencia Española de Protección de Datos (hereinafter AEPD) and Mr. Costeja González. As a Spanish national resident, he filed a complaint before AEPD concerning his name and personal data which appear in links relating to the Spanish daily newspaper La Vanguardia on the search results of Google search engine.[47] Mr. Costeja González requested to remove such search results mentioning Mr. Costeja González's name for a real estate auction having the connection with attachment proceedings to recover the

[40] Berkholz v. Finanzamt Hamburg-Mitte-Altstadt, C-168/84, Judgment, para. 18 (1985).
[41] Merlin Gömann, *The new territorial scope of EU data protection law: Deconstructing a revolutionary achievement*, 54 Common Market Law Review 567, 575 (2017).
[42] *Supra* note 38, 7.
[43] *Ibid.*
[44] *Id.*, 8.
[45] *Ibid.*
[46] Klar, *supra* note 37, 106.
[47] Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12, Judgment, para. 14 (2014).

social security debts.[48] Preliminarily, AEPD upheld such a claim as opposed to the Google search engine and took the view that it should withdraw the concerned personal data. As opposed to this decision, Google Spain and Google Inc. lodged separate action with AEPD on this matter. Due to the complexity of this case, the AEPD referred it to the CJEU to give a preliminary ruling on the basis of three questions. Among these questions, this part will be solely focused on the question concerning Article 4 (1) of the DPD, and the other ones will not be touched upon due to the non-relevancy.

Regarding the question in Article 4 (1) (a) of the DPD, three different scenarios were presented for the CJEU to epitomize the case.[49] Among these scenarios, the Court started the analysis of Article 4 (1) (a) in the case where *"the operator of the search engine sets up in a Member State an office or subsidiary for the purpose of promoting and selling advertising space on the search engine, which orientates its activity towards the inhabitants of that State"*.[50] In this regard, by just relying on Recital 19 of the DPD, the Court reinforced the view that the establishment implies the effective and real exercise of the activity through stable arrangements.[51]

After expounding the notion of the establishment, the Court delved much deeper into the dissection of the *"in the context of the activities of the establishment"*, which was also the turning point in broadening the scope of Article 4 (1) (a). In this regard, the Court stood in line with the argument of Mr. Costeja González and determined that the notion of *"in the context of the activities of the establishment"* should not be read restrictively.[52] The Court pointed out that it is not required for Article 4 (1) (a) to have the data processing carried out by the establishment itself; rather, it suffices to ensure the inevitable link between the establishment and the data processing.[53] Accordingly, the Court noted that although Google Spain itself did not participate in the data processing, such economic activities, e.g., *promoting the sales and advertising space*, made the operation of the data processing by the search engine profitable and could fall within this link.

b. Weltimmo Case

The reasoning of the CJEU in Google Spain and Google Inc. case was followed by Weltimmo judgment after a couple of years. The dispute which occurred between the company of Weltimmo and the Hungarian Data Protection Authority was related to the fine imposed by the latter for encroaching the Hungarian Law on freedom of information.[54] Weltimmo is a

[48] *Ibid*.
[49] *Id.*, para. 45.
[50] *Ibid*.
[51] *Id.*, para. 48.
[52] *Id.*, para. 53.
[53] *Id.*, para. 55-56.
[54] Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, Judgment, para. 2 (2015).

company registered in Slovakia and manages a website dealing with properties located in Hungary. To this end, it conducted the data processing of the advertisers. The advertisements are free of charge for one month and from onwards the fee is charged. Therefore, the advertisers requested Weltimmo to delete their announcements and personal data from the website, nevertheless, it did the contrary, even passing on these data to the debt collection agencies. As a result, the advertisers filed a complaint before the Hungarian Data Protection Authority which declared itself competent to hear the case and fined the company of Weltimmo for the infringement of the relevant legislation.[55] Weltimmo then forwarded the case to the Budapest Administrative and Labor Court and argued that the Hungarian Data Protection Authority is not entitled to apply the Hungarian Law due to the location of the company in another Member State.[56] By the same token, the Court dismissed this defence and upheld the decision of the Hungarian Data Protection Authority. Thereafter, Weltimmo appealed on the same ground to the Hungarian Supreme Court which referred the issue on the applicable law under Article 4 (1) of the DPD to the CJEU for the examination.

The CJEU examined the determination of the applicable law to the data processing carried out by the company which on the one hand, had the registration office in one Member State, on the other hand, operated in another Member State. To this end, the Court predominantly heeded the notion of *"establishment"* and *"in the context of the activities of the establishment"*. By following the traces of the Google Spain and Google Inc. case, the CJEU relied on the same definition of the establishment as implying the effective and real exercise of the activities through stable arrangements.[57] Unlike the Google Spain and Google Inc. case, the Court did not confine its reasoning merely to the above-mentioned explanation and lessened this criterion. The Court stressed that the mere presence of one representative can also be sufficient to fall within this criterion in the case of having a substantial level of stability and necessary equipment for the provision of services.[58]

Furthermore, the Court reinstated the approach made in the Google Spain and Google Inc. case towards the notion of *"in the context of the activities of the establishment"*, which necessitates the flexible and broad interpretation of this notion.[59]

By applying such reasoning, the Court made a big step in adapting to the demands of the modern period. Especially, its findings on the notion of *"the establishment"* can give the green light to the applicability of EU data protection legislation even for the non-EU data controllers fulfilling the data

[55] *Id.*, para. 10.
[56] *Id.*, para. 11.
[57] *Id.*, para. 28.
[58] *Id.*, para. 30.
[59] *Id.*, para. 34-35.

processing through one representative permanently residing in the EU.[60] Such flexible approaches have also played a role of a primary harbinger for the recent shape of EU data protection legislation.

2. The Offering of Goods or Services to the Data Subjects Located in the EU

The criterion of the offering of goods or services is incorporated into the GDPR owing to the incremental ease of the data processing activities at a distance through the rapid development of modern technologies. Accordingly, the initial elaboration and analysis of this criterion is provided for by the GDPR itself in Recital 23 which enshrines the following:

"… In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor ***envisages*** *offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such* ***intention****, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union".*[61]

As a starting point, Recital 23 can provide us with two major benchmarks for an all-inclusive understanding of this criterion: 1) envisaging the offering of goods or services to the data subjects in the EU; 2) having a clear intention.[62] These benchmarks refer to the "targeting" approach as evidenced by the EDPB.[63] Even though this criterion expressly becomes part of the EU data protection law through the GDPR, its roots date back to the operational period of the DPD. Specifically, the Working Party determined the targeting of, or orientating the business activities towards, the EU individuals as an additional criterion for the applicability of the DPD.[64] Moreover, the Working Party spelt out several factors, e.g. the availability of information or advertising in EU languages, the accessibility of the services or products for the EU individuals, and the purchase of the services or products through an EU credit card. That being so, these factors equated, in part, the targeting

[60] Gömann, *supra* note 41, 575.
[61] *Supra* note 18, recital 23.
[62] Maja Brkan, *Data Protection and Conflict-of-Laws: A Challenging Relationship*, 3 European Data Protection Law Review 324, 337-338 (2016).
[63] *Ibid.*; *See also* Dan Jerker B. Svantesson, *Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation*, 5 International Privacy Law Review 226, 231 (2015).
[64] *Supra* note 24, 31.

approach under the data protection law with the criterion of orientating or directing activities in the consumer protection law.[65]

The traces of the targeting approach taken by the Working Party are followed by the GDPR as incorporating the criterion of offering goods or services to persons in the EU. This criterion is approached by Recital 23 of the GDPR and the EDPB in light of the targeting approach.[66] By the same token, the offering of goods or services is also analogous, to a certain extent, to the criterion of orientating or directing activities towards the EU in the consumer protection law.[67] In this regard, it is worth noting that the interservice draft version of the GDPR proposed by the European Commission included the benchmark of directing activities rather than the offering of goods or services.[68] Accordingly, it stems from that the drafters of the GDPR had in mind the criterion of directing activities when drafting the current Article 3 (2) (a). Nevertheless, these two criteria are not equated with each other, and the CJEU cases regarding the directing activities in the consumer protection law could just be assistance in unveiling the offering of goods or services in the data protection law. Prior to having recourse to these cases, it is deemed necessary, firstly, to touch upon the interrelation between the consumer and data protection law.

a. The Interrelation between the Consumer and Data Protection Law

Before the widespread use of modern technologies, the parallelism between consumer law and data protection law existed at a minimum level. However, the over-paced expansion of the Internet and e-commerce can intermingle these fields with each other. Accordingly, the legal systems of some developed states, e.g., the USA, consider data protection law as an inseparable part of consumer law.[69] This tendency is also followed in the framework of the EU legal system. Nevertheless, unlike the USA, the simple fact of being a data subject does not automatically equate it with the notion of the *"consumer"* in the EU legal system.[70] To qualify as a consumer, the data subject is required to conclude a contract for purposes which are beyond their trade or profession. In this context, it should be noted that most of the online services are offered to the data subjects in a contractual arrangement.[71] As an example, some social media websites, e.g., Facebook[72], and LinkedIn[73],

[65] *Ibid.*
[66] *Supra* note 18, recital 23; *supra* note 38, 14.
[67] Svantesson, *supra* note 63, 231; Brkan, *supra* note 62, 338.
[68] Azzi, *supra* note 11.
[69] Paul Bernal, Internet Privacy Rights: Rights to Protect Autonomy, 113 (2014).
[70] Korff, *supra* note 31, 13.
[71] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), art. 17 (1) (2012).
[72] Terms of Service (2022), https://www.facebook.com/terms.php (last visited April 19, 2023).
[73] User Agreement (2022), https://www.linkedin.com/legal/user-agreement (last visited April 18, 2023).

condition the usage of their services upon the Terms of Service which can trigger the contractual arrangement.

Furthermore, the similarity between these legal fields is based on the fact that both the data subjects and consumers are of unequal bargaining power as weaker parties in their contractual relationship in relation to the other contracting party.[74]

Based on the above-mentioned, the data subjects and consumers can be treated alike in most cases, so there is no well-grounded hindrance to using the interpretation of the criterion of *"directing activities"* under the consumer protection law in the analysis of the criterion of *"the offering of goods or services"* under the data protection law.

b. The Criterion of Directing Activities under the Consumer Protection Law

The concept of directing activities in the framework of the consumer protection law is regulated under both Article 17 (1) (c) Brussels I Regulation and Article 6 (1) of the Rome I Regulation. The former states that the jurisdictional rules over the consumer contracts are applicable if the professional directs its business activities towards the EU Member State,[75] in turn, the latter prescribes that the consumer contracts shall be governed by the country of a domicile of the consumer if the professional directs its business activities towards that country.[76] Meanwhile, the CJEU cases intended for the analysis of the directing activities under these Regulations, specifically the Brussels I Regulation, are of relevance in the understanding of the criterion under Article 3 (2) (a) of the GDPR.

i. Joined cases of Pammer and Hotel Alpenhof

The cases of Pammer and Hotel Alpenhof were instituted separately, nevertheless, the identical nature of these cases necessitated their joining by the CJEU in one proceeding for a preliminary ruling.

Regarding the Pammer case, the dispute between Mr. Pammer who resided in Austria, and a German-based company arose from the contract, which was related to the voyage by freighter concluded between Mr. Pammer and a German-based intermediary company.[77] In this case, Mr. Pammer booked his voyage through the website of the intermediary company. However, by arguing the non-compliance of the website conditions with the real vessel conditions, he sued a German-based company before the Austria District Court. In turn, a German-based company dismissed such a claim on the ground that it did not pursue or direct any business activities in Austria and

[74] Brkan, *supra* note 32, 12-13.
[75] *Supra* note 71, art. 17 (1) (c).
[76] Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), art. 6 (1) (2008).
[77] Peter Pammer v. Reederei Karl Schlüter GmbH & Co. KG and Hotel Alpenhof GesmbH v. Oliver Heller, Joined Cases, C-585/08 and C-144/09, Judgment, para. 14 (2010).

the court lacked jurisdiction. In the end, the first instance court upheld Mr. Pammer's claim. Nevertheless, by appealing to the appellate court, a German-based company succeeded in the dismissal of the ruling of the first instance court. In any case, the case was referred to the Supreme Court by Mr. Pammer. As a result of the conflicting issues, the Supreme Court submitted this case to the CJEU for preliminary ruling with two questions one of which is concerned with the criterion of directing activities.

With respect to the Hotel Alpenhof case, the dispute arose between a consumer, Mr. Heller, who resides in Germany and the hotel Company, the Hotel Alpenhof, which was located in Austria. Mr. Heller had reserved a number of rooms through the website of the hotel concerned.[78] However, he found fault with the hotel's services and left his bill without any payment. Accordingly, the Hotel Alpenhof filed a lawsuit before the Austrian District Court on the basis of its domicile. As opposed to this lawsuit, Mr. Heller raised an objection on the ground that the court lacked jurisdiction, and the lawsuit should have been filed before the court of the Member State of his domicile due to being a consumer. Both the first instance court and the appellate court dismissed the claim of the Hotel Alpenhof on the same ground which was raised by Mr. Heller. As a last resort, the Hotel Alpenhof appealed to the Supreme Court to hear this case. As in the Pammer case, the Supreme Court stayed the proceedings and referred the case to the CJEU for a preliminary ruling with the question concerning the directing activities. The CJEU was asked to determine through which criteria a trader's business activity offered on its website or on that of its intermediary can fall under the cloak of the criterion of directing the activity to the Member State of the consumer's domicile, within Article 15 (1) (c) of Brussels I Regulation.

Primarily, the Court approached this issue from the perspective of the subjective intention of the trader. Specifically, it questioned whether the directing business activities relate to the trader's intention in targeting the Member State or refer to any activity which *de facto* targets the Member State regardless of the existence of any intention.[79] In this regard, the CJEU took the view that the trader's intention should exist in relation to be considered as the directing business activities towards the Member State.[80] The Court justified its reasoning on the ground that in case of disregarding such intention, the mere accessibility of the website can trigger the criterion of directing business activities. Likewise, if this was intended by the drafters of the Regulation, the accessibility of the website would have been spelt out rather than directing business activities.[81] By providing this reasoning, the CJEU also relied on the opinion of the Advocate General which stated that *"it is essential for there to be*

[78] *Id.*, para. 26.
[79] *Id.*, para. 63.
[80] *Id.*, para. 75.
[81] *Id.*, para. 71.

active conduct on the part of the undertaking, the objective and outcome of which is to win customers from other Member States".[82] Accordingly, the CJEU formulated that the trader should envisage the business activities with the mind to conclude a contract.

After finding the subjective intention as an integral part of the criterion of the directing activities, the CJEU shifted its focus to the objective factors for revealing such intention.[83] By doing so, the Court intended to prevent the absolute confinement of this criterion into the subjective test and add certain objectivity to simplify the assessment process. The non-exhaustive list of these factors was spelt out by the CJEU as the following: the international nature of the business or commercial activity, the indication of telephone numbers with an international code, mention of itineraries from other Member States for going to the place where the trader is established, the usage of a language or a currency other than the ones generally used in the Member State where the trader is established, outlay of expenditure on an internet referencing service in order to facilitate access to the trader's site or that of its intermediary by consumers domiciled in the other Member States, the usage of a top-level domain name other than the one of the Member State where the trader is established, and mention of an international clientele composed of customers domiciled in various Member States etc.[84] Furthermore, the Court further took the view that these factors are of importance as evidence rather than essential conditions in determining the criterion. Therefore, a case-by-case analysis is necessary for this purpose.

In light of the fact that the criterion of directing activities and the offering of goods or services resemble each other, the reasoning of CJEU in the Pammer and Hotel Alpenhof joined cases can provide ample guidance in evaluating the criterion of the offering of goods or services under Article 3 (2) (a) of the GDPR.[85] Primarily, the non-exhaustive list of the factors spelt out in this case is of a higher relevance on this matter. Specifically, a number of these factors, e.g. the use of language or currency of the directed Member States, the availability of the email and contact details with an international code, and the international nature of the business activities, are also specified in Recital 23 of the GDPR. Moreover, both the reasoning of the CJEU and Recital 23 of the GDPR are tailored to envisaging the business activities for analyzing each of these criteria.[86] Accordingly, it can be drawn that the GDPR followed the traces of the reasoning of the CJEU in this case when formulating its own criterion.[87] Owing to such similarity, it does not seem problematic to utilize

[82] *Id.*, para. 64.
[83] *Id.*, para. 93.
[84] *Ibid.*
[85] *Supra* note 38, 17.
[86] *Supra* note 71.
[87] *Ibid.*

the other factors, which are not included in Recital 23, of this reasoning in gauging the criterion of the offering of goods or services.

In addition, the CJEU ruling in the Pammer and Hotel Alpenhof joined cases plays a significant role in relation to the interactivity of the websites.[88] To put it simply, the question arises as to whether the distinction between passive or active websites is relevant to the assessment for the criterion of directing business activities. Such a distinction between websites is rooted in the USA legal system and came into the picture after the landmark Zippo judgment,[89] which divided the websites into three categories, (passive, interactive and active ones), on the basis of which the jurisdictional questions on the Internet-based disputes could be inquired.[90] On this issue, the CJEU in this case set forth that the distinction between the websites is of no relevance when determining the criterion of directing business activities.[91] The CJEU justified its reasoning on the ground that the firm dependence of this criterion on the technical features and interactivity of the website can impair the major objective of Article 15 (1) (c) of the Brussels I Regulation.[92] In this case, the traders can easily circumvent the applicability of this criterion by just operating a passive website and concluding a contract through traditional means. By means of analogy, this is also the case under Article 3 (2) (a) of the GDPR. Accordingly, such a distinction can lose the whole meaning of this Article by ensuring the data controllers or processors evade the GDPR's application by targeting just the passive websites.

ii. The Emrek Case

The dispute, in this case, occurred between Mr. Emrek, who resided in Germany, and Mr. Sabranovic, who resided in France.[93] As he operates a second-hand car dealership, Mr. Sabranovic used an Internet website which included the location of his place, and mobile and fax address with an international dialling code. Even though the information about this dealership existed on the website, Mr. Emrek heard about this business through traditional acquaintances. Furthermore, he went to France and concluded the contract of sale with Mr. Sabranovic. Later on, Mr. Emrek brought a suit against Mr. Sabranovic under the claim concerning the warranty clause of the contract before the German District Court. However, the Court dismissed the claim on the grounds that Mr. Sabranovic had not directed his business activities towards Germany. As an appeal, Mr. Emrek submitted this case before the Supreme Court, which stayed the proceedings and referred it to the

[88] Zhen Chen, *Internet, Consumer Contracts and Private International Law: What Constitutes Targeting Activity Test?* 32 Information & Communications Technology Law 23, 34 (2021).
[89] Zippo Manufacturing Co v. Zippo Dot Com Inc., 952 F. Supp. 1119 (1997).
[90] *Ibid.*
[91] *Supra* note 77, para. 79.
[92] *Ibid.*
[93] Lokman Emrek v. Vlado Sabranovic, C-218/12, Judgment, para. 10 (2013).

CJEU on the question of whether the causal link between the "directing" of the trader's activity and the consumer's decision to enter into the contract should exist or not.

Prior to analyzing the concerned question, the CJEU recalled and reasserted its previous findings towards the criterion of directing business activities in the Pammer and Hotel Alpenhof joined cases. Specifically, the importance of the non-exhaustive list of the factors in the Pammer and Hotel Alpenhof joined cases was re-emphasized in determining whether a business activity is directed to the Member State.[94] Upon such assertion, the CJEU started to delve into the main question concerning the causal link. The Court decided that the existence of the condition concerning the causal link between the business activities directed to the Member State and the consumer's decision to enter into a contract stood in stark contrast with the context and objective of Article 15 (1) (c) of the Brussels I Regulation.[95] The CJEU stated that the conditions of Article 15 were formulated in an exhaustive form; therefore, the addition of unwritten conditions, such as the causal link, can load this Article unnecessarily and diminish its applicability to the rare cases.[96] Nevertheless, the Court also contended that such reasoning did not lead to the irrelevancy of this criterion as a whole. Namely, it is an undeniable fact that such a causal link is of an evidentiary role in assessing the directing business activities within Article 15 (1) (c) of the Brussels I Regulation.[97] Accordingly, the CJEU expanded the scope of the list of the non-exhaustive factors set out in the Pammer and Hotel Alpenhof joined cases by adding this factor.

As prescribed above-mentioned, the reasoning of the CJEU in the Emrek case can also be utilized in the assessment of the relevant criterion under Article 3 (2) (a) of the GDPR. To put it simply, the criterion of the causal link might have the evidentiary role in assessing the criterion for the offering of goods or services set forth under the GDPR.

c. The Sliding Scale between the Subjective Intention to Target and the End Result of This Targeting

As put forward both in Recital 23 of the GDPR and in the Pammer reasoning, particular attention is drawn to the subjective intention of the data controllers, processors, or the traders, respectively, in the targeting criterion. Likewise, they added the flavour of objectivity to this criterion by listing several factors revealing the subjective intention of the concerned parties. Despite such resemblance, it is worth noting again that the criteria for directing business activities and the offering of goods or services are not identical in their entirety. If this had been the case, the denomination of the

[94] *Id.*, para. 27.
[95] *Id.*, para. 22.
[96] *Id.*, para. 24.
[97] *Id.*, para. 26.

directing business activities would have remained as it was in Article 3 (2) (a) of the GDPR. In this vein, the analysis of the offering of goods or services departs, to a certain extent, from its counterpart in the Brussels I Regulation. Such departure is militated by the approach taken by the CJEU towards the notion of directing business activities in the Pammer and Hotel Alpenhof joined cases. As per this approach, the criterion of directing business activities indispensably requires a conscious and active conduct on the side of the undertaking, the objective and outcome of which are intended for winning the customers from the Member States.[98] The problematic issue with this viewpoint is concerned with the last part of the previous sentence, which focuses on both the undertaking's intention and the end result of such intention conjunctively. As Svantesson contends, it is practically possible to have situations in which the undertaking is of an intention to win the customers, however, such an outcome is not achieved.[99] Conversely, there might be cases in which the outcome of the undertaking's activities can end up winning the customers without having such intention.[100] To this end, the more favourable approach, according to Svantesson, is to solely focus on the end result when evaluating the directing business activities.

Nevertheless, this article partly agrees with Svantesson's approach. Primarily, differentiating between the subjective intention itself and that of the outcome, and only focusing on one of them seem evidently tenable. However, this article, as opposed to Svantesson, puts the main emphasis on the subjective intention rather than the end result in assessing the criterion for offering goods or services. Firstly, such an approach is in line with Recital 23 of the GDPR which centres on the data controllers' or processors' subjective intentions.

Furthermore, this approach is derived from the question of whether the GDPR hinges on real targeting by encompassing only the global actors specifically targeting the EU or it rests upon disguised targeting, which holds all companies acting globally without requiring intentional targeting.[101] Regarding this dilemma, Article 3 (2) (a) of the GDPR has been plagued, at initial times, with criticisms by high-calibre scholars. At this juncture, Kuner stood in such a position that the GDPR extraterritorially applied in a black-or-white fashion and lacked sophisticated boundaries to prevent excessive extraterritoriality.[102] Likewise, Svantesson argued that the formulation of Article 3 (2) (a) of the GDPR ensures uncertainty for the parties with respect to its applicability.[103] As a common point, they argued that the targeting

[98] *Supra* note 77, para. 63.
[99] *Supra* note 63, 232.
[100] *Ibid.*
[101] *Supra* note 17, 240-241.
[102] Christopher Kuner, *Extraterritoriality and regulation of international data transfers in EU data protection law*, 5 International Data Privacy Law 235, 241-242 (2015).
[103] *Supra* note 63, 232.

criterion rests on the straightforward rationale as *"you might be targeted by EU law only if you target"*.[104] Nevertheless, the uncertain and ill-determined formulation of this rationale, according to them, in Article 3 (2) (a) of the GDPR casts more doubts about the exorbitant applicability of this Regulation than what it is intended for. In this regard, this article contends the mere concentration on the outcome and disguised targeting can excessively loosen the applicability of Article 3 (2) (a) of the GDPR and bring approximately all actors acting globally under the umbrella of this Regulation. It further undermines the legitimacy and proportionality principles by paving the way for excessive extraterritoriality.[105] At first glance, such a situation can be referred to solidify the personal data protection of EU individuals; however much deeper examination reveals that it does so illegitimately and disproportionately.

In addition, the disregarding of the subjective intention of the data controllers or processors sidetracks the question of *"who takes the initiative?"*.[106] To put it differently, the role of the data subjects taking a leading initiative in targeting should not be underestimated, and the data subjects have an independent market choice to opt for or opt out of the services offered by the global actors. At this time, the actual party targets is the data subject, and it seems unreasonable to bring such global actors under the cloak of the GDPR.[107]

Based on the above-mentioned examination, this article suggests that particular attention should be drawn to the data controllers' or processors' intention when determining the criterion of the offering of goods or services. In this regard, this article further suggests that the subjective intention of the data controllers or processors shall be evaluated in the light of the objective factors, which wipe out the absolute subjectivity in the assessment process. In other words, the criterion of objective intention should be applied in relation to the assessment of the offering of goods or services.

3. The Monitoring of the Behaviors of the EU Individuals

The second criterion which outstretches the long arm of the GDPR beyond the EU borders is related to the monitoring of the behaviours of the EU individuals under Article 3 (2) (b). This criterion is involved in the composition of the GDPR with the objective of refurbishing the equipment criterion under Article 4 (2) (b) of the DPD and adapting it to the dynamic changes of modern technologies.[108] That is to say, the evolution of smart technologies has made non-EU-based companies reach the EU data subjects

[104] *Supra* note 17, 238.
[105] *Id.*, 239.
[106] *Id.*, 241.
[107] *Ibid.*
[108] Christopher Kuner, Lee A. Bygrave, Christopher Docksey and Laura Drechsler, The EU General Data Protection Regulation (GDPR) A Commentary, 89 (2020).

more easily and conduct data processing activities without any foothold presence. Accordingly, Article 3 (2) (b) intends to prevent the easy circumvention of the rigorous EU data protection legislation by non-EU-based companies through operating remotely.

a. The Notion of the Monitoring of the Behaviors under Article 3 (2) (b)

As a novel concept under the GDPR, this concept has been consecrated to much statutorily and scholarly attention. At the outset, this article can recourse to the analysis of this criterion provided by the GDPR itself and the EDPB. The GDPR stressed the explanation of this criterion through Recital 24 in the following manner:

"…In order to determine whether a processing activity can be considered to monitor the behavior of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviors and attitude".[109]

Pursuant to this explanatory note, it is manifestly emanated that the monitoring criterion can embrace a broad array of activities ranging from tracking to profiling of the data subjects who are in the Union.[110] Despite this broad formulation, the EDPB extends this criterion much further by covering the overlooked issues of Recital 24. Whereas Recital 24 considers the tracking of the data subjects only on the Internet, the EDPB also includes the tracking through other types of networks or smart devices.[111] Accordingly, the widespread monitoring activities include the following:[112]

a) geo-localization activities – these activities are widely used by the data controllers or processors through the Wi-Fi technologies. By using geo-localization technology, the non-EU data controller or processor can identify the exact location of the data subject and offer him/her the nearest services for marketing purposes;[113]
b) closed-circuit television (hereinafter CCTV) – Monitoring by means of CCTV includes the filming or recording of individuals through the video surveillance facilities. However, not any kind of such video recording is considered as monitoring, the necessary requirement is that the natural persons should be identified;[114]

[109] *Supra* note 18, recital 24.
[110] Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), 8 (2016).
[111] *Supra* note 38, 19.
[112] *Id.*, 20.
[113] *Ibid.*
[114] Douwe Korff, The Territorial (and Extra-Territorial) Application of the GDPR With Particular Attention to Groups of Companies Including Non-EU Companies and to Companies and Groups of Companies That Offer Software-as-a-Service, 49 (2019). Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3439293 (last visited Apr. 19, 2023).

c) cookies – a cookie is a *"piece of text stored by a user's web browser and transmitted as part of an HTTP request"*.[115] It includes the information and set by a web server. By using this technology, the website operators can track or monitor the data subjects visiting such website and determine their behavioral activities;
d) behavioral advertising – behavioral advertising is considered compound activity by containing other monitoring activities. It means that the data subjects' behavior is analyzed on the basis of their preferences by embracing various forms of monitoring, including, but not limited to, online tracking, geo-localization, profiling;[116]
e) market surveys – as its name suggests, the major objective of this monitoring activity is concerned with the marketing purposes. By using both online or offline activities, the data subjects' behaviors are identified through the interviews, various forms of questionnaires or surveys and etc.[117]

It is worth mentioning that the criterion on the monitoring of the behaviours does not come into play in an unbridled fashion, it also requires a couple of requirements to be satisfied as being in the criterion on the offering of goods or services. The primary yardstick which clarifies the boundaries of Article 3 (2) (b) is concerned with the question of where the monitoring of the behaviours of the data subjects takes place. This yardstick explicitly stems from the criterion that the data subjects should be within the EU. As explained above, this criterion plays a role of nexus between the EU and the data processing activities and the GDPR seeks to promote the nexus with the EU to a sufficient level.[118] By doing so, it aims to eliminate the overly extraterritorial application of the GDPR on the basis of the mere fact that the data subject resides in the EU. In a similar vein, the EDPB contemplated that as a cumulative criterion, the monitored behaviour should first relate to the data subjects being in the EU and further takes place within the EU.[119] Regarding the duration of the presence of the data subject within the EU, a much looser approach is taken in order to retain the applicability of this Article at a maximum point. It is emphasized that this prerequisite should be evaluated at the moment when the triggering activity takes place. To put it differently, the presence of the data subjects within the EU is required only when the monitoring activities concerned take place.[120] Before or after such monitoring activities, the location of the data subjects is not a decisive factor.

Furthermore, the notion of the monitoring is conditioned upon the requirements of the tracking of the data subjects and the potential subsequent

[115] ENISA, Privacy Considerations of Online Behavioural Tracking, 6 (2012).
[116] *Supra* note 38, 20.
[117] *Ibid.*
[118] *Supra* note 11.
[119] *Supra* note 38, 19.
[120] *Id.*, 20.

use of the personal data processing techniques.[121] To furnish more illustration, the EDPB sets out that this criterion requires the data controllers or processors to collect, process and subsequently (re)use the relevant data about the EU individuals' behaviours with a specific purpose. It highlights that the mere collection and analysis of the concerned data are not sufficient to be counted as monitoring, in addition, the subsequent behavioural analysis, processing, profiling and use of such data should be demanded.[122] Accordingly, the monitoring is a composite criterion which involves two cumulative operations: while the first one is called data warehousing which refers to the collection and storage of the relevant data, the second operation relates to the analysis of the stored data and making predictions for the data subjects' further interests and preferences.[123]

Based on the above-mentioned examination, the composition of the monitoring criterion is constituted by the amalgamation of the targeting approach and data processing. Herewith, it is worth noting that the targeting approach will be inquired about in the following part, henceforth the role of the data processing within the monitoring will be touched upon here. Even though the monitoring activity is not indicated as an element of the data processing in Article 4 (2) of the GDPR, separate structural elements of this activity, however, are listed within the mentioned Article of the GDPR. In other words, the collection, recording, analysis, storage, and profiling, which are an integral part of the monitoring, are counted as the data processing in Article 4 (2) of the GDPR.[124] Consequently, the monitoring itself can fall within the ambit of the data processing activities in a roundabout way.

b. The (Un)intentional Targeting under the Monitoring Criterion

As put forward in the above-mentioned, the monitoring criterion also contains the targeting approach as the criterion of the offering of goods or services. In this regard, the question comes to the forefront that the targeting approaches under these two criteria are twin or alter-ego with each other.

Prior to focusing on the side of the monitoring, it is worth recalling the question of how the targeting approach is formulated under the offering criterion. As afore-mentioned, the offering criterion requires the data controllers or processors to have an intention to specifically target the EU individuals. That is to say, Recital 23 of the GDPR, the EDPB, and the scholarly writings reinforced that the existence of intentional targeting on the part of the undertaking is an indispensable prerequisite for the applicability of Article 3 (2) (a). To this end, it is further indicated that the mere accessibility

[121] *Supra* note 18.
[122] *Supra* note 38, 20.
[123] Council of Europe, The Protection of Individuals with regard to Automatic Processing of Personal Data in the Context of Profiling, Recommendation CM/Rec (2010)13 and explanatory memorandum, 25 (2010).
[124] *Supra* note 18, art. 4 (2).

of the website is not sufficient to bring the data controller or the processor under the same Article of the GDPR.[125]

With respect to the targeting approach under the monitoring criterion, the issue of the peculiarity of this approach has attracted much more statutory and scholarly attention due to its complexity. Primarily, Recital 24 of the GDPR does not consider any acumen concerning the targeting approach and remains silent on the existence of this approach.[126] Thereunder, it comes to the mind that such silence is done on purpose and unintentional targeting is also captured by the monitoring criterion.[127] To delve into much deeper, such premise is, however, muddled with several plights by the high-calibre scholars. As Svantesson argues, if unintentional monitoring takes place, it cannot include the subsequent use of the data processing techniques (such as profiling etc.), which is a precondition of the monitoring criterion, over the collected data.[128] Namely, profiling a data subject and making predictions about their interests, and preferences, according to Svantesson, require a certain level of intention on the part of the data controller or processor.[129] Accordingly, in case of unintentional monitoring, the data processing activities cannot be deemed as monitoring due to the lack of one of the major preconditions.

Such an intricacy concerning the targeting approach has been, to some extent, relieved by the reasoning of the EDPB. At the outset, the EDPB also reinforced that the requirement of intention to target is not explicitly introduced in both Article 3 (2) (b) and Recital 24. Nevertheless, by bearing in mind the deficiencies of unintentional targeting, the EDPB took the view that the monitoring criterion requires a specific purpose in mind for the collection and subsequent use of the relevant data.[130] Unfortunately, the EDPB does not go much further and does not provide any guidance on how to comprehend "the specific purpose in mind".

In this regard, this article seeks to shed more or less light on this finding of the EDPB. Primarily, it is worth mentioning that the monitoring of the data subjects' behaviours is a much more lenient criterion rather than the offering of goods or services due to covering a broad range of activities. Such leniency can be evidenced by the fact that the mere operation of websites through just using cookies can fall within the ambit of the monitoring criterion,[131] as opposed to the offering criterion which expressly denies the mere accessibility of websites for its applicability. Accordingly, as a matter of the same logic, the

[125] *Id*., recital 23.
[126] *Id*., recital 24.
[127] *Supra* note 63, 232.
[128] *Ibid.*
[129] *Ibid.*
[130] *Supra* note 18.
[131] Serge Gutwirth, Ronald Leenes, Paul de Hert, Reforming European Data Protection Law, 37 (2015).

targeting approach under the monitoring criterion is not as stringent as the one under the offering criterion. At this juncture, the approaches taken towards the targeting under these two criteria are diametrically diverging in comparison with each other. To elaborate much further, the targeting approach under the offering criterion is related to the active intention to target the EU whereas the targeting approach under the monitoring criterion is related to the passive intention to target the EU, which does not require the active conduct on the part of the data controller or processor. To put it simply, if the data controller makes the website accessible to the entire world and places the cookies for tracking the behaviours of the data subjects, it is implied that the data controller has a passive intention to monitor the behavioural activities of the website users. The reason lies in the fact that modern technologies, such as geo-blocking technologies, can provide data controllers or processors to confine the accessibility of the website to particular territories.[132] Accordingly, by not using such technologies, the data controllers or processors have the implied or passive intention to target everyone. Consequently, the global actors targeting the entire world can also trigger the applicability of the monitoring criterion under Article 3 (2) (b).

III. The Interplay between the GDPR and Determination of Applicable Law

The determination of applicable law has been at the heart of private international law at all times. Likewise, the applicable law has always weighed much significance within the EU. Accordingly, the EU has taken several essential legislative initiatives, which ended up with the adoption of secondary legislations – Rome I Regulation, and Rome II Regulation – in preventing the conflict of jurisdiction or applicable law between the Member States. Besides such legislative acts, the regulation of the applicable can also permeate into the specific legislative acts concerning the different legal fields within the EU. By the same token, the issue of applicable law is also regulated by the EU data protection regime – the DPD in a discrete manner.

Specifically, the spatial scope under Article 4 of the DPD had been devised in the manner of the applicable law clause and such formulation is no coincidence due to the legislative form of the DPD. Considering that the DPD sought to approximate and harmonize the relevant Member State laws, it would be much more likely that the national laws could be devised differently by the Member States. Accordingly, Article 4 was expressly formulated as a conflict-of-law clause and provided its own connecting factor to prevent the overlapping of the national laws of different Member States.[133]

[132] *Id*., 19.
[133] Christopher Kuner, European Data Protection Law: Corporate Compliance and Regulation, 112 (2nd ed. 2007).

Article 4 drew primarily its attention to the notion of the establishment as a connecting factor, which is inspired by the traditional territorial principle in the private international law.[134] Owing to this rule, this Article can provide clear-cut and straightforward guidance on how to resolve the conflict of national laws in most cases. To put it simply, the law of the Member State in which the data controller is established is applied to the concerned data processing activities in so far as such data processing is carried out within that establishment of the Member State. Regarding the case where the data controller is not established in the EU, the DPD determined the law of the Member State where the equipment for the data processing is located.[135]

In light of the above-mentioned, this chapter will examine the possibility of the overlapping of the Member States' laws within the GDPR in the first instance. Furthermore, this chapter will delve into the possible solutions to the issue of determining the applicable law in case of the overlapping of the Member States' laws within the GDPR.

A. The Overlapping of Member States' Laws is an Inevitable or Neglected Issue within the GDPR

As of 25 May 2018, the European data protection regime came into a new phase through the entry into force of the GDPR. Accordingly, the European data protection regime has started to become directly applicable and binding in all Member States. The primary objective behind such change lies in the fact of precluding the legal fragmentation and inconsistencies across the EU in its entirety. This aim is also conceded by Recital 13 of the GDPR in the following: "*a Regulation is necessary to provide legal certainty and transparency for economic operators, ... and to provide individuals in all Member States with the same level of legally enforceable rights and obligations*".[136]

By bearing this objective in mind, the spatial scope of the GDPR is formulated under Article 3 in a different manner from its counterpart in Article 4 of the DPD. On the one hand, the first major difference is concerned with the restructuring of the applicability of the GDPR into non-EU-based undertakings, on the other hand, the second change, which is at the forefront of this chapter, applies to the avoidance of any rule concerning the applicable law between the national laws.[137] Such avoidance might seem tenable due to the fact that the GDPR is of direct applicability throughout the whole EU.[138] Considering that the GDPR is aimed at establishing the common and universal data protection regime which is harmoniously applied in all Member States, the identification of the applicable law would have been presumed to become no longer a concern before the GDPR. Even though the

[134] *Supra* note 12, art. 4.
[135] *Ibid.*
[136] *Supra* note 18, recital 13.
[137] Chen, *supra* note 1, 321.
[138] Karen Davies, Understanding European Union Law, 75 (5th ed. 2013).

premise of being a single law and having no need to reconcile anymore with the determination of the applicable law can sound promising and feasible, the accuracy of such premise just remains in theoretical confinement.[139] The closer examination revealed that the role of the national laws has still secured its relevancy within the GDPR in practical parlance. The relevancy of the national laws is primarily evidenced by two perspectives, which will be analyzed in the following.

Firstly, the GDPR does not set out any restriction on the Member States to decide the matters, which are not regulated by the GDPR in its entirety, on their own.[140] In this regard, the avoidance of such restrictions by the GDPR can bring about the second perspective which contemplates that the GDPR gives leeway to the Member States to turn away from its provisions and determine their own regulation on certain matters. This is even explicitly acknowledged by the GDPR itself in Recital 10, which contends that the Member States shall be provided with a margin of manoeuvre to specify and maintain its national provisions for the processing of sensitive data or for the processing of personal data in the public interest or in the exercise of official authority.[141]

Recital 10 refers to Article 6 (1) (specifically points c and e) and Article 9 which are concerned with the legal grounds on which the processing of the sensitive data is legitimized. Namely, Article 6 (3) expressly sets out that the data processing under the condition of compliance with the legal obligation or the performance of the action in the public interest can be determined by the Union law or Member State law.[142] Accordingly, the GDPR paves the way for the applicability of the national laws within its framework, and worse than that, such matter is not just confined to the articles concerned. In this regard, Jiahong Chen states the list of 37 issues, which potentially give rise to the conflict of national laws within the GDPR.[143]

Regarding the list of these matters, not all of them are completely procedural rules, which unlikely raises the problem of the applicable law. Furthermore, the matters under this list are divided into the ones having high, moderate and low levels depending on the susceptibility to the issue of the applicable law.[144] Firstly, the issues of the low levels are substantially concerned with either the data processing by the public bodies or the data processing in the pursuit of the public interest. The low susceptibility of these cases to the problem of the applicable law is evidenced by the fact that the law of the Member State in which the public body is established, or the public

[139] *Supra* note 1, 312.
[140] *Ibid.*
[141] *Supra* note 18, recital 10.
[142] *Id.*, art. 6 (3).
[143] *Supra* note 1, 314.
[144] *Supra* note 1, 313.

interest arises is mainly applied to such cases.[145] Accordingly, the situations within the public law domain can fall under the category of low risks. On the other end of the spectrum, the cases which are highly prone to the conflict of national laws exist in the list. To put it differently, the discretion of the Member States over the matters, e.g., the minor's consent, and the processing of the sensitive data are much more likely to give rise to the conflict of national laws.[146] Unlike the situations of the low risks, the cases of the high risks can refer to the private law domain. As a middle ground in causing the applicable law issue, such cases are epitomized under the moderate level. Due to its middle role, it can be said that the cases of moderate risks are wandering between the public and private law frameworks.[147] By way of illustration, Article 9 (2) (j) which is related to the processing for scientific, historical and statistical purposes entails both the involvement of the public and non-public bodies.

It is inferred from the above-mentioned analysis that the Member State laws have still resumed to matter within the GDPR. The GDPR conceivably provides the Member States with the room to manoeuvre independently on certain matters.[148] Nevertheless, the non-existence of perfect uniformity is not the major deficiency within this Regulation. Instead, the GDPR put its developments in peril by not containing the clause of the applicable law.[149] The lack of any rule on how the potential overlapping of the national laws is reconciled can undermine the legal certainty and convergence brought by the GDPR.[150] Accordingly, the GDPR inadvertently lag behinds what the DPD has warranted instead of leaving behind the DPD. To this end, any guidance put forward by the GDPR would be a welcomed action to secure its uniformity at the intended level.

As a counterargument to the above-mentioned deficiency, some might contend that this problem would be precluded by the Member States by following the approach taken by the DPD – the establishment rule. However, the possibility of this case is too low due to the fact that the DPD's approach had not been followed by Member States with enough consistency when this Directive had still been in force.[151] In this regard, Korff conducted an in-depth analysis of the differences within the Member State laws and concluded the viewpoint concerning the territorial applicability that the rules determining the applicable law are construed differently in the Member State laws and

[145] *Supra* note 18, art. 6 (1) (e).
[146] *Id.*, art 8 and art. 9 (2) (a).
[147] Jan-Jaap Kuipers, *Bridging the Gap: The Impact of the EU on the Law Applicable to Contractual Obligations*, *Rabels Zeitschrift Für Ausländisches Und Internationales Privatrecht*, 76 The Rabel Journal of Comparative and International Private Law 562, 573 (2012).
[148] *Supra* note 1, 314.
[149] Brkan, *supra* note 62, 336.
[150] *Supra* note 1, 314.
[151] *Id.*, 315.

such differences can cause the overlapping of national laws in practice.[152] Accordingly, it is unlikely that this rule would be taken by the Member States in the same manner in case of the absence of such a rule within the GDPR. Therefore, it is much needed to examine the other possible solutions to this problem in the context of the GDPR.

B. Private International Law as a Possible Solution

As mentioned at the very beginning of this chapter, private international law steps in and takes a role to establish the conflict-of-law mechanisms to prevent the overlapping of different laws and ensure legal certainty. In order to struggle with the issue of the applicable law, such mechanisms are specifically construed through the Rome I Regulation and Rome II Regulation within the EU. Accordingly, it would be an intriguing question whether the GDPR's deficiency in the applicable law can be healed by the EU's private international law mechanisms. In this vein, the following parts will delve into the analysis of the possible solutions in determining the applicable law within the GDPR.

1. The Relevancy of the Data Protection within the Rome Regulations

Prior to analyzing the relevancy between data protection and the Rome Regulations, it is necessary to provide brief information about the Rome I and Rome II Regulations. Rome I Regulation is a legal instrument of the European Parliament and Council which came into effect in 2009 and governs the applicable law to the contractual obligations.[153] Pursuant to Article 1 (1) of the Rome Regulation, it governs the determination of the applicable law when the issue relating to the contractual obligation in civil and commercial matters is at hand.[154] Likewise, the contractual obligations of the private law matters are required to trigger the applicability of the Rome I Regulation. Contrarily, the Rome II Regulation is a legal instrument which came into effect in 2009 but governs the applicable law to non-contractual obligations. Article 1 (1) of the Rome II Regulation, it intends to identify the applicable law regarding non-contractual obligations in civil and commercial matters.[155]

In light of this information, it is plausible to analyze the interrelation between data protection and the Rome Regulations. Firstly, it can be argued that the data protection regime lies entirely outside the framework of the Rome Regulations.[156] The main reason behind this argument lies in the scope of the matters over which they exert influence. As mentioned above, both the Rome I and Rome II Regulations permeate civil or commercial matters, and

[152] *Supra* note 31, 24.
[153] Regulation (EC) No 593/2008 of the European Parliament and of the Council on the law applicable to contractual obligations (Rome I) (2008).
[154] *Id.*, art. 1 (1).
[155] Regulation (EC) No 864/2007 of the European Parliament and of the Council on the law applicable to contractual obligations (Rome II), art. 1 (1) (2007).
[156] *Supra* note 62, 330.

the public law matters are beyond their applicability scope.[157] It is, however, so much difficult to conceptualize the data protection regime as private law or public law matter. Specifically, data protection falls into the grey area between the public and private law matters.[158] To put it simply, the GDPR provides both administrative and civil remedies for the breach of its provisions. To this end, the conceptualization of the data protection regime is dependent upon the factual analysis of each case at hand.

Likewise, this article takes the view that the relevancy between these two regimes should not be examined as an all-or-nothing concept. To put it differently, the decision depends upon determining the factual circumstances of the case. If the data protection issue raises private law matters, the Rome Regulations can come into the picture, on the contrary, there is no room for the applicability of these conflict-of-law mechanisms.

Upon finding the initial relevancy between these two regimes, further examination is required in relation to the Rome Regulations separately. Regarding the Rome I Regulation, the mere fact that the data protection issue adheres to civil or commercial matters does not directly lead to the applicability thereof. In addition, the contractual arrangements within the civil or commercial matters should exist to trigger the Rome I Regulation.[159] In this vein, it is worth contending that nowadays most of the data processing activities are carried out on the contractual arrangements.[160] Without going into much deeper, the consent, which is given by the data subjects to the privacy policies or settings of social websites, which can bring the data processing to the level of the contractual arrangement. Such consent can be flatly deemed as a contract,[161] which is also reinforced by the Working Party of the DPD that the validity of the consent is assessed in the light of the conditions of the valid contract set down by civil law.[162] For this reason, in case the overlapping of Member States' laws arises out of the contractual arrangement within the framework of the GDPR, the Rome I Regulation could be employed in determining the applicable law.

In relation to the data protection issues arising from the non-contractual arrangements, the Rome II Regulation can come into play in determining the applicable law. Nevertheless, the applicability of the Rome II Regulation to data protection issues is not as straightforward as the Rome I Regulation. Unlike the Rome I Regulation, the Rome II Regulation explicitly excludes the non-contractual obligations arising from violations of privacy and rights

[157] *Supra* note 153, art. 1.
[158] Christopher Kuner, *Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 1)*, 18 International Journal of Law and Technology 176, 178 (2010).
[159] *Supra* note 18, Art. 1 (1).
[160] Article 29 Data Protection Working Party, Opinion, 15/2011 on consent, 6-8 (2011).
[161] *Supra* note 1, 318.
[162] *Supra* note 160, 6.

relating to personality from its scope.[163] To put it simply, privacy-related matters are not regulated by the Rome II Regulation. Accordingly, the question of whether the privacy-related matters under this Regulation also contain data protection is a debatable issue. Indeed, such debate refers to the longstanding question of whether data protection and privacy are distinct rights or whether data protection is an integral part of privacy.[164] On the one end of the spectrum, it is argued that these two rights have a separate scope of application, which is grounded on the fact of having distinct provisions for data protection (Article 8) and privacy (Article 7) in the European Charter on Fundamental Rights.[165] Likewise, it is asserted that while these two rights might partially overlap, privacy also encompasses other issues than personal data as a broader concept.[166] Pursuant to this viewpoint, the non-contractual obligations arising from the data protection do not fall within the scope of the Rome II Regulation. On the other end of the spectrum, it is contended that these two rights are inextricably intertwined with each other. This approach is often taken by the CJEU in its rulings by referring to both data protection and privacy in conjunction.[167] Based on this argument, data protection and privacy are inseparable rights from each other.

In this vein, this article holds the hybrid role with respect to the relation between these two rights. Firstly, from the perspective of fundamental rights, this article takes the former approach which asserts the separation of data protection from the privacy right. Nevertheless, for the perspective of teleological and systemic analysis of the Rome II Regulation, takes the latter approach as contending the inseparable nature of these two rights. Otherwise, the exclusion of privacy, but not data protection, from the scope of the Rome II Regulation would cause difficulties in delineating the boundaries between these two rights and determining the applicable law. To give an example, as Brkan notes, if the disclosure of the data subject's health data and his/her opinions on his/her health state is made by the provider of the health app, it would be much more difficult to draw the line between the issue concerning the privacy (for which Rome II Regulation is not applied) and data protection (for which Rome I Regulation is applied). Likewise, this article takes the viewpoint that the data protection issues are also excluded from the scope of the applicability of the Rome II Regulation.[168] Accordingly, it can be contended that as opposed to the Rome I Regulation, the Rome II Regulation

[163] *Supra* note 155, art. 1 (2).
[164] *Supra* note 1, 318.
[165] Juliane Kokott, Christoph Sobotta, *The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR*, 3 International Data Privacy Law 222, 223 (2013).
[166] Maria Tzanou, *Data Protection as a Fundamental Right next to Privacy? 'Reconstructing' a not so New Right*, 3 International Data Privacy Law 88, 90 (2013).
[167] 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, para. 32-37 (2014).
[168] *Supra* note 62, 331-332.

is not applied as long as the overlapping of Member States' laws arises from the non-contractual arrangement within the GDPR.

2. The General Conflict-of-law Rules

As a substitute for the applicability of the Rome Regulations, the general conflict-of-law rules can play a significant role in determining the applicable law in the data protection context. The bulk of the conflict-of-law rules enshrined in the Rome Regulations has existed much longer than the entry into force of these Regulations.[169] Accordingly, most of these rules have been integrated into the national laws of the Member States, which contain much more similarities with each other. Owing to this similarity, these rules advance into the general nature and become an alternative solution to determine the applicable law.

Regarding the data protection issues arising from contractual obligations, the conflict-of-law rule contending the place where the consumer (data subject) resides can be an applicable law. The reason lies in the fact that most times the data subjects have the weaker position like the consumers and the residence rule of these subjects would be an effective approach. With respect to the data protection issues arising from the non-contractual obligations, the better approach could be the general doctrine of *lex loci delicti commissi* determining the place where the tortious breach happened.[170] In light of this doctrine, it can be argued that the law of the place where the data processing activities happened could be an applicable law to the case at hand.

3. The "subject to" Approach as an Applicable Law

Even though the GDPR lacks any rule to determine the applicable law between the Member States' laws on certain matters, a much deeper analysis reveals that the GDPR drafts its relevant provisions in a cautious form by anticipating the potential problem of the applicable law. This cautious formulation is conditioned upon the approach of "subject to".[171] By way of example, Article 6 (1) (c) sets out "the compliance with the legal obligation to which the controller is subject" or Article 6 (3) determines that the legal basis for the data processing can be laid down by either the Union law or the Member State law to which the data controller is subject. They can indicate that the GDPR does not take an open-ended approach to the Member State law, on the contrary, it contains the "subject to" qualifier to limit the applicability of the Member State laws. Nevertheless, this qualifier does not directly resolve the question of the applicable law, since the GDPR is silent on the meaning of the notion of the "subject to".[172]

[169] *Supra* note 1, 319.
[170] European Commission, MainStrat, Comparative study on the situation in the 27 Member States as regards the law applicable to non-contractual obligations arising out of violations of privacy and rights relating to personality, Final Report, 79 (2009).
[171] *Supra* note 1, 321.
[172] *Ibid.*

The potential possibility in determining the meaning of this qualifier is concerned that the law of the Member State to which the data controller is subject is analogous to the law of the Member State to which the data controller is established. This approach stands in the same line with the applicable law clause under Article 4 of the DPD.[173] However, this approach cannot resolve the issue in its entirety, since the data controller might be subject to the law of the Member State in which it is not established.[174] The possibility of this situation is also reinforced by the GDPR itself through its provisions that it can be applicable to the data controllers not having been established in the EU.[175] Hence, even though the qualifier of "subject to" is included in the relevant provisions of the GDPR, the lack of any guidance on the meaning of this qualifier undermines, to a larger extent, the operability of this approach. Accordingly, the guidance taken by the GDPR for determining the meaning of this qualifier would be welcomed.

4. The Agreements on the Applicable Law for the Data Protection

The further solution is concerned with the agreements concluded by the parties which rest upon the bedrock rule in EU private international law – the principle of party autonomy.[176] This principle is enshrined in Article 3 of the Rome I Regulation and it allows the parties to subject their contract to any legal system as they please without requiring any territorial or other connection to the chosen law. To this end, the question arises as to whether the parties can freely deviate from the GDPR and choose other data protection regimes under the principle of party autonomy.

Prior to analyzing this question, it is worth determining in which cases the GDPR can be potentially disregarded by the parties. As mentioned above, nowadays most of the data processing activities are conducted between the parties not having equal position. To put it simply, the data controllers or processors are mostly the tech giants or huge corporations in the contemporary period. As an example, when the data subjects utilize the online services of the tech giants, e.g. Facebook, Amazon, Google, and Alibaba, there is no room for the data subjects to alter the terms or conditions of such online services as they please. Nevertheless, the party autonomy belongs to the providers of the online services as the data controllers or processors in determining the terms and conditions of these services. Hence, the question comes into the picture as to whether the providers of online services can expose the data processing activities over the EU individuals to the data processing regime other than the GDPR in case of the applicability thereof.

[173] *Supra* note 12, art. 4.
[174] *Ibid*.
[175] *Supra* note 155, art. 3 (2).
[176] Jürgen Basedow, The Law of Open Societies. Private Ordering and Public Regulation in the Conflict of Laws, 115 (2015).

Regarding this issue, some authors argue that the agreements on the applicable law concerning data protection are possible due to the fact that such agreements are not expressly precluded by the Rome I Regulation.[177] According to these authors, the data protection regime under the GDPR does not also have the nature of the overriding mandatory provisions. However, this article takes the opposing viewpoint which argues that the GDPR cannot be disregarded by the parties as far as its applicability is concerned. The reason lies in the fact that the data protection regime under the GDPR is of the nature of the overriding mandatory provisions and it is applicable regardless of the law chosen by the parties.[178] In this regard, it is worth examining the rationales behind this approach.

Prior to analyzing the role of the GDPR in overriding mandatory provisions, it is necessary to give the definition of the overriding mandatory provisions. As per Article 9 (1) of the Rome I Regulation, overriding mandatory provisions are provisions that are regarded as "crucial by a country for safeguarding its public interests".[179] The nature of the GDPR as overriding mandatory provisions is firstly evidenced by the CJEU rulings in Ingmar,[180] Honyvem Informazioni Commerciali,[181] Semen[182] and Unamar cases,[183] which held that not only provisions of Member States' laws but also the provisions of EU law itself can be qualified as such provisions. Henceforth, as an EU legal instrument, there is not any barrier before the GDPR to be regarded as overriding mandatory provisions.

Secondly, the norm needs to have the purpose of pursuing the public interest to be qualified as overriding mandatory provisions.[184] In this vein, the role of the GDPR as such provisions is reinforced by the following reasons. Primarily, the data protection regime under the GDPR contains the administrative provisions and administrative enforcement which trigger the public interest objectives.[185] Furthermore, the public interest of the GDPR can be grounded on the fact that the functioning of the internal market by ensuring the free movement of personal data is pursued as one of the main objectives. In addition, the GDPR is aimed at safeguarding the fundamental rights of data protection, which constitute the rudimentary values of society and fall within the category of overriding reasons of public interest. Meanwhile, this is also reinforced by the German case law – *Facebook v. Independent Data Protection Authority of Schleswig Holstein* – which stipulated

[177] *Supra* note 62, 334.
[178] *Ibid.*
[179] *Supra* note 153, art. 9 (1).
[180] Ingmar GB Ltd v. Eaton Leonard Technologies Inc., C-381/98 (2000).
[181] Honyvem Informazioni Commerciali Srl v. Mariella De Zotti, C-465/04 (2006).
[182] Turgay Semen v. Deutsche Tamoil GmbH, C-348/07 (2009).
[183] United Antwerp Maritime Agencies (Unamar) NV v. Navigation Maritime Bulgare, C-184/12 (2013).
[184] *Supra* note 62, 334.
[185] *Supra* note 18, recital 148.

that pursuant to the Rome I Regulation, it is possible to make an agreement on the applicable law for the contract, but not on data protection law, since its provisions fall within the concept of overriding mandatory provisions. Hence, it can be evidenced that the data protection regime under the GDPR can fall within the scope of the overriding mandatory provisions.

Conclusion

This article provided an overview of the applicability issue in the EU data protection regime, specifically in the framework of the GDPR. The applicability issue has been analyzed from two different angles: 1) the applicability of the GDPR itself; and 2) the determination of the applicable law within the GDPR.

As regards to the applicability of the GDPR, its territorial scope includes two forms of data processing activities: 1) territorial and 2) extraterritorial. The *"establishment"* criterion plays a significant role in assessing the territorial applicability. Meanwhile, this criterion is given a flexible definition which means that one person's physical presence with necessary technical resources can be sufficient to be deemed as established in the EU.

Regarding the extraterritorial applicability, the GDPR includes two cases in which the processing activities are related to the *"offering of goods or services to data subjects in the EU"* or to the *"monitoring of the behavior of those data subjects"*. As per our analysis, the criterion of the *"offering of goods or services"* is conditioned upon 1) the envisaging of offering services to the data subjects in the EU and 2) having the intention to do so. In this vein, this criterion contains the targeting approach and it is analogous to the criterion of *"directing business activities"* in the consumer protection law. Accordingly, this article suggests that the targeting approach under this criterion ought to be assessed in the frames of the objective intention, which means, on the one hand, the existence of subjective intention, on the other hand, the determination of subjective intention in the light of the objective factors. In relation to *"monitoring the data subjects' behaviors"*, this criterion requires the tracking of the individuals and the potential subsequent use of personal data processing techniques for profiling the individual. Likewise, the monitoring criterion requires the existence of intention on the part of the data controllers or processors. This article suggests that the degree of intention under the monitoring criterion is less stringent than the one under the offering criterion. To put it simply, the offering criterion contains an active intention to trigger its applicability whereas the monitoring criterion requires a passive intention for its applicability. Accordingly, the mere accessibility of the website is sufficient to trigger the applicability of the monitoring criterion as opposed to the offering criterion.

This article was further consecrated to the issue of determining the applicable law within the GDPR. Considering that the GDPR is a universal

law throughout the EU, it does not include any rule on determining the applicable law. Nonetheless, the Member States' laws still matter within the GDPR and the possibility of the conflicting of the Member States' laws is not eliminated in its entirety. Considering this, the following alternative mechanisms have been analyzed to alleviate this vexing issue: 1) the EU conflict-of-law instruments (Rome Regulations); 2) the general conflict-of-law rules; 3) the *"subject to"* approach under the GDPR; 4) the principle of party autonomy. Based on this analysis, this article suggests that the Rome I Regulation can be applied in case the conflict of the Member States' laws arises out of the contractual arrangement. On the contrary, the general conflict-of-law rule (*lex delicti commissi)* is employed as far as the conflict of the Member States' laws arises from the non-contractual arrangement.