The Relevance of European Data Protection Standards for US Businesses and Authorities

Dr. Maja Brkan*

Abstract: The article examines the issues of applicable law in the domain of data protection. It focuses on the question which law is applicable to businesses established within the EU and outside the EU and concludes that the rules on applicable law would need to be agreed upon on the global level in a form of an international treaty.

Key words: data protection, conflict-of-laws, applicable law, territorial application, Google Spain judgment

1. Introduction

In order for the European citizens to effectively make use of their right to data protection and in order for data protection authorities (DPAs) to effectively enforce this right, it is important that the rules on jurisdiction and applicable law are not such as to stand in the way of their effective enforcement. Rather, they should be framed in a way to enable effective judicial protection of the rights of the Union citizens. The main purpose of this article is therefore to point out actual and potential obstacles to the effective (judicial) protection of personal data, created by the rules of European private international law, and to put forward a comprehensive scheme regarding issues of jurisdiction and applicable law with regard to data protection. These issues of jurisdiction and applicable law with regard to data protection have recently attracted quite some attention in the academic literature.[1]

2. Applicable law

2.1. The myth of parallelism between jurisdiction and applicable law

Although it is, in principle, desirable that the court deciding on the claim also applies its own laws, notably due to the procedural economy[2], this is not always the case in practice. If one, for example, compares the rules on jurisdiction and applicable law in the field of torts, it is possible to come to the conclusion that such a parallelism is, at best, only partial[3]. The main connecting element or the general rule for determining the applicable law for torts is the place where the *damage* occurs[4], whereas the main connecting element for determining jurisdiction in delictual matters is the place where the *harmful event* occurred or may occur[5]. It is true, however, that the case-law brought the content of the latter notion closer to the content of the former; in fact, in *Bier v Mines de Potasse d'Alsace*[6] and subsequent

---

[1] Wang, "Jurisdiction and Cloud Computing: Further Challenges to Internet Jurisdiction", 24 European Business Law Review (2013), 589–616; Kuner, "Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 1)", 18 *International Journal of Law and Information Technology* (2010), 176-193; Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part 2)", 18 *International Journal of Law and Information Technology* (2010), 227-247; 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* (2011), 28-46; Piltz, "Rechtswahlfreiheit im Datenschutzrecht?", (2012) K&R, 640-645; Schultz, "Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface", 19 *The European Journal of International Law* (2008), 799–839; Swire, "Elephants and Mice Revisited: Law and Choice of Law on the Internet", 153 *University of Pennsylvania Law Review* (2005), 1975-2001.

[2] Unberath, Cziupka, in Rauscher (Ed.), *Europäisches Zivilprozess- und Kollisionsrecht EuZPR/EuIPR. Kommentar. Brüssel I-VO. LugÜbk 2007* (sellier, 2011), 686.

[3] *Ibid.*

[4] See Article 4(1) of the Rome II Regulation.

[5] See Article 5(3) of the Regulation No 44/2001 (now Article 7(2) of Regulation 1215/2012).

[6] Case C-21/76, *Handelskwekerij Bier v Mines de Potasse d'Alsace,* [1976] ECR 1735.

case-law[7], the CJEU confirmed that the notion of "harmful event" from the Article 5(3) of Regulation No 44/2001[8] (recently replaced by Regulation 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters[9]) covers "both the place where the damage occurred and the place of the event giving rise to it". In consequence, the two rules on jurisdiction and applicable law can amount to the same result.

An exception to this lack of parallelism are the rules on consumer jurisdiction and applicable law. As expressly stated in Recital 24 of the Rome I Regulation[10], the concept of "directed activity" should be interpreted harmoniously in this regulation and in the Regulation No 44/2001 (now Regulation 1215/2012). In practice this means that the court deciding the matter will, in principle, apply the law of the consumer's domicile.

Another difference between the rules on jurisdiction and applicable law needs to be stressed. The regulations governing applicable law (Rome I and Rome II[11] Regulations) have universal application, meaning that the law to which one of these regulation points to is applied regardless of whether it is the law of one of the Member States or not[12]. In consequence, neither the fact that the conflict of law rules point to the law of a Member State nor the fact that the claimants are domiciled in one of the Member States plays a role in the application of these regulations. To the contrary, Regulation No 44/2001 (now Regulation 1215/2012) applies only to persons domiciled in a Member State, regardless of their nationality and hence does not have universal application.

2.2.*De lege lata*: applicable law in the Data Protection Directive

The absence of parallelism between the rules on jurisdiction and applicable law is rather striking when one analyses the rules on applicable law within the framework of the Data Protection Directive. According to Article 4(1) of this directive, the law of a particular Member State applies if the controller is established in a particular Member State and data is processed in the context of its activities; if law of a particular Member State applies on the basis of international public law; or if the controller makes use of equipment situated on the territory of a particular Member State.

It is to be noted that – differently from the classic rules on applicable law enshrined in Rome I and II Regulations – Article 4 of the Data Protection Directive does not have universal application[13]. In other words, the law that can be applicable under the Data Protection Directive can only be the law of one of the Member States and not the law of a third country. Thus, Article 4 of the Data Protection Directive seems to have a double function. On the one hand, this article determines when the law of one of the Member States will be applicable *as opposed to the law of a third country.* On the other hand, this article determines *the law of which Member State* will be applicable within the European Union.

---

7 See, for example, Case C-167/00 *Henkel,* [2002] ECR I-8111*,* para 44*;* Case C-18/02 *DFDSTorline,* [2004] ECR I-1417, para 40; Case C-168/02 *Kronhofer,* [2004] ECR I-6009, para 16; and Case C-189/08, *Zuid-Chemie,* [2009] ECR I-6917, para 23.

8 Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2001] OJ L 12/1.

9 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 [2012] OJ L 351/1.

10 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) (OJ L 177, 4.7.2008, p. 6).

11 Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) (OJ L 199, 31.7.2007, p. 40).

12 See Article 2 of the Rome I Regulation and Article 3 of the Rome II Regulation.

13 See above point 2.1. of this article.

A landmark case in the field of applicable law with regard to data protection is the recent *Google Spain and Google* case[14], in which the CJEU interpreted, for the first time, Article 4(1)(a) of the Data Protection Directive. This provision requires the application of the national law of a certain Member State transposing the said directive if "the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State". The CJEU, asked to interpret several notions from this article – notably the notion of "establishment" and the question when such an establishment "processes" personal data "in the context" of its activities – came to the conclusion that the conditions of this article are fulfilled "when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State"[15]. Whereas this decision, following the opinion of the AG Jääskinen[16], might well be appropriate for the factual constellation specific for the *Google Spain and Google* case*,* it is doubtful whether, from a more general perspective, it can be the only plausible and the most appropriate interpretation of this provision.

First, it is not entirely convincing that the application of data protection legislation should be dependent on the business model that the search engine uses to generate its revenues. It is questionable whether selling of advertising space is a criterion that should be taken into account at all, given the fact that the main (and only) criterion that the Data Protection Directive takes into account is the processing of personal data. It is true, however, that both activities form part of the same business model and that it is precisely the selling of advertising space that financially enables the activity of processing of personal data.

What is however even more problematic is the question whether such an interpretation of Article 4(1)(a) of Data Protection Directive would allow for this provision to include also search engines that are built upon different, non-profit, business models[17]. It seems that such search engines, that equally process personal data, would undoubtedly need to be covered by this provision. Such a solution does, however, not stem readily from the reasoning of the CJEU that affirms that the activities of Google in California (operator of the search engine) and of its subsidiary in Spain (selling advertising space) are "inextricably linked" in the sense that the latter activity renders the "search engine at issue economically profitable" and that it is therefore "the means enabling those activities to be performed"[18]. In the case of the absence of this link, would the conditions from Article 4(1)(a) still be fulfilled?

Therefore, it is not entirely clear from the *Google Spain and Google* judgment whether processing of personal data by an operator selling advertising space is the *only* instance that falls under this article or whether this is only *one of* the examples that can be covered by this article. The problem with former interpretation lies in the circumstance that it depends to a too high degree on a business model on which the search engine builds. In fact, such an interpretation only covers certain business models – more precisely, only those search engines that use the sale of advertising space to finance its search activities.

Furthermore, it is important to stress that the solution adopted by the CJEU comes curiously close to the one regarding the interpretation of Article 15 of Regulation No 44/2001 (now Article 17 of Regulation 1215/2012) in the joint cases *Pammer and Hotel Alpenhof*[19] and

---

[14] Case C-131/12, *Google Spain and Google*, [2014] not yet published in ECR.

[15] Case C-131/12, *Google Spain and Google*, [2014] not yet published in ECR, para 60.

[16] Opinion of AG Jääskinen in the Case C-131/12, *Google Spain and Google*, [2014] not yet published in ECR, para 68.

[17] As an example of non-profit search engine is Benelab (http://bene.co/) that donates revenues generated from the internet searches.

[18] Case C-131/12, *Google Spain and Google*, [2014] not yet published in ECR, para 56.

[19] Case C-585/08, *Pammer and Hotel Alpenhof,* [2010] ECR I-12527.

the subsequent case-law, *Mühlleitner*[20] and *Emrek*[21]. The CJEU namely adds as one of the conditions of the application of Article 4(1)(a) of Data Protection Directive the circumstance that the subsidiary of the search engine "orientates" its activity towards the inhabitants of the Member State in which it is established. Adding this criterion to the interpretation of Article 4(1)(a) of Data Protection Directive seems problematic. Not only because this criterion does not appear in the text of the article itself and hence cannot be established on the basis of a textual interpretation of this article, but also because this criterion does not seem to stem either from a teleological interpretation of this provision or from the usual meaning from the term "orientating". It seems that this element, in a way, neutralises the circumstance that the controller has a subsidiary in a certain Member State. While it is certainly possible to imagine circumstances in which a controller would have a subsidiary in a given Member State and *not* orientate its activity towards the inhabitants of this Member State, it seems that such examples would be rather rare in practice. It should be recalled that the criterion of "orientating" of an activity makes the most sense if there is a cross-border element to such "orientating".[22] A cross-border element is also present in the notion of "directing of activities" as used by the Article 15 of Regulation No 44/2001 (now Article 17 of Regulation 1215/2012). In any event, it would seem reasonable that this criterion is used as a subsidiary criterion and not as a primary one in the framework of the interpretation of Article 4(1)(a) of Data Protection Directive.

It is true, however, that the decision of the CJEU can also be understood in the light of the questions asked by the national court. In fact, the answer given by the CJEU on the question regarding applicable law is a mirror image of one of the three possible interpretations given to the CJEU by the national court.[23] It could therefore be claimed that the CJEU only replied affirmatively to the premises already given to it by the national court. The question was not asked in abstract, but with regard to a concrete situation and on the basis of the concrete description of this situation given by the national court.

Another question that needs to be asked is whether the interpretation of the CJEU would be the same if a company from a third country has a subsidiary, in one (or several) EU Member States that processes personal data within the EU. Whereas this does not seem to be the case with Google, it is with regard to Facebook. In the already mentioned German case *Facebook v Independent Data Protection Authority of Schleswig-Holstein*[24], the German administrative court of Schleswig-Holstein held that the German law was not applicable to processing of data of its German users because the German subsidiary of Facebook did not actually process the data, but was only active in the field of marketing[25]. Since it was the Irish subsidiary of Facebook that processed personal data of its European users, it was the Irish law that was exclusively applicable[26].

It can certainly be argued that this decision of the German court is not in accordance with the CJEU decision in *Google Spain and Google* and that the circumstance that the German subsidiary of Facebook exercises marketing activity is sufficient for the German law to be applicable. Such reasoning, however, seems to entirely disregard the different functions of the two European subsidiaries of Facebook (German and Irish). On the other hand, an inverse reasoning (such as the one by the German court) would lead to the

---

20 Case C-190/11, *Mühlleitner,* [2012] not yet published in ECR.

21 Case C-218/12, *Emrek,* [2013] not yet published in ECR.

22 In the sense that an internet service provider, established in one Member State, orientates its activity towards the inhabitants of *another* Member States.

23 Case C-131/12, *Google Spain and Google*, [2014] not yet published in ECR, para 45.

24 Case 8 B 60/12, *Facebook Ireland Ltd. v Independent Data Protection Authority of Schleswig-Holstein, Germany*.

25 *Ibid.*, p. 6.

26 *Ibid.*, p. 7 and 9.

determination of applicable law according to different criteria depending on whether a company from a third country has a subsidiary in the EU that processes personal data of EU users. For such a company, it would be enough for have a marketing subsidiary in one of the EU Member States for the law of this state to apply, whereas, in case of its EU subsidiary processing personal data, this would not suffice. It therefore seems that, after *Google Spain and Google*, the German *Facebook* case would be decided differently. It could be argued, however, that an EU subsidiary that processes personal data is actually an *establishment* within the meaning of Article 4(1)(a) of the Data Protection Directive and that the law of this Member State should be applicable to this establishment.[27]

2.3.*De lege ferenda*: territorial application of the proposed Data Protection Regulation

The proposed Data Protection Regulation no longer contains a conflict-of-laws provision determining the applicable law of a particular Member State to the processing of personal data, since the regulation itself unifies the legal regime on processing of data. After the entry into force of the regulation, several issues with regard to applicable law will thus no longer be relevant except for the question of the (im)possibility to enter into an agreement on applicable law for data protection. The latter will, however, probably have to be answered in the negative, as the parties to a contract cannot deviate from a legal instrument such as regulation. This would be contrary to the binding effect of the regulation and would go against its nature as a legal instrument of unification of the law throughout the entire Union.

The proposed Data Protection Regulation does, however, contain a provision determining its territorial scope of application. According to Article 3(1) of the proposed regulation, the 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". It can be seen that the rule for the territorial application of EU data protection legislation remained the same: processing of data in the context of the activities of a controller or processor, established in the Union. Therefore, the legal issues with regard to the interpretation of this provision also remained the same, in particular the meaning of the phrase "in the context of the activities" and "establishment". It seems therefore that the CJEU would come to the same conclusions had the case *Google Spain* been decided after the entry into force of the regulation.

The second and the third paragraphs of Article 3 of the proposed Data Protection Regulation deal with the situation in which the controller does not have an establishment in the Union. Such a controller has to comply with the rules established in the regulation if his activities relate to the offering of goods or services to data subjects in the Union[28]. In practice this means that all the online stores based in the US and not having a subsidiary in the Union will have to comply with the European legislation[29]. A very extensive reading of this provision could even lead to an interpretation according to which the Union legislation on data protection would apply even if a European data subject buys goods or receives services in the territory of a third state. Such

---

[27] Such a reasoning could also be supported by the Recital 18 of the Data Protection Directive, according to which "processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State".

[28] See Article 3(2)(a) of the proposed Data Protection Regulation.

[29] On extra-territorial application of Data Protection Directive, see 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 of the Article 29 Data Protection Working Party, Adopted on 30 May 2002, 5035/01/EN/Final, WP 56, p. 4. See also Kuner, "Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 1)", 18 *International Journal of Law and Information Technology* (2010), 178.

an interpretation would however lead to a too extensive extraterritorial application of Union legislation on the territory of a third state and cannot be upheld.

The proposed Data Protection Regulation on data protection will apply also if the activities of the controller not established in the Union relate to the monitoring of the behaviour of data subjects in the Union[30]. This seems to imply that the NSA, when processing data about Union citizens or obtained from Union authorities, has to respect Union law. Does it also mean that the US authorities have to observe Union law when a Union citizen travels to the US and gives his fingerprints on the US boarder? Even if such an interpretation seems rather far-reaching, is the situation really different if the US authorities obtain fingerprints from a Union citizen entering its soil or if they receive the same fingerprints from a DPA of the Member State of this citizen's residence?

The third paragraph of Article 3 of the proposed Data Protection Regulation is, again, comparable to the rule set out in the current Article 4(1)(b) of the Data Protection Directive, since both legal instruments provide for the applicability of, respectively, Union and Member State's law, in case where the national law of a Member State "applies by virtue of public international law".

3. Conclusion

The regulation of applicable law can have an important influence on the rights of data subjects in the Union. Too complicated conflict-of-law rules can dissuade data subjects from effectively exercising their rights. However, given the fact that data subjects are still – in an analogous way as consumers – a weaker party in comparison with controllers/processors, the Union legislation would also need to put more emphasis on collective and representative claims and regulate conflict-of-law rules also in this regard. Hopefully, the proposed Data Protection Regulation will be amended so as to overcome the current lacunae in the EU data protection legislation. The current rules on applicable law still do not seem entirely accommodated to the complexity and the global nature of infringements of data protection rules.

On a worldwide level and for the future, it will need to be considered whether the rules on applicable law in the field of data protection can be agreed upon on a global scale, most likely in a form of an international treaty that would also contain jurisdictional rules and rules on applicable law[31]. Some time ago, an idea of a separate international tribunal for resolving Internet-related issues has been introduced in the literature[32]. A step even further would be to introduce universal jurisdiction, but this seems more appropriate for cyberterrorism[33] than for data protection, because the attempts to fight terrorism are global, whereas the standards for data protection vary heavily among different countries in the world. It is also to be seen whether, for data protection litigation, the Hague Convention on Choice of Court Agreements[34] could potentially be relevant. This convention is however not yet in force[35].

---

30 See Article 3(2)(b) of the proposed Data Protection Regulation.

31 A similar idea on a multilateral agreement on jurisdiction, but with regard to defamation over Internet, was raised by Hoare, "Following on from the Australian Dow Jones decision on jurisdiction in Internet defamation, do compelling reasons exist for legislating for a new approach to this issue?", (2004) *Commercial Law Practitioner*, 13.

32 See Blair and Quest, "Jurisdiction, Conflicts of Law and the Internet" in Ferrarini et al. (Ed.), *Capital Markets in the Age of the Euro. Cross-Border Transactions, Listen Companies and Regulation* (Kluwer, 2002), p. 164.

33 See, in this regard, Gable, "Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent", 43 *Vanderbilt Journal of Transnational Law* (2010), 104 et seq.

34 Convention of 30 June 2005 on Choice of Court Agreements, available on <http://www.hcch.net/index_en.php?act=conventions.text&cid=98> (2.8.2014).

35 On the status of the convention, see <http://www.hcch.net/index_en.php?act=conventions.status&cid=98> (2.8.2014).