RSCAS 2015/40
Robert Schuman Centre for Advanced Studies
Florence School of Regulation

Data Protection and European Private International Law

Maja Brkan

European University Institute
Robert Schuman Centre for Advanced Studies
Florence School of Regulation

Data Protection and European Private International Law

Maja Brkan

EUI Working Paper **RSCAS** 2015/40

ISSN 1028-3625

Printed in Italy, July 2015
European University Institute
Badia Fiesolana
I – 50014 San Domenico di Fiesole (FI)
Italy
www.eui.eu/RSCAS/Publications/
www.eui.eu
cadmus.eui.eu

Robert Schuman Centre for Advanced Studies

The Robert Schuman Centre for Advanced Studies (RSCAS), created in 1992 and directed by Professor Brigid Laffan, aims to develop inter-disciplinary and comparative research on the major issues facing the process of European integration, European societies and Europe's place in 21st century global politics.

The Centre is home to a large post-doctoral programme and hosts major research programmes, projects and data sets, in addition to a range of working groups and *ad hoc* initiatives. The research agenda is organised around a set of core themes and is continuously evolving, reflecting the changing agenda of European integration, the expanding membership of the European Union, developments in Europe's neighbourhood and the wider world.

Details of the research of the Centre can be found on:
http://www.eui.eu/RSCAS/Research/

Research publications take the form of Working Papers, Policy Papers, and e-books. Most of these are also available on the RSCAS website:
http://www.eui.eu/RSCAS/Publications/

Florence School of Regulation

The Florence School of Regulation (FSR) is a partnership between the Robert Schuman Centre for Advanced Studies (RSCAS) at the European University Institute (EUI), the Council of the European Energy Regulators (CEER) and the Independent Regulators Group (IRG). Moreover, as part of the EUI, the FSR works closely with the European Commission.

The objectives of the FSR are to promote informed discussions on key policy issues, through workshops and seminars, to provide state-of-the-art training for practitioners (from European Commission, National Regulators and private companies), to produce analytical and empirical researches about regulated sectors, to network, and to exchange documents and ideas.

At present, its scope is focused on the regulation of Energy (electricity and gas markets), of Communications & Media, and of Transport.

This series of working papers aims at disseminating the work of scholars and practitioners on current regulatory issues.

For further information
Florence School of Regulation Transport Area
Robert Schuman Centre for Advanced Studies
European University Institute
Via delle Fontanelle 19
I-50014 Fiesole (FI)
Tel.: +39 055 4685 795
Fax: +39 055 4685 755
E-mail: fsr.transport@eui.eu
Web:
www.eui.eu/DepartmentsAndCentres/RobertSchumanCentre/Research/Programmes/FlorenceSchoolRegulation.aspx

Abstract

The objective of this working paper is to point out actual and potential obstacles to effective protection of the fundamental right to data protection, created by rules on jurisdiction and applicable law, and to put forward solutions for removing those obstacles with regard to data protection. More precisely, the working paper first elaborates on categories of litigation in the field of data protection in order to identify potential claimants, defendants and competent administrative and judicial authorities that may decide on those remedies. Furthermore, building upon these categories of litigation, the working paper seeks to determine jurisdictional issues regarding data protection litigation within the EU, elaborating concretely on potential competent courts in case a data subject wants to file a private enforcement claim against a controller processing his personal data. Finally, the working paper addresses issues of applicable law in data protection litigation, dealing with questions such as the possibility of agreements on applicable law, the questions of applicable law if the controller is situated within the EU and the questions of extraterritorial application of EU data protection law if the controller is established outside of the EU. The working paper concludes with final remarks on the above issues.

Keywords

Data protection, private international law, jurisdiction, applicable law, extraterritoriality

"We're entering a new world in which data may be more important than software."
Tim O'Reilly

1. Introduction*

In only two decades, the increased use of internet, social media and, more generally, information technology has clearly led to profound changes in the functioning of our society – changes that represent an ever-increasing challenge and threat for the protection of fundamental rights of European citizens. Information technologies not only greatly increase access to and exchange of information, facilitate digital trading and enable data transfers, but also, as recent NSA surveillance scandals demonstrate, potentially lead to infringements of the fundamental rights to data protection and privacy of European citizens. In Europe, these fundamental rights are protected with numerous legal instruments. The right to privacy is enshrined in the EU Charter of Fundamental Rights (Art.7), the European Convention on Human Rights (Art.8), and the constitutions of many EU Member States. Some legal sources recognise data protection as a separate fundamental right (EU Charter of Fundamental Rights, Art.8); therefore, for the purposes of this article, the term 'data protection' will be used as encompassing also data protection aspects of privacy.[1] Within the EU, this fundamental right is concretised notably through the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive)[2], and new legislation in this field (proposal for the future Data Protection Regulation[3] and Directive[4]) is currently being considered by the EU legislator.

While it is arguable whether the fundamental right to data protection is directly applicable among individuals[5], it is beyond doubt that this fundamental right and its concretisations in secondary

* The author would like to thank Hielke Hijmans, Jorg Sladič and Joasia Luzak, for their helpful discussions and comments on an earlier draft of this paper. Moreover, the author would like to express gratitude to Colette Cuijpers, Johannes Eichenhofer, Raphaël Gellert, Gloria González Fuster, Andrea Jelinek, Tuomas Ojanen and Christian Welter for providing expertise on Member States' legislation. Errors and omissions remain those of the author.

1 For the purposes of this article, the term 'data protection' is used to encompass also data protection aspects of privacy. For a discussion in the literature on distinction between data protection and privacy see, for example, M. Tzanou, "Is Data Protection the Same as Privacy? An Analysis of Telecommunications' Metadata Retention Measures", (2013) 17 *Journal of Internet Law*, 26 et seq.; O. Lynskey, "Deconstructing Data Protection: The 'Added Value' of a Right to Data Protection in the EU Legal Order", (2014) 63 *International and Comparative Law Quarterly*, 569-597; J. Kokott and C. Sobotta, "The distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR", in H. Hijmans and H. Kranenborg (ed.), *Data Protection Anno 2014: How to Restore Trust?* (Cambridge: Intersentia, 2014) 83-95; P. Hustinx, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", available at *https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Publications/SpeechArticle/SA2014* [Accessed 18 February 2015].

2 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 [1995] OJ L 281/31.

3 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012) 11 final).

4 Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (COM(2012)10 final).

5 Compare J. Kokott and C. Sobotta, "The distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR", in H. Hijmans and H. Kranenborg (ed.), *Data Protection Anno 2014: How to Restore Trust?* (Cambridge: Intersentia, 2014), 91.

legislation are of relevance not only for the relationships between an individual (data subject[6]) and public authorities processing personal data, but also in private law relationships between a data subject and a private controller[7] processing such data. Despite this importance, public (administrative) enforcement through Data Protection Authorities (DPAs) currently still plays a major role in data protection enforcement[8]. However, this type of enforcement shows certain deficiencies, such as lack of resources, limited powers and concerns regarding independence of DPAs[9]. Therefore, there is an increasing need to guarantee effective private (judicial) protection of the fundamental right to data protection, not least because, in data protection, the breaches can affect several data subjects simultaneously, leading to infringements of a potentially larger scope than infringements of other rights. Moreover, judicial authorities are in a most suitable position to guarantee a fair balance of data protection with other competing rights and values, such as intellectual property, freedom of expression, security and economic interests of businesses processing data. Consequently, it is important to address these challenges of effective enforcement of data protection not only through examining enforcement by DPAs, but also by competent judicial authorities that decide in a framework of actions brought by individuals against companies or authorities processing data[10].

The first step towards guaranteeing effective judicial protection of the fundamental right to data protection is that private international law rules regarding jurisdiction and applicable law for this field are framed in a way to enable effective judicial enforcement of this right. More precisely, these rules should be framed in a way to enable the European citizens to effectively make use of and protect their right to data protection. While the issues of jurisdiction and applicable law in the field of data protection have recently attracted attention of the academic literature,[11] this doctrine remains largely focused on the technical question of the applicability of a law of a particular Member State[12] as regulated by Article 4 of the Data Protection Directive[13] and accords somewhat less attention to the

---

6 A 'data subject' is, according to Article 2(a) of the Data Protection Directive, an ' identified or identifiable natural person'.

7 For a definition of a 'controller', see Article 2(d) of the Data Protection Directive.

8 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Towards a European Horizontal Framework for Collective Redress* (COM(2013) 401 final).

9 European Union Agency for Fundamental Rights, Data Protection in the European Union: the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II (Luxembourg: Publications Office of the European Union, 2010), p. 8.

10 Such private enforcement claims are still relatively rare in Europe. The most prominent example of such an action is the Schrems v. Facebook case which is a class action filed by 25.000 European citizens against Facebook before Austrian courts. For more information see *http://europe-v-facebook.org/EN/en.html* [Accessed 23 February 2015].

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

12 See, for example, L. 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?" (2011) 1 *International Data Privacy Law*, 28-46.

13 See, for example, C. Kuner, *European Data Protection Law*, 2nd ed. (OUP, 2012), 114.

theoretical interplay between data protection and the instruments of European private international law[14].

In light of the above, the objective of the present article is to point out actual and potential obstacles to effective protection of the fundamental right to data protection, created by the rules on jurisdiction and applicable law, and to put forward solutions for removing those obstacles with regard to data protection. More precisely, the article first elaborates on the categories of litigation in the field of data protection in order to identify potential claimants, defendants and competent administrative and judicial authorities that may decide on those remedies (section 2 of the article). Furthermore, building upon these categories of litigation, the article seeks to determine jurisdictional issues regarding data protection litigation within the EU (section 3 of the article), elaborating concretely on potential competent courts in case a data subject wants to file a private enforcement claim against a controller processing his personal data. Finally, the article addresses issues of applicable law in data protection litigation (section 4 of the article), dealing with questions such as the possibility of agreements on applicable law, the questions of applicable law if the controller is situated within the EU and the questions of extraterritorial application of EU data protection law if the controller is established outside of the EU. The article concludes (section 5) with final remarks on the above issues.

At the outset, some terminological clarifications are needed. In doctrine, the concepts of jurisdiction and applicable law are often treated as overlapping concepts[15], either in the sense that a court's jurisdiction is determined on the basis of rules regarding applicable law or in the sense that the applicable law is necessarily considered to be the one of the court deciding the matter, as expressed by the Latin phrase *qui elegit iudicem elegit ius*.[16] For the purposes of the present article, the notion of 'jurisdiction' will be used only in the meaning of 'jurisdiction to adjudicate'[17] or, in other words, as the competence of the courts to decide in a particular dispute. The focus will thus be on jurisdiction such as determined pursuant to Regulation 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters[18] which replaced, as of 10 January 2015, Regulation 44/2001[19]. It is considered that this issue is distinct from the issue of applicable law which,

---

14 The connection between data protection and private international law is addressed, for example, by Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part 1)", (2010) 18 *International Journal of Law and Information Technology*, 176 et seq.

15 This is pointed out also by C. Kuner, "Internet Jurisdiction and Data Protection Law: An International Legal Analysis", (2010) 18 *International Journal of Law and Information Technology*, 180, who states that ' national data protection authorities often equate jurisdiction and applicable law'.

16 See, for example, L. 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?", (2011) 1 *International Data Privacy Law*, 45, who talks about 'jurisdiction and applicable law regime for consumer contracts' in Rome I Regulation, whereas this regulation only contains rules on applicable law and not on jurisdiction. Kuner, *Transborder Data Flows and Data Privacy Law* (OUP, 2013), 121, understands the notion "jurisdiction" as a capacity of State or entity to have regulatory power over data protection and not as a competence of the courts to decide in disputes as this notion is generally understood in private international law.

17 Berliri, "Jurisdiction and the Internet, and European Regulation 44 of 2001", (2002) *E-Commerce: Law and Jurisdiction. The Comparative Law Yearbook of International Business. Special Issue*, 1-2, drawing upon the U.S. Third Restatement of Foreign Relations Law, distinguishes between the "jurisdiction to prescribe (or legislate), jurisdiction to adjudicate and jurisdiction to enforce". The notion of "jurisdiction" is used in this sense also in F. F. Wang, "Jurisdiction and Cloud Computing: Further Challenges to Internet Jurisdiction", (2013) 24 *European Business Law Review*, 589-616. Compare also C. Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part 1)", (2010) 18 *International Journal of Law and Information Technology*, 184.

18 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.

19 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.

as is usual in conflict-of-laws, provides an answer to the question which set of rules applies to a certain dispute.

2. Categories of litigation in the field of data protection

In order to understand for which types of litigation the analysis of the interplay between data protection and European private international law is relevant, it is necessary to establish who the potential claimants and defendants are in the litigation involving data protection issues, as well as to identify what type of remedies they have and which authorities (judicial or administrative) are competent to decide about these remedies. The Data Protection Directive regulates the issue of remedies in its Article 22 which allows for a judicial remedy "without prejudice to any administrative remedy" and "prior to referral to the judicial authority". It can be concluded that, on a proper interpretation, this article allows for two categories of remedies in case of breach of rights of data subject.

Administrative remedies constitute the first category of remedies. Since the Data Protection Directive does not specify the type of a particular administrative remedy, this issue is to be regulated by the Member States. Member States' legislation allows for various administrative remedies, for example an order with a warning or objection and other orders, such as to disclose information, to implement specific measures, to rectify, erase or block specific data, to discontinue processing operation or suspend the transfer of data to a third state.[20] Moreover, national administrative law allows for the imposition of fines or for the revocation of licenses.[21]

The second category is judicial remedies to which recourse is possible in two ways. On the one hand, judicial remedies are available *after* the competent administrative authority has issued an administrative decision on the matter, in the sense that this decision can be challenged before the competent judicial authorities. This same conclusion can be reached on the basis of Article 28(3) of Data Protection Directive which allows for "[d]ecisions by the supervisory authority which give rise to complaints" to "be appealed against through the courts". These judicial proceedings fall within the category of 'public enforcement' of data protection law.[22] It is interesting to note in this regard that the Data Protection Directive – neither when distinguishing, in Article 22, between administrative and judicial remedies, nor when providing for a possibility of appeal in Article 28(3) – makes no explicit reference to the remedies before *administrative* courts. Despite the fact that the Data Protection Directive does not expressly require that the judicial litigation needs to be administrative in nature, comparative research of Member States' legal orders shows that this is often the case.[23] In some

---

[20] European Union Agency for Fundamental Rights, *Access to data protection remedies in EU Member States* (Luxembourg: Publications Office of the European Union, 2013), p. 20.

[21] *Ibid*.

[22] This would be the case even if the initial claim before a DPA is lodged by the data subject himself, as allowed for under Article 28(4) of the Data Protection Directive, since the data subject would, in such a case, not be a party to the proceedings and the procedure before a DPA would result in administrative fines. Moreover, even if it is the data subject that lodges an appeal against the decision of a DPA, the procedure still relates to the determination of validity of an administrative decision and therefore falls within the category of public enforcement.

[23] For example, in the Netherlands, the decisions regarding allowing access, rectification or objection to processing of data are considered to be administrative (Art. 45 of the Dutch Data Protection Act, *Wet bescherming persoonsgegevens 2000*) and are, as such, dealt with the administrative courts under the Dutch General Administrative Law Act (*Algemene wet bestuursrecht 1992*). Similarly, in Austrian law, § 39(1) of the *Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000)* stipulates that the appeals against decisions of DPA are to be decided by the Federal Administrative Court (*Bundesverwaltungsgericht*). In Spain, the decisions of the Spanish Data Protection Agency can be challenged in the contentious administrative procedure on the basis of Article 18(4) of the *Organic Law 15/1999*. In Finnish law, a challenge of an administrative decision of DPA before judicial authorities would be dealt by administrative courts (see Section 45(1) of the *Personal Data Act 523/1999*). A similar conclusion can be reached for Luxembourg law

Member States, however, the opinions of DPAs are not considered to be legally binding and can thus not be challenged before the courts.[24]

On the other hand, data subjects have the right to start judicial proceedings *parallel to* and *independently of* administrative proceedings before DPAs. These judicial proceedings, initiated by data subject, could be categorised as 'private enforcement' of data protection law because a data subject is a party to the proceedings and the remedies he seeks recourse to are created for his own benefit.[25] The Data Protection Directive does not specify whether this litigation needs to be initiated before civil courts, but in several Member States this is indeed the case[26]. The identification of litigation as administrative or civil seems particularly important since the determination of jurisdiction and applicable law and the use of European private international law instruments also depends on the question whether the claim is administrative or civil in nature.[27]

Finally, the last possible category of litigation is criminal litigation. While EU law does not provide for a legal basis for criminal sanctions for data protection breaches, national laws of some Member States[28] allow for such criminal sanctions. Such enforcement obviously qualifies as 'public enforcement' of data protection law. The table below demonstrates that criminal litigation and criminal penalties are possible in the field of data protection. Whereas the present article will not further elaborate on the issues of criminal litigation, it will point out under which conditions this type of litigation can nevertheless be pertinent in the framework of Regulation 1215/2012 and data protection.

The tables below, illustrating the three main categories of litigation (administrative, civil and criminal), take into account the variables mentioned above and are therefore organised according to potential parties in data protection litigation as well as the remedies at their disposal.

(Contd.)

(see Article 33(2) of *Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel*).

24 For example, in German law, it is not possible to challenge an administrative decision of DPA, issued upon request of the data subject pursuant to § 21 of the *Bundesdatenschutzgesetz 1990*, since this article does not oblige the DPA to take specific actions against a controller. Similarly, in Belgian law, when the DPA decides on the basis of complaint, it tries to reach an agreement between the parties, in the absence of which it issues a non-binding opinion (Article 31(3) of the *Loi vie privée 1992*).

25 For the purposes of definition of the notion of 'private enforcement' in the field of data protection, inspiration can be drawn from EU competition law where this term is defined as 'a litigation, in which private parties advance independent civil claims or counterclaims based on the EC competition provisions'; see C. D. Ehlermann and I. Atanasiu, *European Competition Law Annual 2001: Effective Private Enforcement of EC Antitrust Law* (Oxford/Portland: Hart, 2003), p. xxiv.

26 In German law, this is not explicitly regulated by the *Bundesdatenschutzgesetz 1990*, but rather by the general rules on allocation of jurisdiction to specific courts (§ 13 of the *Gerichtsverfassungsgesetz 1975*). In Austrian law, a claim for damages pursuant to the *Datenschutzgesetz 2000* has to be lodged with the regional civil court (*Landesgericht*) in whose district the plaintiff has his domicile or seat (see Article 33(4) *juncto* Article 32(4) of *Datenschutzgesetz 2000*). In Spanish law, in cases where the data controller it is a private party, claims for compensation have to be lodged with the ordinary (i.e. civil) jurisdiction (Article 19 of the *Organic Law 15/1999*). Similarly, in Finnish law, cases involving liability in damages are decided by the civil courts (see Section 47 of the *Personal Data Act 523/1999*).

27 For example, according to its Article 1, Regulation 1215/2012 does not apply to administrative matters.

28 See, for example, Spanish law (Arts. 197-201 of the *Criminal Code 1995*); Austrian law (Article 51 of *Datenschutzgesetz 2000*); Slovenian law (Article 143 of the *Criminal Code 2008*).

Administrative litigation path

Claimant	Defendant	Remedies	Legal base	Type of enforcement	Competent authority
DPA	Controller Processor	Administrative remedies (e.g. erasure of data)	Art.28(3) of Data Protection Directive	Public	DPA or other administrative authority
Controller Processor	DPA	Challenging of DPA decision	Art.28(3) of Data Protection Directive	Public	Judicial: in principle administrative court
Data subject	DPA	Challenging of DPA decision	Art.28(3) of Data Protection Directive[29]	Public	Judicial: in principle administrative court

Civil litigation path

Claimant	Defendant	Remedies	Legal base	Type of enforcement	Competent authority
Data subject[30]	Controller Processor	Judicial remedies - injunction[31] - damages	Art. 22 and 23 of Data Protection Directive	Private	Judicial: civil court
Collective/ representative claims on behalf of data subject	Controller Processor	*Ibid.*	Member States' legislation	Private	*Ibid.*
Controller Processor	DPA/Member State	Damages action against DPA/Member State for wrongful administrative decision (state liability)		Public	Judicial: civil court

[29] Since Article 28(3) of Data Protection Directive does not specify who can lodge the appeal against the decision of DPA, an appeal by data subject is possible only if the law of the Member State allows for challenging of a DPA decision by the data subject in case he is not a party to the administrative proceedings before the DPA. The legislation of Member States provides only for limited possibilities to a data subject to challenge such a decision. For example, in Spain, according to the Judgments of the Tribunal Supremo of 6 November 2007, 10 December 2008 and 6 October 2009, the data subject can only challenge the part of the decision that does not concern the sanction. In Dutch law, a data subject can make a request to court to invalidate a decision of a DPA to approve a code of conduct or decision not to take enforcement measures (see Article 6:162 of the *Dutch Civil Code*). In Austrian law, a data subject can challenge a decision of a DPA issued upon a complaint pursuant to Art. 31 DSG 2000 before the Federal Court of Administration (see Article 39 of *Datenschutzgesetz 2000* and Art. 130 of *Federal Constitutional Law* - B-VG).

[30] It seems somewhat difficult to imagine instances where the claimant would be a controller or processor that would institute proceedings against a data subject. One could potentially imagine a breach, by a data subject, of a contract concluded between him and the data controller/processor, but since data subject is not the one processing data, such a breach would not constitute a breach of data protection legislation.

[31] For example, ordering access to data or ordering to delete/erase/rectify data.

Criminal litigation path

Claimant	Defendant	Remedies	Legal base	Type of enforcement	Competent authority
Prosecutor (private or public)	Controller Processor	Criminal penalties (fines, imprisonment)	Member States' law	Public	Judicial: criminal court

3. Jurisdiction regarding data protection litigation within the EU

3.1 Does Regulation 1215/2012 apply to data protection disputes?

In order to determine which court is competent within the framework of data protection litigation, it is first necessary to clarify whether EU rules on jurisdiction are applicable at all in this domain. More precisely, a clarification is needed as to whether data protection is covered by the notion of 'civil and commercial matters' within the meaning of Regulation 1215/2012.[32] Given that it is debatable whether data protection should be classified under administrative or civil law[33], doubts could be raised as to whether this field is covered by the scope *ratione materiae* of Regulation 1215/2012. Whereas civil and commercial matters are, in principle, covered by private law, administrative law falls within the domain of public law[34], which could make it difficult to extend the application of the regulation to this field, in particular because, in continental legal orders, the courts are still relying on the public-private law divide[35] in order to determine the applicability of the Regulation 1215/2012.[36]

It seems however that the Court of Justice of the EU (CJEU), when determining the scope of application of Regulation 1215/2012, bases itself neither on the public-private law divide[37] nor on the issue before which court the claim is brought[38]. Rather, the criterion that is pertinent is which parties are involved in the dispute: if the dispute arises between two private parties, the regulation applies[39];

---

32 See, in particular, Article 1(1) of Regulation 1215/2012.

33 An indication that data protection law could form part of administrative law can be inferred from the fact that Data Protection Directive provides for the possibility, in its Article 22, for administrative remedies, which would not be the case if the area was qualified as civil or commercial law. See for example also P. Cane, *Administrative Law*, 5th ed. (OUP, 2011), 138, who seems to treat the UK Data Protection Act as a part of administrative law.

34 P. Rogerson, in: U. Magnus, P. Mankowski, *Brussels I Regulation*, 2nd ed. (Munich: sellier, 2012), 54, stresses that the Member States from the civil law system recognise a clear distinction between public and private law, whereas the common law countries do not have such a firm conception of this distinction.

35 The doctrine points out that data protection law can be placed on the boarderline between public and private law. See L. Bygrave, "Determining applicable law pursuant to European Data Protection Legislation" (2000) 16 *Computer Law and Security Report*, 252; C. Kuner, "Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 1)", (2010) 18 *International Journal of Law and Information Technology*, 178.

36 B. Hess, T. Pfeiffer, P. Schlosser, Report on the Application of Regulation Brussels I in the Member States, Study JLS/C4/2005/03, 34. Moreover, P. Mankowski, in T. Rauscher (ed.), Europäisches Zivilprozess- und Kollisionsrecht EuZPR/EuIPR. Kommentar. Brüssel I-VO. LugÜbk 2007 (Munich: sellier, 2011), 95, points out that, even though the Regulation No 44/2001 (now Regulation 1215/2012) expressly refrains from using the public-private divide, the use of the term 'civil and commercial matters' leads to the same the same result.

37 For example, in cases of private enforcement of competition law, it does not matter whether the law that is enforced is public in nature. See pending case C-352/13, *CDC* [2013] OJ C 298/2.

38 See Article 1(1) of Regulation 1215/2012, according to which this regulation 'shall apply in civil and commercial matters *whatever the nature of the court or tribunal*'. Emphasis added.

39 For example, in Case C-265/02, *Frahuil* [2004] ECR I-1543, the Court focused only on the relationship between the parties to the procedure which was governed by private law. The circumstance that the content of the claim was the recovery of sums paid to discharge customs duties, was not relevant for the application of the Brussels convention.

if, on the contrary, one of the parties is a public authority, exercising its public powers, the scope of application of the regulation is not triggered[40]. The precise scope of the notion of 'exercise of public powers' can be best understood by reference to the subsequent case-law of the CJEU in which this court excluded from the scope of Regulation 44/2001 (now Regulation 1215/2012), for example, actions against a State for damages caused during the Second World War[41]; a claim brought by a body of public law (Eurocontrol) against a company governed by private law for the payment of charges imposed by this body[42]; or an action brought by the agent responsible for administering public waterways against a private person to recover the costs of the removal of a wreck[43]. In other cases, however, the Regulation was nevertheless deemed applicable, despite the fact that one of the parties was a public authority, due to the fact that this authority acted as a private party. This was the case, for example, regarding an action of recovery, by a public body lacking prerogatives of its own, of sums of social assistance to the divorced spouse and child[44]; a claim of a State against a private person for enforcement of a guarantee contract enabling a third person to supply a guarantee required and defined by that State[45] or even damages action of a public authority against a private person for loss caused by a tortious conspiracy to commit tax fraud[46].

When applying the abovementioned case-law concerning the scope of application of Regulation 1215/2012 to the field of data protection, it is necessary to bear in mind that the line of demarcation between cases falling under the notion of 'civil and commercial matters' and those not falling under that notion is based on a case-by-case approach, making it difficult to discern *a priori* a clear scope of application of the regulation. In each particular litigation involving administrative authorities dealing with data protection, an exact analysis of the prerogatives of these authorities would need to be conducted. In data protection disputes, the main issue which will arise in this regard will be the circumstance that one of the parties, the DPA, can in principle be qualified as a public authority, as explained below.

3.1.1 Administrative litigation path

It seems that Regulation 1215/2012 will not be applicable to cases brought under the administrative litigation path, not because the competence for them is in principle vested in the administrative courts[47], but because it appears that such a litigation is covered by the abovementioned notion of 'certain actions between a public authority and a person governed by private law' in which 'the public authority is acting in the exercise of its public powers'. The test of the applicability of Regulation 1215/2012 in administrative disputes relating to data protection is thus two-pronged: on the one hand, it needs to be established whether the party to the proceedings is a public authority and, on the other hand, whether it is acting in the exercise of its public powers.

---

40 See, for example, Case 29/76, *LTU* [1976] ECR 1541, para 4; Case 814/79, *Rüffer* [1980] ECR 3807, para 8; Case C-167/00, *Henkel* [2002] ECR I-8111, para 26; Case C-271/00, *Baten* [2002] ECR I-10489, para 30; Case C-266/01, *Préservatrice foncière TIARD* [2003] ECR I-4867, para 22; Case C-172/91, *Sonntag* [1993] ECR I-1963, paragraph 20; Case C-292/05, *Lechouritou and Others* [2007] ECR I-1519, para 31; Case C-420/07, *Apostolides* [2009] ECR I-3571, para 43; Case C-154/11, *Mahamdia*, [2012] ECR I-0000, para 56; Case C-645/11, *Sapir and Others*, [2013] ECR I-0000, para 33; and Case C-49/12, *Sunico and Others*, [2012] ECR I-0000, para 34.

41 Case C-292/05, *Lechouritou and Others*, [2007] ECR I-1519.

42 Case 29/76, *LTU*, [1976] ECR 1541.

43 Case 814/79, *Rüffer*, [1980] ECR 3807.

44 Case C-271/00, *Baten*, [2002] ECR I-10489.

45 Case C-266/01, *Préservatrice foncière TIARD*, [2003] ECR I-4867.

46 Case C-49/12, *Sunico and Others*, [2013] ECR I-0000.

47 As already mentioned, Regulation 1215/2012, according to its Article 1(1), applies 'whatever the nature of the court or tribunal'.

Regarding the first issue, the most obvious party in data protection litigation that can have the capacity of public authority is the DPA. It is beyond doubt that the DPAs have the quality of public authorities, since it stems clearly from the Data Protection Directive that the supervisory authority in charge of monitoring the application of this directive has to be a *public* authority[48]. To be more precise, DPAs are public supervisory bodies responsible for the enforcement of the law towards controllers. The proposal for the future Data Protection Regulation brings out even more clearly the public nature of the supervisory authority. In fact, according to the proposed regulation[49], the supervisory authority 'shall be empowered to impose administrative sanctions'[50]. Moreover, since controllers can also act in the capacity of a public body, administrative litigation is possible also if the controller or processor that process data of a data subject act as a public authority.

Concerning the second issue, it is submitted that the DPAs would indeed exercise their public powers when enforcing data protection legislation not only because they are empowered to issue 'administrative remedies' within the meaning of Article 22 of the Data Protection Directive, but also because they are endowed with the powers of investigation and intervention as provided for by the Article 28(3) of this directive[51]. Therefore, in cases where one of the interested parties – either a controller/processor or a data subject – challenges the administrative decision of a DPA before an administrative court, this DPA therefore seems to act as a public authority in the exercise of its public powers. This is because the administrative dispute concerns the legality of an administrative decision in the adoption of which the DPA acted through the exercise of its public powers. Consequently, in the light of the CJEU case-law exposed above, it does not seem that an administrative law dispute in which a private party challenges the decision of the DPA before national courts should be considered as being covered by the notion of 'civil and commercial matters' within the meaning of Regulation 1215/2012 which therefore does not apply in such cases. However, if a controller is a public body, it seems less clear whether the processing of data by this controller would amount to the exercise of its public powers; in such instances, the applicability of Regulation 1215/2012 would need to be assessed on a case-by-case basis.

As explained below, with regard to the civil litigation path, the analysis regarding the applicability of Regulation 1215/2012 will be comparable as the one regarding the administrative litigation.

3.1.2 Civil litigation path

Similarly, in civil path of data protection litigation, the question whether the claim falls within the notion of 'civil and commercial matters' will primarily depend on the question who the parties to the procedure are. In this regard, several potential claimants can be identified. The most obvious claimant is of course the data subject, defined in the Data Protection Directive as 'identified or identifiable natural person',[52] a wording that indicates that companies, for example, cannot be qualified as data

---

48 See Article 28 of the Data Protection Directive.

49 See Article 79 of the proposed Data Protection Regulation.

50 However, considering that the range of sanctions varies from 250.000 EUR to 1.000.000 EUR, one might wonder whether the latter amount of sanctions can still be considered as administrative and not criminal in nature. From a comparative perspective, in French law, a sanction of 300.000 EUR is already considered as being criminal in nature (Art. 226-16 of the French Criminal Code 2004). In German law, administrative fines range from 50.000 to 300.000 EUR (§ 43 of the German Federal Data Protection Act). See also G. Thüsing, J. Traut, "The Reform of European Data Protection Law: Harmonisation at Last?" (2013) 5 *Intereconomics*, 275, who equally point out the controversy around the amount of administrative sanctions, drawing a parallel with sanctions in EU competition law.

51 Such public powers are confirmed also in the legislation of different Member States. See, for example, Article 11 of the French *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* or Article 30 of the Austrian *Datenschutzgesetz 2000*.

52 See Article 8(a) of the Data Protection Directive.

subjects. The individuals engaging in civil data protection litigation[53] can, depending on the legal order of a particular Member State, request damages[54] or an injunction, for example a request to remove/erase or modify data appearing online[55].

Another alternative of civil litigation path is a national collective action on behalf of data subject, depending on whether such a collective action is available in a particular Member State.[56] Despite the initiatives in this sense, collective redress is currently not (yet) regulated on the EU level.[57] Nevertheless, the importance of collective or representative claims in the field of data protection should not be neglected, notably given the fact that data protection infringements can simultaneously affect a large number of data subjects. An example of such a collective claim on a national level is the currently pending Austrian case *Schrems v. Facebook*[58]. Collective claims raise important issues of jurisdiction and applicable law.[59] The current jurisdictional rules in force, however, ill-suited for collective claims.[60]

Yet another alternative are representative claims filed by an authority or organisation on behalf of data subject, although it might be debatable whether such claims could be qualified as civil litigation if the data subject is represented by a public authority. In any event, the current Data Protection Directive does not provide for the express possibility of representative claims before the courts. While its Article 28(3) does give DPAs the right to 'engage in legal proceedings' and to bring violations 'to the attention of judicial authorities', it is not entirely clear whether this Article could also cover claims for damages on behalf of data subject. To the contrary, the proposed Data Protection Regulation includes the possibility of such representative claims in its Article 76(1).

---

53 An example of such a claim is an action of an individual against an internet service provider requesting, by way of injunction, that his data is treated according to the data protection laws in force or a claim for damages against this same internet service provider for unauthorised publishing of his personal data.

54 See Article 23 of the Data Protection Directive. It is to be noted, however, that these laws do not specify whether the data subject can request both pecuniary and non-pecuniary damages.

55 European Union Agency for Fundamental Rights, *Access to data protection remedies in EU Member States* (Luxembourg: Publications Office of the European Union, 2013), p. 20.

56 In the Netherlands, for example, the *Wet collectieve afhandeling massaschade 2005 is currently under review so as to include also* collective actions for compensation of damages (see the proposal *Wijziging van het Burgerlijk wetboek en het Wetboek van burgerlijke rechtsvordeing teneinde de afwikkeling van massaschade in een collective actie mogelijsk te maken, Consultatieversie Juli 2014, available at 2014-06_Voorstel_Titel_14a_sv_305a_consultatieversie.pdf [Accessed 25 February 2015]).* In Germany, the legislator is currently adopting legislation that would allow for collective actions in the field of data protection. See Entwurf eines Gesetzes zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts, available at <www.bmjv.de/SharedDocs/Downloads/DE/pdfs/Gesetze/RegE-UKlaG.pdf?__blob=publicationFile>. *In Austria, collective redress is available on the basis of several procedural rules, such as joinder of claims, in order to develop the 'Austrian model of the class action'; see G. E. Kodek, "Collective Redress in Austria", (2009) 622 Annals of the American Academy of Political and Social Science, The Globalization of Class Actions, 86 et seq. Furthermore, see also the Danish Class Action Act 2008 and the Swedish Group Proceedings Act 2003.*

57 See Commission Recommendation of 11 June 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law (2013/396/EU) [2013] OJ L 201/60.

58 See http://europe-v-facebook.org/EN/en.html [Accessed 23 February 2015].

59 Such as demonstrated for example by Case C-167/00, Henkel [2002] ECR I-8111; C-292/05, *Lechouritou and Others* [2007] ECR I-1519; C-21/76, *Handelskwekerij Bier v Mines de Potasse d'Alsace*, [1976] ECR 1735. Compare, for example, also in the field of competition law, pending case C-352/13, *CDC* [2013] OJ C 298/2. B. Hess, "A Coherent Approach to European Collective Redress", in D. Fairgrieve, E. Lein, *Extraterritoriality and Collective Redress* (Oxford: Oxford, 2012), stresses the need for a coherent instrument on cross-border collective redress in the EU.

60 E. Lein, "Cross-Border Collective Redress and Jurisdiction under Brussels I: A Mismatch", in D. Fairgrieve, E. Lein, *Extraterritoriality and Collective Redress* (Oxford: Oxford, 2012), 129 et seq.

Finally, the controller or processor can institute a claim of state liability due to a wrong assessment by the DPA before the civil courts. However, since this is not a classic example of private enforcement of data protection law, it will not be further elaborated upon in this article.

Analysing the issues above from the perspective of Regulation 1215/2012, it is to be stressed that claims between private parties would, in general, be covered by the scope of the regulation, save for cases expressly excluded due to their subject matter.[61] Hence, the claims of a data subject against a controller/processor requesting injunction or damages will undoubtedly be covered by the scope of application of the regulation.

3.1.3 Criminal litigation path

According to CJEU case-law, Regulation 1215/2012[62] can sometimes be used even to determine jurisdiction in criminal litigation if the litigation is instituted by a private prosecutor. As it stems from the case *Sonntag*, a damages action for civil compensation brought before a criminal court against a teacher having caused injury to a pupil by way of a culpable and unlawful breach of his duties of supervision falls under the notion of 'civil matters'[63]. Therefore, in case of a (civil) claim for damages made by a private prosecutor in the framework of criminal proceedings, Regulation 1215/2012 would still be applicable. However, since the Data Protection Directive does not provide for criminal sanctions for wrongful processing of personal data, this jurisdictional basis will be less important in the field of data protection and will not be further elaborated upon in the framework of this article.

3.2 Possible jurisdictional bases for data protection litigation under Regulation 1215/2012

Once it is determined that Regulation 1215/2012 applies for a particular data protection litigation, the claimant can, apart from instituting an action in the domicile of the defendant (Article 4(1)), also make use of several special jurisdictional bases, notably the jurisdiction for consumer contracts (Articles 17 *et seq*.), for contracts in general (Article 7(1)) as well as jurisdiction for torts (Article 7(2)).

3.2.1 Jurisdiction of the domicile of defendant

The most general rule for determining jurisdiction according to Regulation 1215/2012 is the rule *actor sequitur forum rei*[64], according to which the defendant can be sued in the courts of his domicile, as stipulated by Article 4(1) of this regulation. However, with regard to data protection, several observations need to be made.

At the outset, it is important to clarify that Regulation 1215/2012 will in principle not be applicable when the defendant has his domicile outside the EU.[65] The notion of 'domicile' in this regulation

---

61 P. Rogerson, in: U. Magnus, P. Mankowski, *Brussels I Regulation*, 2nd ed. (Munich: sellier, 2012), 55.

62 Note that the case-law still relates to Regulation No 44/2001 or even the Convention of 27 September 1968 on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters [1978] OJ L 304/36, 'the Brussels Convention'), but for reasons of consistency, this article refers to Regulation 1215/2012.

63 Case C-172/91, *Sonntag* [1993] ECR I-1963.

64 For the use of this expression, see for example P. Vlas, in: U. Magnus, P. Mankowski, *Brussels I Regulation*, 2nd ed. (Munich: sellier, 2012), 78. In case-law, see for example, Cases C-412/98, *Group Josi* [2000] ECR I-5925, para 35; C-256/00, *Besix* [2002] ECR I-1699, para 52.

65 As it stems from Article 4 of Regulation 1215/2012, this Regulation is only applicable if the lawsuit is filed against a person 'domiciled in a Member State'. Moreover, Recital 14 of this regulation clarifies that a 'defendant not domiciled in a Member State should in general be subject to the national rules of jurisdiction applicable in the territory of the Member State of the court seised', although there might be exceptions to this rule, such as jurisdiction for consumers and

covers both domicile of natural and legal persons and, in a case of a company, encompasses its statutory seat, central administration or principal place of business.[66] Therefore, if the data subject wants to file a lawsuit, for example, directly against a company providing services of a search engine or against another company providing online services, established in the US, this data subject will not be able to rely on the rules of the Regulation. In practice this means that a European data subject who wants to sue a company established in a third country can only rely on the rules of private international law of his own Member State; if these rules do not give him the possibility to file a lawsuit in the Member State of his domicile, he will be obliged to do so before the courts of that country.[67] This would lead, however, to a rather interesting result where civil litigation could not be brought within the EU, whereas administrative litigation could, since under the Data Protection Directive, a DPA could request compliance also from a controller not established in the EU.[68] A comparable issue arose in the CJEU case *Google Spain and Google*[69] where the Spanish DPA issued a decision both against the US parent company Google Inc. as well as against its Spanish subsidiary Google Spain. The two companies brought separate actions against that decision before the Spanish National High Court that decided to join the two actions.[70] It is not clear from the facts of the case whether the US company Google Inc. contested the jurisdiction of the Spanish courts in this matter, but since it was challenging an (administrative) decision of a national DPA, its only possibility was to challenge it before the courts of that same Member State. It is nevertheless important to bear in mind that, in the *Google Spain and Google* case, Regulation 1215/2012 was not applicable for several reasons: not only because the Spanish DPA was, when issuing a decision against Google, most likely acting in the exercise of public powers,[71] but even if this was not the case, this regulation would not be applicable due to the fact that one of the defendants (Google Inc.) was domiciled in the US and another defendant (Google Spain) in the same Member State as the applicant which would trigger the application of domestic conflict-of-law rules and not those of Regulation 1215/2012[72]. Therefore, within the EU, there was an absence of a cross-border element because the data subject and the European subsidiary of the controller were situated in the same Member State.[73]

Furthermore, going beyond the legal issues of the case *Google Spain and Google*, two important questions need to be addressed. On the one hand, a question can be asked whether, in the field of data protection, there should be an exception to this general rule of non-applicability of Regulation 1215/2012 if the defendant is domiciled in a third country in the same way as provided for consumers or employees[74] which are traditionally regarded as weaker (contractual) parties. It is submitted that

(Contd.)

employees. For the definition of the notion of 'domicile', see for example P. Vlas, in: U. Magnus, P. Mankowski, *Brussels I Regulation*, 2nd ed. (Munich: sellier, 2012), 80.

66 See Article 63 of Regulation 1215/2012.

67 Along these lines, the current President of the European Commission Juncker suggested that European citizens should enforce their data protection rights in US courts. See J. C. Juncker, *A New Start for Europe: My Agenda for Jobs, Growth, Farness and Democratic Change. Political Guidelines for the next European Commission* (2014), available at *http://ec.europa.eu/about/juncker-commission/docs/pg_en.pdf* [Accessed 26 February 2015].

68 See Article 4 *juncto* Article 28 of the Data Protection Directive. For more on jurisdiction over foreign entities, see Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part 2)", 18 *International Journal of Law and Information Technology* (2010), 228 et seq.

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

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

71 See heading 0. of the present article.

72 See the first paragraph of Recital 14 of Regulation 1215/2012, according to which a defendant that is not domiciled in a Member State is subjected to the jurisdictional rules applicable in the Member State of the court seised.

73 See P. Mankowski, in T. Rauscher (ed.), Europäisches Zivilprozess- und Kollisionsrecht EuZPR/EuIPR. Kommentar. Brüssel I-VO. LugÜbk 2007 (Munich: sellier, 2011), 154-155.

74 See the second paragraph of Recital 14 of Regulation 1215/2012, according to which, "in order to ensure the protection of consumers and employees […] certain rules of jurisdiction in this Regulation should apply regardless of the defendant's domicile".

such a modification of Regulation 1215/2012 would not only be beneficial for the European data subjects, but it would also strike a fair balance between different positions of a stronger controller and a weaker data subject, regardless of whether data is processed on a contractual basis or not.[75]

On the other hand, it is important to address the question whether, for the purposes of civil litigation, the notion of 'domicile' in Regulation 1215/2012[76] and the notion of 'establishment' in data protection legislation[77] necessarily have to be given the same meaning. It needs to be specified, however, that for the purposes of data protection legislation, it is the establishment that *processes* personal data of data subject *in the context of its activities* that is pertinent and not any other establishment. It is true that in practice, this problem might not be as pressing, given the fact that many of the third country companies that process personal data often have a subsidiary within the EU, such as Google, Facebook or Amazon. Yet, in case of other companies established in third countries this issue might be important. It is submitted that such an interpretation, leading to parallelism between jurisdictional rules and rules regarding applicable law would be beneficial since it would give legal certainty to a company processing personal data on where it can be sued and according to which rules. Moreover, it would also greatly facilitate the work of national courts since they would know that, once they establish a domicile of a company pursuant to Regulation 1215/2012, they could also reasonably assume that data protection legislation applies.[78]

3.2.2 Consumer jurisdiction: contractual jurisdiction

3.2.2.1 Relevance of consumer jurisdiction for data protection

Given the fact that the data subject has to be, as per the definition from the Data Protection Directive, a natural person[79], it is possible to qualify him as a 'consumer' within the meaning of Regulation 1215/2012. However, it is to be stressed that, unlike in the US[80], data protection law in the EU is not considered as part of consumer law and the simple fact that the data subject is a natural person does not immediately make him a consumer within the meaning of Regulation 1215/2012. In fact, in order to be covered by this regulation, such a consumer has to conclude a contract 'for a purpose which can be regarded as being outside his trade or profession'[81]. If a person concludes a contract for the sale of goods or uses services online for his private purposes only and his data is processed in the framework of this contract, then he will be able to rely on the consumer jurisdiction.

A problem that can arise with regard to the qualification of the data subject as a consumer is the fact that he will often use (especially online) services (or even goods) for a dual, private and professional use. Typically, e-mail accounts, Skype, web messengers or even Facebook will often be

---

75 For a proposed modification of Regulation 1215/2012, see section 0. of this article.

76 See Article 4 *juncto* Article 63 of Regulation 1215/2012 as well as Article 18(1) of this Regulation.

77 See Article 4(1) of the Data Protection Directive or in Article 3(1) of the proposal for the future Data Protection Regulation.

78 A counterargument against such parallel interpretations could be the fact that Article 4(1) of the Data Protection Directive or in Article 3(1) refer to processing "*in the context* of the activities of an establishment" (emphasis added) and not merely to an establishment of data controller or processor.

79 Article 2(a) of the Data Protection Directive.

80 In the US, the protection of privacy is entrusted with the Federal Trade Commission (FTC) that is empowered, pursuant to the *Federal Trade Commission Act 1914*, to enforce unfair and deceptive practices towards consumers under Section 5 of the FTC Act; this same section has also been used to enforce the right to privacy. In theory, see also P. Bernal, *Internet Privacy Rights. Rights to Protect Autonomy* (New York: Cambridge University Presss, 2014), 113, who points out that the FTC has a role 'as a protector of consumer rights'.

81 Article 17(1) of Regulation 1215/2012.

used for both purposes. According to the *Gruber*[82] case of the CJEU, such a dual usage would not trigger consumer jurisdiction[83]. In fact, the purpose of specific jurisdictional clauses to protect the consumer as the weaker contractual party would not be attained if a contract is partially linked to a trade or profession of a contractual party.[84] The degree of professional use according to this case-law has to be 'so slight as to be marginal' and has to have 'only a negligible role' relating to the entire contract.[85] It is interesting to note that the test to determine whether a person is to be considered a consumer is not the one of the 'centre of gravity' of the activities of a person, but rather, one could say, one of 'contamination'. For a data subject, this means that, in case of the slightest non-marginal professional use of goods or services, he will not be considered as a consumer for the purposes of Regulation 1215/2012 unless he proves otherwise[86].

In cases where the data subject is considered to be a consumer, it will further need to be established whether other conditions of applicability of consumer jurisdiction are fulfilled. What can be particularly problematic is to determine whether a consumer (data subject) concluded a contract with a professional who *directs* his activities to the Member State of his domicile.[87] The case-law in this regard, starting with *Pammer and Hotel Alpenhof*[88] and continuing with *Mühlleitner*[89] and *Emrek*[90], is well established. In *Pammer and Hotel Alpenhof*, the CJEU set up a non-exhaustive list of factors indicating when a professional directed his commercial activity to the Member State of the consumer's domicile.[91] In *Mühlleitner*, the CJEU further specified that the application of a special consumer jurisdiction does not depend on the conclusion of a consumer contract at a distance[92] and, in *Emrek*, the CJEU decided that a causal link between the means of directing an activity through an internet site

---

82 Case C-464/01, *Gruber*, [2005] ECR I-439.

83 For a commentary of the case in the doctrine, see L. Idot, "Notion de contrat conclu par les consommateurs", (2005) *Europe*, 27-28; P. Mankowski, "'Gemischte' Verträge und der persönliche Anwendungsbereich des Internationalen Verbraucherschutzrechts", (2005) *Praxis des internationalen Privat- und Verfahrensrechts*, 503-509; J. Vannerom, "Consumer Notion: Natural or Legal Persons and Mixed Contracts", in E. Terryn *et al.* (ed.), *Landmark cases of EU consumer law: in honour of Jules Stuyck* (Cambridge: Intersentia, 2013), 57-72.

84 Case C-464/01, *Gruber*, [2005] ECR I-439, para 39. A. Staudinger, in T. Rauscher (ed.), *Europäisches Zivilprozess- und Kollisionsrecht EuZPR/EuIPR. Kommentar. Brüssel I-VO. LugÜbk 2007* (Munich: sellier, 2011), 379, points out that the protection of weaker contractual party as well as the circumstance that consumer jurisdiction represents an exception to the general jurisdictional rules, require a restrictive interpretation of the notion of 'consumer'. Moreover, as pointed out by L. Gillies, "European Union: Modified Rules of Jurisdiction for Electronic Consumer Contracts" (2001) 17 *Computer Law & Security Report* 6, 397, the CJEU ruled already in 1978 in Case 150/70, *Bertrand v Ott* [1978] ECR 1431, that consumer jurisdiction applies only to consumers as private individuals and not to companies.

85 Case C-464/01, *Gruber*, [2005] ECR I-439, para 39.

86 The fact that the consumer carries the burden of proof regarding marginal use for professional purposes is pointed out by A. Staudinger, in T. Rauscher (ed.), *Europäisches Zivilprozess- und Kollisionsrecht EuZPR/EuIPR. Kommentar. Brüssel I-VO. LugÜbk 2007* (Munich: sellier, 2011), 383.

87 See Article 17(1)(c) of Regulation 1215/2012. Less problematic will be the criterion, equally contained in this article, seeking to determine whether a professional pursues his activities in the Member State of consumer's domicile.

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

89 Case C-190/11, *Mühlleitner*, [2012] published in the electronic Reports of Cases.

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

91 See Case C-585/08, *Pammer and Hotel Alpenhof*, [2010] ECR I-12527, para 93. Those criteria are, for example, "the international nature of the activity, […] use of a language or a currency other than the language or currency generally used in the Member State in which the trader is established […], mention of telephone numbers with an international code, 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 other Member States, use of a top-level domain name other than that of the Member State in which the trader is established, and mention of an international clientele […]".

92 See case Case C-190/11, *Mühlleitner*, [2012] published in the electronic Reports of Cases, para 45. It is, however, not clear from this case-law whether any of the other phases leading to the conclusion of contract (negotiation, offer, acceptance) needs to be done per distance; see, in this regard, Brkan, "Arrêt Mühlleitner: vers une protection renforcée des consommateurs dans l'U.E.", (2013) *European Journal of Consumer Law*, 116.

and the actual conclusion of a contract is not necessary[93]. However, it is yet to be seen, for data protection, whether these criteria will have to be adjusted to take into account the place of processing of data and other particularities of data protection.

If all the criteria for the applicability of consumer jurisdiction are fulfilled, the competent court will be determined according to the rules on consumer jurisdiction in Regulation 1215/2012[94]. Therefore, if such a data subject files a lawsuit against a controller/processor for an injunction or damages, he will be able to choose whether to sue either in the place of the domicile of the defendant (i.e. establishment of the controller/processor) or in the place of his own domicile[95], whereas the other contracting party will be able to file a lawsuit against the data subject only in the place of the domicile of the latter[96].

Finally, it is important to address the issue of the link between the rules on applicable law and the rules on jurisdiction with regard to consumer law and with regard to data protection law. Regarding consumer protection, the currently applicable rules of European private international law in principle lead to a result according to which a court that would have jurisdiction regarding certain matter would also apply its own domestic law.[97] Therefore, the area of consumer protection is, in principle, one of the rare areas with parallelism between the rules on applicable law and jurisdiction. In data protection law, however, rules on jurisdiction and on applicable law can lead to different results. This means that, in practice, the consumer (data subject) will be able to sue the controller/processor in the Member State of his domicile, but the law with which this controller/processor will have to comply when processing data – determined according to Article 4 of the Data Protection Directive – will (most probably) not be the law of that Member State, which can lead to a lower level of consumer protection in the field of data protection than in other fields of law. The field of data protection therefore does not lead to parallelism[98] between jurisdiction and applicable law.

3.2.2.2 Difficulties regarding prorogation of jurisdiction in consumer contracts

In practice, the general terms of use of most companies providing services and selling goods online – companies that also process data and can hence be qualified as data controllers/processors – most frequently contain a contractual clause allocating jurisdiction to the courts in the place of establishment of the company.[99] Despite the fact that this seems to be a common practice as regards online contracts of companies operating on the internet, it is submitted that such a prorogation of

---

93 See Case C-218/12, *Emrek*, [2013] not yet published in ECR, para 32.

94 See Section 4 of Regulation 1215/2012.

95 In application of Article 18(1) of Regulation 1215/2012.

96 In application of Article 18(2) of Regulation 1215/2012.

97 See Recital 24 of the 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) [2008] OJ L 177/6. According to this recital, the "concept of directed activity" should be "interpreted harmoniously" in Regulation 44/2001 (now Regulation 1215/2012) and in Regulation Rome I.

98 See more regarding this in point 0. of this article.

99 See, for example, clause 18.9 of the "Skype Terms of Use", according to which "[t]hese Terms […] shall be governed by and interpreted in accordance with the laws of Luxembourg and shall be subject to the jurisdiction of the courts of the district of Luxembourg. […]" It can be understood from the point 15 of these Terms of Use that the Skype Privacy Policy forms an integral part of the Terms of Use. For the complete Skype Terms of Use, see *http://www.skype.com/en/legal/tou/#16* [Accessed 26 February 2015]. Interestingly, the "Conditions of Use & Sale" of Amazon.co.uk stipulate what would have been the result of determining consumer jurisdiction pursuant to Regulation 1215/2012, by giving the consumer the choice between filing a suit in the place of his domicile or in the place of the subsidiary of the American company in Europe (Luxembourg): "These conditions are governed by and construed in accordance with the laws of the Grand Duchy of Luxembourg […]. We both agree to submit to the non-exclusive jurisdiction of the courts of the district of Luxembourg City, which means that you may bring a claim to enforce your consumer protection rights in connection with these Conditions of Use in Luxembourg or in the EU country in which you live." See *http://www.amazon.co.uk/gp/help/customer/display.html?nodeId=1040616* [Accessed 26 February 2015].

jurisdiction in consumer contracts could be problematic under the current EU rules. Two lines of reasoning speak against such a prorogation of jurisdiction.

On the one hand, such a clause in a consumer contract, stipulating jurisdiction in favour of the place of establishment of the internet company, can be considered as an unfair term in consumer contract pursuant to the Directive 93/13 on unfair terms in consumer contracts[100] due to the fact that, not having been individually negotiated, 'it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer'[101]. As confirmed by the CJEU in the case *Océano Grupo*[102], such a jurisdictional clause, included in a consumer contract, that was not individually negotiated and that establishes an exclusive jurisdiction in the place of establishment of the seller, is to be regarded as unfair within the meaning of Directive 93/13 if it causes a significant imbalance between the parties[103]. In practice, this means that such a contractual clause is not binding on the consumer and that the contract in itself is binding only if it can exist without the unfair term.[104] It is rather evident that the consumer contract will be able to exist without such a jurisdictional clause, thus making only this clause non-binding for consumer. For data subject this means that he can rely on another jurisdictional base, either the one for consumer jurisdiction, contractual jurisdiction or the general rule of the domicile of the defendant.

On the other hand, such a prorogation of jurisdiction would also not be in accordance with the provisions of Regulation 1215/2012. According to Article 19 of Regulation 1215/2012[105], a prorogation of jurisdiction in consumer contracts is possible after the dispute has arisen[106] – which is generally not the case for such general terms of use. Such a prorogation is possible also if the consumer is given the possibility of additional *fora* to bring his claim and does therefore not deprive him from the choice between the jurisdiction of the courts of his domicile and the domicile of the defendant[107] – which is normally also not the case of the general terms of use by virtue of which the controller/processor tries to bring the claim to the Member State of its establishment. Hence, a jurisdictional agreement that is contrary to these special jurisdictional clauses for consumers does not have any legal force[108] and hence does not bind the data subject. The only possibility when such an agreement could potentially be in accordance with Regulation 1215/2012 is if both the consumer and the defendant are domiciled in the same Member State and the parties prorogate jurisdiction of these courts, under the condition that such an agreement does not infringe the law of that Member State[109]. In such a case, however, prorogation of jurisdiction is not even necessary, as the consumer will be able

---

[100] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L 95/29.

[101] Article 3(1) of the Directive 93/13.

[102] Case C-240/98, *Océano Grupo Editorial and Salvat Editores*, [2000] ECR I-4941. The CJEU confirmed in further case-law that the "national court must investigate of its own motion whether a term conferring exclusive territorial jurisdiction in a contract concluded between a seller or supplier and a consumer falls within the scope of Directive 93/13 and, if it does, assess of its own motion whether such a term is unfair"; see, in this regard, Case C-618/10, *Banco Español de Crédito*, [2012], not yet published in ERC, para 44; and Case C-137/08, *VB Pénzügyi Lízing*, [2010] ERC I-10847, para 56.

[103] Case C-240/98, *Océano Grupo Editorial and Salvat Editores*, [2000] ECR I-4941, para 24.

[104] See Article 6(1) of Directive 93/13.

[105] It seems that, in the field of consumer contracts, Article 19 of Regulation 1215/2012 *ab initio* excludes the application general rule on prorogation of jurisdiction, namely its Article 25.

[106] See Article 19(1) of Regulation 1215/2012.

[107] See Article 19(2) of Regulation 1215/2012.

[108] See Article 25(4) of Regulation 1215/2012. In the doctrine, see in this regard A. Staudinger, in T. Rauscher (ed.), *Europäisches Zivilprozess- und Kollisionsrecht EuZPR/EuIPR. Kommentar. Brüssel I-VO. LugÜbk 2007* (Munich: sellier, 2011), 408.

[109] See Article 19(3) of Regulation 1215/2012.

to sue in the Member State of his domicile already on the basis of jurisdictional rules for consumers from the regulation itself.

Therefore, European data subjects that can also be qualified as consumers will be able to invoke that they are not bound by clauses which prorogate jurisdiction and will be able to avail themselves of more beneficial rules on consumer jurisdiction.

3.2.3 Non-consumer jurisdiction: contracts

In all cases where the data subject cannot be qualified as a consumer, but nevertheless concludes a contract with the controller/processor, the general contract jurisdiction – vesting jurisdiction in the courts of the place of performance of the obligation in question[110] – will be applicable. Jurisdiction will depend, however, on the question whether the contract in question is a contract for the sale of goods[111] or the provision of services[112]. In the former case, the data subject will be able to sue in the place where the goods were delivered or should have been delivered[113] whereas in the latter, the place where the services were provided or should have been provided[114], will be pertinent to determine jurisdiction. If the contract cannot be fitted into any of those two categories, the place of performance of the obligation in question[115] will have to be determined according to the *Tessili*[116] case-law, confirmed, in the framework of Regulation 1215/2012 (at the time of deciding the case still Regulation No 44/2001), by the *Falco Privatstiftung and Rabitsch*[117] case. According to this case-law, the national court will have to determine in three steps whether it has jurisdiction: it first has to identify the contractual obligation that is the subject of the dispute between the contractual parties; secondly, on the basis of the private international law of its Member State, it has to determine the substantive law applicable to the contract (*lex causae*); and thirdly, it has to identify, on the basis of this *lex causae*, the place of performance of the contractual obligation in question.[118]

While for the place of performance of a contract for the sale of goods it does in principle not make a difference whether the contract is concluded by traditional means or online, this issue can be problematic in case of delivery of digitised products[119] such as software[120] or e-books[121]. A preliminary

---

110 See Article 7(1)(a) of Regulation 1215/2012.

111 For example, a law professor buys a book online from the publishing house and provides the latter with her personal data which is being processed by the publisher.

112 For example, a law professor concludes a contract with a professional social network, such as LinkedIn, biznik, Cofoundr, Ecademy or Perfecctbusiness.

113 See Article 7(1)(b), first alinea, of Regulation 1215/2012.

114 See Article 7(1)(b), second alinea, of Regulation 1215/2012.

115 See Article 7(1)(c) of Regulation 1215/2012.

116 Case 12/76, Industrie Tessili Italiana v Dunlop AG, [1976] ECR 1473.

117 Case C-533/07, *Falco Privatstiftung and Rabitsch*, [2009] ECR I-3327.

118 See the opinion of Advocate General Trstenjak in Case C-533/07, *Falco Privatstiftung and Rabitsch*, [2009] ECR I-3327, para 81.

119 A good definition of digitised products is provided by D. J. B. Svantesson, *Private International law and the Internet* (Hague: Kluwer, 2012), 432, who defines a digitised product as "a product that has been transformed from a physically tangible object to a purely digital combination of binary code (e.g., electronic books), or a product that has been removed from its physically tangible carrier and is kept as a purely digital combination of binary code (e.g., mp3 files, MPEG videos and software)."

120 The issue of software is relevant also within the framework Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs [2009] OJ L 111/16, interpreted by the CJEU in the Case C-128/11, *UsedSoft GmbH* [2012] published in the electronic Reports of Cases.

121 Compare also F. F. Wang "Obstacles and Solutions to Internet Jurisdiction: A Comparative Analysis of the EU and US laws" (2008) 3 *Journal of International Commercial Law and Technology* 235, 237.

question that should be asked in this regard is whether those items constitute 'goods'[122] for the purpose of determining jurisdiction. The theory considers that this is not the case because they are not considered to be corporal objects, thus making applicable Article 7(1)(a) of Regulation 1215/2012 rather than 7(1)(b).[123] In practice, this means that the place of performance of such a contract will be determined on the basis of national law that is applicable to the contract (*lex causae*). In the literature, it is argued that the place of performance can be either at the 'place of dispatch and receipt' or, alternatively, at the place of the connecting factor either with the seller or with the buyer.[124] National law does not therefore seem to be more suited for the determination of the place of performance than European law.

Moreover, it is even more difficult to determine the place of performance of the contractual obligation for services offered online. The main issue regarding the place of performance is the question whether it is the activity (e.g. uploading the content online) or the result of that activity (e.g. downloading of the content by service recipient) that should be pertinent.[125] The doctrine points out that it is the activity that should be relevant.[126] Another alternative is to locate the place of performance at the place of business of the service provider, but it is submitted that such an approach would put too little emphasis on the actual service performed and too much emphasis on the person actually performing the service. Therefore, it is probably more sensible to locate it in the place of the recipient of a service. [127]

However, it is questionable whether, for the purpose of determining jurisdiction for claims alleging the breach of data protection rules, it should really be relevant whether the background contract is a contract for the sale of goods, for the provision of services or any other type of contract. Data protection standards are not a contractual issue that can be freely negotiated between the parties[128] and the breach of data protection rules would not necessarily amount to a breach of contract. Thus, it seems somewhat difficult to justify why jurisdiction in this matter should depend on the type of the contract at stake. It would therefore seem more appropriate to create a special jurisdictional forum for data protection, vesting jurisdiction either in the courts of the place where the data subject has his habitual residence or the place where the data is processed which would mostly amount to the place of establishment of the controller/processor.[129]

---

[122] The question of whether digitised products constitute 'goods' or 'services' was not yet directly addressed in the CJEU case-law, but was, for example, underpinning the Court's analysis in the Case C-128/11, *UsedSoft* [2012] published in the electronic Reports of Cases, and in the Case C-403/08, *Football Association Premier League and Others* [2011] ECR I-9083. In this regard, T. Dreier, "Online and Its Effect on the 'Goods' Versus 'Services' Distinction", 44 *International Review of Intellectual Property and Competition Law* (2013), 139 stresses that the CJEU has, by now, not yet developed clear criteria for distinguishing when such digitised products should be treated as 'goods' and when as 'services'. Moreover, it is to be stressed that, in the field of fundamental freedoms, this question seems less important, since the provisions on free movement of goods and services can be applied simultaneously as it stems from the Case C-390/99, *Canal Satélite Digital* [2002] ECR I-607, para. 33. However, for the purposes of determining jurisdiction on the basis of Regulation 1215/2012, this issue remains important.

[123] S. Leible, in: T. Rauscher (ed.), Europäisches Zivilprozess- und Kollisionsrecht EuZPR/EuIPR. Kommentar. Brüssel I-VO. LugÜbk 2007 (Munich: sellier, 2011), 48.

[124] F. F. Wang, "Obstacles and Solutions to Internet Jurisdiction: A Comparative Analysis of the EU and US laws" (2008) 3 *Journal of International Commercial Law and Technology*, 237.

[125] P. Mankowski, in: U. Magnus, P. Mankowski, *Brussels I Regulation,* 2nd ed. (Munich: sellier, 2012), 189.

[126] P. Mankowski, in: U. Magnus, P. Mankowski, *Brussels I Regulation,* 2nd ed. (Munich: sellier, 2012), 189-190.

[127] See in this sense for example F. F. Wang, "Obstacles and Solutions to Internet Jurisdiction: A Comparative Analysis of the EU and US laws" (2008) 3 *Journal of International Commercial Law and Technology,* 237.

[128] See section 0. of this article.

[129] See section 0. of this article.

3.2.4 Non-consumer jurisdiction: torts

For all non-contractual claims regarding data protection, the tort jurisdiction from Article 7(2) of Regulation 1215/2012 will be relevant, mostly when the data subject will file an action against the controller/processor for damage from wrongful processing of his personal data (for example, if data were made public without his consent) or request an injunction to remove his personal data from the internet.[130] In such cases, the Regulation vests competence in the courts of the 'place where the harmful event occurred or may occur'. It is submitted that the judgment in *eDate Advertising*[131] – where the CJEU judged on the issue of jurisdiction in case of infringement of personality rights with the content placed online on an internet website – can be applied per analogy to the field of data protection[132]. This leads to a result according to which the 'place where the harmful event occurred or may occur' can mean one of the three possibilities of jurisdiction: either the jurisdiction of the courts of establishment of the controller/processor, the courts of the centre of interests[133] of the data subject or, according to the 'mosaic theory', for damage caused in the territory of a particular Member State, the courts of each Member State in the territory of which content placed online is or has been accessible.[134]

Tort jurisdiction can be problematic in cases of claims brought in parallel by several data subjects against a data controller/processor for the same type of breach, notably because data subjects can have their centre of interests in different Member States and the damage can arise in different Member States. This can result in parallel proceedings which can, in turn, lead to irreconcilable judgments by different national courts.[135] Regulation 1215/2012 does not contain express rules on jurisdiction concerning regrouping of such claims brought by different claimants, but only rules allowing a court of one Member State to decline its jurisdiction and stay proceedings, either in case of the same cause of action between the same parties[136] or in case of related actions[137]. However, if courts in different Member States decline their jurisdiction in favour of a court in one Member State (in favour of the court that was seized first), a question that can be raised is whether this would not, *de facto*, create a collective action in favour of such a data subject – a remedy that is currently not yet in place in EU law.[138]

---

[130] The general theory on tort jurisdiction raises also the issue whether this type of jurisdiction can be used for unjustified enrichment. See for example O. Weber, "EuGH: Gerichtliche Zuständigkeit und Heimatstaat-Kontrolle bei Verletzung von Persönlichkeitsrechten im Internet" (2012) 1 *MultiMedia und Recht*, 49.

[131] Case C-509/09, *eDate Advertising and Others*, [2011] ECR I-10269.

[132] The judgment in *eDate Advertising* is applicable to 'an alleged infringement of personality rights by means of content placed online on an internet website' (para 52). It can be argued that data protection also fall within the category of personality rights. In order for the judgment to be applied to the field of data protection, the 'publisher' from the judgment would then be replaced by the 'controller/processor'. The question of analogous application of eDate judgment for other fields is raised for example also by S. Francq, "Responsabilité du fournisseur d'information sur Internet: affaires eDate Advertising et Martinez" (2012) *La Semaine Juridique Edition Générale* 1, 28.

[133] The theory points out that the criterion of the centre of interests as developed in the eDate judgment is particularly problematic; see for example B. Hess, "Der Schutz der Privatsphäre im Europäischen Zivilverfahrensrecht" (2012) 4 *JuristenZeitung*, 192.

[134] See, per analogy, case *eDate Advertising*, para 52.

[135] Per analogy, for such a jurisdictional issue the field of private enforcement of competition law, see M. Danov, *Jurisdiction and judgments in relation to EU competition law claims* (Oxford: Hart Publishing, 2011), 119 et seq.

[136] See Article 29 of Regulation 1215/2012.

[137] See Article 30 of Regulation 1215/2012.

[138] A reverse issue in a case currently pending before the CJEU and concerning private enforcement of competition law involves the question whether it is possible to regroup claims against different defendants domiciled in different Member States. See pending case C-352/13, *CDC* [2013] OJ C 298/2.

3.3 The proposed Data Protection Regulation

In 2012, the European Commission proposed a new Data Protection Regulation[139] that is intended to replace the current Data Protection Directive due to its overly fragmented EU data protection regime and due to the inappropriateness of the current regime from the perspective of the development of new technologies.[140] While some of the changes that the proposed Regulation brings about have been welcomed (such as strengthened definition of 'data subject'[141] and increase of rights of individuals[142], introduction of data protection-specific rights[143], one-stop shop[144], introduction of mechanisms to harmonise administrative practice[145] and abolishing the registration requirement[146]), its other characteristics have been criticised (e.g. maintaining the distinction between 'controller' and 'processor'[147], absence of a strong supervisory authority at the European level[148], introducing the right to be forgotten[149] and the costs for companies linked to hiring a Data Protection Officer[150]).

In addition to these issues, the Data Protection Regulation also aims to clarify the issue of remedies in the field of data protection.[151] The proposed Data Protection Regulation not only regulates judicial remedies against a supervisory authority (Article 74) and direct judicial remedies against a controller or processor (Article 75), but also includes specific rules on the right of compensation (Article 77) and common rules for court proceedings (Article 76). These remedies also open a question of jurisdiction and applicable law in case the data subject wants to effectively use them. Since the remedies can be directed both against a supervisory authority as well as directly against the controller or processor, it is necessary to distinguish between the administrative path of data protection enforcement and the civil path of this enforcement.

---

139 See Footnote 3. In terms of legislative process, the European Parliament adopted its opinion in the first reading on 12 March 2014 (*European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)). The Council is currently in the process of discussing the proposed amendments of the European Parliament.

140 See Explanatory Memorandum to the Proposal of General Data Protection Regulation, COM(2012) 11 final, p. 4.

141 P. De Hert, V. Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals" (2012) 28 *Computer Law & Security Review*, 133.

142 F. Gilbert, "EU Data Protection Overhaul: New Draft Regulation" (2012) 29 *Computer & Internet Lawyer*, 5.

143 P. De Hert, V. Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals" (2012) 28 *Computer Law & Security Review*, 136.

144 Article 51(2) if the Proposal of General Data Protection Regulation.

145 G. Thüsing, J. Traut, "The Reform of European Data Protection Law: Harmonisation at Last?" (2013) 5 *Intereconomics*, 272.

146 J. Castro-Edwards, "The Proposed European Data Protection Regulation" (2013) *Journal of Internet Law*, 4.

147 P. De Hert, V. Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals" (2012) 28 *Computer Law & Security Review*, 134.

148 G. Thüsing, J. Traut, "The Reform of European Data Protection Law: Harmonisation at Last?" (2013) 5 *Intereconomics*, 274.

149 J. Castro-Edwards, "The Proposed European Data Protection Regulation" (2013) *Journal of Internet Law*, 6.

150 J. Castro-Edwards, "The Proposed European Data Protection Regulation" (2013) *Journal of Internet Law*, 7.

151 F. Gilbert, "Proposed EU Data Protection Regulation: the Good, the Bad, and the Unknown" (2012) 15 *Journal of Internet Law*, 30, points out that the new regulation of remedies "would significantly increase companies' exposure to complaints, enforcement, and legal expenses".

3.3.1 Jurisdiction in administrative and civil litigation path

The distinction between the administrative litigation path and the civil litigation path in the proposed Data Protection Regulation can be inferred from the allocation of jurisdiction to a certain court for certain types of remedies pursuant to Regulation. According to Article 74(3) of this regulation, proceedings against a supervisory authority – and hence against an administrative decision – 'shall be brought before the courts of the Member State where the supervisory authority is established'. For an administrative litigation path, jurisdiction is therefore, logically, vested in the courts of the Member State of the administrative authority.[152] It is rather evident that the jurisdictional issues covered by Article 74 of the proposed regulation fall outside 'civil and commercial matters' as defined by Regulation 1215/2012. In fact, this article regulates jurisdiction for proceedings against a supervisory authority if this authority fails to act in order to protect the rights of the data subject.[153] The supervisory authority acting as a defendant is a public authority that is supposed to act in the exercise of its public powers. Therefore, this litigation will not covered by the scope of application of Regulation 1215/2012.

With regard to the civil litigation path, Article 75(2) of the proposed Data Protection Regulation contains a specific jurisdictional clause, vesting jurisdiction in the courts 'of the Member State where the controller or processor has an establishment' or, alternatively, in the courts 'of the Member State where the data subject has its habitual residence' except for the cases where 'the controller is a public authority acting in the exercise of its public powers'. Despite the fact that it seems that the latter phrase seems to follow the CJEU case-law on the scope of application *ratione materiae* of Regulation 1215/2012, it is submitted that Article 75 of the proposed Data Protection Regulation can be attributed a somewhat different scope of application than Regulation 1215/2012. In fact, it is not entirely clear whether Article 75 – preventing the data subject to bring proceedings before the courts of his habitual residence if the controller is public authority acting in the exercise of its public powers – is to be understood in the sense that jurisdiction is then determined by the first sentence of that provision (i.e. establishment of controller/processor) or in the sense that such a case is not covered by that provision at all and the jurisdiction is determined according to the national rules of private international law. Even though the practical outcome might be the same – leading to the jurisdiction of the courts of the Member State where the public authority is located – the first reading of the provision would go much further than Regulation 1215/2012, as it would cover matters that do not fall within the definition of 'civil and commercial matters' within the meaning of this regulation.

For that reason – and for the reason of systematically regulating all jurisdictional issues in one legal act – it would seem more appropriate not to include this jurisdictional clause in the future Data Protection Regulation, but rather in Regulation 1215/2012. That way it could also be ensured that this jurisdictional clause does not come in conflict with other heads of jurisdiction provided by the latter legal act.

Moreover, specifically with regard to Article 75(2) of the proposed Data Protection Regulation, it is to be noted that this provision properly takes into account particular vulnerability of a data subject by allowing him to file a claim in the Member State of his habitual residence and by de-coupling jurisdiction in data protection from a specific type of contract. Hence, a particular consumer jurisdiction in data protection matters does not seem necessary. This jurisdictional clause does, however, not address several important issues.

The first is the possibility of collective claims. The importance of jurisdictional issues for collective claims in data protection litigation should not be underestimated, in particular because certain Member

---

[152] For example, in Austrian legal order, a data subject can challenge a decision of the Austrian DPA before the Federal Administrative Court (see § 39(1) of *Datenschutzgesetz* 2000 and Article 130 of *Federal Constitutional Law* - B-VG).

[153] See Article 74(2) of the proposed Data Protection Regulation.

States already allow for such a possibility[154] and because the EU is striving to regulate that matter[155]. Collective claims can be relevant in particular in case of systematic and large-scale violations of the rights of data subjects (for example, in case of the unlawful transfer of data to third countries).[156] It is true that the proposed Data Protection Regulation allows a court in one Member State to suspend proceedings in case of parallel proceedings in another Member State (Article 76(3) and (4)), but this provision does not directly deal with jurisdiction in collective claims. Moreover, it is not entirely clear whether 'parallel proceedings' encompass only proceedings between the same parties or also related proceedings between the same controller/processor and different data subjects.

Second, Article 75(2) does not address the (im)possibility of prorogation of jurisdiction in data protection matters. Hence, for reasons explained above[157], the article should contain a clear paragraph stating that such a prorogation of jurisdiction is not possible.

Third, it is unclear whether the personal jurisdiction in this article (habitual residence of the data subject) should be coupled with a criterion of 'targeting' of controller's activities towards the Member State of the domicile of data subject, in a similar way as in the context of E-commerce[158] and torts against personality rights committed over the internet[159]. The targeting test seeks to determine whether a certain website favoured the country of the forum[160]. This would mean that such a test would not only be used to determine consumer jurisdiction ('directing' of activities pursuant to Article 17(1)(c) of Regulation 1215/2012), but in principle internet-related jurisdiction in general[161]. It is debatable whether the CJEU in *Google Spain and Google* considered the criterion of 'directing' of activities as relevant when determining the territorial application of the Data Protection Directive[162]. On the one hand, it is true that the CJEU considered that 'processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State…which *orientates* its activity towards the inhabitants of that Member State'.[163] On the other hand, however, this 'orientating' did not concern directing of activities of a controller/processor from one Member State to another, but directing of activities to the Member State of establishment of the subsidiary of the controller. Therefore, this criterion is different from that of 'targeting' or 'orientating' as used in other legislative instruments. Regarding the question whether the jurisdictional clause should contain the criterion of 'targeting', it is submitted that such a clause should indeed be added as a criterion for

---

154 See Footnote 56.

155 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Towards a European Horizontal Framework for Collective Redress* (COM(2013) 401 final).

156 However, the proposed Data Protection Regulation does regulate representative claims; see its Article 76(1).

157 See section 0. of this article.

158 Such a criterion is proposed, for example, by R. C. Casad, "Internet Jurisdiction", in *Essays in Honour of Konstantinos D. Kerameus* (Sakkoulas/Bruylant, 2009), 232. On targeting in internet jurisdiction, see also T. Schultz, "Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface", (2008) 19 *The European Journal of International Law*, 816 et seq.

159 M. Reymond, "Jurisdiction in Case of Personality Torts Committed over the Internet: A Proposal for a Targeting Test", 14 *Yearbook of Private International Law* (2012/2013), 205-246. Compare also M. A. Geist, "Is There a There There? Toward Greater Certainty for Internet Jurisdiction", (2001) *Berkeley Technology Law Journal*, 1381.

160 M. Reymond, "Jurisdiction in Case of Personality Torts Committed over the Internet: A Proposal for a Targeting Test", 14 *Yearbook of Private International Law* (2012/2013), 211.

161 Farah, for example, uses the notion of 'targeting' even in the context of consumer jurisdiction, by claiming that the notion 'directs such activities' from Article 15(1)(c) of Regulation 44/2001 (now Regulation 1215/2012) 'should be interpreted to include all cases where a website has entered into an online contract with a consumer, whether purposefully *targeting* the consumer's jurisdiction or in absence of such an intention'. Y. Farah, "Allocation of jurisdiction and the internet in EU law", (2008) 33 *E.L.Rev*, 266.

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

163 *Ibid*. Emphasis added.

establishing jurisdiction for data protection claims, not only because this criterion would prevent potential exorbitant jurisdiction[164], but also because – through the application of this criterion – the jurisdictional rules could potentially be more aligned with the rules on applicable law[165].

Fourth, Article 75(2) of the proposed Data Protection Regulation does not deal with the relationship to other provisions of Regulation 1215/2012, in particular to its clauses on exclusive jurisdiction. Suppose that the data subject's data was wrongly processed during the entry of this data into a public register and he wants to challenge this, relying on Article 24(3) of Regulation 1215/2012 which gives jurisdiction to the courts of the Member State in which the register is kept. In such a case, does a data subject still have the right to file an action for compensation for wrongful processing of his data in the Member State of his habitual residence pursuant to Article 75(2) of the proposed Data Protection Regulation? What if the data subject concludes a contract of sale to buy a house in Member State A and his data is processed wrongly[166] in this context by the real estate agent established in Member State B? Which jurisdictional clause should be applicable in such a case? One possibility is to argue that the claims relating to the wrongful processing of data should be separated from other claims relating to exclusive jurisdiction, meaning that the data subject retains the right to file a claim in the Member State of his habitual residence. However, it is also possible to argue that, in case of several claims stemming from the same contract whereby some of claims give rise to exclusive jurisdiction and some of them do not (such as processing of data), the data subject should have the right to file all claims before the court having exclusive jurisdiction.

3.3.2 Enforcement of judgments in the field of data protection

As regards the possibility of enforcement of judgments issued in the field of data protection, both Article 74(5) and Article 75(4) of the proposed Data Protection Regulation seem to be *lex specialis* with regard to enforcement provisions of Regulation 1215/2012. In fact, these two provisions require enforcement of a judicial decision without following the general rules on enforceability laid down in Regulation 1215/2012. Despite the fact that the previously valid system of declaration of enforceability[167] is abolished in the new Regulation 1215/2012[168], the latter still provides for certain procedural guarantees with regard to enforcement, such as a certificate of enforcement[169] and certain grounds for refusal of enforcement[170]. From the provisions of the proposed Data Protection Regulation, it is not clear whether those general safeguards would apply also in the field of data protection, in particular since there is no reference to those general rules in the proposed Data Protection Regulation. It is submitted that, if Regulation 1215/2012 was to be applied by analogy, this would need to be specifically laid down in the proposed Data Protection Regulation. Moreover, even if it could be assumed that the general provisions on enforcement would be used also for the enforcement of judgments rendered in the area of data protection, this could not be the case if, *ab initio*, the litigation is not covered by the notion of 'civil and commercial matters'. Therefore, such

---

[164] Exorbitant jurisdiction can be defined as "jurisdiction validly exercised under the jurisdictional rules of a State that nevertheless appears unreasonable to non-nationals because of the grounds used to justify jurisdiction"; see K.A. Russell, "Exorbitant Jurisdiction and enforcement of judgements: the Brussels system as an impetus for the United States action", (1993) *Syracuse Journal of International Law and Commerce*, 2.

[165] This criterion seems to be favoured also by Article 29 Data Protection Working Party, *Opinion 8/2010 on applicable law* (16.12.2010, 0836-02/10/EN, WP 179), p. 24, 31.

[166] For example, his e-mail is added to a mailing list and made available to other real estate agents without his consent.

[167] See Article 38 *et seq*. of the Regulation No 44/2001.

[168] See Article 39 of the Regulation No 1215/2012, according to which, in order for a judgment to be enforceable in a Member State, a declaration of enforceability is not required, but merely the enforceability of the judgment in a Member State where the judgment was rendered.

[169] See Article 53 of the Regulation No 1215/2012.

[170] See Article 46 *juncto* Article 45 of the Regulation No 1215/2012.

broadening of the scope of application of enforcement mechanisms also raises the issue of the competence of the Union to regulate enforcement outside of civil and commercial matters. The legal base of the proposed Data Protection Regulation, namely Article 16 TFEU, does not seem to justify such a general jurisdictional clause.[171]

3.4 A necessary revision of Regulation 1215/2012

It stems from the above that the most appropriate way to deal with the jurisdictional issues in the field of data protection would be to include a special provision for this field in Regulation 1215/2012. A relevant article of Regulation 1215/2012 could be drafted in the following manner:

Section 5a: Jurisdiction in matters relating to data protection

Article 23a

1. In matters relating to data protection, jurisdiction shall be determined by this Section if the data is processed either on the basis of a contract concluded between a data subject and a controller or processor or, in the absence of such a contract, directly on the basis of applicable data protection legislation.
2. A data subject and an authority or an association representing that data subject may bring proceedings against a controller or processor processing data relating to this data subject either in the courts of the Member State in which the controller or processor is domiciled or, regardless of the domicile of controller or processor, in the courts for the place where the data subject is domiciled, provided that the controller or processor directs its activities to the Member State of domicile of data subject or to several States including that Member State.
3. Proceedings may be brought against a data subject by a controller or processor only in the courts of the Member State in which the data subject is domiciled.
4. Prorogation of jurisdiction between a data subject on the one hand and controller or processor on the other hand is possible only under the conditions set out in Article 23b.

Article 23b

The provisions of this Section may be departed from only by an agreement:

1. which is entered into after the dispute has arisen;
2. which allows the data subject to bring proceedings in courts other than those indicated in this Section; or
3. which is entered into by the data subject and the other party to the contract, both of whom are at the time of conclusion of the contract domiciled or habitually resident in the same Member State, and which confers jurisdiction on the courts of that Member State, provided that such an agreement is not contrary to the law of that Member State.

Moreover, once the European legal order allows for collective claims of data subjects, Regulation 1215/2012 will also need to provide for rules regarding a jurisdictional basis for such collective

[171] It is to be noted that the proposed Data Protection Regulation makes reference also to Article 114(1) TFEU as a legal base. However, as specified in the Explanatory memorandum to this Regulation (COM(2012) 11 final, p. 6), the reference to this article is only necessary for amending the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), [2002] OJ L 201/37.

claims.[172] The European legislator will therefore hopefully re-think the strategy and include a special jurisdictional clause in this regulation rather than in the proposed Data Protection Regulation. Regulating jurisdiction is however not the only issue that needs to be addressed and thought through with regard to data protection. Another issue is the one of applicable law which is discussed below.

4. Applicable law[173]

4.1 The myth of parallelism between jurisdiction and applicable law

In principle, the substantive scope and the concepts contained in regulations determining applicable law[174] (Rome I[175] and Rome II[176]) should be interpreted consistently with those in Regulation 1215/2012.[177] The reason for this parallelism in interpretation stems from a common objective of both sets of legal rules which is to prevent *forum shopping*.[178] A closer reading of both sets of provisions shows that, with regard to certain concepts, parallel interpretation of certain concepts is even expressly required.[179] Such parallel interpretation could often lead the competent court to apply its own rules which would significantly facilitate its decision making.[180]

Although it is, in principle, desirable that the court deciding the claim also applies its own law, notably due to procedural economy[181], this is not always the case in practice. If one compares, for example, the rules on jurisdiction and applicable law in the field of contracts, they can amount to a different result with regard to applicable law and jurisdiction.[182] While jurisdictional rules use as a

---

[172] See more precisely on jurisdictional issues regarding collective claims E. Lein, "Jurisdiction and applicable law in cross-border mass litigation", in F. Pocar, I. Viarengo, F.C. Villata (eds), *Recasting Brussels I* (Padua: Cedam, 2012), 159-172.

[173] This part is an extended version of the paper M. Brkan, "The Relevance of European Data Protection Standards for US Businesses and Authorities", presented at the 6th International Conference on Society and Information Technologies: ICSIT 2015, 10-13 March 2015 in Orlando, Florida, USA and published in conference proceedings.

[174] This article does not take into account Rome III and Rome IV Regulations as they seem somewhat less relevant for the field of data protection. See Council Regulation (EU) No 1259/2010 of 20 December 2010 implementing enhanced cooperation in the area of the law applicable to divorce and legal separation [2010] OJ L 343/10; Regulation (EU) No 650/2012 of the European Parliament and of the Council of 4 July 2012 on jurisdiction, applicable law, recognition and enforcement of decisions and acceptance and enforcement of authentic instruments in matters of succession and on the creation of a European Certificate of Succession [2012] OJ L 201/107.

[175] 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) [2008] OJ L 177/6.

[176] 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) [2007] OJ L 199/40.

[177] See, in this sense, Recital 7 of Rome I Regulation.

[178] J. von Hein, in T. Rauscher (ed.), Europäisches Zivilprozess- und Kollisionsrecht EuZPR/EuIPR. Kommentar. Brüssel I-VO. LugÜbk 2007 (Munich: sellier, 2011), 31.

[179] Such as, for example, with regard to concepts of 'provision of services' and 'sale of goods'. See Recital 17 of Rome I Regulation. Another example of parallelism between the rules on jurisdiction and applicable law are the rules in the field of consumer law. As expressly stated in Recital 24 of the Rome I Regulation, the concept of 'directed activity' should be interpreted harmoniously in this regulation and in Regulation 1215/2012. In practice this means that the court deciding upon a claim initiated by a consumer, in principle, apply the law of the consumer's domicile.

[180] For a more sceptical view on the question of the applicable law being the law of the forum, see D. J. B. Svantesson, *Private International law and the Internet* (Hague: Kluwer, 2012), 331.

[181] H. Unberath and J. Cziupka, in T. Rauscher (ed.), Europäisches Zivilprozess- und Kollisionsrecht EuZPR/EuIPR. Kommentar. Brüssel I-VO. LugÜbk 2007 (Munich: sellier, 2011), 686.

[182] J. von Hein, in T. Rauscher (ed.), Europäisches Zivilprozess- und Kollisionsrecht EuZPR/EuIPR. Kommentar. Brüssel I-VO. LugÜbk 2007 (Munich: sellier, 2011), 32.

connecting factor 'the place of performance of the obligation in question'[183], the rules on applicable law point to the applicability of the law of 'habitual residence' of the seller or the service provider[184] which is not necessarily the same as the place of performance of contractual obligation.

Similarly, in the field of torts, it is possible to come to the conclusion that such a parallelism is, at best, only partial[185]. The general rule for determining applicable law for torts is the place where the *damage* occurred[186], whereas the main connecting element for determining jurisdiction in delictual matters is the place where the *harmful event* occurred or may occur[187]. 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*[188] and subsequent case-law[189], the CJEU confirmed that the notion of 'harmful event' from Article 5(3) of Regulation 44/2001 (now Article 7(2) of Regulation 1215/2012) covers 'both the place where the damage occurred and the place of the event giving rise to it'. In consequence, with regard to torts, the rules on jurisdiction and applicable law can potentially amount to the same result, although this is not necessarily the case.

Moreover, it is important to stress another difference between rules on jurisdiction and applicable law. The general regulations governing applicable law (Rome I and Rome II 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[190]. 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 1215/2012 applies, pursuant to its Article 4(1), only to 'persons domiciled in a Member State', regardless of their nationality, and hence does not have universal application.

4.2 No room for Rome I and II Regulations in data protection matters?

The current doctrine dealing with issues of applicable law in the framework of data protection within the EU bases its analysis mostly – or even solely – on Article 4 of Data Protection Directive[191], without first addressing the issue of the relationship between the Rome I and II Regulations on the one hand and the Data Protection Directive on the other hand. However, in particular with regard to the issue of agreements on applicable data protection law as well as in the field of consumer protection, where rules on applicable law are different than with regard to general contract or tort law, it is of utmost importance to address the issue whether the provisions of Rome I and II Regulations bear any significance for the field of data protection.

In practice, there seems to be still some confusion as to what is the legal base for determining applicable law in the field of data protection. Whereas the CJEU in the case *Google Spain and*

---

183 Article 7(1) of Regulation 1215/2012.

184 Article 4(1)(a) and (b) of Rome I Regulation.

185 H. Unberath and J. Cziupka, in T. Rauscher (ed.), Europäisches Zivilprozess- und Kollisionsrecht EuZPR/EuIPR. Kommentar. Brüssel I-VO. LugÜbk 2007 (Munich: sellier, 2011), 686.

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

187 See Article 7(2) of Regulation 1215/2012.

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

189 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.

190 See Article 2 of Rome I Regulation and Article 3 of Rome II Regulation.

191 See, for example, C. Kuner, *European Data Protection Law*, 2nd ed. (OUP, 2012), 111-112. Rome I and II Regulations are also not mentioned in Article 29 Data Protection Working Party, *Opinion 8/2010 on applicable law* (16.12.2010, 0836-02/10/EN, WP 179).

Google[192] did not refer to either Rome I or II Regulations or the issue of the relationship between these regulations and Article 4 of the Data Protection Directive – a reasoning which would seem to imply that the former has to give way to the latter –, a German court in the case *Facebook v Independent Data Protection Authority of Schleswig-Holstein*[193], on the contrary, qualified data protection provisions as overriding mandatory provisions within the meaning of Article 9 of Rome I Regulation,[194] and thus did not entirely exclude the applicability of the latter in the field of data protection. While the reasoning of the CJEU can be understood from the perspective of systematic interpretation of data protection legislation and from the perspective of the questions posed by the national court to the CJEU, the reasoning of the German court can be fitted more into the fundamental rights perspective. It can be argued that, given the fact that data protection constitutes a fundamental right which is concretised through the Data Protection Directive, it is not possible to deviate from this fundamental right or the rules adopted for its implementation.[195]

The analysis of the rules of both Rome regulations, as well as the relevant provisions of the Data Protection Directive, allow for two potential conclusions with regard to the relationship between the two sets of legal documents.

The first possibility is to argue that Article 4 of the Data Protection Directive lies entirely outside the scope of application of both Rome I and II Regulations, thus leaving no possibility of overlap between their respective scopes of application or integration of the former provision into the system of the two regulations. In this regard, it is to be noted that both the Rome I and II Regulations expressly stipulate that they do not apply to 'administrative matters'.[196] The core of the analysis of applicability of both regulations to the field of data protection will therefore be the question whether data protection can fall under the notion of 'civil matters' within the meaning of the two regulations. Data protection is rather difficult to conceptualise, since it falls into 'the grey area between public and private'[197], but already from this argument it can be difficult to qualify it as civil law. It is therefore most likely that it will be excluded from the scope of application of the two regulations already on this basis.

In addition, Rome II Regulation expressly excludes from its scope 'non-contractual obligations arising out of violations of privacy'[198]. In this regard, it is not entirely clear whether, for the purposes of Rome II Regulation, violations of privacy include also violations of data protection, notably due to the fact that neither the textual nor historical[199] interpretation of this provision seem to include data protection issues in its scope. It can, however, be reasonably assumed that this is the case[200]. Such an interpretation would be based on reasoning that data protection forms an integral part of privacy and that rules regarding data protection are covered by the rules on protection of privacy. This approach

---

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

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

194 See p. 4 and 5 of the judgment.

195 Compare also J.-J. Kuipers, EU law and private international law: the interrelationship in contractual obligations (Leiden: Nijhoff, 2012), 75.

196 See Article 1 of both Rome I and II Regulations.

197 J.-J. Kuipers, "Bridging the Gap. The Impact of the EU on the Law Applicable to Contractual Obligations", (2012) 76 *RabelsZ*, 573. See also See L. Bygrave, "Determining applicable law pursuant to European Data Protection Legislation" (2000) 16 *Computer Law and Security Report*, 252; C. Kuner, "Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 1)", (2010) 18 *International Journal of Law and Information Technology*, 178.

198 See Article 1(g) of Rome II Regulation.

199 During the legislative process, the European parliament modified the wording of this provision to include violations 'resulting from the handling of personal data', but this modification was not retained in the final version of the Regulation. See, in this regard, A. Dickinson, *The Rome II Regulation: The Law Applicable to Non-Contractual Obligations* (OUP, 2008), 240.

200 See, in this sense, A. Dickinson, The Rome II Regulation: The Law Applicable to Non-Contractual Obligations (Oxford: Oxford, 2008), 240.

would also be consistent with the approach taken in the Data Protection Directive which itself uses the term the 'right to privacy with respect to the processing of personal data'[201]. Moreover, the CJEU, which repeatedly used this term in its case-law,[202] very often considers both rights together[203]. Even in the recent *Google Spain* judgment, the CJEU referred both to the right to privacy and the right to protection of personal data[204], which is an indication that the two rights are inextricably intertwined. This would seem to suggest that not only the issues of privacy, but also the issues relating to data protection are excluded from the scope of application of the Rome II Regulation.[205]

However, the question remains whether such reasoning would not render the provisions (and the fundamental right) on data protection redundant. As argued in the doctrine – and confirmed by the circumstance that these two are distinct fundamental rights in the Charter – privacy has to be distinguished from data protection at least to a certain extent.[206] While these two rights certainly partially overlap, privacy seems to be a broader concept that encompasses also other issues than just personal data; on the other hand, not all personal data necessarily fall into the sphere of privacy.[207]

The second possibility is to see the two sets of legal sources (Rome I/Rome II Regulations and Data Protection Directive) as being in a *lex generalis – lex specialis* relationship. Both Rome I and Rome II Regulations allow for the inclusion of conflict-of-law rules with regard to 'particular matters' into other EU law instruments. As it stems from Article 23 of Rome I Regulation and Article 27 of Rome II Regulation[208], such conflict-of-law rules relating to particular matters shall not be prejudiced

---

201 See Article 1(1) of the Data Protection Directive.

202 For a recent case in this regard, see, for example Joined Cases C-141/12 and C-372/12, *YS and Others*, [2014] not yet published in ECR.

203 See for example Case C-293/12, *Digital Rights Ireland and Seitlinger and Others*, [2014] not yet published in ECR, where the CJEU, in paras. 32 et seq., addressed the interference with both Articles 7 and 8 of the Charter. See also Case C-92/09, *Volker und Markus Schecke and Eifert*, para. 47, where the CJEU affirms that the right to the protection of personal data from Article 8 of the Charter 'is closely connected with the right to respect of private life expressed in Article 7 of the Charter'.

204 See Case C-131/12, *Google Spain and Google*, [2014] not yet published in ECR, para. 38, 80.

205 Another argument in favour the position that Article 1(g) of Rome II Regulation includes also violations of data protection laws can be inferred from a systematic interpretation of this regulation. According to its Article 30(2), the Commission had to prepare a study covering not only the issues of "the law applicable to non-contractual obligations arising out of violations of privacy and rights relating to personality", but also conflict-of-law issues regarding the Data Protection Directive. It seems to result from this study, completed in 2009, that this article covers also data protection issues. See 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, p. 61 et seq. See *http://ec.europa.eu/justice/civil/files/study_privacy_annexe_3_en.pdf* [Accessed 27 February 2015].

206 See in this sense M. Tzanou, "Is Data Protection the Same as Privacy? An Analysis of Telecommunications' Metadata Retention Measures", (2013) 17 *Journal of Internet Law*, 26 et seq.; O. Lynskey, "Deconstructing Data Protection: The 'Added Value' of a Right to Data Protection in the EU Legal Order", (2014) 63 International and Comparative Law Quarterly, 569-597 who stresses, at p. 597, that it "is time to recognize the merits of a truly independent right to data protection". See also J. Kokott and C. Sobotta, "The distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR", in H. Hijmans and H. Kranenborg (ed.), *Data Protection Anno 2014: How to Restore Trust?* (Cambridge: Intersentia, 2014) 83-95; P. Hustinx, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", available at *https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Publications/SpeechArticle/SA2014* [Accessed 18 February 2015].

207 M. Tzanou, "Is Data Protection the Same as Privacy? An Analysis of Telecommunications' Metadata Retention Measures", 17 *Journal of Internet Law* (2013), 26.

208 See also Recital 40 of Rome I Regulation and Recital 35 of Rome II Regulation. It is however interesting to note that, whereas these recitals make a specific reference to the Directive on electronic commerce (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L 178/1), they do not mention Article 4 of the Data Protection Directive.

by either of these regulations, thereby expressly allowing for *lex specialis* conflict-of-law provisions. It can be argued that Article 4 of the Data Protection Directive is such a special provision.

The argument of *lex specialis* seems to imply, however, that Article 4 of the Data Protection Directive cannot be placed entirely outside of the system of Rome I and II Regulations. Whereas Article 4 could potentially be a *lex specialis* with regard to the general or specific rules on applicable law in these regulations[209], it is not entirely clear whether this is also the case with regard to the provisions on freedom of choice[210] or regarding the overriding mandatory provisions[211]. Does Article 4 of the Data Protection Directive preclude the possibility of parties agreeing on applicable law in the field of data protection? Can the provisions on consumer protection be seen as the overriding mandatory provisions that can prevail in the case of data protection? Or can data protection provisions themselves be seen as such as overriding mandatory provisions? These are the issues discussed below.

4.3 The controversy around agreements on applicable data protection law

The current doctrine and practice[212] is divided regarding the question whether the parties to a contract can freely choose data protection law that is applicable in a framework of this contract.[213] While certain authors advocate the thesis that the parties to a contract have the freedom to make such a choice[214], others are of the opinion that Member States' data protection laws should be qualified as overriding mandatory provisions that do not allow for an agreement on applicable law between the parties[215].

The German case *Facebook v Independent Data Protection Authority of Schleswig-Holstein*[216] is an example in this regard. Despite the fact that the case has been decided by an administrative court in a dispute between a DPA and Facebook and that the content of the claim was to set aside a(n) (administrative) decision of a DPA, the German court still considered that the Rome I Regulation could be relevant. The reason for that seems to be that the relationship between Facebook and its users – the two contractual parties that agreed on the application of German data protection law for the purposes of this contract –, is in nature a civil-law relationship to which the Rome I Regulation applies.[217] According to the German court, data protection law falls within the concept of overriding

---

209 Articles 3-8 of the Rome I Regulation and Articles 4-9 of the Rome II Regulation.

210 Article 3 of the Rome I Regulation and Article 14 of the Rome II Regulation.

211 Article 9 of the Rome I Regulation and Article 16 of the Rome II Regulation.

212 See, for example, the judgment of LG Berlin, 6 March 2012, Az. 16 O 551/10 (allowing for such an agreement on applicable data protection law); as well as the judgment in the Case 8 B 60/12, *Facebook Ireland Ltd. v Independent Data Protection Authority of Schleswig-Holstein, Germany* (not allowing for such an agreement).

213 A similar issue can arise also in the framework of the Rome II Regulation regarding the question whether Article 16 of this regulation regarding overriding mandatory provisions can be applicable in the field of data protection.

214 See, for example, N. Härting, "Rechtswahlklauseln in Datenschutzbestimmungen – Was ist zu beachten?", available on *http://www.cr-online.de/blog/2013/07/25/rechtswahlklauseln-in-datenschutzbestimmungen-was-ist-zu-beachten/* [Accessed 27 February 2015]. Compare also S. Polenz, "Die Datenverarbeitung durch und via Facebook auf dem Prüfstand", (2012) *Verbraucher und Recht*, 208-209, commenting upon the judgment of LG Berlin, 6 March 2012, Az. 16 O 551/10.

215 See, for example, C. Piltz, "Rechtswahlfreiheit im Datenshutzrecht?", (2012) *R&R*, 640-645.

216 Case 8 B 60/12, Facebook Ireland Ltd. v Independent Data Protection Authority of Schleswig-Holstein, Germany. For a comment of the decision, see for example C. Piltz, "Facebook Ireland Ltd. v Independent Data Protection Authority of Schleswig-Holstein, Germany – Facebook is not subject to German data protection law", (2013) 3 International Data Privacy Law, 210-212.

217 Case 8 B 60/12, Facebook Ireland Ltd. v Independent Data Protection Authority of Schleswig-Holstein, Germany, p. 4.

mandatory provision within the meaning of Article 9 of the Rome I Regulation, making it impossible for the parties to make an agreement on applicable law in this regard.[218]

According to 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'[219]. Overriding mandatory provisions[220] are those that are applicable regardless of the law that would be applicable on the basis of Rome I Regulation and regardless of the law that the parties have chosen.[221] As it stems from the case-law of the CJEU, starting with *Ingmar*[222], not only provisions of Member States' law, but also provisions of EU law itself can be qualified as overriding mandatory provisions. In *Ingmar*[223], confirmed notably by *Honyvem Informazioni Commerciali*[224], *Semen*[225] and *Unamar*[226], the CJEU held that the provision of the Directive on self-employed commercial agents[227] on the protection of the commercial agent after termination of the contract is mandatory in nature. Although not all EU law provisions have a character of overriding mandatory provisions, it can be claimed that, if those CJEU rulings are applied per analogy to the Data Protection Directive, its Article 4 could have a mandatory character. In the EU, the question of mandatory nature of data protection provisions can arise in two different settings: as mandatory nature of provisions stemming from EU law and of those stemming from Member States' law.

On the one hand, contractual parties might agree on the applicability of third-country law (for example US law), which amounts to a case containing a similar factual constellation to the one in *Ingmar*[228]. In such a case, a question of mandatory nature of Article 4 of the Data Protection Directive itself will arise. In order for a provision to be qualified as an overriding mandatory provision, the norm has to have the purpose of pursuing public interest.[229] It has been argued in the doctrine that the public interest of the provisions of Data Protection Directive is demonstrated by the fact that the directive pursues internal market objectives by ensuring free movement of personal data.[230] Whereas the adoption of legislation on the basis of the provision relating to the internal market undeniably demonstrates public interest of this legislation, it is not clear whether this suffices for a legal

---

[218] *Ibid*., p. 4-5.

[219] It is to be noted that different Member States interpret the scope of this notion differently, notably as to the question whether it covers only the overriding interests of the state or also of a weaker contractual party. See in this regard J.-J. Kuipers, "Bridging the Gap. The Impact of the EU on the Law Applicable to Contractual Obligations", (2012) 76 *RabelsZ*, 569.

[220] This notion should be distinguished from the notion of 'provisions which cannot be derogated from by agreement', used in other provisions of this regulation. In fact, apart from the notion of 'overriding mandatory provisions', Rome I Regulation contains also the notion 'rules that cannot be derogated from by agreement' in Articles 3(3), 3(4), 6(2) and 8. As expressly stipulated in the Recital 37 of the Rome I Regulation, the former concept should be construed more restrictively than the latter. On the parallelism and distinction between the two concepts, see A. J. Bělohlávek, *Rome Convention. Rome I Regulation. Commentary*, Vol. 2 (Huntington, N.Y. : Juris, 2010), 1478-1480.

[221] A. J. Bělohlávek, *Rome Convention. Rome I Regulation. Commentary*, Vol. 2 (Huntington, N.Y. : Juris, 2010), 1478.

[222] Case C-381/98 *Ingmar GB,* [2000] ECR I-9305.

[223] Case C-381/98 *Ingmar GB,* [2000] ECR I-9305, para 21.

[224] Case C-465/04 *Honyvem Informazioni Commerciali,* [2006] ECR I-2879, para 22.

[225] Case C-348/07 *Semen,* [2009] ECR I-2341, para 17.

[226] Case C-184/12 *Unamar,* [2013] ECR, para 40.

[227] Council Directive 86/653/EEC of 18 December 1986 on the coordination of the laws of the Member States relating to self-employed commercial agents [1986] OJ L 382/17.

[228] Case C-381/98 *Ingmar GB,* [2000] ECR I-9305, para 10.

[229] A. J. Bělohlávek, Rome Convention. Rome I Regulation. Commentary, Vol. 2 (Huntington, N.Y. : Juris, 2010), 1474; Thorn, in Rauscher (ed.), Europäisches Zivilprozess- und Kollisionsrecht EuZPR/EuIPR. Kommentar. Rom I-VO. Rom II-VO (Munich: sellier, 2011), 425 et seq.

[230] C. Piltz, "Rechtswahlfreiheit im Datenshutzrecht?", (2012) *R&R*, 643.

instrument to contain mandatory provisions. Such reasoning would imply that all EU (civil and commercial) legislation based on Article 114 TFEU has, by that very fact, the nature of an overriding mandatory provision within the meaning of Article 9 of the Rome I Regulation. Given the fact that the Treaties do not provide for a specific legal base for adopting legislation in civil matters and that such legislation will always be based on Article 114 TFEU, it might be a bit far-reaching to treat all the legislation adopted on the basis of this article as mandatory within the meaning of Article 9(1) of the Rome I Regulation.

Another argument in favour of designating data protection provisions as mandatory provisions could be the circumstance that it stems from Recital 18 of the Data Protection Directive that the processing of personal data in the Union '*must* be carried out in accordance with the law of one of the Member States' and that the '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'[231]. However, these provisions can also be understood as an expression of binding nature of the directive rather than their quality as overriding mandatory provisions.

On the other hand, a question of mandatory nature of the law of one of the Member States that is transposing Article 4 of the Data Protection Directive into the national legal order can be relevant. This would mean that it would need to be checked in the national law of each Member State whether data protection constitutes such overriding mandatory provisions within the meaning of Article 9(1) of Rome I Regulation. Such a solution means, however, the possibility of divergent results in different Member States.[232] One can imagine that data protection laws have a different importance in some Member States than in others.

4.4 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 transposing the Data Protection Directive applies if the controller is established in this Member State and data is processed in the context of its activities (subparagraph (a))[233]. If the controller does not have an establishment within the EU, the law of a particular Member State transposing the Data Protection Directive can apply either on the basis of public international law (subparagraph (b)) or if the controller makes use of equipment situated on the territory of this particular Member State (subparagraph (c)). These latter rules can therefore lead to the application of national measures transposing the directive even in case of absence of establishment of the controller in the EU. Quite differently, in such a situation when the controller is not established in the EU, the jurisdictional rules of Regulation 1215/2012 would not apply.[234] This means that the jurisdiction would be determined on the basis of jurisdictional rules of Member States.

Moreover, it stems from the above that – differently from the classic rules on applicable law enshrined in Rome I and II Regulations – Article 4 of Data Protection Directive does not have universal application[235]. In other words, the law that can be applicable according to the Data Protection

---

[231] Emphasis added. This argument is pointed out by C. Piltz, "Rechtswahlfreiheit im Datenschutzrecht?", available on *http://www.delegedata.de/2013/07/rechtswahlfreiheit-im-datenschutzrecht/* [Accessed 27 February 2015].

[232] J.-J. Kuipers, "Bridging the Gap. The Impact of the EU on the Law Applicable to Contractual Obligations", (2012) 76 *RabelsZ*, 570, points out that such divergent interpretations are compatible with the Rome I Regulation.

[233] According to this same article, if the controller is established in several Member States, each of the establishments of this controller has to comply with the obligations laid down by the national law applicable.

[234] See Article 4(1), pursuant to which this regulation applies only to 'persons domiciled in a Member State'.

[235] See above point 0. of this article.

Directive can only be the law of one of the Member States and not the law of a third country. Thus, Article 4 of 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.

A landmark case in the field of applicable law with regard to data protection is the *Google Spain and Google* case[236], in which the CJEU interpreted, for the first time, Article 4(1)(a) of Data Protection Directive. As already mentioned, this provision requires the application of national law of a certain Member State transposing the 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'[237]. Whereas this decision, following the opinion of the Advocate General Jääskinen[238], 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.[239] 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[240]. It seems that such search engines, that equally process personal data, would equally 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

---

[236] Case C-131/12, *Google Spain and Google*, [2014] not yet published in ECR. The majority of academic literature comments upon this case from the perspective of the right to be forgotten and puts the issues of applicable law less in the forefront; see for example E. Frantziou, "Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos" (2014) 14 *Human Rights Law Review*, 761–777; H. Crowther, "Google v Spain: is there now a 'right to be forgotten'?", (2014) 11 Jo*urnal of Intellectual Property Law & Practice*, 892-893; Jones, Joseph, "Control-alter-delete: the 'right to be forgotten'", (2014) *European Intellectual Property Review*, 595-601; M. Griguer, "Conditions et modalités d'exercice du droit à l'oubli numérique - ou les apports de l'arrêt CJUE, 13 mai 2014, C-131/12", (2014) 24 *La Semaine Juridique Entreprise et Affaires*, 1326; G. Busseuil, "Arrêt Google: du droit à l'oubli de la neutralité du moteur de recherché", (2014) 24 *La Semaine Juridique - entreprise et affaires*, 51-54.

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

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

[239] In more general terms, J. W. Kropf, "Google Spain SL v. Agencia Española de Protección de Datos (AEPD)", (2014) 108 *The American Journal of International Law*, 507, wonders whether 'other search engines with fewer ties to the European Union be able to determine with any certainty that they are subject to application of the Directive'.

[240] As an example of non-profit search engine is Benelab [*http://bene.co/*, accessed 2 February 2015] that donates revenues generated from the internet searches.

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'[241]. In the case of the absence of this link, would the conditions from Article 4(1)(a) still be fulfilled? It seems that this would not be the case and that such a situation could potentially be covered by subparagraph (c) of the same article, requiring that the controller 'makes use of equipment' on the territory of a particular Member State.

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 provision. 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 is built upon. In fact, such an interpretation only covers certain business models – more precisely, it encompasses 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*[242] and the subsequent case-law, *Mühlleitner*[243] and *Emrek*[244]. 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. It is true that the Working Party 29 considered the 'targeting' of individuals in the EU as a potential additional criterion when the controller does not have an establishment in the EU in order to provide for a sufficient link with EU territory.[245] However, adding this criterion through an interpretation of Article 4(1)(a) of Data Protection Directive without a legislative revision of this provision seems problematic.[246] 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 most sense if there is a cross-border element to such 'orientating'.[247] A cross-border element is also present in the notion of 'directing of activities' as used by Article 17 of Regulation 1215/2012. In any event, it would seem reasonable that this criterion is used as a subsidiary criterion

---

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

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

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

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

245 See Article 29 Data Protection Working Party, *Opinion 8/2010 on applicable law* (16.12.2010, 0836-02/10/EN, WP 179), p. 31.

246 L. 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), for example, proposes a legislative revision of Article 4(1)(a) and (c) of Data Protection Directive that could provide that the national laws apply 'to the processing of personal data in the context of the activities of the controller on or directed at the territory of the Member State'.

247 In the sense that an internet service provider, established in one Member State, orientates its activity towards the inhabitants of *another* Member States. It is true, however, that a cross-border element can also be established if a controller established in a third country orientates (through its subsidiary) its activity towards the EU.

and not as a primary one in the framework of the interpretation of Article 4(1)(a) of the Data Protection Directive.

It is true, however, that the decision of the CJEU can also be understood in the light of the preliminary questions asked by the national court. In fact, the answer given by the CJEU to the question regarding applicable law is a mirror image of one of the three possible interpretations put forward by the national court.[248] It could therefore be claimed that the CJEU only affirmatively replied to a premise 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 a situation given by the national court.

Another question that needs to be asked is whether the interpretation given by 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. In the already mentioned German case *Facebook v Independent Data Protection Authority of Schleswig-Holstein*[249], the German administrative court of Schleswig-Holstein held that 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[250]. 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[251].

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 should be sufficient for German law to be applicable. Such reasoning, however, seems to entirely disregard different functions of the two European subsidiaries of Facebook (German and Irish). However, an inverse reasoning (such as the one by the German court) leads to 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 its EU users. For such a company, it would be enough to 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.[252]

4.5 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. Therefore, after the entry into force of the regulation, the issues regarding applicable law will hardly be relevant. However, in two instances such issues might nevertheless arise despite the entry into force of the regulation. On the one hand, questions of applicable law might be relevant if the Member States, despite the regulation, maintain in

---

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

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

[250] *Ibid.*, p. 6.

[251] *Ibid.*, p. 7 and 9.

[252] Such 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'.

force divergent provisions on issues not addressed in detail by the regulation.[253] On the other hand, such questions might be relevant regarding the (im)possibility to enter into an agreement on applicable law for data protection. After the entry into force of the regulation, such agreements will most probably not be allowed, 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. Similarly as the current Data Protection Directive, the proposed regulation distinguishes between situations where the controller is established in the EU and where it is not. If the controller has an establishment in the EU, the regulation applies, according to its Article 3(1), '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'. Therefore, the reasoning of the CJEU in the case *Google Spain* will be pertinent also after the entry into force of the regulation.

The second and the third paragraph 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[254]. 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 data protection legislation when they offer goods or services online to European data subjects[255]. 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 physically in the territory of a third state and not online. Such 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.[256]

Furthermore, 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[257]. The explanatory memorandum to the regulation does not specify how broad this provision should be interpreted. On a more narrow interpretation, this provision would cover monitoring of behaviour by companies established in third countries (such as Google or Facebook), in order, for example, to use the gathered information for commercial purposes, such as targeted advertising. On a rather broad interpretation, it could also be argued that even the NSA, when

---

253 For example, Article 77 of the proposed Data Protection Regulation gives the data subject the right to claim damages in case of an unlawful processing of data. However, different Member States can have more or less favourable rules on causal link or quantification of damage. Since the regulation does not specify which law is applicable in case of absence of specific unified rules, such cases might lead to *forum shopping* in favour of regimes of certain Member States.

254 See Article 3(2)(a) of the proposed Data Protection Regulation.

255 On extra-territorial application of Data Protection Directive, see 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 (2002), 5035/01/EN/Final, WP 56, p. 4. See also C. Kuner, "Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 1)", (2010) 18 International Journal of Law and Information Technology, 178.

256 Compare also L. 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?" (2011) 1 *International Data Privacy Law*, 44; who points out that 'an unbridled expansion of applicability of EU data protection laws to processing of data on EU citizens wherever in the world should be prevented'.

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

processing data of Union citizens or obtained from Union authorities, has to respect Union law. Although this is, admittedly, an extremely broad interpretation of this article, nothing in the text of the article or the explanatory memorandum seems to limit such an application *ratione personae* of this article. One could stretch this interpretation even further and ask a question whether this would 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 border. Such an interpretation, however, seems to be rather far-reaching, in particular because it would lead to a rather broad extraterritorial application of the EU data protection legislation.

Finally, 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".

5. Conclusion

In addition to public enforcement of data protection law by the national DPAs, private enforcement directly by data subjects before the civil courts will undoubtedly increase in the future, notably if data subjects become more aware of their rights. The regulation of jurisdiction and applicable law can have an important influence on the rights of data subjects in the Union. Too complicated jurisdictional and conflict-of-law rules can dissuade data subjects from effectively exercising their rights.

On the basis of the analysis in this article, the following conclusions can be made. First, with regard to jurisdictional issues, it can be concluded that data subjects are – in an analogous way as consumers – a weaker party in comparison with controllers/processors. For that reason, special jurisdictional rules need to be developed that would suit the needs of data subjects and respond to specificities of the field of data protection. In order to achieve coherence between jurisdictional rules in the field of data protection and other jurisdictional rules, it would be most appropriate to include these specific rules directly into Regulation 1215/2012 and not in the proposed Data Protection Regulation. Consequently, the proposed Data Protection Regulation would need to be amended and not deal with this specific matter. In addition, in order to effectively protect the rights of data subjects, EU legislation would also need to put more emphasis on collective and representative claims and, consequently, regulate jurisdictional rules in this regard.

Moreover, rules concerning applicable law in the field of data protection would need to be clarified. On the one hand, the question of relationship between the 'classic' conflict-of-law rules (Rome I and II Regulations) and the provisions of the Data Protection Directive should be clearer, notably the question whether data protection can constitute overriding mandatory provisions from which no deviation is possible. Given the nature of data protection as a fundamental right, it seems indeed preferable that it also qualifies as an overriding mandatory rule. Furthermore, the rules on territorial scope of the proposed Data Protection Regulation should be amended so as to prevent its broad extraterritorial or even universal application.

Therefore, on a worldwide level and for the future, it will need to be considered whether the rules on jurisdiction and applicable law in the field of data protection can be agreed upon on a global scale, perhaps in a form of an international treaty[258]. Some time ago, an idea of a separate international

[258] The Hague Conference on Private International Law, in a document *Cross-Border Data Flows and Protection of Privacy* (2010), available on *http://www.hcch.net/upload/wop/genaff2010pd13e.pdf* [Accessed 27 February 2015], para. 22-23, stressed that there is 'no system in place to address fundamental cross-border issues from a global private international law perspective', and that there is 'the need to co-ordinate work in this area'. A comparable idea on a multilateral

tribunal for resolving Internet-related issues has been raised in the literature[259]. An even further step would be to attempt to align, on a global level, data protection rules that currently vary heavily among different countries in the world, but it is highly questionable whether this is politically feasible.[260] It is also to be seen whether, for data protection litigation, the Hague Convention on Choice of Court Agreements[261], which is however not yet in force[262], could potentially be relevant.

To conclude, it can be stated that the current EU rules on jurisdiction and applicable law still do not seem entirely accommodated to the complexity and the global nature of infringements of data protection.

(Contd.)

agreement on jurisdiction, but with regard to defamation over Internet, was raised by A. 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.

259 See W. Blair, D. Quest, "Jurisdiction, Conflicts of Law and the Internet" in G. Ferrarini (ed.), *Capital Markets in the Age of the Euro. Cross-Border Transactions, Listen Companies and Regulation* (Hague: Kluwer, 2002), 164.

260 Moreover, this seems more appropriate for cyberterrorism than for data protection because the attempts to fight terrorism are global; see, in this regard, K. Gable, "Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent", (2010) 43 *Vanderbilt Journal of Transnational Law*, 104 et seq.

261 Convention of 30 June 2005 on Choice of Court Agreements, available on *http://www.hcch.net/index_en.php?act=conventions.text&cid=98* [Accessed 27 February 2015].

262 On the status of the convention, see *ibid*.

Author contacts:

Maja Brkan

Faculty of Law, Maastricht University

Bouillonstraat 1-3

6211 LH Maastricht

The Netherlands

Email: maja.brkan@maastrichtuniversity.nl