www.jusletter-it.eu

Anabela Susana de Sousa Gonçalves

The Cross Border Regulation of Online Data Privacy and the Judicial Cooperation

The EU legislative instruments that exist in the field of judicial cooperation in civil matters complement the regime of Directive 95/46/EC and help to put into practice real data protection in online cases and enforcement of data protection rights across borders. Relying on judicial cooperation and the principle of trust between judicial authorities of different Member States, these legal instruments unify conflict-of-law rules, international jurisdiction provisions, setting up a system of recognition and automatic enforcement of foreign judgments. This paper explains how this system is crucial to protect the right to data privacy and to give effectiveness to the rights provided for in Directive 95/46/EC.

Collection: Conference Proceedings IRIS 2015; Top 10 – Peer Reviewed Jury LexisNexis Best Paper Award of IRIS2015
Category: Articles
Field of law: Data Protection
Region: Portugal

Citation: Anabela Susana de Sousa Gonçalves, The Cross Border Regulation of Online Data Privacy and the Judicial Cooperation, in: Jusletter IT 26. Februar 2015 – IRIS

Contents

1 Data Privacy

1.1 The right to privacy and personal data

[Rz 1] It is difficult to find a uniform definition of privacy. However, the right to privacy is a significant notion of human rights law and European law. Art. 12 of the Universal Declaration of Human Rights recognizes the right to privacy as a fundamental human right in establishing that «[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks». The respect for private life is also acknowledged in several international instruments about human rights with a very similar wording, like in Art. 17 of International Covenant on Civil and Political Rights, in Art. 8 of the European Convention on Human Rights and Fundamental Freedoms, in Art. 11 of the American Convention on Human Rights. These international law provisions are the foundations national data privacy laws are based on.

[Rz 2] On the level of European Union law, the Charter of Fundamental Rights of the European Union distinguishes the protection of the right of respect for private and family life (Art. 7) and the right to protection of personal data (Art. 8). This distinction is the result of the European Union's concern to implement an effective protection of personal data and to regulate the transmission of such data, and is often identified as a consequence of the traumatic experiences of the Second World War[1]. The heart of this effort is Directive 95/46/EC on the protection of individuals with regard to the protection of personal data and on the free movement on such data. Directive 95/46/EC established a harmonized system based three principles — transparency, legitimate purpose and proportionality, because it was clear that the difference of data protection legislation between Member States was an obstacle to the free flow of data and the development of the internal market. The objective is set in Recital 10 of the Directive 95/46/EC which states that the approximation of the European legislations would guarantee a minimal level of data protection on the European Union. That would make the free movement of personal information easier (Recital 9 of the Directive 95/46/EC). So, when using the expression data privacy, I plan to cover the use and handling of personal data, protected by the Directive, which could harm the right to privacy of individuals[2].

1 See Svantesson, Extraterritoriality in Data Privacy Law. Ex Tuto Publishing, Denmark, p. 43 (2013).

2 About the concept of data privacy, v. Svantesson, Extraterritoriality in Data Privacy Law. Ex Tuto Publishing, Denmark, pp. 25—26 (2013). The infringement of data privacy law already was considered by the European Court of Human Rights in several cases, as reported by Nardell, Levelling up: Data Privacy and the European Court of Human Rights. Gutwirth/Poullet/De Hert, Data Protection in a Profiled World, Springer, Dordrecht, Heidelberg, London, NewYork, pp. 43—52 (2010).

1.2 The cross border flow of data

[Rz 3] With technological evolution, cross-border data transfer became regular. The advent of the internet and its features as a global system of interconnected networks, characterized by a diffuse and a global nature, has made easy the wide spreading of information across borders, and simplified the establishing of contacts and the data exchange. The increase of cross-border flows of personal data drew attention to the need of protecting the privacy of the subjects as a fundamental right, on one hand, and the importance of free flow of the personal data to economic ends, on the other hand. It also became clear that harmonization in Europe was far below the required level. The complexity of personal data processing as a result of information and communication technology showed that there are relevant differences between the legislation of the Member States and the level of harmonization is deficient[3]. Outside the European Union the approaches to data privacy protection are varied and with profound differences[4].

[Rz 4] The need for legal security determines the importance of establishing in which situations the standard of protection of Directive 95/46/EC will be applicable and which law will be applicable in cross-border situations to the right of claiming compensation for damages resulting of the infringement of those rules. In addition, real data protection requires the enforcement of data protection rules and, for this purpose, it is essential to determine which court has jurisdiction and how can the decisions of national courts be enforced in other countries. This paper seeks to enlighten these problems trying to demonstrate the importance of judicial cooperation in solving them.

2 The applicable law to cross-border data transfer under Directive 95/46/EC

[Rz 5] It is important for individuals and economic agents to know which law will rule the processing of cross-border data flows. Through the conflict-of-law rules[5], we can establish to which transnational situations we are going to apply the standards of protection of the EU law (that are present in national laws by the transposition of Directive 95/46/EC).

[Rz 6] However, as a previous step, it is important to determine which situations are included in the material scope of application of Directive 95/46/EC. The Directive is applicable to the processing of personal data, in order to guarantee the right to privacy (Art. 1). Art. 2 (a) of Directive 95/46/EC defines personal data as information relating to an identified or identifiable individual, such as identification number, physical, psychological, economic, cultural or social factors. Examples of processing of personal data are listed on Art. 2 (b), like for example: collection, re-

3 About the lack of harmonization, see De Hert/Papakonstantinou, The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. Computer Law & Security Review, Vol. 28, pp. 132—141 (2012); Wong, Data Protection: The Future of Privacy. Computer Law & Security Review, Vol. 27, pp. 54—55 (2011).

4 Bygrave, Privacy Protection in a Global Context — A Comparative Overview. Scandinavian Studies in Law, Vol. 47, pp. 320—338 (2004).

5 In private relations related with more than one legal system, the conflict-of-law rules determine which law shall apply and in which legal system the solution must be reached. About the choice of law problem, see Audi, Droit International Privé. Economica, 4th Ed, Paris, pp. 81—83 (2006); Hoffman/Thorn, Internationales Privatrecht einschlielich der Grundzüge des Internationalen Zivilverfahrensrechts. Verlag C.H. Beck, München, pp. 177—178 (2005); Fawcett/Carruthers, M., Cheshire, North & Fawcett Private International Law. Oxford University Press, 14th Ed, Oxford, pp. 8—9 (2008).

cording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. Sometimes, the personal data are collected by e-mail and other techniques; at times the subject voluntarily puts his personal data online, for example in social networks like *Facebook* or *Google Plus*. Because of the global nature of the internet, most of the times, these situations are related with more than one country. If the subject tries to revoke his consent and to retrieve those personal data, under which law can he do it? Sometimes personal information is collected without the knowledge and consent of the subject, and that information can be sold to other users, or can be collected by tracking the behavior of the subject online by the website operators, and this information can circulate easily across the borders. The question is under which law we can determine that those behaviors are unlawful and we can be retrieved the damages resulting from them? An example of the relevance of difference of legislations in the cross-border flow of personal information, that shows the importance of determining the applicable law, is given by a European Commission text of 2012: «[a] multinational company with several establishments in the EU has deployed an online mapping system across Europe which collects images of all private and public buildings and also take pictures of people on the street. In one Member State, the inclusion of un-blurred pictures of persons unaware that they were being photographed was considered to be unlawful», but not in others[6].

[Rz 7] The conflict-of-law rule that lays down the scope of application of Directive 95/46/EC is set in Art. 4. Directive 95/46/EC is applicable when the establishment of the controller in the context of his activities is situated in the European Union, regardless of the place where the data processing occurs [Art. 4 sec. 1 (a)]. In those situations where the controller is established on the territory of several Member States, each establishment should comply with the obligations laid down by the national law of its situation. In what concerns online exchange of data, it may be difficult to determine the location of the establishment, because the activity of the controller may be widespread on the internet throughout several countries. But the concept of establishment laid down in Directive 95/46/EC helps to overcome this problem, because establishment is defined in a broad sense in Recital 19, as a stable arrangement through which is exercise an effective and real activity, regardless the form it takes — branch, subsidiary... If a controller has several establishments in the EU, each one of them should be in accordance with the national rules of the Member States of its situation (Recital 21, 2nd part). The controller, according to Art. 2 (d), is the legal or natural person or entity that alone or with others decides which will be the objective of the processing of personal data and the means used to that purpose[7]. Recital 47 helps to fulfill this concept giving the example of the messages that have personal data and are transmitted by mail or other communications technology, with the only objective of transmission: «(...) the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates (...)», rather the transmission service providers; however these «(...) will normally be considered controllers in respect of the processing of the

6 European Commission, Safeguarding Privacy in a Connected World, A European Data Protection Framework for the 21st Century, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels, 25 January 2012, COM(2012) 9 final, p. 7.

7 As Bygrave, European Data Protection, Determining Applicable Law Pursuant to European Data Protection Legislation. Computer Law & Security Report, Vol. 16—4, p. 255 (2000), points out, in cases of several controllers, it is possible that the situation of processing of personal data is subject to more than one national law.

additional personal data necessary for the operation of the service»[8].

[Rz 8] The protection level of the Directive is also applicable when the place of establishment of the controller is situated in a third State, where the national law of a Member State is applicable as a result of public international law (Art. 4 sec. 1 (b)).

[Rz 9] At last, the protection level of the Directive is also applicable when the controller is not established on Community territory but uses equipment situated on the territory of a Member State to process personal data — the applicable law will be the law of that country (Art. 4 sec. 1 (c)). According to the Art. 29 Data Protection Working Party, equipment should be interpreted as means automated or otherwise and this leads to a broad interpretation of the concept as including «(...) human and/or technical intermediaries, such as in surveys or inquires»[9].

[Rz 10] The justification of Art. 4 is in Recital 20: «[w]hereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice». With this rule the application of EU provisions in situations where the processing of data is not done in the European territory or the controller is established outside the EU is achieved. In the example of the individuals that upload personal data «onto an online social network operated from a server outside the EU»[10], it the application of Directive 95/46/EC is possible trough Art. 4 sec. 1 (c), because even if the establishment of the controller is situated in a third State, the processing of the personal data is done through equipment situated on the territory of a Member State. Likewise Directive 95/46/EC will be applicable in situations where, for example, the online social network is operated from a server inside the EU, that allows the upload of personal data from third States, by the application of Art. 4 sec. 1 (a). Through these rules the application of the protective personal data rules of the EU is enlarged. These are examples of extraterritorial application of the European Union legislation that can raise problems of enforcement of the rights protected by Directive 95/46/EC.

[Rz 11] However Directive 95/46/EC, although being a harmonization instrument, has several gaps and does not regulate comprehensively the protection of personal data, and many matters are left for the national laws of the Member States to regulate. In all those situations that are not governed by Directive 95/46/EC, it is necessary to use the national conflict-of-law rules to determine the applicable law, and those rules are different from Member State to Member State. This means that the courts of different Member States will apply to similar situations different laws and that will produce different solutions. In this regard, the differences between the personal data protection in national laws of the Member States introduces distortion in the internal market.

[Rz 12] The proposed European Union Data Protection Regulation tries to eliminate the differences in the level of protection of the right to privacy inside the EU[11]. The aim is to avoid the

8 The controller must be distinguished from the processor, as the person or entity «(...) which processes personal data on behalf of the controller» (Art. 2 (e)).

9 Art. 29 Data Protection Working Party, Opinion 8/2010 on applicable law. Working Paper 179, p. 20 (2010).

10 Kuner, Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. OECD Digital Economy Papers 187, p. 25 (2011).

11 European Commission, 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). Brussels, 25 January 2012, COM(2012) 11 final, pp. 1—118.

legal fragmentation that exists currently in the EU, in order to implement legal certainty, eliminate distortions of competition and to create conditions of trust between economic operators and individuals that may allow digital economy to develop. It was clear that it was essential to adjust the existing legal framework to the development of new technologies that favors the globalization of information and the transfer of personal data on an international level (inside the EU and between the Member States and third countries)[12]. With the internet the reality of processing personal data has changed: the individuals share their personal data on the internet, for example, on social networks and, most of the times, they lose control over the storage or the availability of these information; sometimes this information is sold without the subject's knowledge or consent; personal data are also collected by tracking the behavior of individuals online, for example through *cookies*. The proposed European Union data protection Regulation enhances the data subjects´ rights and enlarges data controllers' obligations[13], and tries to eliminate the differences in the level of protection of the individuals inside the EU, so that the processing of personal data is equivalent in all Member States[14]. However, it will be also important to know to which situations the rules of the proposed Regulation will apply, because the choice-of-law problems remains in situations not ruled by the Regulation or regarding third states. The European Commission has identified this problem in 2010, stating that «increased outsourcing of processing, very often outside the EU, raises several problems in relation to the law applicable to the processing and the allocation of associated responsibility»[15].

3 The right of claiming compensation for unlawful actions as a result of infringement of Directive 95/46/EC

[Rz 13] The proposed European Union Data Protection Regulation lays down a set of principles relating to personal data processing, rights of the data subjects, and obligations of controllers and processors, that will be uniform on the European Union, as currently is done by Directive 95/46/EC in a more circumscribed way. Both establish also the right of any natural person to receive from the controller or the processor compensation if he suffered damage as a result of an unlawful processing operation or an action incompatible with their rules (Art. 23 sec. 1 of Directive 95/46/EC, Art. 77 sec. 1 of the Regulation proposal). In situations where there is more than one controller or processor involved in the operation, Art. 77 sec. 2 of the Regulation proposal establishes a joint obligation: «(. . .) each controller or processor shall be jointly and severally liable for the entire amount of the damage».

---

12 European Commission, Safeguarding Privacy in a Connected World, A European Data Protection Framework for the 21st Century, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels, 25 January 2012, COM(2012) 9 final, p. 7.

13 For a detailed analysis, see Hert/Papakonstantinou, The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. Computer Law & Security Review, Vol. 28, pp. 132—141 (2012).

14 European Commission, Safeguarding Privacy in a Connected World, A European Data Protection Framework for the 21st Century, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels, 25 January 2012, COM(2012) 9 final, p. 20.

15 European Commission, A comprehensive approach on personal data protection in the European Union, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels, 4 November 2010, COM(2010) 609 final, , p. 4.

[Rz 14] If Directive 95/46/EC and the Regulation proposal establish the right of compensation for damages resulting from the violation of the rights and obligations present in both instruments, they have gaps because they do not have rules about the nature and the assessment of damage or remedy claimed, about the measures which a court may take to prevent or terminate injury or damage or to ensure the provisions of compensation, the transfer of a right to claim damages or remedy, the persons entitled to compensation for damages sustained personally, the extinction of the obligation of compensation or rules of prescription or limitation. Regulation No 846/2007 of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) determines the applicable law to cross-border non-contractual obligations, arising out of tort/*delict*, and answers to the question of the law applicable to those issues. This regulation is one of the EU instruments developed within the policy of cooperation in civil matters (Art. 81 of the Treaty of the Functioning of the European Union)[16]. However, according to Art. 1 sec. 2 (g) of the Rome II Regulation the non-contractual obligations arising out of violation of privacy and rights relating to personality, including defamation are excluded from the material scope of the Rome II Regulation[17]. A literal interpretation of the Art. means that despite the rules of Directive 95/46/EC and the proposed Data Protection Regulation[18], including the right of claiming compensation for unlawful actions, all those issues that the Directive and the Regulation proposal do not provide for, shall be ruled by national conflict-of-law rules and similar situations can have different solutions. As a result, similar actions producing damages, unlawful under the Directive, and done across Europe, can have different solutions by the application of different national conflict-of-law rules. This is not a fair and equitable outcome, because if individuals domiciled in different countries have the same dispute, in their countries, against the same tortfeasor, they are likely to get different results by the infringement of the same European legislation, as a result of application of different conflict-of-law rules in their countries of origin. In practice, this means that a company or a person can draw competitive advantages as a result of the application of different laws to identical disputes. This is compounded by the system of Regulation No 1215/2012 on jurisdiction and recognition and enforcement of judgments in civil and commercial matters (Brussels I *recast*)[19]. The most obvious way to avoid this result is the revision of the Rome II Regulation and the inclusion of a rule about violations of data privacy and personality rights. The European Parliament has already undertaken some initiatives to this end through a non-legislative report[20].

16 About the EU policy of cooperation in civil matters, see Gonçalves, Anabela Susana de Sousa, Da Responsabilidade Extracontratual em Direito Internacional Privado, A mudança de paradigma. Almedina, Coimbra, pp. 212—226 (2013).

17 The initial proposal of the Rome II Regulation, dated of 2003, had a conflict-of-law rule for non-contractual obligations arising out of violations of privacy and personality rights: European Commission, Proposal for a Regulation of the European Parliament and the Council on the law applicable to non-contractual obligations («Rome II»). Brussels, 22 July 2003, COM(2003) 427 final, pp. 17—18, 35.

18 See a possible systematic interpretation of Art. 1 sec. 2 (g) of Rome II Regulation, Gonçalves, Da Responsabilidade Extracontratual em Direito Internacional Privado, A mudança de paradigma. Almedina, Coimbra, pp. 265—267 (2013).

19 This regulation replaced the Regulation No 44/2001 (Brussels I) after 10 January 2015 in accordance with the conditions set in Art. 66 of Brussels I *rescast*.

20 European Parliament, Report with recommendations of the Commission on the amendment of Regulation (EC) No 864/2007 on the law applicable to non-contractual obligations (Rome II). A7-0152/2012, 2 May 2012, pp. 2—9.

4 Jurisdiction and enforcement in online cross-border infringements of data privacy

[Rz 15] Brussels I *recast* Regulation also falls within the EU policy of judicial cooperation in civil matters, which aims to establish cooperation between judicial authorities of Member States in order to facilitate the effective exercise of rights across borders. One of the landmarks of this policy is the principle of trust that must exist between judicial authorities of different Member States and the principle of recognition and enforcement of decisions coming from different Member States. The Regulation provides for a system of automatic recognition and enforcement of foreign judgments (Art. 36 and 39) in civil and commercial matters in the European Union (Art. 1). However, this system is based on a set of provisions of international jurisdiction.

[Rz 16] Brussels I *recast* is applicable to cross border infringements of personality rights, including the unlawful processing of personal data. The general rule of jurisdiction (Art. 4, sec. 1) establishes the principle of *sequitur forum rei*: the jurisdiction belongs to the courts of the Member State where the defendant is domiciled. However, there is an alternative jurisdiction in matters of torts/*delicts* in Art. 7, sec. 2. This provision is based in the principle of proximity — it is assumed that those courts are spatially or procedurally best placed to judge the question, because a greater connection between the dispute and the court will aid an easier conduction of the dispute and the production of evidence. So, according to Art. 7, sec. 2, in matters of tort/*delict*, the courts of the place where the harmful event occurred or may occur have jurisdiction. This is an alternative jurisdiction which means that the claimant may choose to bring an action before the courts of the Member State where the defendant is domiciled or before the courts designated by Art. 7, sec. 2. This option generates a *forum shopping* situation, because the party that prevents jurisdiction can choose the court, considering which one will apply the substantive law more favorable to his claims[21].

[Rz 17] However, the dispersion of forums under Art. 7, sec. 2[22], is greater. Called to interpret the expression *place where the harmful event occurred or may occur rule*, the ECJ has decided that the plaintiff has the option to sue, either in the courts of the place of the event which gives rise to and is at the origin of that damage, or in the courts for the place where the damage occurred[23]. According to the ECJ, the relevant damage is only the direct damage[24]. Therefore, the place where the direct results of the wrongful act or omission occurred is relevant. The difference is that the court of the place of the wrongful action has jurisdiction to decide the compensation of all the damages resulting of that behavior, whereas the court of the place of the damage has only jurisdiction to decide about the damages that occur in its territory. This was decided in the *Shevill* case — a case involving the infringement of a personality right, namely a situation of libel by a newspaper article distributed in several Member States[25]. The place of the event giving rise to

21 This is annulled when the Rome II Regulation is applicable, because the Member State courts will apply the same conflict-of-law rules to similar situations and consequently apply the same law. But the infringement of personality rights is excluded from the material scope of application of the Rome II Regulation: so, each Member State Court will apply his national conflict-of-law rules.

22 Corresponding to Art. 5, sec. 3, of the Regulation No 44/2001 (Brussels I).

23 See, e.g., Handelskwekerij G. J. Bier B.V. v Mines de Potasse d'Alsace S.A., case 21/76, ECR 1735 (1976).

24 Zuid-Chemie v. Philippo´s Mineralenfabriek NV/SA, case C-189-08, ECR I-06917(2009); Rudolf Kronhofer v Marianne Maier and Others, case C-168/02, I-06009(2004); Dumez France SA and Tracoba SARL v Hessische Landesbank and others, case C-220/88, I-00049(1990).

25 ECJ, Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA,

the damage was considered to be the place where the publisher of the newspaper was established, because it was in that place that the harmful event was originated and «(...) from which the libel was issued and put into circulation»[26]. The place of the damage (that would have only jurisdiction to award the damages produced in its own territory) was the place where the harmful effects upon the victim were produced, which was, in that case, the Member States «(...) in which the defamatory publication was distributed and in which the victim claims to have suffered injury to his reputation (...)»[27]. In this situation, the plaintiff should take action before the courts of each Member State in which territory the damage occurred (*Mosaikbetrachtung*).

[Rz 18] In the *eDate* case the ECJ addressed a situation of online infringement of personality rights and data privacy and recognized the specificity of the ubiquitous nature of the internet and its world-wide reach. The ECJ weighted in this case the impact of a content that was put online on a website on an individual's personality rights and the large extent of the damages that it could cause. In the *eDate* case, it the interpretation of Art. 7, sec. 2 was upheld, that the claimant can bring the action for all the damages caused in the court of the place of the event (in the case the place of the establishment of the publisher of that content) or the courts of each Member State where the damage occurred (in the case, each Member State in the territory of which the content placed online is or has been accessible)[28]. However, the ECJ adapted the interpretation of the rule to the nature of the internet, noting that content that is placed online can be consulted all over the world, which increases the impact of the damage, regardless of the intention of the person who placed that content online, and noting that «(...) it is not always possible, on a technical level, to quantify that distribution with certainty and accuracy in relation to a particular Member State or, therefore, to assess the damage caused exclusively within that Member State»[29]. Consequently the ECJ considered that another court should have jurisdiction to decide the compensation of all the damages caused — the court of the place where the victim has his center of interests[30]. The center of interests of the victim would be generally his habitual residence, but the ECJ admitted that it can also be the place where the victim follows his professional activity if the person has a close connection with that State[31]. The jurisdiction of the court of the place of the victim´s center of interests is justified by the ECJ for the purpose of predictability underlying the rules of jurisdiction, because the publisher of the harmful content is in a position to know the center of interests of the person that will suffer the damage.

[Rz 19] This interpretation has created another jurisdiction in online cross-border infringement of personality rights and data privacy, raising the number of possible relevant forums to four. This creates an unjustifiable favor of the claimant who may choose the court that will apply the law that is most favorable to him. Therefore, it is pressing the unification of the conflict of law provisions relating to data privacy so that, regardless of the court where the matter is judged, the same law should be applied.

---

case C-68/93, ECR pp. I—415 *et seq* (1995).

26 *Idem*, *ibidem*.

27 *Idem*, *ibidem*.

28 eDate Advertising GmbH v X (C-509/09) and Olivier Martinez and Robert Martinez v MGN Limited (C-161/10), joined cases C-509/09 and C-161/10 ECR pp. I—10269 *et seq* (2011).

29 *Idem*, *ibidem*.

30 *Idem*, *ibidem*.

31 *Idem*, *ibidem*.

5 Conclusions

[Rz 20] The EU legislative instruments that exist in the field of judicial cooperation complement the regime of Directive 95/46/EC and help to put into practice real data protection in online cases and the enforcement of data protection rights across borders. Relying on judicial cooperation and the principle of trust between judicial authorities of different Member States, these legal instruments unify conflict-of-law rules, international jurisdiction provisions, setting up a system of recognition and automatic enforcement of foreign judgments. I consider this system crucial for the protection of the right to data privacy and for giving effect to the rights provided for in Directive 95/46/EC. However, for those issues not covered by the Directive, it is necessary to apply the national law of the Member States and problems arise due to the lack of unified conflict-of-law rules on the infringement of data privacy in the EU. As a result of the Brussels I *recast* Regulation, there is a dispersion of forums that generates a situation of forum shopping which puts in question the principle of equality between the parties and the foreseeability in the resolution of these disputes across borders within the Union, and it is a disturbance factor in the functioning of the internal market. Resorting to national conflict-of-law rules means that the courts of the Member States will apply different laws to similar cases. In addition to the unequal treatment of similar situations, this results in an uncertainty for the parties involved in the dispute. Therefore, in my opinion, the revision of the Rome II Regulation in order to include in its material scope the infringement of personality rights and data privacy should be a priority of the EU. The similarity of solutions resulting from the adoption of uniform conflict-of-law rules in all Member States would be a way of achieving the equilibrium of the parties' positions and fairer solutions.

Anabela Susana de Sousa Gonçalves, Professor, Law School — University of Minho, Department of Private Law, Campus de Gualtar, 4710-057 Braga, Portugal, asgoncalves@direito.uminho.pt; www.direito.uminho.pt