II.1

The interface between the jurisdictional rules of Reg. (EU) No 2016/679 and those of Reg. (EU) No 1215/2012

SUMMARY: 1. Introduction. – 2. The interface between the jurisdictional rules of the GDPR and those of the B1R: Recital (147) GDPR and 67 B1R. – 3. Jurisdiction and coordination of multiple proceedings in the GDPR: Arts 79(2) and 81. – 4. The interface with Arts 4(1), 7, 18, 25, 26, 29 and 30 B1R. – 5. The interface in collective redress and mass harm situations. – 6. Conclusions.

1. In addition to administrative ones, Reg. (EU) No 2016/679 (hereafter "GDPR")[253] provides for private enforcement remedies that are purported to protect the fundamental right to data protection. In particular, where his rights are impaired by an infringement of the GDPR, the data subject entertains the right to an effective judicial remedy and to receive compensation, respectively under Arts 79(1) and 82(1) of the regulation.

Effective judicial remedies referred to in Art 79(1) GDPR are those provided for in the laws of each Member State (hereafter "MS"), and, in essence, injunctions[254] directed against a controller or processor (hereafter jointly referred to as "controller"). Furthermore, Art 82(1) GDPR grants the data subject the right to receive compensation for material and non-material damage resulting from the infringement of the regulation[255].

Considering that single infringements of the GDPR may affect a large number of data subjects simultaneously, Art 80(1) of the regulation provides that, where permitted by the laws of the MS courts seised, the rights granted by Art 79(1) and 82(1) of the same regulation may be exercised by the data subject through a «non-for-profit body, organisation or association».

Moreover, assuming that infringements of the right to data protection may have cross-border implications, the GDPR implements specific jurisdictional rules. Where disputes arising from infringements of the GDPR are characterized by an international element, Art 79(2) of the regulation determines the courts of which MSs may grant the remedies provided for in Art 79(1) and 82(1)[256] of the same regulation. Art 79(2) GDPR clearly favors the data subject[257], by allowing him to sue either in the courts of the MS where he habitually resides, or where the controller has an

253 Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1, 4.5.2016, p. 1 ff (http://data.europa.eu/eli/reg/2016/679/oj).

254 See P. FRANZINA, *Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, in A. DE FRANCESCHI (edited by), *European Contract Law and the Digital Single Market*, Cambridge-Antwerp-Portland, 2016, p. 97; C. KOHLER, *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union*, in *RDIPP*, 2016, p. 667-668.

255 Recitals (75) and (85) GDPR provide examples of damage that may result from the infringements of the regulation.

256 See Art 82(6) GDPR.

257 On the protective policy underlying Art 79(2) GDPR, see L. LUNDSTEDT, *International jurisdiction over cross-border private enforcement actions under the GDPR*, in *Stockholm Faculty of Law Research Paper Series*, 2018, p. 2 ff. Available at SSRN: https://ssrn.com/abstract=3159854 (accessed 15.8.2018); P. FRANZINA, *Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, p. 97-98.

establishment[258].[259] Furthermore, Art 81 GDPR governs the coordination of proceedings concerning the same infringement of the regulation and instituted in the courts of different MSs.

However, the specific jurisdictional rules of the GDPR are not the only rules on the conflict of jurisdiction that may apply to disputes between data subjects and controllers. In particular, provided that such disputes are, in principle, civil and commercial in nature, where characterized by an international element, the general jurisdictional rules of Reg. (EU) No 1215/2012 (hereafter "the B1R")[260] may purport to be applicable to proceedings instituted under Art 79(1) and 82(1) GDPR[261].

2. The GDPR deals with the issue of the interface between its specific jurisdictional rules and the general ones of the B1R. Recital (147) GDPR stipulates that, general rules on jurisdiction of the B1R must not prejudice the application of the specific ones of the GDPR, «in particular as regards proceedings seeking a judicial remedy including compensation».

However, the recital is not reflected in any provision of the regulation, and, as such, it has an uncertain legal force[262]. Attention should thus be drawn on a provision of the B1R: Art 67, which actually inspired the wording of Recital (147) GDPR. «Shall not prejudice» are, in fact, the keywords in Recital (147) and Art 67 B1R. Akin to Recital (147) GDPR, Art 67 B1R provides that

258 This, by the way, gives the data subject the chance of suing the Third State controller in a MS, in all cases, even where the latter lacks an establishment in a MS. Cf. M. BRKAN, *Data protection and European private international law: observing a bull in a China shop*, in *IDPL*, 2015, p. 265.

259 For sake of completeness, Art 79(2) GDPR allows the data subject to sue in the courts of the MS where he habitually resides, unless the controller is a public authority of a MS in the exercise of its public powers. Certain scholars posit that, under Art 79(2) GDPR, the data subject should be allowed to sue the public authority in the courts of the MS where the latter has an establishment. However, the wording of the provision is not conclusive and the one employed in Recital (145) GDPR rather suggests that proceedings against a public authority acting in the exercise of its public powers fall outside the scope of the provision. Cf. M. BRKAN, *Data protection and European private international law: observing a bull in a China shop*, p. 272-273.

260 Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), OJ L 351/1, 20.12.2012, p. 1 ff (http://data.europa.eu/eli/reg/2012/1215/oj).

261 The civil and commercial nature of disputes and the existence of an international element are in fact the two elements that define the scope *ratione materiae* of the B1R. In principle, following the findings of the CJEU in the *Eurocontrol* case, the first element is traced where the controller is a private party or a public authority acting in a private capacity, whereas it is excluded where the latter is acting in the exercise of its public powers. See C. KOHLER, *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union*, p. 669 and footnote 51; M. BRKAN, *Data protection and European private international law: observing a bull in a China shop*, p. 261-262, 272-273; and CJEU, 14.10.1976, C-29/76, *LTU Lufttransportunternehmen GmbH & Co. KG v Eurocontrol*, ECLI:EU:C:1976:137 (http://curia.europa.eu/juris/showPdf.jsf;jsessionid=77A4E0AAF7FC923395E75488EAF2BAF4?text=&docid=89285&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1160263).

262 See CJEU, 2.4.2009, C-134/08, *Hauptzollamt Bremen v J. E. Tyson Parketthandel GmbH hanse j.*, ECLI:EU:C:2009:229, point 16 (http://curia.europa.eu/juris/document/document.jsf?text=&docid=73634&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1160390).

the latter regulation must «not prejudice the application of provisions governing jurisdiction[263] (…) in specific matters which are contained in instruments of the Union (…)»[264].

What follows from Art 67 B1R is that specific jurisdictional rules such as those of the GDPR, do not supersede the general rules of the former regulation, but rather prevail[265] «to the extent of any inconsistency» with the latter regulation[266]. In other words, the specific rules of the GDPR are not to be understood as *lex specialis* vis-à-vis the general ones of the B1R, but rather as a «*lex formidabilis*»[267]!

Hence, the rules on jurisdiction of the B1R must be disregarded whenever their application may «contradict (…) or affect the integrity and consistency of the special regime provided [in the GDPR]»[268], whereas in all other cases, the former rules may continue to be applicable[269]. This means that the rules of the B1R may still be applicable, unless their application hampers the jurisdictional favor granted to the data subject, by reducing the number of MSs where he may sue the controller under Art 79(2) GDPR[270], or by providing the latter with a greater number of MS courts where it may sue the former.

3. Art 79(2) GDPR governs jurisdiction over actions brought by data subjects – and, apparently, by NGOs too (§ 5) –, but does not cover actions brought by controllers, which instead may fall within the purview of the general rules of the B1R[271].

This said, the MS of habitual residence referred to in Art 79(2) GDPR is likely to be that where the infringement of the regulation affects the data subject, and, namely, where damage is

263 Unlike Recital (147) GDPR, mentioning «rules on jurisdiction», Art 67 B1R makes broader reference to «provisions governing jurisdiction», which thus covers both the special rule on jurisdiction (Art 79(2)) and that on coordination of proceedings (Art 81) of the GDPR.

264 Few pieces of EU legislation on specific matters contain jurisdictional rules. See L. LUNDSTEDT, *International jurisdiction over cross-border private enforcement actions under the GDPR*, p. 31-32; A. DICKINSON, E. LEIN (eds.), *The Brussels I regulation recast*, Oxford, 2015, p. 564, footnote 4.

265 See A. BARLETTA, *La tutela effettiva della privacy nello spazio (giudiziario) europeo nel tempo (della "aterittorialità") di internet*, in *Europa e diritto privato*, 2017, p. 1197.

266 See A. DICKINSON, E. LEIN (eds.), *The Brussels I regulation recast*, p. 564.

267 G. VAN CLASTER, *Sur des bases fragiles. Le RGPD et les règles de compétence concernant les infractions au droit respect de la vie privée*, in *L'Observateur de Bruxelles*, July 2018, p. 29. Cf. L. LUNDSTEDT, *International jurisdiction over cross-border private enforcement actions under the GDPR*, p. 32 ff.

268 P. FRANZINA, *Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, p. 104.

269 See F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernenti il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I*-bis*"*, in *Cuadernos de Derecho Transacional*, 2017, p. 451; I. REVOLIDIS, *Judicial Jurisdiction over Internet Privacy Violations and the GDPR: a Case of "Privacy Tourism"?*, in *Masaryk University Journal of Law and Technology*, 2017, p. 22 and footnote 59; P. FRANZINA, *Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, p. 104; C. KOHLER, *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union*, p. 669.

270 See L. LUNDSTEDT, *International jurisdiction over cross-border private enforcement actions under the GDPR*, p. 33-34; C. KOHLER, *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union*, p. 669.

271 See F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernenti il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I*-bis*"*, p. 451.

caused[272]. Though being used as a connecting factor also in other European private international law instruments, the notion of habitual residence within the meaning of Art 79(2) GDPR is far from being undisputed[273] and yet less controversial than that of establishment mentioned in the first period of the same provision.

As concerns the notion of establishment, it is submitted that, following the first period of Art 79(2) GDPR, the data subject may elect to sue in the MS where the controller has an establishment[274] and not only in that where the latter has its main establishment[275]. This gives the data subject a wider choice, since the notion of establishment in Recital (22) GDPR is broader than that of main establishment in Art 4(16) of the regulation[276].

272 See ID., p. 455.

273 Cf. G. VAN CLASTER, *Sur des bases fragiles. Le RGPD et les règles de compétence concernant les infractions au droit respect de la vie privée*, p. 29-30; L. LUNDSTEDT, *International jurisdiction over cross-border private enforcement actions under the GDPR*, p. 28-29; P. FRANZINA, *Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, p. 101 ff.

274 Provided that the provision only refers to cases where the controller has an establishment in a MS, it should not apply where the controller has none. However, Kohler posits that the provision may vest jurisdiction in the courts of the MS of the representative appointed by a controller lacking establishments in a MS, in accordance with Art 27 GDPR. Actually, this opinion is backed by the last period of Recital (80) GDPR, which stipulates that enforcement proceedings should also be available against representatives. However, the recital is not reflected in any provision of the GDPR, including Art 79(2) thereof. Furthermore, in the *Weltimmo* case, the CJEU found that a processor had an establishment in a MS, by taking into account a number of facts, among which, the appointment of a representative with an address in that MS. It appears that, in principle, the mere appointment of a representative in a MS should not be sufficient to consider a controller as having an establishment in the same MS. Therefore, the preferred reading of the first period of Art 79(2) GDPR, is that the provision does not vest jurisdiction in the courts of the MS where a representative is based, unless it may qualify as an establishment within the meaning of the regulation. See C. KOHLER, *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union*, p. 668; CJEU, 1.10.2015, C-230/14, *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, ECLI:EU:C:2015:639, points 32 ff (http://curia.europa.eu/juris/document/document.jsf?docid=168944&text=&dir=&doclang=EN&part=1&occ=first&mode=DOC&pageIndex=0&cid=3527546).

275 See F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernenti il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I*-bis*"*, p. 453, echoing P. FRANZINA, *Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, p. 99-100. But see L. LUNDSTEDT, *International jurisdiction over cross-border private enforcement actions under the GDPR*, p. 27-28, 34, according to which establishment referred in Art. 79(2) GDPR is actually to be understood as main establishment.

276 The recital reflects the «flexible definition» of establishment in Recital (19) Directive 95/46/EC, endorsed by the CJEU in the *Google Spain*, *Weltimmo* and *Wirtschaftsakademie* cases. See, respectively, CJEU, 14.5.2014, C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317, point 49 (http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=en); *Weltimmo*, points 32 ff; 5.6.2018, C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, ECLI:EU:C:2018:388, point 55 (curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=3527736).

Generic reference to an establishment also implies that, though likely[277], the relevant establishment is not necessarily that where the infringement of the GDPR took place[278]. On the contrary, that is to say, if the data subject were required to fulfil the cumbersome task of proving that the infringement of the GDPR took place in the establishment located in the MS of the seised courts, the aim pursued by the regulation of granting the data subject with more favorable rules on jurisdiction could be undermined[279]. This is why, following a first reading, the establishment mentioned in Art 79(2) GDPR may lack any connection with the infringement of the regulation, even if this would admittedly encourage forum shopping by data subjects[280].

But a second and different reading should be preferred, one that better reflects the principles enshrined in the case law of the Court of Justice (hereafter "CJEU") on EU data protection legislation[281]. Following such case law, establishment is not just that where the unlawful handling of personal data took place, but also that in the context of whose activities such handling was carried out[282]. The latter being the case where such activities are «inextricably linked» with the unlawful handling[283]. If these findings were applied to the first period of Art 79(2) GDPR, then the provision could vest jurisdiction in the courts of the MS of the establishment where the infringement of the regulation took place, and where activities carried out were inextricably linked with the same infringement. Where followed, this reading could lower the risk of forum shopping and yet favor the data subject sufficiently[284].

The second reading should thus be preferred in that it better reflects the case law of the CJEU, whereas the first reading, a part from encouraging forum shopping, could lead to the application of Art 79(2) GDPR also in cases lacking an international element[285].

277 See F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernenti il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I*-bis*"*, p. 451; D. COOPER, C. KUNER, *Data Protection Law and International Dispute Resolution*, in *RCADI*, CCCLXXXII, 2017, p. 121.

278 See G. VAN CLASTER, *Sur des bases fragiles. Le RGPD et les règles de compétence concernant les infractions au droit respect de la vie privée*, p. 29; F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernenti il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I*-bis*"*, p. 453.

279 See P. FRANZINA, *Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, p. 100.

280 See ID., p. 101.

281 Namely, on Directive 95/46/EC and, in particular, on Art 4(1)(a) thereof.

282 See Art 3(1) and the first period of Recital (22) GDPR. See also the findings of the CJEU on Art 4(1)(a) Directive 95/46/EC in *Google Spain*, point 52, and *Wirtschaftsakademie Schleswig-Holstetin*, point 57.

283 See CJEU, *Google Spain*, points 51 ff; *Wirtschaftsakademie Schleswig-Holstein*, point 60.

284 However, alike the first, the second reading does not secure a strong connection between the seised court and the infringement of the GDPR in all cases. This is the consequence of taking the flexible notion of establishment, which is linked to a wider issue: the far reaching scope of European data protection legislation. Cf. I. REVOLIDIS, *Judicial Jurisdiction over Internet Privacy Violations and the GDPR: a Case of "Privacy Tourism"?*, p. 26 ff.

285 The international element that triggers the application of Art 79(2) GDPR consists in the difference between the MS where the data subject habitually resides and that where the establishment of the controller is located. The first reading examined above appears to imply that the existence of an establishment in a foreign MS may be sufficient to trigger the application of Art 79(2) GDRP. If so, the provision could be applicable in purely domestic cases, that is to say, where the data subject, the controller, the infringement and the damage caused are located in the same MS, insofar as the controller has an establishment in a different MS. Instead, following the second and preferred reading also examined

Drawing on Art 81 GDPR, the provision addresses the issue of multiple proceedings concerning «the same subject matter as regards processing by the same controller». Pursuant to Art 81(1) and (2) GDPR, where such proceedings are pending before the courts of different MSs, the MS court second seised may elect to suspend proceedings instituted before it, but only after having taken contact with the MS court first seised, to confirm the existence of proceedings concerning the processing by the same controller. Art 81(3) GDPR further provides that, where proceedings are pending at first instance before the MS court second seized, the latter may also, on application of one of the parties, decline jurisdiction if the MS court first seised has jurisdiction over the actions in question and its law permits consolidation thereof[286].

Recital (144) GDPR might suggest that Art 81 of the regulation only refers to proceedings instituted under Art 78 of the same regulation, that is to say against a decision by a supervisory authority[287].[288] However, the recital may not lead to a narrower reading of Art 81 GDPR and the broad wording of the provision suggests that it should also be applicable to multiple proceedings instituted under Art 79(2) of the regulation[289].

If this is correct, then a following question arises: whether the provision applies where multiple proceedings are instituted by data subjects only, or also where such proceedings are pending in parallel with those instituted by a controller, under different heads of jurisdiction, say Art 7(2) B1R (§ 4).

Though the wording of Art 81 GDPR appears to be broad enough to cover also the latter case, it has been held that, where multiple proceedings are instituted respectively by data subjects and controllers, their coordination should be governed by the general rules of the B1R and not those of the GDPR[290].

Unlike Art 81 GDPR, general rules of the B1R on related proceedings and *lis pendens* are based on the principle of temporal priority: the MS courts second seised must stay proceedings. As discussed below (§ 5), the principle enshrined in these general rules is inadequate in mass harm situations, such as those that may arise from infringements of the GDPR.

above, the international element may exist only if the MS where the data subject habitually resides is different from that of the establishment where the infringement of the GDPR took place, or where activities inextricably linked to the same infringement were carried out. There appears to be also another element that should be deemed international and thus trigger the application of Art 79(2) GDPR: damage resulting from the infringement of the regulation caused in a MS other than that where the data subject habitually resides.

286 This provision was clearly inspired from Art 30(2) B1R.

287 P. FRANZINA, *Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, p. 106.

288 Actually, this reading may be upheld by referring to Art 76(3) and (4) of the proposed text of the GDPR. See Proposal for a Regulation of the European Parliament and 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), COM(2012) 11 final, (http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf).

289 See F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernenti il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I*-bis*"*, p. 458 and footnote 29.

290 See F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernenti il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I*-bis*"*, p. 458 ff.

These are the reasons why the preferred reading of Art 81 GDPR is that the provision may apply in cases of multiple proceedings concerning the processing by the same controller, irrespective of the party that has instituted them.

4. Indeed, domestic courts, and, ultimately, the CJEU will have the last say as to which jurisdictional rules of the B1R will survive the GDPR[291]. In the meantime, scholars have faced the issue with reference to, in particular, Arts 4(1), 7, 18, 25, 26, 29 and 30 B1R, which respectively provide for the general head of jurisdiction, special heads of jurisdiction, the head of jurisdiction over consumer contracts, prorogation of jurisdiction, related proceedings and *lis pendens*.

Before examining each of the provisions mentioned above and the interface with the GDPR, it must be recalled that Art 79(2) of the regulation does not govern jurisdiction over actions brought by controllers, which instead may fall within the purview of the B1R.

Having this recalled, under Art 4(1) B1R, a person domiciled in a MS may be sued in the courts of that MS. This provision is not exactly the same as the one in the first period of Art 79(2) GDPR, since the notion of domicile is narrower than that of establishment within the meaning of the latter provision. In particular, when it comes to companies, following Art 63 B1R, domicile is the place of the MS where the company (or other legal person or association) has its statutory seat, central administration or principal place of business. As a consequence, where the place of domicile is not the establishment within the meaning of the first period of Art 79(2) GDPR, the data subject should be allowed to sue the controller also in the courts of the MS where the controller has its domicile under Arts 4(1) and 63 B1R[292].

Moving to special heads of jurisdiction of the B1R, these apply in addition to the general head of jurisdiction and thus, under the latter regulation, a claimant may elect whether to sue a defendant domiciled in a MS either in the courts mentioned in Art 4(1), or, alternatively, in those mentioned in Art 7 of the same regulation[293].

Art 7(1) B1R provides that, in matters relating to contract, courts having jurisdiction are those of the MS where the place of performance of the obligation in question is located[294]. It is submitted that, where the provisions of the GDPR are embedded in a contract between a data subject and a controller, and disputes arise from the infringement of the same provisions, the latter should also be allowed to sue in the courts of the MS mentioned in Art 7(1) B1R[295], which – though unlikely – may be different from those mentioned in Art 79(2) GDPR.

291 See I. REVOLIDIS, *Judicial Jurisdiction over Internet Privacy Violations and the GDPR: a Case of "Privacy Tourism"?*, p. 22.

292 See L. LUNDSTEDT, *International jurisdiction over cross-border private enforcement actions under the GDPR*, p. 13; I. REVOLIDIS, *Judicial Jurisdiction over Internet Privacy Violations and the GDPR: a Case of "Privacy Tourism"?*, p. 22.

293 See Art 5(1) B1R.

294 See Art 7(1)(a) B1R.

295 See L. LUNDSTEDT, *International jurisdiction over cross-border private enforcement actions under the GDPR*, p. 13-14; C. KOHLER, *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union*, p. 669-670; M. BRKAN, *Data protection and European private international law: observing a bull in a China shop*, in *International Data Privacy Law*, p. 266.

Instead, where disputes concern contracts entered into by weaker parties[296], protective heads of jurisdiction apply[297]. These heads of jurisdiction take precedence over the other rules of the B1R[298] and purport to favor weaker parties on a jurisdictional level. Art 18 B1R deals with jurisdiction over consumers contracts. Akin to Art 79(2) GDPR, Art 18(1) B1R provides that a consumer may sue the professional either in the courts of the MS where he is domiciled or where the latter is based. Hence, where a contract embedding the provisions of the GDPR exists and the data subject is a consumer, the latter should be able to rely on Art 18 B1R[299], especially if his domicile is different from that where he habitually resides within the meaning of Art 79(2) GDPR.

Art 18 B1R also provides that the professional may sue the consumer only in the MS where the latter is domiciled[300]. Though clearly inspired by the protective rules on jurisdiction of the B1R, including Art 18 thereof, surprisingly, neither Art 79 GDPR, nor any other provision of the latter regulation, governs jurisdiction over actions brought by the controller against the data subject and thus, as repeatedly mentioned above, jurisdiction over such actions may be governed by the general rules of the B1R.

Drawing back to special heads of jurisdiction, under Art 7(2) B1R, in matters relating to tort jurisdiction lies with the court of the MS where the harmful event occurred or may occur. This is the provision of the B1R that has raised major debate among scholar as to the interface of the latter regulation and the GDPR.

Following the sc. ubiquity approach taken by the ECJ, Art 7(2) B1R vests jurisdiction both in the courts of the MS where damage is caused and in those of the MS where the event giving rise to it takes place[301].

In the specific case of claims for compensation of damages arising from the infringement of personality rights by means of content placed online on an internet website[302], the CJEU held that

296 During the recasting of Reg. (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, by its letter of 20 September 2011, the European Data Protection Supervisor urged the Commission to consider whether «jurisdictional rules [should] protect the weaker party also in data protection litigation». The proposal was dropped and, ultimately, only consumers, insured (policyholders and beneficiaries) and individual employees qualify as weaker parties under the B1R. See the letter of the 20th of September 2011, by the European Data Protection Authority, addressed to the Commission and bearing the following record number: GB/HH/et/D(2011)1571 C 2011-0106 (https://edps.europa.eu/sites/edp/files/publication/11-09-20_letter_reding_en.pdf).

297 See Sections 3, 4 and 5 B1R, which respectively apply in cases of insurance, consumer and individual employment contracts.

298 Except exclusive heads of jurisdiction in Art 23 B1R.

299 See M. BRKAN, *Data protection and European private international law: observing a bull in a China shop*, in *International Data Privacy Law*, p. 276-278. See also L. LUNDSTEDT, *International jurisdiction over cross-border private enforcement actions under the GDPR*, p. 14 ff.

300 See Art 18(2) B1R.

301 See CJEU, 30.11.1976, C-21/76, *Handelskwekerij G. J. Bier BV v Mines de potasse d'Alsace SA.*, ECLI:EU:C:1976:166 (http://curia.europa.eu/juris/showPdf.jsf?text=&docid=89372&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3528393).

302 See, for further readings, M. A. LUPOI, *Attività online e criteri di collegamento giurisdizionale*, in *RTDPC*, 2018, p. 509 ff; Opinion of Advocate General Bobek, delivered on 13.7.2018, in C-194/16, *Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB,* ECLI:EU:C:2017:554 (http://curia.europa.eu/juris/document/document.jsf?text=&docid=195583&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3528548); B. HESS, *The Protection of Privacy in the Case Law of the CJEU*, in B. HESS, C. M. MARIOTTINI (eds.), *Protecting Privacy in Private*

courts having jurisdiction under Art 7(2) B1R are those of the MS where the injured party has his center of interests – which, though unlikely, may be different from his habitual residence – or those where the publisher is established, or, alternatively, those where the content placed online is or has been accessible[303]. Following such case law, in the first two cases, the courts have jurisdiction over damage to the injured party, wherever it was caused, whereas, in the third case, the courts of the MS have jurisdiction only over damage caused in that State[304].

Provided that, potentially, content placed online may be accessed in all 28 MSs, the courts of all such MSs could take jurisdiction, though only in relation to damage caused in their respective territory[305]. This solution leads to a fragmentation of jurisdiction amongst the courts of the MSs and is why the approach taken by the CJEU is known as the "mosaic" approach.

It is doubt whether the "mosaic" approach should extend to Art 79(2) GDPR[306]; the preferred reading is it should not[307]. In cases of claims for compensation of damages arising from the infringement of the right to data protection on the internet, the courts of the MS seised under Art 79(2) should be allowed to assess the entire damage suffered by the data subject, even where such courts are not those of the MS where the latter has his center of interests or where the controller is established[308]. If otherwise, the aim pursued by the GDPR of granting data subjects «full and effective compensation for the damage they have suffered»[309] could be undermined.

Furthermore, scholars disagree as to whether Art 79(2) GDPR may apply in parallel with Art 7(2) B1R, even if the latter provision admittedly increases the number of MS courts the data subject may rely on. Those who rule out the possibility stress that, if both provisions were applicable, in case of infringements of the right to data protection on the internet, data subjects would be granted

International and Procedural Law and Data Protection, Baden-Baden, 2015, p. 89 ff.

303 See CJEU, 25.10.2011, C-509/09 and C-161/10, *eDate Advertising GmbH and Others v X and Société MGN LIMITED*, ECLI:EU:C:2011:685 (http://curia.europa.eu/juris/document/document.jsf?text=&docid=111742&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=3528601) and, most recently, 17.10.2018, C-194/16, *Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB*, ECLI:EU:C:2017:766 (http://curia.europa.eu/juris/document/document.jsf?text=&docid=195583&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=3528684).

304 See CJEU, *eDate Advertising*, points 42 ff, citing CJEU, 7.3.2005, C-68/93, *Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA.*, ECLI:EU:C:1995:61 (http://curia.europa.eu/juris/showPdf.jsf?text=&docid=98911&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3528759), on a case of defamation through the press, where the court took, for the first time, the "mosaic" approach.

305 See Opinion of AG Bobek, in *Bolagsupplysningen*, points 77 and 80.

306 See G. VAN CLASTER, *Sur des bases fragiles. Le RGPD et les règles de compétence concernant les infractions au droit respect de la vie privée*, p. 29.

307 Cf. L. LUNDSTEDT, *International jurisdiction over cross-border private enforcement actions under the GDPR*, p. 29; M. BRKAN, *Data protection and European private international law: observing a bull in a China shop*, in *International Data Privacy Law*, p. 271.

308 In the *eDate Advertising* the notion of establishment is that taken in Directive 2000/31/EC, which appears to be slightly narrower than that of the GDPR. See CJEU, *eDate Advertising*, points 53 ff; Recital (19) 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 ("Directive on electronic commerce"), OJ L 178, 17.7.2000, p. 1 ff (http://data.europa.eu/eli/dir/2000/31/oj).

309 Recital (146) GDPR.

an «overextended jurisdictional privilege»[310] and this «would harm the clarity and unity of the special regime laid down in Art 79(2) GDPR»[311].

Even if these assumptions were correct, there appears to be a reason why the concurrent application of Art 7(2) B1R and 79(2) GDPR should be endorsed.

Art 7(2) B1R governs jurisdiction also over actions brought by alleged tortfeasors for negative declarations seeking to establish the absence of their liability in tort[312]. Now, bearing in mind that jurisdiction over actions brought by controllers seeking a declaration of non-liability under the GDPR may be, in principle, governed by Art 7(2) B1R[313], if the latter provision were not applicable in parallel with Art 79(2) GDPR, then controllers could sue in a greater number of MSs than those where the data subject could. This imbalance would be even greater where the data subject were claiming together with data subjects from different MSs, through an Art 80(1) GDPR NGO, in which case, the only courts available would be those of the MS where the controller has an establishment (§ 5). All this appears to be inconsistent with the protective policy underlying the GDPR and is why a concurrent application of Art 79(2) thereof and Art 7(2) B1R should be endorsed.

Coming to prorogation of jurisdiction by consent, under Art 25 B1R, parties may agree that «the courts of a Member State are to have jurisdiction to settle any disputes which have arisen or which may arise between them in connection with a particular legal relationship». A similar agreement on jurisdiction may be either exclusive or non-exclusive; it is exclusive where the parties have not agreed otherwise. Where exclusive, the agreement confers jurisdiction on the selected MS court and derogates jurisdiction of any other court, whereas a non-exclusive one only bestows authority upon the selected courts. This means that, where a non-exclusive jurisdiction agreement applies, a part from the selected MS courts, other courts may take jurisdiction over the prorogued disputes, insofar as they are provided with such under different rules of the B1R, say, for instance, Arts 4(1) or 7 thereof.

But a jurisdiction agreement may also be asymmetric. An asymmetric jurisdiction agreement is one which provides one of the parties with a greater number of courts to resort to. A particular kind of asymmetric agreements are sc. one-sided jurisdiction agreements, whereby one party may sue only in the courts of one State and the other may sue in the courts of that and other States. In other words, such a kind of jurisdiction agreements are exclusive for one party and non-exclusive for the other.

Similar agreements are the only that, according to the B1R, weaker parties, amongst which consumers, may enter into[314]. In fact, following Art 19 B1R, in case disputes have arisen between a consumer and a professional, the litigants may enter into a jurisdiction agreement according to

310 I. REVOLIDIS, *Judicial Jurisdiction over Internet Privacy Violations and the GDPR: a Case of "Privacy Tourism"?*, p. 23.

311 P. FRANZINA, *Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, p. 105.

312 See CJEU, 25.10.2012, C-133/11, *Folien Fischer AG and Fofitec AG v Ritrama SpA*, ECLI:EU:C:2012:664 (curia.europa.eu/juris/document/document.jsf?text=&docid=128908&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3529058).

313 But see P. FRANZINA, *Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, p. 92 and 105.

314 See Arts 15, 19 and 23 B1R.

which the consumer may sue in more MS courts than those made available in Art 18(1) B1R, whilst leaving the professional with no other choice than suing in the courts where the same consumer is domiciled.

Under the GDPR, jurisdiction agreements should be permitted, as far as they increase the number of MS courts where the data subject may sue the controller[315], whilst reducing or leaving unaffected the number of MS courts made available to the controller. Hence, a one-sided jurisdiction agreement favoring the data subject should be permitted, whereas an exclusive or a non-exclusive jurisdiction agreement should not[316].

This said, prorogation of jurisdiction may also take place tacitly. According to Art 26 B1R, tacit prorogation of jurisdiction occurs when a party enters into an appearance before the court of a MS without challenging jurisdiction, thereby vesting the seised court with such. Art 26(2) B1R provides that, where the defendant is a weaker party, such as a consumer, the seised courts must inform the latter that he may contest jurisdiction and the consequences of entering or not an appearance.

Also the latter provision of the B1R should be applicable in parallel with the jurisdictional rules of the GDPR, unless the data subject is the defendant[317]. In the latter case, where the data subject is the defendant, Art 26 B1R should not be applicable[318], or, perhaps, it could be, insofar as the latter be granted the same protection weaker parties enjoy under the second paragraph of the provision.

Drawing on the rules on the coordination of proceedings provided for in the B1R, Art 29 thereof deals with the case of «proceedings involving the same cause of action and between the same parties brought before the courts of different MSs», whilst following Art 30 of the regulation deals with «related actions (…) pending in the courts of different MSs». In essence, these rules aim at preventing conflicting decisions and, in both cases, this risk is addressed by providing that the MS courts second seised must stay proceedings and, where applicable, decline jurisdiction in favor of the MS courts first seised[319]. Unless an exclusive jurisdiction agreement applies[320], the courts second seised have no discretion. On the contrary, Art 81 GDPR leaves the MS courts second seised free to elect whether to stay proceedings[321].

315 See I. REVOLIDIS, *Judicial Jurisdiction over Internet Privacy Violations and the GDPR: a Case of "Privacy Tourism"?*, p. 23-24; F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernenti il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I*-bis*"*, p. 452; P. FRANZINA, *Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, p. 107-108.

316 Cf. C. KOHLER, *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union*, p. 669.

317 See F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernenti il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I*-bis*"*, p. 452.

318 See I. REVOLIDIS, *Judicial Jurisdiction over Internet Privacy Violations and the GDPR: a Case of "Privacy Tourism"?*, p. 24-25.

319 See, respectively, Arts 29(1) and 30(2) B1R.

320 See Art 31(2) B1R.

321 See above § 2.

Where proceedings concern the processing by the same controller, it appears that the latter provision should take precedence over Arts 29 and 30 B1R[322]. This, as mentioned above (§ 3), in the light of the broad wording of Art 81 GDPR and for the further reasons discussed below (§ 5).

5. Infringements of data protection legislation often affect a large number of data subjects based in different States and, in mass harm situations, injured parties are keen to seek redress collectively, rather than separately.

I t is likely that the assumptions above were the basis for Art 80(1) GDPR, according to which the rights granted by Art 79(1) and 82(1) of the regulation may be exercised by data subjects collectively through a «non-for-profit body, organisation or association»[323], to the extent that the laws of the MS courts seised permit collective actions[324]. Actually, despite Recommendation 2013/396/EU encouraging MSs to introduce injunctive and compensatory collective redress mechanisms for the implementation of rights granted under EU law[325], not all MSs have[326] and only in a small number of them such mechanisms appear to be «relatively well-functioning»[327].[328]

This said, the GDPR does not provide for a specific rule on jurisdiction applicable to collective claims[329]. Nonetheless, Art 79(2) GDPR should also be deemed applicable where the claimant is an NGO seeking an effective judicial remedy or compensation on the behalf of data subjects. In fact, though Art 79(1) GDPR speaks of the data subject's right to an effective judicial remedy, the second paragraph of the provision only mentions court proceedings instituted against a controller. The wording of Art 79(2) GDPR thus suggests that the scope *ratione personae* of the

322 Cfr. A. BARLETTA, *La tutela effettiva della privacy nello spazio (giudiziario) europeo nel tempo (della "aterittorialità") di internet*, 1199.

323 For sake of completeness, the second and last paragraph of Art 80 GDPR stipulates that MSs may provide that NGOs may exercise the right referred to in Art 79 – but not that referred to in Art 82(1) – autonomously.

324 Art 80(1) GDPR further provides that the NGO may represent the data subject, as far as it has been «properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of the data subjects' rights and freedoms with regard to the protection of their personal data».

325 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), in OJ L 201, 26.7.2013, p. 60 ff (http://data.europa.eu/eli/reco/2013/396/oj).

326 See Report from the Commission to the Parliament, the Council and the European Economic and Social Committee on the implementation of the 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), COM(2018) 40 final (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:40:FIN).

327 On the shortcomings of collective redress in the EU and the need for a uniform framework of law in the field of data protection, see L. JANČIŪTĖ, *Data protection and the construction of collective redress in Europe: exploring challenges and opportunities* (February 27, 2018). Available at: https://ssrn.com/abstract=3136040 (accessed 15.8.2018).

328 Most recently, on the 11th of April 2018, the European Parliament and the Council passed a proposal for a directive on representative actions for protection of the collective interests of consumers, which should cover «a variety of areas such as data protection». See Recital (6) Proposal for a Directive of the European Parliament and of the Council on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC, COM(2018) 184 final (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0184).

329 See M. BRKAN, *Data protection and European private international law: observing a bull in a China shop*, in *International Data Privacy Law*, p. 273.

provision is determined by the defendant (a controller or processor) and regardless of who the claimant is[330]. Furthermore, Art 80(1) GDPR provides that the NGO may exercise the right to receive compensation on behalf of data subjects, whilst Art 82(6) of the regulation provides that proceedings for exercising such right shall be instituted in the MS courts referred to in Art 79(2) of the same regulation. Hence, the combined reading of Art 80(1) and 82(6) GDPR further suggests that Art 79(2) of the regulation might be applicable where the NGO is appointed by the data subjects to seek compensation on their behalf.[331]

If so, where data subjects have their habitual residence in the same MS, Art 79(2) GDPR should allow the NGO to sue either before the courts of that MS or those of the MS where the controller has an establishment, provided that – it must be recalled – the laws of such MSs permit collective actions. Instead, in the case where the data subjects have their habitual residence in different MSs, the NGO they have appointed should be allowed to sue on their behalf only in the courts of the MSs where the controller has an establishment, since the courts of the MS where only part of the data subjects have their habitual residence would be lacking jurisdiction with respect to the rest of them.

What follows from the above is also that, where data subjects acting collectively have their habitual residence in different MSs, Art 79(2) GDPR could provide the appointed NGO with just one forum, that of the MS where the controller has an establishment, as far as – once again – the laws of such MS permit collective actions.

If this is correct and if Art 79(2) GDPR were the only applicable head of jurisdiction in similar cases, a controller could prevent the risk of being the subject of a collective action brought by an NGO appointed by data subjects habitually residing in different MS, by placing its one and only establishment in a MS where collective claims are not permitted or difficult to be pursued.

But Art 79(2) GDPR should not be the only head of jurisdiction NGOs should be able to rely on. NGOs should also be allowed to sue in the courts of the MSs having jurisdiction under Art 4(1) and 7(2) B1R. In fact, though also heads of jurisdiction of the B1R are ill-suited for collective actions, the two provisions of the latter regulation allow several claimants to sue one or more defendants in the courts of the same MS simultaneously[332].

330 See also Recital (145) GDPR, which refers to the «plaintiff», rather than to the «data subject».

331 On the contrary, as underlined by Lein, the head of jurisdiction over consumer contracts in Art 19 B1R is «lost in cases in which an association or representative is acting for the consumers». In fact, the CJEU holds that the head of jurisdiction applies only where the consumer is, «in his personal capacity, the plaintiff or defendant», provided that, in accordance with the wording of Art 16 Reg. (EC) No 44/2001 (today, Art 19 B1R), the provision applies «only to an action brought by a consumer against the other party to the contract, which necessarily implies that a contract has been concluded by the consumer with the trader or professional concerned». Nonetheless, there are strong reasons why the rule on jurisdiction should be opened to class actions. See, respectively, E. LEIN, *Cross-Border Collective Redress and Jurisdiction under Brussels I: A Mismatch*, in D. FAIRGRIEVE, E. LEIN (eds.), *Extraterritoriality and Collective Redress*, Oxford, 2012, p. 135; CJEU, 25.1.2018, C-498/16, *Maximilian Schrems v Facebook Ireland Limited*, ECLI:EU:C:2018:37, points 44 and 45 and the case law cited therein (http://curia.europa.eu/juris/document/document.jsf?text=&docid=198764&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3530052); M. MORANI, *L'azione di classe in Europa, aspettando la Corte di giustizia europea sul caso Schrems vs. Facebook*, in *Int'l Lis*, 2016.

332 See A. STRADLER, *The Commission's Recommendation on Common Principles of Collective Redress and Private International Law,* in E. LEIN, D. FIRGRIEVE, M. OTERO CRESPO, V. SMITH (eds.), *Collective Redress in Europe – Why and How?*, London, 2015, p. 242 ff; E. LEIN, *Cross-Border Collective Redress and Jurisdiction under Brussels I: A*

The reason why NGOs should be allowed to bring collective claims also in the courts mentioned in Arts 4(1) and 7(2) B1R is that, on the contrary, the controller could resort to a greater number of MS courts, where to file an action seeking a declaration of non-liability under Art 7(2) B1R[333].

Conversely, it is submitted that rules on the coordination of jurisdiction set forth in the B1R based on the principle of temporal priority do not «provide adequate solutions» in mass harm situations, where «there is a high probability that [such situations] will be picked up by various representative associations or claimants in different Member States»[334].

In similar situations, where harm results from the same infringement of the GDPR, if the general rules of the B1R were applicable, the instituting of proceedings by a single data subject or NGO in the courts of a Member State could block the proceedings instituted by the other injured data subjects or Art 80(1) GDPR NGOs in the courts of a different MS. The data subjects or Art 80(1) GDPR NGOs would be tripping themselves… Furthermore, if such general rules were deemed applicable, controllers could be encouraged to practice "forum running": to sue first in the most favorable courts and block any following proceeding instituted by the data subjects or NGOs in a different MS.

Hence, in mass harm situations, a rule bestowing discretion upon the Member State courts second seised, such as that in Art 81 GDPR, appears to be consistent with the protective policy underlying the regulation, as well as a more appropriate rule in mass harm situations[335]. Besides, Art 81 GDPR, addresses the risk of conflicting decisions adequately, by placing on the MS court second seised the duty to take contacts with the MS court first seised.

This is the reasons why, a part from the far reaching wording employed in Art 81 GDPR, Arts 29 and 30 B1R should be no longer deemed applicable where multiple proceedings concern the processing by the same controller.

6. The parallel application of the heads of jurisdiction of the GDPR and those of the B1R might be a "forensic nightmare", but it should be endorsed to the largest extent possible.

Most of the issues examined above appear to be the result of a drafting shortcoming in Art 79(2) GDPR: unlike protective heads of jurisdiction of the B1R, the provision does not deal with jurisdiction over actions brought by the stronger party, the controller. As a consequence, provided that the controller may rely on the rules of the B1R, the data subject should be allowed to rely on the same rules too. If otherwise, especially in the case of actions in tort and those brought by NGOs, there is a risk that the data subjects may resort to a lower number of MS courts than those made available to the controller, and this would be inconsistent with the protective policy underlying the GDPR.

Mismatch, p. 132 ff.

333 This is true to the extent that it is submitted that the jurisdictional favor that reflects the protective policy underlying the GDPR also concerns NGOs.

334 A. STADLER, *Focus on Collective Redress: Cross-border Problems*. Available at https://www.collectiveredress.org/collective-border-problems (accessed 15.8.2018). See also ID, *The Commission's Recommendation*, p. 247-248.

335 But see A. BARLETTA, *La tutela effettiva della privacy nello spazio (giudiziario) europeo nel tempo (della "aterittorialità") di internet*, p. 1199.

Conversely, since they appear to be inadequate in mass harm situation, in cases where multiple proceedings concern the processing by the same controller, rules on the coordination of such proceedings provided for in the B1R should no longer be deemed applicable.

In conclusion, though criticized by most scholars, yet the jurisdictional rules of the GDPR represent an effort that must be praised, in that they are the first known uniform rules that govern jurisdiction over civil and commercial claims in matters relating to the right to data protection.

ENNIO PIOVESANI