UDK 342.7:341.9]:004
Original scientific paper

PRIVATE INTERNATIONAL LAW AS A MEANS TO PROJECT EU DIGITAL VALUES ABROAD*

Edoardo Benvenuti, PhD, Postdoctoral Fellow
University of Milan, Department of International,
Legal, Historical and Political Studies
Via Conservatorio 7, 20 122 Milan, Italy
edoardo.benvenuti@unimi.it

ABSTRACT

In light of the pivotal role that new technologies play for the achievement of policy objectives, and considering their ability to negatively affect rights and freedoms in a ubiquitous manner, EU law is adopting a number of instruments to regulate those matters that are particularly influenced by digitalisation. Such instruments include substantive rules applicable to several online activities. This legislation aims at establishing an environment where digital interactions take place in accordance with fundamental rights, whose protection is enshrined within EU primary law, as well as to ensure the proper functioning of the internal market. Given the ubiquitous nature of digital technologies, and in order for these rules to be effective, their scope of application is designed to also include cases that may be strongly related to Third States. In this way, the EU aims at strengthening its digital sovereignty by creating a strong digital single market, and by guaranteeing the protection of European users, whose rights should benefit from the protection of EU substantive law even when digital activities take place abroad.

Although the EU has a strong interest in ensuring a broad application of its substantive rules, the possibility for EU law to be concretely applicable abroad depends – in the first place – on the existence of jurisdictional rules specifically designed to apply to disputes that may involve parties from Third States. Nonetheless, while some of the instruments adopted in this area ensure the application of substantive rules by providing for specific grounds of jurisdiction, litigation in these matters will normally fall within the scope of Regulation (EU) n. 1215/2012, whose rules apply – in general – only when the defendant has her/his domicile in the Union.

In light of these considerations, the paper will assess the coherence between the broad scope of some of the instruments that the EU has adopted (or is going to adopt) in fields strongly affected by digitalisation – such as the GDPR, as well as other EU's initiatives pertaining to Artificial

* This paper is co-funded by the Erasmus+ Programme of the European Union. The paper reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Intelligence and to digital platforms – and Regulation (EU) n. 1215/2012, in order to evaluate the ability of the latter to support the application of EU digital standards world-wide.

***Keywords**: Digitalisation, online infringement, personality rights, private international law, jurisdiction, Third States*

1. INTRODUCTION

In a number of fields, the European Union (EU) is promoting the dissemination of its policies world-wide.[1] Such phenomenon has been analysed by scholars, who distinguished (at least) two main "techniques", through which the EU is – *de facto* – exercising its regulatory power globally.[2]

On the one hand, the European legislature is adopting substantive rules that are designed to apply when a territorial link with the EU is established, for example, by virtue of activities that, although carried out in a Third State, produce their effects within the Union.[3] On the other hand, the EU does not impose the unilateral application of its rules, but it rather creates incentives that encourage foreign companies to voluntarily adhere to its standards in order for them to operate in the European market.[4]

EU's inclination to act as a "global regulator" is justified by multiple reasons, one of the main causes of the spread of EU values abroad being related to digitalisation. As a matter of fact, digital technologies contribute to create an environment where interactions are dematerialised, and where the principle of territoriality cannot be applied according to its traditional meaning.[5] Moreover, in light of their ubiquitous nature, digital activities and operations that avail themselves of sophisticated technologies are particularly insidious, as they can easily impair fundamental rights, whose protection is enshrined within EU primary law.[6] These circumstances make the need to control and regulate foreign activities even more urgent.

Due to its peculiar features, digitalisation affects the concept of jurisdiction on at least two levels.

---

1 On this topic, see Cremona, M.; Scott, J. (eds.), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*, Oxford, 2019.

2 See Scott, J., *Extraterritoriality and Territorial Extension in EU Law*, The American Journal of Comparative Law, Vol. 62, No. 1, 2014, pp. 87–125; Bradford, A., *The Brussels Effect: How the European Union Rules the World*, New York, 2020.

3 This is the so called "territorial extension" of EU law, on which see Scott, *op. cit.*, note 2.

4 See Bradford, *op. cit.*, note 2.

5 See Chia, C. W., *Sketching the Margins of a Borderless World: Examining the Relevance of Territoriality for Internet Jurisdiction*, Singapore Academy of Law Journal, Vol. 30, No. 2, 2018, pp. 833–870.

6 Charter of Fundamental Rights of the European Union [2016] OJ C 202/389 (CFREU).

In the first place, the non-territorial nature of the Internet imposes adjustments in the application of rules regulating activities that take place online. The scope of the instruments adopted by the EU in this field must necessarily include activities that, while not taking place in the Member States, are likely to compromise EU's interests. Accordingly, EU law in this field is designed to apply not only to persons and undertakings operating from the Union, but also to those that, albeit located in Third States, direct their activities to Member States through the Internet or by means of digital technologies.

Secondly, the non-territorial nature of the Internet affects the issue of jurisdiction from the perspective of private international law (PIL). Indeed, the concrete application of EU standards to companies and persons located abroad depends on the possibility to enforce the rights enshrined in EU law (even) when one of the parties to a dispute is domiciled in a non-EU State. Thus, rules on jurisdiction have paramount importance: the law applicable to transnational litigations is determined through the conflict-of-laws rules of the forum; consequently, the existence of rules on jurisdiction specifically designed to attract this kind of disputes before a court in a Member State has a key-role in ensuring the application of EU rules when activities taking place abroad are involved. From this point of view, PIL is an important tool for the regulation of matters strongly affected by digitalisation, as it contributes to the projection of EU digital values abroad.[7]

In light of these considerations, the present paper aims at assessing the role of EU PIL in regulating online activities and in projecting EU policies and values pertaining to digital matters abroad. For this purpose, I will take into account some of the main instruments that the EU has adopted (or that it is going to adopt) in digital matters. Since the scope of such instruments normally transcends Member States' borders, I will evaluate the ability of EU rules on adjudicative jurisdiction to support the "extraterritorial" application of EU substantive rules in this field.

2. THE "EXTRATERRITORIAL" SCOPE OF EU POLICIES IN DIGITAL MATTERS

Due to the paramount relevance of the interests that are normally at stake in matters affected by digitalisation, the main concern of each legal system is to ensure

[7] In relation to the potential role of PIL in contributing to the regulation of matters related to the Internet, see Lutzi, T., *Private Ordering, the Platform Economy, and the Regulatory Potential of Private International Law*, in: Pretelli, I. (eds.), Conflict of Laws in the Maze of Digital Platforms/ Le Droit International Privé Dans le Labyrinthe des Plateformes Digitales, Zürich, 2018, pp. 129–145; Pretelli, I., *Protecting Digital Platform Users by Means of Private International Law*, Cuadernos de Derecho Transnacional, Vol. 13, No. 1, 2021, pp. 574–585.

the application of its own standards with respect to activities that might undermine those values. In fact, in regulating this field, States may give relevance to different policies; as a consequence, the conclusion of international agreements pertaining to this area of law appears to be a difficult outcome to achieve, since each Country will try to prioritise its own policies during the drafting process. Under this perspective, the unilateral adoption of substantive rules with a broad territorial scope thus remains the preferable solution, especially when digital activities risk impairing fundamental rights.

The need to ensure the protection of fundamental rights with respect to activities incorporating high-tech features is especially evident when it comes to data protection law: while the European approach pays special attention to the protection of personal data,[8] other legal systems give priority to different policies or do not ensure natural persons a level of protection that is sufficiently high according to EU standards.[9]

However, data protection law is not the only example of how the EU displays the ambition to spread its digital values in Third States, as the European legislature adopted (and is going to adopt) a number of acts that are meant to apply not only within the Union, but also abroad. In fact, the scope of application of this legislation goes beyond the borders of the Member States, and it is usually defined according to criteria that, although territorial in nature, end up triggering a sort of extraterritorial effect. These rules may then be relevant not only in perfectly intra-EU cases, but also when the proceedings are brought against subjects that are not based nor operate within the Union.

---

8 At the Council of Europe level, the protection of personal data has been essentially pursued through Art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11, 14 and 15, 4 November 1950, ETS 5 (ECHR), as well as through the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, ETS No. 108; with respect to the application of Art. 8 ECHR in the field of data protection, see, *inter alia*, judgment *Amann v Switzerland* (2000) 30 EHRR 843. At the EU level, the need to ensure the protection of personal data not only stems from EU secondary law instruments, but it is also enshrined in Art. 8 CFREU. Moreover, Art. 16 TFEU (Treaty on the Functioning of the European Union [2007] OJ C 326/01) empowers the European Parliament and the Council to lay down the rules relating to the protection of individuals with regard to the processing of personal data. On the protection of personal data according to the European approach, see Vogiatzoglou, P.; Valcke, P., *Two decades of Article 8 CFR: A critical exploration of the fundamental right to data protection in EU law*, in: Kosta, E.; Kamara, I.; Leenes, R. (eds.), Research Handbook on EU Data Protection Law, Northampton, 2022, pp. 11–49.

9 See, in particular, the judgment of the Court of Justice of the EU (CJEU) in Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* [2020] not yet published.

2.1. The scope of EU data protection law

Within the framework of EU law, the matter at stake is currently regulated by the General Data Protection Regulation (GDPR),[10] which repealed the Data Protection Directive.[11] In line with the abrogated instrument, the GDPR aims at removing the obstacles to flows of personal data within the EU by creating a level of protection of the rights and freedoms of natural persons with regard to the processing of their personal data that is equivalent in all Member States.[12] The protection of natural persons in relation to the processing of their personal data is thus a policy objective that is not only relevant not only for its implication on human rights, as it is also instrumental in guaranteeing the proper functioning of the internal market. Under this perspective, the adoption of a Regulation in this field – which is, in principle, directly binding in all its parts[13] – is aimed at ensuring a greater level of harmonisation within the EU, since the margin of appreciation left to the Member States in the implementation of the Data Protection Directive was addressed as one of the main shortcomings of the previous regime in reaching the aforementioned goals.[14]

In order to achieve such goals, EU legislation in this field is conceived not only to apply to data processing that is entirely conducted in a Member State. Under this perspective, the Regulation reproduces the tripartite division adopted by the Directive, even though the GDPR's scope of application is shaped according to elements that partially diverge from those employed in the context of the Data Protection Directive,[15] as the Regulation was specifically designed to have a wide

---

10 Regulation (EU) 2016/679 of the European Parliament and of the Council 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 [2016] OJ L 119/1 (General Data Protection Regulation).

11 Directive 95/46/EC 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 [1995] OJ L 281/31 (Data Protection Directive).

12 In particular, see Recital 10 of the GDPR.

13 Nonetheless, it has been pointed out that the GDPR still leaves room for manoeuvre for Member States, since several aspects of its implementation require the intervention of national legislators in order to regulate specific issues of the data protection regime. This situation, together with the lack of an explicit conflict-of-laws rule, open up to possible private international law challenges. On this topic, see Mantovani, M., *Horizontal Conflicts of Member States' GDPR-Complementing Laws: The Quest for a Viable Conflict-of-Laws Solution*, Rivista di diritto internazionale privato e processuale, Vol. 55, No. 3, 2019, pp. 535–562.

14 See Hustinx, P., *EU Data Protection Law: The Review of Directive 95/46/CE and the General Data Protection Regulation*, in: Cremona, M. (ed.), New Technologies and EU Law, Oxford, 2017, pp. 148–151.

15 De Miguel Asensio, P., *Conflict of Laws and the Internet*, Cheltenham and Northampton, 2020, pp. 134–135.

international dimension.[16] As a result, it was suggested that the adoption of the GDPR would have been an opportunity to expand the scope of application of EU data protection law, as to ensure the coherent application of EU standards against both EU based and non-EU based undertakings, thus leading to benefits in terms of fair competition.[17]

First, according to Art. 3(1) of the GDPR, non-EU undertakings can be subject to the application of the Regulation when they are considered to have an establishment in one or more Member States.[18] Such evaluation should be carried out *in concreto*, and in light of the rather broad terms defined by the CJEU with regard to the criteria set forth in the Directive. Notably, in *Google Spain*, the CJEU gave an extensive interpretation of Art. 4(1)(a), according to which national provisions adopted pursuant to the Data Protection Directive applied to the processing of personal data "where the processing (was) carried out in the context of the activities of an establishment of the controller on the territory of (a) Member State".[19] In this regard, the CJEU focused on the meaning of the expression "an establishment", and adopted a teleological interpretation of the criterion in order to ensure the achievement of the human rights goals set forth in the Data Protection Directive.[20] Accordingly, the CJEU stated that the processing of personal data for the purposes of the service of a search engine having its seat in a Third State and an establishment in a Member State was carried out "in the context of the activities" of that establishment, even when the latter was not directly involved in the processing activities but it only carried out marketing activities in order to make

16 Hustinx, P., *op.cit.*, note 14, p. 155.

17 Redic, V., *The EU data protection Regulation: Promoting technological innovation and safeguarding citizens' rights*, 2014, [https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_14_175], Accessed 24 July 2023. See also European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), adopted on 16 November 2018 (version 2.1 of 7 January 2020), p. 4.

18 See Art. 3(1) of the GDPR, which states that the Regulation "applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not". Interestingly, Art. 4 of the GDPR (headed "Definitions") does not provide a definition of "establishment" for the purpose of Art. 3(1), as Art.4(16) only defines the notion of "main establishment", which is mainly relevant in order to determine the competence of the lead supervisory authority according to Art. 56 of the GDPR. Nonetheless, some clarifications with regard to the definition of "establishment" are provide by Recital22 of the GDPR, which substantially reproduces the wording of the abovementioned CJEU's case-law.

19 It is worth noting that, in addition to the "establishment" criterion, Art. 3(3) of the GDPR confirms the application of EU data protection law also when the processing takes place where Member State law applies by virtue of public international law, which was first incorporated in Art. 4(1)(b).

20 de Hert, P.; Czerniawski, M., *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context*, International Data Privacy Law, Vol. 6, No. 3, 2016,, pp. 234–235.

the service offered by that engine profitable.[21] In the CJEU's view, such conclusion was justified in light of the paramount importance of the right to privacy, which imposed to not interpret the wordings of Art. 4(1)(a) restrictively.[22]

Moreover, if it is not possible to include a non-EU controller or processor within the scope of EU data protection law through Art. 3(1) of the GDPR, it is possible to refer to other criteria set forth in the Regulation.[23] In particular, while Art. 4(1)(c) of the Data Protection Directive adopted the location of the equipment as a criterion to determine the application of EU law against controllers not established in the Union,[24] the GDPR's approach is shaped on the basis of a targeting test. In fact, Art. 3(2) states that the Regulation also applies "to the processing of

---

21 Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzále* [2014] published in the electronic Reports of Cases, par. 55. See also Case C-230/14 *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* [2015] published in the electronic Reports of Cases, paras. 19–41, in which the Court stated that a controller that exercises, through stable arrangements in a Member State, a real and effective activity in the context of which the processing is carried out, will be considered to have an "establishment" in that Member State, even when such activity appears to be "minimal" in the context of the processing of data. Such interpretation applies even when the controller is registered in a different Member State or in a Third State.

22 Case C-131/12 *Google Spain and Google*, note 21, par. 53. In several occasions the CJEU recalled that the protection of fundamental rights represented the guiding principle through which it developed its case-law concerning the (broad) scope of the Data Protection Directive (see, *ex multis*, Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* [2018] published in the electronic Reports of Cases, par. 26).

23 See European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), adopted on 16 November 2018 (version 2.1 of 7 January 2020), p. 9.

24 According to Art. 4(1)(c), national provisions adopted by Member States pursuant to the Directive applied where the controller, albeit not established in the EU, processed personal data making use of equipment, automated or otherwise, situated on the territory of a Member State, unless such equipment was used only for purposes of transit through the territory of the Union. See also Recital 20 of the Directive, according to which "Whereas 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" (emphasis added). Even though some scholars emphasised the terminological shift from the term "means" of the Recital20 to the term "equipment" of Art. 4(1)(c), addressing that it represented the attempt of the EU legislature to narrow the scope of Art. 4(1)(c).(see Moerel, L., *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?*, International Data Privacy Law, Vol. 1, No. 1, 2011, p. 33), such a reading collided with the case-law of the CJEU on Art. 4, as well as with the interpretation suggested by the Article 29 Data Protection Working Party, according to which the term "equipment" should have been understood in broad terms (Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law, adopted on 16 December 2010, 0836-02/10/EN, WP 179, p. 19). The meaning of the term "equipment" could have been clarified by the CJEU in *Rease and Wullems*, but the case was dismissed (Case C-192/15, *T. D. Rease and P. Wullems v College bescherming persoonsgegevens* [2015] OJ C78/11). On this topic, see de Hert, P.; Czerniawski, M., *op.cit.*, note 20, p. 236.

personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (i) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union;[25] or (ii) the monitoring of their behaviour as far as their behaviour takes place within the Union".[26] The declared intention of the targeting test incorporated in Art. 3(2) of the GDPR is to ensure the protection of natural persons according to the provisions enshrined therein.[27]

This approach appears to be consistent with the criteria that, according to public international law, justify the extraterritorial intervention of a given legal system, since EU jurisdiction against processing activities by controllers or processors that are not established in a Member State is only triggered where those activities are in some way connected to the EU.[28] Accordingly, the extension of the scope of application of EU data protection law, which represents an important rationale of the reform,[29] has been pursued by requiring some sort of territorial link between the processing activities and the EU.[30] In fact, on the one hand, Art. 3(1) ensures that the territorial application of the GDPR against a non-EU controller/processor is triggered by the presence in the Union of an "establishment" in the context of whose activities the processing is carried out, while the place where the processing is carried out and the geographical location of data subjects are not relevant for the purpose of Art 3(1);[31] on the other, Art. 3(2) employs a targeting test that gives relevance to the presence of data subjects within the EU, in order to ensure the effective protection of fundamental rights.

---

25 Art. 3(2)(a) of the GDPR.

26 Art. 3(2)(b) of the GDPR.

27 Recital 23 of the GDPR.

28 De Miguel Asensio, P., *op. cit.*, note 15, p. 135. The importance of public international law restrictions in this field has also been underlined by the Commission in its amicus brief released in relation to the *Microsoft Warrant* case (European Commission amicus brief, *United States v Microsoft Corporation* [2017] No. 17-2, pp. 5–8). On this point, see Svantesson, D. J. B., *Article 3. Territorial scope*, in: Kuner, C.; Bygrave, L. A.; Docksey, C. (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford, 2020, pp. 76–77.

29 See note 17.

30 Svantesson, D. J. B., *op. cit.*, note 28, p. 76.

31 See European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), adopted on 16 November 2018 (version 2.1 of 7 January 2020), p. 14, that underlines that this approach is supported by Recital 14 of the GDPR, which states that "The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data".

2.2. The scope of EU's approach to Artificial Intelligence

The EU Commission is currently working on the adoption of several instruments in the field of Artificial Intelligence (AI), which are meant to benefits the internal market by regulating a framework on the usage of AI-systems, in order to foster the free movement of AI-based goods and services cross-border while ensuring a high level of protection of health, safety and fundamental rights. In light of both the policy objectives underlying this legislation and the possible cross-border impacts of the employment of AI-systems, the proposed instruments are likely to apply in situations involving actors established outside the EU.

More specifically, the proposed Artificial Intelligence Act (AI Act Proposal)[32] – which aims at imposing obligations for several actors in the value chain – strives to have a manifestly broad scope, since it proposes to apply to providers placing on the market or putting into service AI-systems in the Union, irrespective of whether those providers are physically present or established within the Union (Art. 2(1)(a)), as well as to users located in the EU (Art. 2(1)(b)).[33] Moreover, according to Art. 2(1)(c), the proposed legislation "should also apply to providers and users of AI-systems that are established in a third country, to the extent the output produced by those systems is used in the Union".[34]

However, as regards the AI Act Proposal, it has been pointed out that some aspects of its scope are vague; in particular, with regard to Art. 2(1)(b), it is not clear whether a temporary presence of the user on the territory of a Member State is sufficient to trigger the application of EU law.[35] Such uncertainties are not completely clarified by the amendments proposed by the EU Parliament,[36] which include new rules pertaining to the scope of application of the AI Act Proposal that – to some extent – appear as vague as those enshrined in the Commission's proposal.

---

32 Proposal for a Regulation of the European Parliament and of the council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM(2021) 206 final (AI Act Proposal).

33 See Recital 10 of the AI Act Proposal, underlining that the Regulation should apply in a non-discriminatory manner to providers of AI-systems, irrespective of whether they are established within the Union or in a third country, and to users of AI-systems established within the Union.

34 See Recital 11.

35 See Pato, A., *The EU's Upcoming Framework on Artificial Intelligence and its Impact on PIL*, 12 July 2021 [https://eapil.org/2021/07/12/the-eus-upcoming-regulatory-framework-on-artificial-intelligence-and-its-impact-on-pil/], Accessed 24 July 2023.

36 Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD).

In particular, on the one hand, the amendments aim at changing the aforementioned Art. 2(1)(b) of the AI Act by referring to "deployers" (and not "users") of AI systems that have their place of establishment or who are located within the EU; on the other, (new) Art. 2(1)(cc) states that the Regulation will apply to "affected persons" – as defined in Art. 3(8a)[37] – "that are located in the Union and whose health, safety or fundamental rights are adversely impacted by the use of an AI system that is placed on the market or put into service within the Union".[38] Once again, the latter amendment not only omits to clarify whether a temporary presence on the EU territory is sufficient to trigger the application of the AI Act, but it also refers to concepts – like the one to the "adverse impact" – that are not clearly defined and whose contours are blurred.

Since the AI Act Proposal concerns the public interest, the infringements of its rules may raise issues that appear to pertain mostly to administrative law.[39] Thus, the lack of provisions in the area of private international law is not a surprise. Nonetheless, the proposed instrument plays a pivotal role in the identification of EU policies and definitions in this field; moreover, the instrument's broad scope of application shows that – in order for these policies to be concretely implemented – compliance with EU standards should be ensured at a global level.

Accordingly, the Union is working on the implementation of these policies also from the angle of civil liability. In particular, in 2022, the EU Commission proposed to adopt the Artificial Intelligence Liability Directive (AI Liability Directive Proposal)[40] and to revise the Product Liability Directive,[41] as to make the latter instrument resilient to technological progress.[42] The two instruments follow the

---

37 According to the proposed Art. 3(8a), "'affected person' means any natural person or group of persons who are subject to or otherwise affected by an AI system".

38 In particular, according to the amendments of the EU Parliament, the AI Act should apply to "providers placing on the market or putting into service AI systems referred to in Article 5 outside the Union where the provider or distributor of such systems is located within the Union" (Art. 2(1)(ca)), as well as to "importers and distributors of AI systems as well as authorised representatives of providers of AI systems, where such importers, distributors or authorised representatives have their establishment or are located in the Union" (Art. 2(1)(cb)).

39 With regard to private international law issues within the framework of the AI Act Proposal, see Pato, A., *op. cit.*, note 35.

40 Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 final (AI Liability Directive Proposal).

41 Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products [1985] OJ L 210/29 (Product Liability Directive)

42 Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM(2022) 495 final.

EU Parliament's Resolution of 20 October 2020 with recommendations on the adoption of a Regulation on Liability for the Operation of Artificial Intelligence-Systems,[43] which intended to provide a liability regime for AI-related harms by distinguishing between "high-risk AI-systems" (subject to a strict liability mechanism), and "other AI-systems" (subject to a fault-based liability regime).[44] The proposed Directives aim at ensuring the adoption of harmonised rules in the field of civil liability for damages caused by the usage of AI-systems in order to complement the obligations set forth in the AI Regulation Proposal.[45] More specifically, they aim at ensuring the proper functioning of the internal market by: (i) guaranteeing the injured persons the respect of their right to compensation; (ii) increasing the legal certainty about the liability risks that businesses face when doing business; (iii) promoting consumer trust in AI-enabled products and services.

In particular, and in order to ensure the achievement of the aforementioned goals, the AI Liability Directive Proposal intends to increase the changes of successfully obtain redress by providing a system of rebuttable presumptions (Art. 4) and mechanisms on disclosure of evidence aimed at favouring the victims of AI-related harms (Art. 3). For its part, the proposed amendments to the Product Liability Directive clarifies that goods incorporating an AI-system are "products", and that compensation is available when defective AI causes damage, without the injured person having to prove the manufacturer's fault, just like for any other product.

Like the GDPR and the Online Platform Regulation, the proposed legislation aims at applying against non-EU subjects; accordingly, the scope of EU's approach to AI is defined in a broad (and sometimes unclear) manner.

In particular, the territorial scope of the Regulation proposal attached to the EU Parliament's Resolution was defined in light of criteria that appear to be vague; namely, according to Art. 2(1), the application of the proposed instrument is triggered when AI-systems "caused significant immaterial harm resulting in a verifiable economic loss" in the EU, Without further specifying these notions.[46] Thus, the instrument attached to the Parliament's resolution actually defined its scope of

---

43 European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)) (AI Liability Regime Resolution).

44 See Chamberlain, J., *The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective*, European Journal of Risk Regulation, Vol. 14, No. 1, 2023, pp. 9–12.

45 See Recital 2 of the AI Liability Directive Proposal.

46 On this point, see Poesen, M., *Regulating Artificial Intelligence (AI) in the European Union (EU): Exploring the Role of Private International Law*, X, Recht in beweging – 29ste VRG-Alumnidag 2022, 2022, par. II.2 [Available at SSRN: https://ssrn.com/abstract=3959643 or http://dx.doi.org/10.2139/ssrn.3959643].

application by referring to the criterion of damage, albeit in vague and imprecise terms; this solution would have allowed for the application of the liability rules even to persons domiciled in a Third State.

Similarly, the AI Liability Directive Proposal, as well as the amendments concerning the Product Liability Directive, aims at applying even when some of the subjects within the supply chain are not established in the EU.

As regards the AI Liability Directive Proposal, Art. 1(2) clarifies that it applies to non-contractual fault-based civil law claims for damages caused by an AI system, i.e. regimes that provide for a statutory responsibility to compensate for damage caused intentionally or by a negligent act or omission. The aforementioned AI Act Proposal will play a pivotal role in the identification of the Directive's scope of application. In fact, in order to ensure the coherent application of the proposed legislation, the scope of the AI Liability Directive Proposal is defined according to the definitions provided in the AI Act Proposal,[47] which includes – to some extent – operators and users established outside the EU.[48]

Yet, the approach followed in the field of product liability is slightly different. As a matter of fact, the amendments concerning the Product Liability Directive identify several economic operators – other than the manufacturer – who can be held liable in the event that the manufacturer is established in a Third State (Art. 7).[49] As a matter of fact, the proposed instrument aims at ensuring that "there is always a business based in the EU that can be held liable for defective products bought directly from manufacturers outside the EU, in light of the increasing trend for consumers to purchase products directly from non-EU countries without there being a manufacturer or importer based in the EU".[50] In this way, the issue of the direct application of EU rules against non-EU subjects is (at least in part) circumvented, as the amendments define a series of economic operators in order to enable victims of damages caused by AI-products to file a claim before the authorities of a Member State. Nonetheless, the proposal confirms the EU's tendency to

47 See Recital 26, Art. 2(3) and Art. 2(4) of the AI Liability Directive Proposal.

48 See note 34.

49 See also Recital 27, stating that "In order to ensure that injured persons have an enforceable claim for compensation where a manufacturer is established outside the Union, it should be possible to hold the importer of the product and the authorised representative of the manufacturer liable".

50 See the explanatory memorandum attached to the Proposal, p. 2.

act as a "global regulator", since it aims at affecting non-EU undertakings too,[51] namely in light of the phenomenon known among scholars as "Brussels effect".[52]

2.3. The scope of EU's initiatives in the field of digital platforms

EU's legal instruments and initiatives in matters affected by digital technologies are numerous, and it is not possible to analysed all of them in this contribution. Nonetheless, it seems appropriate to recall, at least, two initiatives undertaken by the European legislature in the field of digital platform: the Regulation (EU) 2019/1150 (Online Platforms Regulation),[53] which regulates the relationship between platforms that provide online intermediation services and businesses using such platforms to supply products or services to consumers, and the Platform Workers Directive Proposal.[54]

The overall objective of the first instrument is to contribute to the proper functioning of the internal market by laying down rules to ensure that business users are granted appropriate transparency, fairness and effective redress possibilities.[55] In particular, given the increased dependence of undertakings that use intermediation services to reach consumers, the providers of those services might have superior bargaining power, enabling them to behave "in a way that can be unfair and that can be harmful to the legitimate interests of their businesses users and, indirectly, also of consumers in the Union".[56]

In order for the instrument to be effective, its scope of application is designed in light of the de-materialised nature of the Internet,[57] as well as of the "intrinsic cross-border potential" of the intermediation services and the transactions that such services aim at facilitating.[58] Accordingly, the Regulation applies to online intermediation services and online search engines "irrespective of the place of es-

---

51 *Ibid.*, p. 6, stating that the Directive "will also encourage all businesses, including non-EU manufacturers, to place only safe products on the EU market in order to avoid incurring liability. This will in turn reinforce product safety".

52 See note 4.

53 Regulation (EU) 2019/1150 of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services [2019] OJ L 186/57 (Online Platforms Regulation).

54 Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work, COM(2021) 762 (Platform Workers Directive Proposal).

55 Art. 1(1) of the Online Platform Regulation.

56 Recital 2 of the Online Platform Regulation.

57 See Recital 9 of the Online Platform Regulation, which emphasises the global dimension of online intermediation services and online search engines.

58 Recital 6 of the Online Platform Regulation.

tablishment or residence of the providers of those services and irrespective of the law otherwise applicable", as long as two cumulative conditions are met: (i) such platforms provide their services to business users established in the Union; and (ii) those business users offer goods and services to consumer located in the EU.[59] As a consequence, the Regulation applies to the relationship between a non-EU based platform operator and a business established in a Member State, as long as the latter makes usage of the former in order to trade with consumers who are located within the EU.

Like the GDPR, the criteria that define the territorial scope of the Online Platform Regulation are thus based on a targeting test, which responds to the ubiquitous features and means that are employed in this field by requesting a link between the activities that the Regulation intends to regulate and the EU; such link is based on the presence – within the EU's territory – of the businesses using the platforms and of the consumers.

Another example can be in the directive proposal that the EU Commission presented on 9 December 2021 in order to improve the working conditions of platform workers.[60] Such initiative aims at improving the protection of this type of workers "by ensuring correct determination of their employment status, by promoting transparency, fairness and accountability in algorithmic management in platform work and by improving transparency in platform work, including in cross-border situations" (Art. 1(1)).

With regard to the policy objectives underlying the proposed legislation, it can be observed that the Council 's General Approach on the Directive[61] clarified the objective scope of the future instrument, and strengthen the link between the platform workers' rights, data protection and AI.[62]

---

59 Art. 1(2) of the Online Platform Regulation. See also Recital 9, clarifying that this criterion should be interpreted in accordance with the relevant case-law of the CJEU on Art. 17(1)(c) of Brussels I-*bis* Regulation and Art. 6(1)(b) 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 (Rome I Regulation).

60 Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work, COM (2021) 762 (Platform Workers Directive Proposal).

61 General Approach adopted by the Council on 12 June 2023 on the Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work (Document ST_10758_2023_INIT).

62 See in particular Recital 29, 32, 37, 47 and Art. 1(1) of the proposal included in the General Approach, stating that "The purposes of this Directive are to improve the working conditions of workers and the protection of persons performing platform work, regarding the processing of their personal data through the use of automated monitoring or decision-making systems".

The final goal of the Platform Worker Directive Proposal is thus to prevent the use of digital technologies from impairing the working condition and the rights of the workers, as well to avoid that – by creating new business models and new forms of employment – platform work results in abuses, for example by enabling the employer to take advantage of the blurred boundaries between employment relationships and self-employed activities.[63]

Consistently with the need to ensure the protection of workers' rights, as well as the proper functioning of the internal market, the Platform Workers Directive aims at applying also to non-EU employers, as long as their activities have an impact on the EU market. Namely, according to Art. 1(3) of the Proposal attached to the Council's General Approach, the Directive is meant to apply "to persons performing platform work in the Union, to digital labour platforms organising platform work performed in the Union, irrespective of the platform's place of establishment and irrespective of the law otherwise applicable" (Art. 1(3))".[64]

The scope of the two initiatives in the field of digital platforms is thus consistent with the approach generally adopted by the European legislature in matters affected by digital technologies, as it is designed to transcend the borders of the EU's territory, in order to ensure the comprehensive and coherent application of EU law, as well as the complete achievement of EU's policy objectives.

3. EU RULES ON INTERNATIONAL JURISDICTION WITHIN THE CONTEXT OF ONLINE ACTIVITIES

As already mentioned, the unilateral adoption of legal instruments with a broad territorial scope is not sufficient to ensure the application of EU law in situations that are strongly connected to Third States. In fact, even though the recalled EU

---

63 See Recital 6 of the proposal included in the General Approach. In this regard, it should also be pointed out that the CJEU clarified that the status of "worker" within the meaning of EU law is an autonomous concept, as "the classification of a 'self-employed person' under national law does not prevent that person being classified as an employee within the meaning of EU law if his independence is merely notional, thereby disguising an employment relationship" (Case C-413/13 *FNV Kunsten Informatie en Media v Staat der Nederlanden* [2014] published in the electronic Reports of Cases, par. 35).

64 See Art. 1(2) of the Commission's Proposal (which the General Approach intends to abrogate), according to which the Directive "lays down minimum rights that apply to every person performing platform work in the Union who has, or who based on an assessment of facts may be deemed to have, an employment contract or employment relationship as defined by the law, collective agreements or practice in force in the Member States with consideration to the case-law of the Court of Justice. In accordance with Article 10, rights laid down in this Directive pertaining to the protection of natural persons in relation to the processing of personal data in the context of algorithmic management also apply to every person performing platform work in the Union who does not have an employment contract or employment relationship".

legislation defines the spatial scope of its rules according to criteria that include non-EU subjects or activities taking place abroad, the interest of the EU to apply its own rules extraterritorially might collide with the parallel interest of other legal systems to regulate the same situations according to policies that are divergent from those of the EU. As a consequence, in order to ensure the coherent application of EU law, it is not enough to expect non-EU undertakings to adhere to EU standards when their activities have a more tenuous connection with the European Union, but it is also fundamental to ensure that EU subjects have the opportunity to concretely enforce their rights against non-EU operators.

3.1. The "general" application of the Brussels I-bis Regulation to relationships presenting digital elements

Since the concrete application of a given legal act in cross-border cases requires the actual opportunity to seek a judicial remedy where the rights conferred under the act itself have been violated, it is apparent the connection between prescriptive and adjudicatory jurisdiction. Accordingly, several EU acts deal with adjudicatory jurisdiction in cross-border cases, and in particular the Brussels I-*bis* Regulation, which – among other things – lays down jurisdiction rules in the field of civil and commercial matters.[65]

The application of the Brussels I-*bis* Regulation is "general", since – in the lack of specific rules on international jurisdiction in other sectorial instruments of the EU – the grounds for jurisdiction enshrined therein apply to any proceedings in the field of civil and commercial law, as long as such proceedings fall outside the excluded matters that are listed in Art. 1 of the Regulation itself.[66] As a matter of fact, the notion of "civil and commercial matters" encompasses a great number of fields, among which data protection and, more generally, contractual and non-contractual relationships presenting a digital element; thus, the Brussels I-*bis* Regulation applies not only to proceedings in the field of data protection law,[67] but virtually to any civil claim originating from a digital infringement.

---

65 Regulation (EU) 1215/2012 of the European Parliament and of the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) [2012] OJ L 351/1.

66 Franzina, P., *Jurisdiction Regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, in: De Franceschi, A. (ed.), European Contract Law and the Digital Single Market. The Implications of the Digital Revolution, Cambridge, 2017, p. 87.

67 See Requejo Isidro, M., *Procedural Harmonization and Private Enforcement in the Area of Personal Data Protection*, MPILux Research Paper Series, No. 3, 2019, [Available at SSRN: https://ssrn.com/abstract=3339180 or http://dx.doi.org/10.2139/ssrn.3339180], section 3.2.1. See also Brkan, M., *Data*

Under the Brussels I-*bis* Regulation, a person (e.g. a data subject) who considers that his or her rights have been infringed by means of an unlawful activity presenting a digital element (e.g. a processing activity) may – in principle – sue the counterparty (e.g. the controller/processor) before the courts of multiple Member States, and in particular: (i) under Art. 4(1), in the place of domicile of the defendant;[68] (ii) under Art. 7(1), where the activity takes place in the context of the performance of a contract, in the place of performance of the obligation in question, as defined by the rule itself; (iii) under Art. 7(2), in matters relating to tort, delict or quasi-delict (including pre-contractual liability),[69] in the place where the harmful event occurred or may occur, with the clarification that such place includes both the place where the damage occurred and the place of the event giving rise to it,[70] notwithstanding the possibility for the victim of a personality right infringement to file a claim in the Member State where he/she has his/her centre of interests;[71] (iv) under Art. 7(5), with regard to a dispute arising out of the operations of a branch, agency or other establishment, in the place where the branch, agency or other establishment is situated; (v) under Art. 25, in the place indicated by the parties in a prorogation agreement (such jurisdiction shall be exclusive unless the parties have agreed otherwise); (vi) under Art. 18(1), where the plaintiff qualifies as a "consumer" according to the criteria listed in the Regulation itself, in the Member State of his or her domicile; and (vii) in matters relating to individual contracts of employment, in the courts for the place where or from where the employee habitually carries out his/her work or in the courts for the last place where he/she did (Art. 21(1)(b)(i)), or, if the employee does not or did not habitually carry out his/her work in any one country, in the courts for the place where the business which engaged the employee is or was situated (Art. 21(1)(b)(ii).

As a matter of fact, a great part of CJEU's case-law pertains to the adaptation of EU's rules on jurisdiction to the online context,[72] with particular regards to the

---

protection and European private international law: Observing a bull in a China shop, International Data Privacy Law, Vol. 5, No. 4, 2015, pp. 261–271.

68 While the domicile of natural persons is defined by the national rules of Member States, according to Art. 63 of the Brussels I-*bis* Regulation the domicile of a legal person corresponds – equally – to its statutory seat, its central administration, or its principal place of business.

69 Case C-334/00 *Fonderie Officine Meccaniche Tacconi SpA v Heinrich Wagner Sinto Maschinenfabrik GmbH (HWS)* [2002] ECR I-07357, par. 27.

70 Case C-21/76 *Handelskwekerij G. J. Bier BV v Mines de potasse d'Alsace SA* [1976] ECR 01735, par. 19. Moreover, come si preciserà immediatamente, the victim of a personality right infringement may file a claim – under Art. 7(2) – in the Member State where he/she has his/her centre of interests.

71 Joined Cases C-509/09 and C-161/10 *eDate Advertising GmbH and Others v X and Société MGN LIMITED* [2011] ECR I-10269 (see *infra*, note 73).

72 See Trooboff, P. D., *Globalization, Personal Jurisdiction and the Internet Responding to the Challenge of Adapting Settled Principles and Precedents*, Collected Courses of the Hague Academy of International

protection of personality rights.[73] In this last regard, the CJEU clarifies that – under Art. 7(2) of the Brussels I-*bis* Regulation – the victim of such infringements may sue the alleged tortfeasor for the entire damage not only in the Member State of the publisher's place of establishment,[74] but also in the Member State where the plaintiff has his or her centre of interests;[75] such place normally corresponds to the habitual residence of the victim, unless other factors, like "the pursuit of a professional activity" in a different Member State, "establish the existence of a particularly close link with that State".[76] The CJEU also clarified that the plaintiff may seek injunctive relief, as well as the rectification and the removal of content placed online, only before a court with jurisdiction to rule on the entire damage.[77]

Law, Vol. 415, 2021, pp. 137–248, and Marongiu Buonaiuti, F., *La giurisdizione nelle controversie relative alle attività on-line*, Diritto Mercato Tecnologia, Special Issue, 2017, pp. 107–117.

73 For a recent overview of CJEU's case-law in this field, see Svantesson, D.J.B.; Revolidis, I., *From eDate to Gtflix: Reflections on CJEU Case Law on Digital Torts under Art. 7(2) of the Brussels Ia Regulation, and How to Move Forward*, in: Alapantas, P.; Anthimos, A.; Arvanitakis, P. (eds.), National and International Legal Space - The Contribution of Prof. Konstantinos Kerameus in International Civil Procedure, Athens, 2022, pp. 319–371. On this topic, see also Márton, E., *Violations of Personality Rights through the Internet: Jurisdictional Issues under European Law*, Baden-Baden, 2016. The importance of PIL in regulating online infringements of personality rights has been also recalled at the international level by the Institut de Droit International (IDI), which highlighted the regulatory role ofPIL in this field in its 2019 resolution (Institut de Droit International, Resolution on Internet and the Infringement of Privacy: Issues of Jurisdiction, Applicable Law and Enforcement of Foreign Judgments, 2019 (2019 IDI Resolution) [https://www.idi-iil.org/fr/publications-par-categorie/resolutions/], Accessed 24 July 2023).

74 Case C-68/93 *Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA* [1995] ECR I-00415, par. 25; conversely, according to the "mosaic principle", "the courts of each Contracting State in which the defamatory publication was distributed and in which the victim claims to have suffered injury to his reputation have jurisdiction to rule on the injury caused in that State to the victim's reputation" (par. 30).

75 Joined Cases C-509/09 and C-161/10 *eDate*, note 71, par. 48. In the CJEU's view, this additional ground of jurisdiction not only benefits the plaintiff, but it is al-so predictable for the defendant (par.50), as long as the connection between the dispute and the courts of the centre of the interests of the alleged victim is based "not on exclusively subjective factors, relating solely to the individual sensitivity of that person, but on objective and verifiable elements which make it possible to identify, directly or indirectly, that person as an individual" (Case C-800/19 *Mittelbayerischer Verlag KG v SM* [2021] not yet published, paras. 41–43).

76 Joined Cases C-509/09 and C-161/10 *eDate*, note 71, par. 49. The CJEU also clarified that the centre of interests for a legal person is in the Member State where "its commercial reputation is most firmly established and must, therefore, be determined by reference to the place where it carries out the main part of its economic activities"; such place may coincide or not with the Member State where the legal person has is registered office (Case C-194/16 *Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB* [2017] published in the electronic Report of Cases, par. 41).

77 Case C-251/20 *Gtflix Tv v DR* [2021] not yet published, par. 43, where the Court, besides confirming the solution adopted in *Bolagsupplysningen*, (acritically) upheld the mosaic approach, stating that the plaintiff "may claim, before the courts of each Member State in which those comments are or were accessible, compensation for the damage suffered in the Member State of the court seised, even though

This solution is consistent not only with the ubiquitous nature of the information and content placed online,[78] but also with the need to prevent abusive forum and law shopping,[79] especially given that the Rome II Regulation[80] does not apply to "non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation".[81]

The solution adopted in *eDate* is an important example of how some of the rules of the Brussels I-*bis* can be adapted to the online context; nonetheless, such case-law pertains to the infringement of personality rights (which are constitutionally protected), and thus it cannot be automatically transposed to every kind of on-line activities.[82] Accordingly, in several occasions the CJEU clarified that – in the context of online infringements – the place of damage "may vary according to the nature of the right allegedly infringed",[83] and that the *e-Date* approach cannot be extended to any kind of online infringements, even when such infringements produce "dematerialised" damages.[84]

Although the Brussels I-*bis* Regulation provides several heads of jurisdiction, they are normally available only against EU-based controllers or processors. Indeed, according to Art. 5(1), the Regulation normally applies when the defendant is domiciled in a Member State, while, under Art. 6(1), national rules on jurisdiction apply with regard to claims against non-EU defendants. Nonetheless, some of the uniform rules of the Regulation apply irrespective of the defendant's domicile;[85]

---

those courts do not have jurisdiction to rule on the application for rectification and removal". For a critical assessment of the *Gtflix Tv* judgment, see, *inter alia*, Marongiu Buonaiuti, F., *Jurisdiction Concerning Actions by a Legal Person for Disparaging Statements on the Internet: The Persistence of the Mosaic Approach*, European Papers, Vol. 7, No. 1, 2022, pp. 345–360.

78 Case C-194/16 *Bolagsupplysningen*, note 76, par. 48.

79 See Zarra, G., *Conflitti di giurisdizione e bilanciamento dei diritti nei casi di diffamazione internazionale a mezzo Internet*, Rivista di diritto internazionale, Vol. 98, No. 4, 2015, pp. 1242–1243.

80 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 (Rome II Regulation).

81 Art. 1(2)(g) of the Rome II Regulation.

82 See Hess, B., *The Protection of Privacy in the Case Law of the CJEU*, in: Hess, B.; Mariottini, C. (eds.), Protecting Privacy in Private International and Procedural Law and by Data Protection: European and American Developments, Farnham, 2015, pp. 95–99.

83 Case C-170/12 *Peter Pinckney v KDG Mediatech AG* [2013] published in the electronic Report of Cases, par. 32.

84 Case C-441/13 *Pez Hejduk contro EnergieAgentur.NRW GmbH* [2015] published in the electronic Report of Cases.

85 Indeed, according to Art. 6(1), "If the defendant is not domiciled in a Member State, the jurisdiction of the courts of each Member State shall, subject to Article 18(1), Article 21(2) and Articles 24 and 25, be determined by the law of that Member State".

this is the case, e.g., of the aforementioned Art. 25 and Art. 18(1), as well as of Art. 21(1)(b), which is applicable against non-EU employers according to Art. 21(2).[86]

However, the application of the said EU jurisdictional rules over non-EU defendants requires various degrees of connection to be established between the dispute and the EU's territory. In particular, while a choice of courts agreement in favour of a court of a Member State is admissible even where the proceedings has no particular connections with the European Union, the jurisdiction rule for consumer contract requires some connection. Namely, under Art. 17(1)(c), in order for the consumer to sue the professional in the Member State of his or her domicile, the latter should pursue commercial or professional activities in the forum country or should direct such activities there, provided that the contract falls within the scope of the activities at stake. The contractual consumer jurisdiction is thus defined on the basis of a targeting test, which is intended to benefit the consumer as well as to make the competent forum predictable for the defendant, and which goes in parallel with the one normally employed to define the scope of EU rules against natural persons and undertakings established in a Third State.

Accordingly, the CJEU identified a non-exhaustive list of factors indicating when a professional – who runs his or her activities online – is directing his or her activities to the consumer's domicile. In particular, the CJEU clarified that the mere accessibility of a website from a Member State is not sufficient to conclude that the professional was directing his or her commercial activities to that country, and that other elements should be taken into account, among which: (i) the international nature of the activity; (ii) the 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; (iii) the mention of telephone numbers with an international code; (iv) 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; (v) use of a top-level domain name other than that of the Member State in which the trader is established; (vi) and mention of an international clientele composed of customers domiciled in various Member States.[87]

---

[86] See also Art. 20(2) states that where the employer who is not domiciled in a Member State but has a branch, agency or other establishment in one of the Member States, the employer shall, in disputes arising out of the operations of the branch, agency or establishment, be deemed to be domiciled in that Member State.

[87] Joined Cases C-585/08 and C-144/09 *Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG and Hotel Alpenhof GesmbH v Oliver Heller* [2010] ECR I-12527, par. 93; see also Case C-190/11 *Daniela Mühlleitner v Ahmad Yusufi and Wadat Yusufi* [2012] published in the electronic Reports of Cases, par. 45, where the Court stated that the consumer protective framework set forth in the Brussels regime does not require the contract between the consumer and the trader to be concluded at a distance, while in Case C-218/12 *Lokman Emrek v Vlado Sabranovic* [2013] published in the electronic Reports of

The case-law of the CJEU thus shows not only that the Brussels regime is adaptable to the online and digital context, but also that the need to balance different policy objectives – such as the need to protect the party who appears to be the weaker, on the one hand, and the need to ensure predictability regarding the competent courts, on the other – might give rise to different solutions, depending on the issue at stake.[88]

3.2. Jurisdiction against non-EU defendant under the GDPR

As already observed, the Brussels I-*bis* Regulation applies to data protection disputes involving private parties. Accordingly, in light of the *eadem ratio*, the "centre of interests" rule developed in the context of online defamation is also relevant with regard to the infringements of data subjects' rights.[89] However, the possibility to rely on the jurisdictional grounds provided under the Brussels I-*bis* Regulation in order to foster the application of EU law in this field depends on the scope of the Regulation itself, which applies – in principle – only when the defendant is domiciled within the EU.[90] This means that the *forum actoris* developed by CJEU for the victims of digital infringements of personalities rights is prevented when the defendant is domiciled outside the Union, and that the possibility for a European data subject to sue a non-EU company in the Union will depend on the private international law rules of his or her Member State.[91]

It appears that these shortcomings were considered in the drafting of the GDPR, as it includes several rules aiming at strengthening the protection of data subjects' rights also from a procedural perspective.

First, the GDPR specifies the remedies that data subjects can invoke when their rights under the Regulation are violated, including the right to receive compensa-

---

Cases, par. 32 the CJEU clarified that a causal link between the means employed to direct the commercial or professional activity to the Member State of the consumer's domicile and the conclusion of the contract with that consumer is not required.

88 See Marongiu Buonaiuti, F., *op.cit.*, note 72, pp. 112–113, confronting the *eDate* solution (enabling the victims of online defamation to sue the alleged tortfeasor before the authorities of his/her centre of interests) with the one adopted in the field of consumer contracts, which requires a much stronger connection between the professional (online) activities and the Member State where the consumer has is domicile.

89 Joined Cases C-509/09 and C-161/10 *eDate*, note 71, par. 52. See also Brkan, M., *op. cit.*, note 67, p. 270.

90 See *supra*, par. 3.1.

91 See Brkan, M., *op. cit.*, note 67, p. 265, asking "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, which are traditionally regarded as weaker (contractual) parties".

tion from the controller or processor for the material and non-material damage suffered as a result of an infringement of EU data protection law (Art. 82).

Moreover, Art. 80 of the GDPR provides a rule on the right of representation of data subjects, according to which data subjects can mandate a not-for-profit body, organisation or association meeting the listed requirements to exercise the rights referred to in the Regulation, including the right to receive compensation *ex* Art. 82, where provided for by Member State law.[92] This rule appears to reflect the need to strengthen access to justice not only where there is a general lack of knowledge of statutory rights and remedies in a given field (like in the case of data protection),[93] but also where a huge number of violations may arise from the same activities.[94] Under this latter perspective, Art. 80 of the GDPR is consistent with both the level of protection accorded by the CJEU[95] and some initiatives of the EU legislature, namely with the Representative Actions Directive, which provides minimum standards for procedural rules on collective redress and injunction for consumers.[96]

In addition, the GDPR sets out two rules on international jurisdiction, as a reaction to the intrinsic cross-border nature of the activities (and infringements) taking place on the Internet. The policy underlying the adoption of specific rules

---

92 Since the right to mandate data subject's right to compensation can be exercised only where Member State law provides for it, the GDPR does not set forth a general right in this sense, to such an extent that the possibility to rely on this peculiar tool will vary among Member States.

93 See the report published by FRA, *Access to data protection remedies in EU Member States*, 2013, [https://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states], Accessed 24 July 2023, *passim*, which underlines the need to raise awareness on data protection violations as a first step to ensure access to remedies. On this point, see Gonzáles Fuster, G., *Article 80. Representation of data subjects*, in: Kuner, C.; Bygrave, L. A.; Docksey, C. (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford, 2020, pp. 1143–1144.

94 On this topic, see Jančiūtė, L., *Data protection and the construction of collective redress in Europe: Exploring challenges and opportunities*, International Data Privacy Law, Vol. 9, No. 1, 2018, pp. 2–14. As an example of the collective feature of this kind of claims, see the CJEU judgment in the Case C-498/16 *Maximilian Schrems v Facebook Ireland Limited* [2018] published in the electronic Reports of Cases. At the national level, see Cases C/13/702849, C/13/706680, C/13/706842 *Stichting Onderzoek Marktinformatie et al. v TikTok et al.* [2022] Amsterdam District Court; on this topic, see Silva de Freitas, E.; Kramer, X., *First strike in a Dutch TikTok class action on privacy violation: court accepts international jurisdiction*, 2022, [https://conflictoflaws.net/], Accessed 24 July 2023.

95 Case C-40/17 *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV* [2019] published in the electronic Reports of Cases, par. 63.

96 Directive (EU) 2020/1828 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC [2020] OJ L 409/1 (Representative Actions Directive). On this topic, see Agulló Agulló, D., *La interacción entre las normas de protección de datos, de defensa de las personas consumidoras y de Derecho internacional privado en el ámbito del acceso colectivo a la justicia en la Unión Europea*, Cuadernos de Derecho Transnacional, Vol. 14, No 2, 2022, pp. 71–91.

on jurisdiction in this field is to protect the data subject also from a procedural perspective.[97] As a matter of fact, Art. 79(2) of the GDPR states that proceedings against a controller or a processor shall be brought: (i) before the courts of the Member State where the controller or processor has an establishment; or (ii) before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority acting in the exercise of its public powers.

Since one of the main objectives underlying the adoption of the GDPR is the protection of fundamental rights, it appears that the European legislature has adopted a *forum actoris* that resembles the one developed in *eDate*, but whose application is not limited to proceedings against non-EU defendant.[98] As a matter of fact, Art. 79(2) strengthen the protection of data subjects not only because it enables them to seise their "home court", but also because it support the "extra-territorial" and coherent application of EU rules by ensuring equal access to justice against non-EU controller/processors.[99]

Since the availability of multiple fora may give rise to multiple proceedings against the same controller or processor, the Regulation also provides a mechanism for cases where several proceedings "concerning the same subject matter as regards processing by the same controller or processor" are pending before the authorities of different Member States,[100] even though – in light of Recital 144 of the GDPR – it appears that such rule applies only to proceedings against a decision issued by supervisory authority, and not when proceedings in civil and commercial matters are pending in several Member States.[101]

As private claims against controllers or processors normally relate to civil and commercial matters, problems of coordination between the jurisdictional grounds set forth in Art. 79(2) of the GDPR and those of the aforementioned Brussels I-*bis* Regulation may arise.[102] The relationship between the two instruments is tackled

---

97 See Franzina, P., *op. cit.*, note 66, pp. 97–98.

98 De Miguel Asensio, P., *op. cit.*, note 15, p. 159.

99 In this regard, see Art. 27(5) of the GDPR, requiring non-EU controllers or processors that are within the scope of the Regulation according to Art. 3(2) to designate a representative in the Union, with the clarification that such designation "shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves".

100 Art. 81 of the GDPR. However, scholars have pointed out that this provision is "less sophisticated" than the general regime laid down in Art. 29 and Art. 30 of the Brussels I-*bis* Regulation. In this regard, see Franzina, P., *op. cit.*, note 66, p. 106.

101 *Ibid.*, pp. 105–106; see also De Miguel Asensio, P., *op. cit.*, note 15, pp. 162–163.

102 On this topic, see also Marongiu Buonaiuti, F., *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernente il trattamento dei dati personali e il suo coordinamento con la disciplina conte-*

in Recital 147 of the GDPR, which clarifies that "(w)here specific rules on jurisdiction are contained in this Regulation (…), general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council should not prejudice the application of such specific rules". This solution is consistent with Art. 67 of the Brussels I-*bis* Regulation, according to which the Regulation does not prejudice the application of provisions governing jurisdiction in specific matters which are contained in other EU instruments, like those laid down in Art. 79(2) of the GDPR. Thus, the coordinated reading of the two provisions appears to suggest the prevalence of the jurisdictional rules set forth in the GDPR, which are *leges speciales* in disputes initiated against controllers/processors for infringements of the right to data protection.[103] This conclusion is also confirmed by Recital 145 of the GDPR, underlining that the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides.

Even though Art. 79(2) of the GDPR is specifically designed for claims in the field of data protection (and in this sense it "prevails" on the rules laid down in the Brussels I-*bis* Regulation), it is not exclusive in nature. This means that the jurisdictional grounds set forth in the GDPR are additional, and that the rules of the Brussels I-*bis* Regulation continue to apply as long as their application is compatible with EU data protection law. Accordingly, the possibility for the plaintiff to rely on Art. 79(2) of the GDPR cannot be impaired by the application of Brussels I-*bis* Regulation's rules, as in the case where an exclusive prorogation agreement concluded between the data subject and the controller or processor exists. Nonetheless, such rules are still applicable where they expand the range of possible *fora* in favour of the plaintiff.[104]

Thus, the question arise whether the jurisdiction rules of the Brussels I-*bis* Regulation, where applied in the context of data protection infringements, are in practice capable of enlarging the possibilities provided by Art. 79(2) of the GDPR.[105] In particular, the Member State where the controller or processor has an establishment for the purpose of Art. 79(2) of the GDPR will normally correspond

nuta nel regolamento "Bruxelles I-bis", Cuadernos de Derecho Transnacional, Vol. 9, No. 2, 2017, pp. 448–464.

103 Kotschy, W., *Article 79. Right to have an effective remedy against a controller or processor*, in: Kuner, C.; Bygrave, L. A.; Docksey, C. (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford, 2020, p. 1137.

104 Kohler, C., *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union*, Rivista di diritto internazionale privato e processuale, Vol. 52, No. 3, 2016, p. 669. For an in-depth analysis of the coordination of Art. 79(2) of the GDPR and the Brussels I-*bis* Regulation, see Franzina, P., *op. cit.*, note 66, pp. 103–108.

105 Kohler, C., *op. cit.*, note 104, pp. 669–670.

to the place where the defendant is domiciled under Art. 4 of the Brussels I-*bis* Regulation,[106] and the *forum delicti* according to Art. 7(2) of the Brussels I-*bis* Regulation, as interpreted by the CJEU,[107] may frequently coincide with the data subject's habitual residence.[108] Moreover, if the processing of personal data is connected to a contract between the data subject and the defendant, the plaintiff could also rely on the *forum contractus* under Art. 7(1) of the Brussels I-*bis* Regulation, and – where the criteria listed in Art. 17(1)(c) are met – on the consumer jurisdiction rule set forth in Art. 18(1). Once again, this last ground for jurisdiction may most likely coincide with the habitual residence of data subject in the sense of Art. 79(2) of the GDPR.

As already mentioned, when the defendant is not domiciled in the EU, the uniform jurisdiction rules under Brussels I-*bis* Regulation (generally) does not apply. By contrast, the rule on jurisdiction included in the second indent of Art. 79(2) of the GDPR is designed to apply also against controllers or processors not established in the EU. Accordingly, also national rules on jurisdiction – which have been incorporated into EU law by means of the aforementioned Art. 6(1) of the Brussels I-*bis* Regulation[109] – shall not prejudice the application of the jurisdiction rules set forth in the GDPR.[110]

3.3. EU's approach to Artificial Intelligence and PIL issues: the lack of specific rules on jurisdiction

In light of the role played by civil liability in balancing the protection of victims of AI-related harms with the need to promote digital innovation within the EU,[111] scholars highlighted the role of PIL in regulating AI in a cross-border context.[112] Nonetheless, the (proposed) legislation does not explicitly refers to private international law issues, and it only declares the application of EU rules within its own territorial scope, to such an extent that EU rules in this field operate as "unilateral conflict rules". Accordingly, the instruments at stake aim at applying to

---

106 Franzina, P., *op. cit.*, note 66, p. 104.

107 See par. 3.2. of this paper.

108 De Miguel Asensio, P., *op. cit.*, note 15, pp. 159–160.

109 Opinion of the CJEU No 1/03 on the competence of the Community to conclude the new Lugano Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2006] ECR I-01145, paras. 144–148.

110 De Miguel Asensio, P., *op. cit.*, note 15, p. 159.

111 Recital B of the AI Liability Regime Resolution.

112 See, in particular, Poesen, M., *op.cit.*, note 46. See also Wagner, G., *Liability for Artificial Intelligence: A Proposal of the European Parliament*, 14 July 2021, pp. 25–26 [Available at SSRN: https://ssrn.com/abstract=3886294 or http://dx.doi.org/10.2139/ssrn.3886294].

the relationships that are within their scope irrespective of the law designated as applicable under the Rome II Regulation.

Where analysed through the prism of PIL, it appears that such substantive rules are not always capable to properly reflect the relevant EU policy in AI matters. This is particularly evident when it comes to the proposal for Regulation attached to the EU Parliament's Recommendation, whose territorial scope reflected the *lex loci damni* approach.[113] It has been pointed out that this solution – according to which the proposed Regulation should apply every time an AI-system causes harms or damages within the territory of the Union – is questionable, among other things, because it resembles the general conflict-of-laws rule for torts envisaged by Rome II Regulation (Art. 4), and it does not appear to be consistent with the special rule for cases relating to product liability (Art. 5).[114]

Recital 20 of the Rome II Regulation underlines that "(t)he conflict-of-law rule in matters of product liability should meet the objectives of fairly spreading the risks inherent in a modern high-technology society, protecting consumers' health, stimulating innovation, securing undistorted competition and facilitating trade". Accordingly, Art. 5 provides a solution which is more "victim friendly" than the one envisaged in Art. 4,[115] since it establishes a cascade system of connecting factors that privilege proximity with the person sustaining the damage, but also predictability for the person claimed to be liable. Then, although the purposes recalled in the aforementioned Recital 20 are similar to those underlying the proposed framework in the field of AI liability, the EU Parliament Recommendation adopted a solution which is less "sophisticated" than that enshrined in the Rome II Regulation, as it deploys an approach that appear to be overly simplistic, especially in the light of the specific feature of AI-related harms.[116]

---

113 Art. 2(1) of the Regulation Proposal attached to the AI Liability Regime Resolution.

114 This rule establishes a cascade system of connecting factors, with the first of them being the law of the country where the victim has his or her habitual residence when the damage occurred, provided that the product was marketed there (Art. 5(1)(a)); whether this criterion could not be used, the law of the country in which the product was acquired should apply (Art. 5(1)(b)); failing that, the applicable law should be the law of the country in which the damage occurred (Art. 5(1)(c). Also these two latter criteria apply provided that the product was marketed in those countries.

115 See von Hein, J., *Forward to the Past: A Critical Note on the European Parliament's Approach to Artificial Intelligence in Private International Law*, 22 October 2020 [https://conflictoflaws.net/2020/forward-to-the-past-a-critical-note-on-the-european-parliaments-approach-to-artificial-intelligence-in-private-international-law/] Accessed 24 July 2023.

116 *Ibid*. See also Poesen, M., *op. cit.*, note 46, par. II.2, pointing out that "the place-of-injury rule burdens those whose behaviour may incur liability", as the applicable law may not always be foreseeable, and that, in conclusion, "the Parliament Recommendations have not seized the opportunity to open the debate about the role of EU PrIL in regulating AI".

Disconnections have also been underlined between the EU Parliament's approach and Art. 14 of the Rome II Regulation. In fact, Art. 2(2) of the proposal attached to the EU Parliament Recommendation aimed at enhancing the protection of AI-users by limiting the autonomy of the parties. More specifically, the rule intended to bar the possibility for the operator of an AI-system to conclude (before or after the harm or damage occurred) an agreement with the victim, in order to circumvent or limit the rights and obligations set out in the proposed Regulation. Where adopted, this proposal would be in strong conflict with the rationale underlying EU's liberal approach in private international law, as the possibility for the parties to select freely the law governing their relationships is the cornerstone of EU PIL, not only in contractual matters (Art. 3 of Rome I Regulation), but also in non-contractual matters.[117]

Even considering EU rules on AI liability as unilateral conflict rules", their effective application may be pacifically ensured only before a court in the EU. Since there are no indications regarding the issue of international jurisdiction, claims within the scope of the proposed instruments will be regulated under the Brussels I-*bis* Regulation, and namely under Art.7(2), which – albeit not shaped in order to tackle AI-related harms – appear to be suited to the emerging framework on AI and civil liability.

In particular, and as long as liability for defective products is concerned, it appears to be relevant the solution adopted in *Zuid-Chemie*, where the CJEU specified that the place where the damage occurred is the place where the damage caused by the defective product actually manifests itself; therefore, it must not be confused with the place where the event which damaged the product itself occurred, which corresponds to the place of the event giving rise to the damage.[118] In the same occasion, the CJEU also clarified that Art. 7(2) designates "the place where the initial damage occurred as a result of the normal use of the product for the purpose for which it was intended".[119]

As observed above, the proposed amendments to the Product Liability Directive take "into account the growing significance of products manufactured outside the Union, and ensures that there is always an economic operator in the Union against

117 See von Hein, J., *op.cit.*, note 115.

118 Case C-189/08 *Zuid-Chemie BV v Philippo's Mineralenfabriek NV/SA.* [2009] ECR I-06917, par. 27. With regard to the applicability of the solution developed in *Zuid-Chemie* in the field of AI-related harms, see Cappiello, B., *AI-systems and non-contractual liability. A European private international law analysis*, Torino, 2022, p. 176, according to whom AI-related harms "fit within the solution already provided for by the ECJ", to such an extent that "a special head for jurisdiction for AI-systems would be superfluous".

119 Case C-189/08 *Zuid-Chemie BV*, note 118, par. 32.

whom a compensation claim can be made".[120] Accordingly, the issue of jurisdiction against non-EU operator appears to be less of an urgent point in this field, as Art. 7(2) of the Brussels I-*bis* Regulation may apply in a wide range of cases.

However, the lack of provisions concerning private international law raises few concerns in all those cases that – although related to damages caused by AI-systems – may fall outside the scope of the Product Liability Directive.

First, it is not consistent with the solution adopted in the GDPR, which incorporates a specific set of rules on jurisdiction in order to support the effective (and in some way "extraterritorial") application of the Regulation. Moreover, jurisdiction against defendants established in Third States will be mostly assessed in the light of the national rules of the Member States, which may not always be capable to attract this kind of proceedings before a court in the EU, and which – in light of the differences among national laws – do not ensure the victims of AI-related torts equal access to justice. As a consequence, it appears that there is a degree of uncertainty with regard to the concrete application of EU rules in the field of AI-systems, at least in cases related to non-EU States.

3.4. The issue of jurisdiction in the Online Platform Regulation and in the Platform Workers Directive Proposal

Even though the Online Platform Regulation aims at applying in broad terms (and with the specific objective of making redress possibilities accessible to business users of online platforms), the European legislature did not provide for a complete set of procedural provisions specifically designed to ensure its effective application world-wide. Indeed, unlike the GDPR, the Online Platform Regulation does not enshrine rules on international jurisdiction, and the only procedural tool set out in the instrument concerns the right of action of organisations and associations having a legitimate interest in representing business users (Art. 14), which resembles the aforementioned Art. 80 of the GDPR.

In the lack of specific jurisdiction rules, the Brussels I-*bis* Regulation applies with regard to the situations covered by the Online Platform Regulation. Accordingly, notwithstanding the general competence of the court of the Member State where the defendant has his or her domicile, jurisdiction against EU-based platform operator may be conferred, in contractual matters, pursuant to Art. 7(1)(b), and, in matters relating to torts, pursuant to Art. 7(2).[121] Therefore, absent a choice-

[120] See the explanatory memorandum attached to the Proposal, p. 12.

[121] For disputes arising out of the operations of a branch, agency or other establishment, the claimant has also the opportunity to sue the platform operator in the courts for the place where the branch, agency

of-court agreement conferring jurisdiction on a court in the EU under Art. 25 of the Brussels I-*bis* Regulation (as well as a tacit prorogation *ex* Art. 26), jurisdiction against non-EU domiciled defendants is regulated, in principle, according to the internal rules of the Member States. This circumstance does not ensure equal access to justice for European businesses, since national rules vary – quite consistently in some cases – from one Member State to another.[122] As a consequence, EU claimants will be able to litigate in their home country only if they are domiciled[123] in a Member State that employs a jurisdictional ground enabling them to do so, i.e. the nationality of the plaintiff.[124]

The absence of a specific set of jurisdiction rules in the Online Platform Regulation, designed to support its application against defendant established in Third States, is even more surprising if one considers that the substantive rules contained therein appears to qualify as "overriding mandatory provisions" pursuant to Art. 9 of the Rome I Regulation and Art. 16 of the Rome II Regulation.[125] The effective application of such mandatory rules may indeed be unproblematic only when claims are heard by a court in the EU. In the absence of uniform EU rules suited to assert jurisdiction over defendants domiciled in Third States, proceedings involving non-EU platform operators may be attracted before foreign courts that apply conflict-of-laws rules that do not guarantee the application of the Regulation's provisions.[126]

The same line of reasoning is applicable to the Platform Workers Directive Proposal. In fact, and in order for the instrument to be effective, the Proposal requires Member States to ensure that platform workers – both individually and collectively – "have access to effective and impartial dispute resolution and a right to redress, including adequate compensation, in the case of infringements of their rights arising from this Directive" (Art. 13 and Art. 14). Then, since the rights and

---

or other establishment is situated, under Art. 7(5).

122 See Nuyts, A., *Study on residual jurisdiction. General report*, 3 September 2007, [https://gavclaw.files.wordpress.com/2020/05/arnaud-nuyts-study_residual_jurisdiction_en.pdf], Accessed 24 July 2023.

123 Indeed, according to Art. 6(2) of the Brussels I-*bis* Regulation, "any person domiciled in a Member State may, whatever his nationality, avail himself in that Member State of the rules of jurisdiction there in force".

124 See Franzina, P., *Promoting Fairness and Transparency for Business Users of Online Platform: The Role of Private International Law*, in: Pretelli, I. (eds.), Conflict of Laws in the Maze of Digital Platforms/ Le Droit International Privé Dans le Labyrinthe des Plateformes Digitales, Zürich, 2018,, p. 156.

125 *Ibid.*, p. 151.

126 *Ibid.*, pp. 152–153, that highlights that, except where – according to the conflict-of-laws rules applied by a foreign court – the relationship is governed by the law of a Member State, the rules of the Online Platform Regulation "would in fact be regarded as overriding mandatory provisions of a legal system which is neither the *lex fori* nor the *lex cause*…".

obligations enshrined in the Directive Proposal also apply to Platforms established outside the EU, as long as they organise work performed in the Union, Member States' obligation to ensure access to redress mechanisms includes claims against non-EU platforms. Nonetheless, the Proposal does not provide any provision in the field of PIL: once again, jurisdiction in cases involving non-EU actors may mostly fall under the Brussels I-*bis* Regulation.

In particular, claims concerning rights set forth in the Directive may fall – in a number of cases – under the protective rules designed for individual contracts of employment, that, among other things, enable employees to sue employers – irrespective of their place of establishment[127] – in the Member State where or from where the employees habitually carries out their work or in the last Member State where they did so (Art. 21(1)(b)(i)). Moreover, according to the protective framework regarding employment matters, a choice-of-court agreement in this matter is admissible only if it is entered into after the dispute has arisen or if it allows the employee to bring proceedings in courts other than those indicated in the Section 5 of the Regulation,[128] thus enlarging the opportunities for the employee to sue the employer before a (different) court in the EU.

In this last regard, the CJEU clarified that, although the Brussels regime does not directly address the issue of choice-of-courts agreements conferring jurisdiction on a court in a Third State,[129] such an agreement is admissible only if it is not "exclusive" in nature, i.e. if it does not prohibit the employee from bringing proceedings before the courts which have jurisdiction under Art. 20 and 21 of the Brussels I-*bis* Regulation.[130] Nonetheless, it is open to question whether this solution is specific

127 See Art. 21(2) of the Brussels I-*bis* Regulation.

128 See Art. 23 of the Brussels I-*bis* Regulation.

129 Suffice it to observe that the enforceability of an agreement conferring jurisdiction on the courts of non-EU countries will mostly fall within the scope of the 2007 Lugano Convention (Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2007] OJ L 339/3) or within the scope of the 2005 Hague Convention (Hague Convention on Choice of Court Agreements, concluded on 30 June 2005, entered into force on 1 October 2015), and that, according to the Conventions at stake, judges in the EU might be required to decline their jurisdiction even when, in doing so, the effective application of EU law would be undermined. In this regard, see Franzina, P., *op. cit.*, note 124, p. 157, observing that is open to question whether, in such cases, the enforceability of the choice-of-court agreement might be precluded according to Art. 6(c) of the 2005 Hague Convention, which states that "A court of a Contracting State other than that of the chosen court shall suspend or dismiss proceedings to which an exclusive choice of court agreement applies unless… giving effect to the agreement would lead to a manifest injustice or would be manifestly contrary to the public policy of the State of the court seised".

130 Case C-154/11 *Ahmed Mahamdia v République algérienne démocratique et populaire* [2012] published in the electronic Report of Cases, paras. 61–66). On this topic, see Villata, F. C., *L'attuazione degli accordi di scelta del foro nel regolamento Bruxelles I*, Cedam, Padova, 2012, pp. 199–254.

for claims regarding employment matters (and might theoretically be extended to other cases for which the Brussels I-*bis* regulation prescribes protective rules), or if instead it might be adopted as a general solution.[131] In the latter case, the solution adopted in *Mahamdia* would prevent jurisdiction before a court in the EU to be barred, for example, when service providers operating within the scope of the Online Platform Regulation include in their terms and conditions an exclusive choice-of-court clause designating a court in a Third State.[132]

Finally, since platform work can blur the boundaries between employment relationship and self-employed activity,[133] it might be questionable whether the protective rules provided in the Brussels regime are accessible to any platform worker. Even though the Brussels I-*bis* Regulation does not provide any definition of "contract of employment", the CJEU clarified that it is an independent concept, which "create a lasting bond which brings the worker to some extent within the organisational framework of the business of the undertaking or employer… in return for which he [or she] received remuneration".[134] Thus, the question is whether such definition is sufficient to preclude that the features of platform work give rise to misclassification of the employment status, in order to preclude the workers' access to protective *fora*. In the event of the disconnection within the definition provided by the CJEU and the characteristics of platform work, workers may not be able to rely on the protective rules set forth in the Regulation, which are also applicable against employers that are not established in the EU. As a consequence, in this kind of proceedings, jurisdiction against non-EU platforms may be assessed in light of the residual application of national rules on jurisdiction: this solution does not ensure equal access to justice for EU workers.

This is even more problematic if one considers that the obligation set forth in Art. 13 should not affect the application of Art. 79 and Art. 82 of the GDPR. This means that, where a worker's rights under the Directive Proposal are infringed by means of activities that are partially related to the processing of his or her personal data, claims pertaining to privacy infringements may be regulated according to EU jurisdiction rules (namely through Art. 79(2) of the GDPR), while jurisdic-

131 See Magnus, U., *Article 25*, in: Magnus, U.; Mankowski, P. (eds.), Brussels Ibis Regulation, Köln, 2023, pp. 604–605.

132 See Franzina, P., *op. cit.*, note 124, p. 158.

133 See note 63.

134 See, *inter alia*, Case C-47/14 *Holterman Ferho Exploitatie BV et al. v F.L.F. Spies von Büllesheim* [2015] published in the electronic Report of Cases, paras. 39–45. On this point, see Esplugues Mota, C.; Palao Moreno, G., *Article 20*, in: Magnus, U.; Mankowski, P. (eds.), Brussels Ibis Regulation, Köln, 2023, pp. 539–540.

tion over claims not related to the misuse of personal data could be assessed in the light of Member States national rules.

4. CONCLUSIONS

In light of the pivotal role that new technologies play for the achievement of policy objectives, and considering their ability to negatively affect rights and freedoms in a ubiquitous manner, the EU is adopting a number of instruments to regulate those matters that are particularly affected by digitalisation, especially (but not only) in the field of personality rights. Indeed, this legislation aims at regulating the usage of digital technologies in order to ensure the proper functioning of the internal market, as well as the protection of the rights recognised under EU law, even when digital activities take place abroad.

Accordingly, some recent EU acts and proposals in this field define their own territorial scope in a broad way and by means of "unilateral conflict rules" that are meant to prevail over the application of conflict-of-laws rules enshrined in Rome I and Rome II Regulation. Nonetheless, it appears that limited attention is generally paid to other issues in the field of PIL. In particular, even though such instruments are aimed at applying outside the EU borders, they do not usually provide special provisions on international jurisdiction supporting the "extraterritorial" application of EU substantive rules.

This is rather counterintuitive, if one considers that – in other occasions – EU acts in this field have been equipped with special grounds for jurisdiction, suited to support such broad application. This is the case of Art. 79(2) of the GDPR, providing that proceedings against the controller or the processor of personal data may be brought not only before the court of the Member State where the controller or processor has an establishment, but also before the court of the Member State where the user has his or her habitual residence, the latter ground being suitable also for claims against non-EU domiciled defendants.

In the absence of special jurisdiction rules within the context of other EU instruments – i.e. the Online Platforms Regulation and several proposals in the field of digital technologies –, the Brussels I-*bis* Regulation may apply in the event of cross-border infringements of the rights enshrined in such legislation. This circumstance is open to criticisms. In the first place, EU rules on jurisdiction in civil and commercial matters were not drafted in light of the characteristics of digitalisation. Accordingly, they have been progressively interpreted in order to tackle the issue of infringements related to the use of technologies. Nonetheless, whether the CJEU will be able to adapt – under all circumstances – EU jurisdiction rules to

the lack of jurisdictional grounds suited to digital infringements is open to question. Moreover, the Brussels I-*bis* Regulation normally applies where the defendant is domiciled within the European Union, and only a limited number of EU jurisdiction rules applies to non-EU domiciled defendants. Even if some of these latter rules appear to be relevant within the context of claims in digital matters, a number of cases may fall within the scope of the residual application of Member States' national rules on jurisdiction. This appears to be problematic, since persons located in the EU may not have equal access to justice in the EU to enforce their rights against non-EU actors.

This circumstance also ends up affecting the role of the EU as a "global regulator" in the digital field. In fact, although the EU aims at projecting its digital policies abroad by adopting instruments with a broad territorial scope, the concrete application of EU rules outside EU borders will mostly depend on the existence, within the national rules of the Member States, of jurisdiction rules suited to attract this kind of proceedings before a court in the European Union. Accordingly, in order for the EU to improve its regulatory power, a number of solutions might be considered.

A first approach would consist in equipping EU substantive legislation in digital matters with jurisdiction rules suited to support their "extraterritorial" application, in the vein of Art. 79(2) of the GDPR. Nevertheless, the framework set up in the GDPR could only partially represent a valid model of how the interplay between the extraterritorial application of EU substantive rules and the rules on jurisdiction should work. As a matter of fact, the adoption of special jurisdictional grounds does not ensure, *per se*, the achievement of such result. Thus, a number of other actions should be taken, especially with regard to parallel proceedings and recognition and enforcement of judgments issued by courts in Third States.

Another possible solution would consist in emending the Brussels I-*bis* Regulation, in order to make (at least some of) its jurisdiction rules applicable against non-EU defendants. In particular, enlarging the scope of application of the aforementioned Art. 7(1) and Art. 7(5) would be a valid solution,[135] even for proceedings pertaining to digital matters. Extending the former would allow an EU actor (that is not a consumer) to sue a non-EU party before a court in a Member State, as long as the defendant directs his or her activities to the internal market; extending the latter would consent to consider a non-EU company that has a branch in a Member State as domiciled in the Union, at least with regard to disputes arising

[135] On the opportunity to extend these two heads of jurisdiction to non-EU defendants, see Hess, B., *et al.*, *The Reform of the Brussels Ibis Regulation*, MPILux Research Paper Series, No. 6, 2022 [Available at SSRN: https://ssrn.com/abstract=4278741 or http://dx.doi.org/10.2139/ssrn.4278741], pp. 15–16.

out of the operations of such branch. Conversely, a general extension of Art. 7(2) to non-EU defendants would be more problematic in terms of predictability.[136]

A better approach would thus consist in adopting special heads of jurisdiction reflecting the policies of the EU in digital matters. In particular, in light of the need to ensure the concrete projection of EU digital values abroad, such rules could be designed in the same vein of the protective rules that are already enshrined within the Brussels I-*bis* Regulation, with regard to the so-called "weaker parties".[137] In fact, since digital technologies have the ability to seriously affect individuals, their use in certain contexts could result in the creation of new categories of protective grounds for jurisdiction, aimed at conferring benefits in terms of access to courts upon the victims of digital infringements.[138] Moreover, this solution appears to be consistent with the case-law of the CJEU pertaining to online defamation, where the Court creates a *forum actoris* that ensure the defamed person the possibility to claim compensation for the entire damage in the Member State where he or she has is habitual residence.

Under this perspective, a sectorial approach should thus be preferred to the reform of the Brussels I-*bis* Regulation, at least as long as digital matters are involved. Indeed, a similar solution would permit to select the situations for which the creation of similar protective grounds is needed, and it would also allow for better shaping the terms of the intervention of the European legislature in this field.

REFERENCES

BOOKS AND ARTICLES

1. Agulló Agulló, D., *La interacción entre las normas de protección de datos, de defensa de las personas consumidoras y de Derecho internacional privado en el ámbito del acceso colectivo a la justicia en la Unión Europea*, Cuadernos de Derecho Transnacional, Vol. 14, No 2, 2022, pp. 71–91
2. Bradford, A., *The Brussels Effect: How the European Union Rules the World*, New York, 2020
3. Brkan, M., *Data protection and European private international law: Observing a bull in a China shop*, International Data Privacy Law, Vol. 5, No. 4, 2015, pp. 257–278

136 *Ibid*., p. 16.

137 In this regard, and in relation to platform users within the context of the Online Platform Regulation, see Franzina, P., *op. cit.*, note 124, p. 160.

138 See also Brkan, M., *op. cit.*, note 67, p. 265, stating that enlarging the scope of the Brussels I-*bis* Regulation to non-EU defendants in the field of data protection 'would not only be beneficial for 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 are processed on a contractual basis or not'.

4. Cappiello, B., *AI-systems and non-contractual liability. A European private international law analysis*, Torino, 2022
5. Chamberlain, J., *The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective*, European Journal of Risk Regulation, Vol. 14, No. 1, 2023, pp. 1–13
6. Chia, C. W., *Sketching the Margins of a Borderless World: Examining the Relevance of Territoriality for Internet Jurisdiction*, Singapore Academy of Law Journal, Vol. 30, No. 2, 2018, pp. 833–870
7. Cremona, M.; Scott, J. (eds.), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*, Oxford, 2019
8. De Miguel Asensio, P., *Conflict of Laws and the Internet*, Cheltenham and Northampton, 2020
9. Esplugues Mota, C.; Palao Moreno, G., *Article 20*, in: Magnus, U.; Mankowski, P. (eds.), Brussels Ibis Regulation, Köln, 2023, pp. 537–543
10. Franzina, P., *Promoting Fairness and Transparency for Business Users of Online Platform: The Role of Private International Law*, in: Pretelli, I. (eds.), Conflict of Laws in the Maze of Digital Platforms/ Le Droit International Privé Dans le Labyrinthe des Plateformes Digitales, Zürich, 2018, pp. 147–162
11. Franzina, P., *Jurisdiction Regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, in: De Franceschi, A. (ed.), European Contract Law and the Digital Single Market. The Implications of the Digital Revolution, Cambridge, 2017, pp. 81–108
12. Gonzáles Fuster, G., *Article 80. Representation of data subjects*, in: Kuner, C.; Bygrave, L. A.; Docksey, C. (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford, 2020, pp. 1142–1152
13. de Hert, P.; Czerniawski, M., *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context*, International Data Privacy Law, Vol. 6, No. 3, 2016, pp. 230–243
14. Hess, B., *et al.*, *The Reform of the Brussels Ibis Regulation*, MPILux Research Paper Series, No. 6, 2022 [Available at SSRN: https://ssrn.com/abstract=4278741 or http://dx.doi.org/10.2139/ssrn.4278741]
15. Hess, B., *The Protection of Privacy in the Case Law of the CJEU*, in: Hess, B.; Mariottini, C. (eds.), Protecting Privacy in Private International and Procedural Law and by Data Protection: European and American Developments, Farnham, 2015, pp. 81–113
16. Hustinx, P., *EU Data Protection Law: The Review of Directive 95/46/CE and the General Data Protection Regulation*, in: Cremona, M. (ed.), New Technologies and EU Law, Oxford, 2017, pp. 123–173
17. Jančiūtė, L., *Data protection and the construction of collective redress in Europe: Exploring challenges and opportunities*, International Data Privacy Law, Vol. 9, No. 1, 2018, pp. 2–14
18. Kohler, C., *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union*, Rivista di diritto internazionale privato e processuale, Vol. 52, No. 3, 2016, pp. 653–675

19. Kotschy, W., *Article 79. Right to have an effective remedy against a controller or processor*, in: Kuner, C.; Bygrave, L. A.; Docksey, C. (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford, 2020, pp. 1132–1141
20. Lutzi, T., *Private Ordering, the Platform Economy, and the Regulatory Potential of Private International Law*, in: Pretelli, I. (eds.), Conflict of Laws in the Maze of Digital Platforms/ Le Droit International Privé Dans le Labyrinthe des Plateformes Digitales, Zürich, 2018, pp. 129–145
21. Magnus, U., *Article 25*, in: Magnus, U.; Mankowski, P. (eds.), Brussels Ibis Regulation, Köln, 2023, pp. 580–665
22. Mantovani, M., *Horizontal Conflicts of Member States' GDPR-Complementing Laws: The Quest for a Viable Conflict-of-Laws Solution*, Rivista di diritto internazionale privato e processuale, Vol. 55, No. 3, 2019, pp. 535–562
23. Marongiu Buonaiuti, F., *Jurisdiction Concerning Actions by a Legal Person for Disparaging Statements on the Internet: The Persistence of the Mosaic Approach*, European Papers, Vol. 7, No. 1, 2022, pp. 345–360
24. Marongiu Buonaiuti, F., *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernente il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I-bis"*, Cuadernos de Derecho Transnacional, Vol. 9, No. 2, 2017, pp. 448–464
25. Marongiu Buonaiuti, F., *La giurisdizione nelle controversie relative alle attività on-line*, Diritto Mercato Tecnologia, Special Issue, 2017, pp. 89–128
26. Márton, E., *Violations of Personality Rights through the Internet: Jurisdictional Issues under European Law*, Baden-Baden, 2016
27. Moerel, L., *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?*, International Data Privacy Law, Vol. 1, No. 1, 2011, pp. 28–46
28. Poesen, M., *Regulating Artificial Intelligence (AI) in the European Union (EU): Exploring the Role of Private International Law*, X, Recht in beweging – 29ste VRG-Alumnidag 2022, 2022, pp. 297–314 [Available at SSRN: https://ssrn.com/abstract=3959643 or http://dx.doi.org/10.2139/ssrn.3959643]
29. Pretelli, I., *Protecting Digital Platform Users by Means of Private International Law*, Cuadernos de Derecho Transnacional, Vol. 13, No. 1, 2021, pp. 574–585
30. Requejo Isidro, M., *Procedural Harmonization and Private Enforcement in the Area of Personal Data Protection*, MPILux Research Paper Series, No. 3, 2019 [Available at SSRN: https://ssrn.com/abstract=3339180 or http://dx.doi.org/10.2139/ssrn.3339180]
31. Saluzzo, S., *The Principle of Territoriality in EU Data Protection Law*, in: Natoli, T., Riccardi A.(eds.), Borders, Legal Spaces and Territories in Contemporary International Law, Cham, 2019, pp. 121–141
32. Scott, J., *Extraterritoriality and Territorial Extension in EU Law*, The American Journal of Comparative Law, Vol.62, No. 1, 2014, pp. 87–125
33. Svantesson, D.J.B.; Revolidis, I., *From eDate to Gtflix: Reflections on CJEU Case Law on Digital Torts under Art. 7(2) of the Brussels Ia Regulation, and How to Move Forward*, in: Alapantas, P.; Anthimos, A.; Arvanitakis, P. (eds.), National and International Legal Space - The

Contribution of Prof. Konstantinos Kerameus in International Civil Procedure, Athens, 2022, pp. 319–371

34. Svantesson, D. J. B., *Article 3. Territorial scope*, in: Kuner, C.; Bygrave, L. A.; Docksey, C. (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford, 2020, pp. 74–99
35. Trooboff, P. D., *Globalization, Personal Jurisdiction and the Internet Responding to the Challenge of Adapting Settled Principles and Precedents*, Collected Courses of the Hague Academy of International Law, Vol. 415, 2021
36. Villata, F. C., *L'attuazione degli accordi di scelta del foro nel regolamento Bruxelles I*, Cedam, Padova, 2012
37. Vogiatzoglou, P., Valcke, P., *Two decades of Article 8 CFR: A critical exploration of the fundamental right to data protection in EU law*, in: Kosta, E.; Kamara, I.; Leenes, R. (eds.), Research Handbook on EU Data Protection Law, Northampton, 2022, pp. 11–49
38. Wagner, G., *Liability for Artificial Intelligence: A Proposal of the European Parliament*, 14 July 2021, pp. 1–36 [Available at SSRN: https://ssrn.com/abstract=3886294 or http://dx.doi.org/10.2139/ssrn.3886294]
39. Zarra, G., *Conflitti di giurisdizione e bilanciamento dei diritti nei casi di diffamazione internazionale a mezzo Internet*, Rivista di diritto internazionale, Vol. 98, No. 4, 2015, pp. 1231–1262

COURT OF JUSTICE OF THE EUROPEAN UNION

1. Case C-251/20 Gtflix Tv v DR [2021] not yet published
2. Case C-800/19 Mittelbayerischer Verlag KG v SM [2021] not yet published
3. Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] not yet published
4. Case C-40/17 Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV [2019] published in the electronic Reports of Cases
5. Case C-498/16 Maximilian Schrems v Facebook Ireland Limited [2018] published in the electronic Reports of Cases
6. Case C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH [2018] published in the electronic Reports of Cases
7. Case C-194/16 Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB [2017] published in the electronic Report of Cases
8. Case C-192/15, T. D. Rease and P. Wullems v College bescherming persoonsgegevens [2015] OJ C78/11
9. Case C-230/14 Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság [2015] published in the electronic Reports of Cases
10. Case C-47/14 Holterman Ferho Exploitatie BV et al. v F.L.F. Spies von Büllesheim [2015] published in the electronic Report of Cases

11. Case C-441/13 Pez Hejduk contro EnergieAgentur.NRW GmbH [2015] published in the electronic Report of Cases
12. Case C-413/13 FNV Kunsten Informatie en Media v Staat der Nederlanden [2014] published in the electronic Reports of Cases
13. Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzále [2014] published in the electronic Reports of Cases Case C-218/12 Lokman Emrek v Vlado Sabranovic [2013] published in the electronic Reports of Cases
14. Case C-170/12 Peter Pinckney v KDG Mediatech AG [2013] published in the electronic Report of Cases
15. Case C-190/11 Daniela Mühlleitner v Ahmad Yusufi and Wadat Yusufi [2012] published in the electronic Reports of Cases
16. Case C-154/11 Ahmed Mahamdia v République algérienne démocratique et populaire [2012] published in the electronic Report of Cases
17. Joined Cases C-509/09 and C-161/10 eDate Advertising GmbH and Others v X and Société MGN LIMITED [2011] ECR I-10269
18. Joined Cases C-585/08 and C-144/09 Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG and Hotel Alpenhof GesmbH v Oliver Heller [2010] ECR I-12527
19. Case C-189/08 Zuid-Chemie BV v Philippo's Mineralenfabriek NV/SA. [2009] ECR I-06917
20. Opinion of the CJEU No 1/03 on the competence of the Community to conclude the new Lugano Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2006] ECR I-01145
21. Case C-334/00 Fonderie Officine Meccaniche Tacconi SpA v Heinrich Wagner Sinto Maschinenfabrik GmbH (HWS) [2002] ECR I-07357
22. Case C-68/93 Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA [1995] ECR I-00415
23. Case C-21/76 Handelskwekerij G. J. Bier BV v Mines de potasse d'Alsace SA [1976] ECR 01735

ECHR

1. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, ETS No. 108
2. European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11, 14 and 15, 4 November 1950, ETS 5 (ECHR)
3. *Amann v Switzerland* (2000) 30 EHRR 843

EU LAW

1. Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules

on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)

2. Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law, adopted on 16 December 2010, 0836-02/10/EN, WP 179
3. Charter of Fundamental Rights of the European Union [2016] OJ C 202/389 (CFREU)
4. Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2007] OJ L 339/3
5. Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products [1985] OJ L 210/29 (Product Liability Directive)
6. Directive 95/46/EC 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 [1995] OJ L 281/31 (Data Protection Directive)
7. Directive (EU) 2020/1828 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC [2020] OJ L 409/1 (Representative Actions Directive)
8. European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), adopted on 16 November 2018 (version 2.1 of 7 January 2020)
9. European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)) (AI Liability Regime Resolution)
10. General Approach adopted by the Council on 12 June 2023 on the Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work (Document ST_10758_2023_INIT)
11. Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 final (AI Liability Directive Proposal)
12. Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work, COM(2021) 762 final (Platform Workers Directive Proposal)
13. Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM/2022/495 final
14. Proposal for a Regulation of the European Parliament and of the council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM(2021) 206 final (AI Act Proposal)
15. 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 (Rome II Regulation)
16. 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 (Rome I Regulation)

17. Regulation (EU) 1215/2012 of the European Parliament and of the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) [2012] OJ L 351/1 (Brussels I-*bis* Regulation)
18. Regulation (EU) 2016/679 of the European Parliament and of the Council 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 [2016] OJ L 119/1 (General Data Protection Regulation)
19. Regulation (EU) 2019/1150 of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services [2019] OJ L 186/57 (Online Platforms Regulation)
20. Treaty on the Functioning of the European Union [2007] OJ C 326/01

LIST OF REGULATIONS

1. Hague Convention on Choice of Court Agreements, concluded on 30 June 2005, entered into force on 1 October 2015

LIST OF NATIONAL REGULATIONS, ACTS AND COURT DECISIONS

1. Cases C/13/702849, C/13/706680, C/13/706842 *Stichting Onderzoek Marktinformatie et al. v TikTok et al.* [2022] Amsterdam District Court
2. European Commission amicus brief, *United States v Microsoft Corporation* [2017] No. 17-2

WEBSITE REFERENCES

1. Silva de Freitas, E.; Kramer, X., *First strike in a Dutch TikTok class action on privacy violation: court accepts international jurisdiction*, 2022, [https://conflictoflaws.net/], Accessed 24 July 2023
2. Pato, A., *The EU's Upcoming Framework on Artificial Intelligence and its Impact on PIL*, 12 July 2021 [https://eapil.org/2021/07/12/the-eus-upcoming-regulatory-framework-on-artificial-intelligence-and-its-impact-on-pil/], Accessed 24 July 2023
3. von Hein, J., *Forward to the Past: A Critical Note on the European Parliament's Approach to Artificial Intelligence in Private International Law*, 22 October 2020 [https://conflictoflaws.net/2020/forward-to-the-past-a-critical-note-on-the-european-parliaments-approach-to-artificial-intelligence-in-private-international-law/], Accessed 24 July 2023
4. Institut de Droit International, *Resolution on Internet and the Infringement of Privacy: Issues of Jurisdiction, Applicable Law and Enforcement of Foreign Judgments*, 2019 (2019 IDI Resolution) [https://www.idi-iil.org/fr/publications-par-categorie/resolutions/], Accessed 24 July 2023
5. Redic, V., *The EU data protection Regulation: Promoting technological innovation and safeguarding citizens' rights*, 2014, [https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_14_175], Accessed 24 July 2023
6. FRA, *Access to data protection remedies in EU Member States*, 2013, [https://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states], Accessed 24 July 2023
7. Nuyts, A., *Study on residual jurisdiction. General report*, 3 September 2007, [https://gavclaw.files.wordpress.com/2020/05/arnaud-nuyts-study_residual_jurisdiction_en.pdf], Accessed 24 July 2023