

INTERNATIONAL LAW ASSOCIATION

SYDNEY CONFERENCE (2018)

PROTECTION OF PRIVACY IN PRIVATE INTERNATIONAL AND PROCEDURAL LAW

Members of the Committee:

Professor Burkhard Hess (Luxembourg/Germany), *Chair*
Professor Jan von Hein (Germany), *Co-Rapporteur*
Dr. Cristina M. Mariottini (USA), *Co-Rapporteur*

Professor Stefania Bariatti (Italy)
Alternate: Professor Francesca C. Villata
Dr. Mario Viola de Azevedo Cunha (Brazil)
Professor Pedro A. de Miguel Asensio (Spain)
Professor Fabienne Jault Seseke (France)
Alternate: Ms. Nathalie Meyer Fabre
Professor Patrick Kinsch (HQ)
Professor Christopher Kuner (Nominee of the Chair)
Professor Claudio Lucena Neto (Brazil)
Professor Peter Malanczuk (HQ)
Professor Alex Mills (UK)
Professor Yoshiaki Nomura (Japan)

Dr. Rui Pereira Dias (Portugal)
Professor Thomas Pfeiffer (Germany)
Mr. Gustavo Rabay Guerra (Brazil)
Professor Marta Requejo Isidro (Spain)
Dr. David Rolph (Australia)
Professor Daphne-Ariane Simotta (Austria)
Professor David P. Stewart (USA)
Professor Dan Jerker B. Svantesson (Australia)
Professor Naoshi Takasugi (Japan)
Professor Louise Ellen Teitz (USA)
Professor Celia Zolynski (France)

INTERIM REPORT AND COMMENTARY TO THE DRAFT GUIDELINES ON JURISDICTION AND APPLICABLE LAW

I. Introduction	2
II. Draft Guidelines and Commentary 2	
Preamble	2
A – General provisions	4
B – Jurisdiction	18
C – Applicable law	27
1. Non-Contractual Obligations	27
2. Contractual Obligations	35
3. General Provisions on the Applicable Law	36

III. Conclusions and Future Steps 42

I. Introduction

1. In accordance with the mandate conferred in 2013 by the International Law Association (ILA), the ILA Committee on the Protection of Privacy in Private International and Procedural Law (the Committee), focuses on the promotion of international co-operation and the contribution to predictability on issues of jurisdiction, applicable law, and circulation of judgments on privacy, including personal data, rights.

2. To date, the Committee has met five times. Additionally, in August 2016 it held an Open Working Session meeting at the 77th ILA Biennial Conference in Johannesburg.¹

3. The Committee will submit and present this Interim Report, including the draft Guidelines and the commentary thereto, at the 78th ILA Biennial Conference, from 19 until 24 August 2018 in Sydney (Australia).

4. The Committee’s resolution is scheduled to be submitted for adoption by the ILA at the 80th ILA Biennial Conference in 2022.²

II. Draft Guidelines and Commentary

PREAMBLE³

[These Guidelines set forth general principles concerning privacy rights, including the right to the protection of personal data, in private international and procedural law.

They may serve as a model for national, regional, supranational or international instruments.⁴

¹ The Report of the Open Working Session, along with the other documentation concerning the Committee’s activity, is available on the Committee’s page at <www.ila-hq.org/index.php/committees>, under the tab ‘Documents’. For further information concerning the Committee’s activity, see also *ivi*, under the tab ‘News’.

² The Chair and the Co-Rapporteurs avail themselves of this opportunity to extend their gratitude to all those Committee Members who contributed to the Committee’s work by submitting detailed National Reports and by sharing insights that shaped the Committee’s discussions and outputs. Furthermore, they wish to convey their appreciation, for their involvement and valued participation, to Judge Vesna Tomljenovic (Croatia), Prof. Ilaria Viarengo (Italy), Prof. Haksoo Ko (Republic of Korea), Mr. Peter Trooboff (Covington & Burling LLP), Prof. Gloria González Fuster (Vrije Universiteit Brussel) and Prof. Kevin D. Benish (NYU). Finally, they wish to acknowledge Ms. Anna F. Bizer (University of Freiburg) for her assistance in the Committee’s research and drafting activity.

³ The Committee Officers wish to convey that the Preamble was drafted by them, and has not yet been adopted by the Committee.

⁴ For instance, in the context of exclusions from scope, the 2018 Hague Draft Convention on the Recognition and Enforcement of Foreign Judgments addresses defamation and privacy separately at Article 2(1)(k)-(l) (it should

They may be used to interpret, supplement and develop rules of private international and procedural law.]

5. Although the protection of privacy has become a compelling issue in cross-border settings, most international⁵ and regional instruments⁶ on private international law do not address this matter, notably because it raises sensitive issues of conflicting rights and interests. These Guidelines are aimed at bridging this gap. The Committee is conscious of the underlying conceptual divergences in the national systems in this area of the law. However, these Guidelines shall assist lawmakers and courts to tackle cross-border privacy and data protection disputes arising out of the use of the cyber world, in the digital area and to bridge conceptual divergences. They shall provide for a framework of private international law where conflicts relating to the protection of privacy rights, the freedom of press and the use of data need to be accommodated.

6. The Guidelines aim to encourage the development and refinement of a suitable treatment of the right to privacy, including the right to the protection of personal data, in private international and procedural law, with certain innovations. Today, infringements of privacy usually take place in the cyberspace. Therefore, the scope of the Guidelines transcends the boundaries of traditional privacy to address, also and in particular, cross-border questions of privacy in the digital era.⁷

7. While data protection commonly refers to the specific area of the law that regulates ‘the processing of data associated with an identifiable individual’, privacy is identified with ‘the notion of an individual’s space’.⁸ Cognizant of the fact that privacy and the processing of personal data are closely adjacent areas of the law,⁹ the Committee has included data protection

be noted that the exclusion of privacy has been placed in squared brackets to indicate that further discussion is needed). The ‘Judgments Convention: Revised Preliminary Explanatory Report’ (Prel. Doc. No 10 of May 2018 for the attention of the Special Commission of May 2018, by F.J. Garcimartín Alférez and G. Saumier) identifies, at paras 53-54, the rationale for both exclusions in the fact that judicial decisions in matters of both defamation and privacy ‘are usually based on a delicate balance between constitutional rights, and therefore is a sensitive matter for many States’.

⁵ Article 2(1)(k)-(l) of the 2018 Draft Convention of the Hague Conference (supra).

⁶ Article 1(2)(g) of 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 L199/40.

⁷ With respect to human rights challenges relating to the right to privacy in the digital age, in 2018 the Office of the High Commissioner for Human Rights has indicated that it collected input from relevant stakeholders, including on principles, standards and best practices with regard to the promotion and protection of the right to privacy, and a report is forthcoming. See <<http://www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportPrivacy.aspx>>.

⁸ D. Cooper and C. Kuner, *Data Protection Law and International Dispute Resolution*, 382 *Recueil des Cours* (2017), at 25. On the history, policies, and future of transborder data flow regulation see esp. C. Kuner, *Transborder Data Flows and Data Privacy Law* (2013). See also the Modernised Convention for the Protection of Individuals with regard to the Processing of Personal Data (Convention 108) adopted in the framework of the Council of Europe in 1981 and ‘modernised’ in May 2018 (CM/Inf(2018)15-final). Convention 108 remains, to date, the only legally binding international instrument in the data protection field. It applies to all data processing carried out by both the private and public sectors.

⁹ The link between privacy and data protection rights was highlighted, i.a., by the **French Conseil Constitutionnel** in 2004 (Decision No 2004-499 DC of 29 July 2004), and by the European Court of Human Rights which consistently stated that the protection of personal data is of fundamental importance to a person’s enjoyment

in the scope of its activity. Provided, however, that the two concepts are adjacent but not identical, the Committee is aware that some fine-tuning may be necessary as a result of the specificities that are inherent to data protection.

8. One of the objectives of the Guidelines is the acceptance of its principles in present and future private international and procedural law instruments, to advance a substantial degree of specialised harmonization of law on a national, regional, supranational and international level. As such, the Guidelines contribute to increasing predictability and facilitating access to justice. The Guidelines may be used to interpret, supplement and develop rules of private international and procedural law. They may be employed to explain, clarify or construe the meaning of existing rules of private international and procedural law. They may be employed for the refinement of existing rules that do not sufficiently or appropriately provide for a particular type of situation. They may be employed in the shaping by legislatures or, where possible, by courts, of new rules where none existed before or effecting fundamental changes to pre-existing ones.¹⁰

9. The Guidelines do not have as their purpose to change the substantive law which governs matters of privacy, including the protection of personal data. Accordingly, for instance, the applicable law shall remain decisive as to whether privacy rights are accorded to a legal entity.

A – GENERAL PROVISIONS

Article 1

Scope

- (1) These Guidelines apply to civil claims arising out of the actual or threatened violation of privacy rights in cross-border cases. They include compensatory and injunctive relief as well as provisional measures.
- (2) The Guidelines apply to both contractual and non-contractual claims.
- (3) The following matters are excluded from the scope of these Guidelines:

of his or her right to respect for private and family life (see *MS v. Sweden* [GC], Application No 20837/92, 1997, para. 41 and *S. and Marper v. the United Kingdom* [GC], Application Nos 30562/04 and 30566/04, 2008, para. 41). Along these lines, in Opinion 1/2008 on data protection issues related to search engines the ‘Article 29 Data Protection Working Party’, set up under Article 29 of Directive 95/46/EC, underscored the link between the right to personal data and identity as selfhood when it noted that: ‘The extensive collection and storage of search histories of individuals in a directly or indirectly identifiable form invokes the protection under Article 8 of the European Charter of Fundamental Rights (WP 148 of 4.4.2008, at 7). An individual’s search history contains a footprint of that person’s interests, relations, and intentions. These data can be subsequently used both for commercial purposes and as a result of requests and fishing operations and/or data mining by law enforcement authorities or national security services’.⁹ In **Spain** courts have acknowledged the connection between privacy and personal data rights, but have gone further, providing a more detailed analysis of the role played by data protection. They have labeled data protection as a hybrid product that, on the one hand, guarantees other fundamental rights, particularly the right to honour and to privacy; and, on the other hand, establishes an independent right to protect individuals from the threats derived from new technologies (*Sentencia del Tribunal Constitucional* – STC 254/1993).

¹⁰ Similarly, see the Preamble to the Hague Principles on Choice of Law in International Commercial Contracts, paras 2 and 3.

(a) claims made by or the liability of governmental entities acting in the exercise of public authority;

(b) intellectual property rights.

10. Article 1(1) indicates that the Guidelines apply to the protection of privacy rights as broadly defined in Article 2. It further clarifies that the scope of the Guidelines is confined in two ways: the Guidelines apply only to civil claims, and only to cross-border cases.

11. The indication that the Guidelines apply to civil claims is intended to exclude from scope claims related to a situation where the State (including a government, a governmental agency or any person acting for a State) acted in its sovereign capacity ('*acta iure imperii*'). In the Committee there was consensus that the concept of civil claims is to be defined autonomously and that, to assess whether a claim is 'civil' for the purposes of the Guidelines, it is necessary to identify the legal relationship between the parties to the dispute, and to examine the basis and the rules governing the action brought. Provided a public authority did not act in its sovereign capacity (in accordance with the criteria indicated above), the claim qualifies as 'civil' and falls within the scope of the Guidelines.¹¹

12. As a result of the confinement of the scope to civil claims, both enforcement actions by public authorities and lawsuits against public authorities are excluded from scope, provided such authorities are acting in the exercise of their public powers (see also Article 1(3)(a)). Thus, for example, enforcement actions by data protection authorities (DPAs) do not fall within the scope of the Guidelines. Nevertheless, as observed during the discussions within the Committee, regardless of this exclusion from scope interfaces with public law are inevitable, especially in the area of personal data protection.¹² The regulatory framework of personal data protection is, in fact, characterized by a distinctive intertwinement of private and public enforcement. On the one hand, such intertwinement is exemplified in the fact that public policy, protection of local values and extraterritoriality are progressively assigned an extended role in the protection of personal data, and, as a result, a strengthening of the extraterritorial application of mandatory laws may be

¹¹ With regard to the nature of the claim, significant questions of characterization may arise. See *Bundesgerichtshof* (BGH), *Neue Juristische Wochenschrift* (NJW) 1979, 1101, where the Court rejected a lawsuit for defamation brought by the Official Church of Scientology against the head of Scotland Yard. See, on the other hand, BGH, 25 October 2016 – VI ZR 678/15 qualifying as 'civil' the claim for the violation of personal rights brought by the wife of the retired racing driver Michael Schumacher against the website of a Swiss State-owned broadcaster. Furthermore, in this context, the question arises as to whether the defamation lawsuits filed in response to President Trump's activity from his Twitter account should be characterized as civil or as covered by the sovereign immunity exception. While such claims at present are interstate and intrastate, they may be pictured as cross-border and provide a useful example of characterization and defamation via social media for the purposes of the commentary to this article. In this respect, see B. Hess, *The Private-Public Divide in International Dispute Resolution*, 388 *Recueil des Cours* (2018), at 108 and esp. fn 195 stating that Mr. Trump's tweets are part of the official communication of the U.S. President. Thus, they qualify as 'public' acts performed with the authority of the U.S. President. Consequently, individuals targeted by those tweets cannot institute litigation against Mr. Trump based on their 'private' nature.

¹² Under the Guidelines, privacy rights include the processing of personal data, as stated at Article 2.

observed in this area of the law.¹³ On the other hand (and against this backdrop), in the protection of personal data enforcement instruments of different nature are involved and combined: these are, namely, private remedies, public supervision and control, as well as substantive standards and procedural remedies. In particular, in this context the accessibility of private law remedies, including collective redress, has been reinforced and extended in a manner that transcends the realm of the mere private enforcement. This is evidenced, for instance, by Article 80(1) of the EU General Data Protection Regulation (GDPR)¹⁴ in the part where it states that EU Member States may confer (not only to individuals, but also) to qualified entities the right to file a complaint with the competent supervisory authority and to initiate collective redress actions, independently of a data subject's mandate.¹⁵ The enforcement of public values and interests by private entities is included in the scope of these Guidelines. Any limitations under public international law (such as immunities) remain unaffected.

13. The delimitation of the scope to civil claims is common in private international law instruments¹⁶ and is meant to overcome the discrepancies between national laws – and, in particular, to ensure that criminal proceedings, as well as constitutional, administrative and tax related matters are excluded from scope.¹⁷ However, this does not entail that claims characterized by preliminary (or incidental) issues (such as the permission of a processing activity by a data protection authority) are excluded from the scope of the Guidelines.

14. Private international law instruments often identify their scope making use of the term 'civil and commercial' or 'civil or commercial' (accompanied by both a set of autonomous definitions and a list of exclusions from scope). The inclusion of 'and/or commercial' is usually also meant to emphasize that the goal of the instrument is linked to facilitating cross-border business dealings. As emphasized by the joint reading of Article 1(1)-(2), the focus of the Committee's activity is on contractual and non-contractual claims brought on the grounds of an alleged violation of privacy rights. Accordingly, commercial claims are included as civil claims in the scope of the Guidelines.

15. Criminal law is excluded from the notion of civil claims. However, since the focus of the Guidelines is on the nature of the cause of action rather than the type of court where the claim is brought, compensatory civil claims brought in conjunction with, or within the framework of, criminal proceedings fall within the scope of the Guidelines. Assuming the claim may be characterized as 'civil', the Guidelines are meant to apply regardless of the nature of the court.

¹³ Illustrating such complex intertwinement, its nature and ramifications: B. Hess, *The Private-Public Divide in International Dispute Resolution*, 388 *Recueil des Cours* (2018), 49-266, esp. 167-177.

¹⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1.

¹⁵ *Id.*, 172-173.

¹⁶ B. Hess and C. Oro Martinez, 'Civil and Commercial Matters', *Encyclopedia of Private International Law* (2017), 347.

¹⁷ On the one hand, some civil law jurisdictions consider commercial matters as a sub-category of civil matters, whereas others regard them as mutually exclusive categories. On the other hand, in common law countries the term 'civil law' is used to distinguish civil from criminal proceedings, and constitutional, administrative and tax related matters fall within the category of 'civil law'. See B. Hess and C. Oro Martinez, Civil and Commercial Matters, in: *Encyclopedia of Private International Law* (2017), 347.

This entails that the Guidelines apply, for instance, regardless of whether the action is brought before a civil, criminal, or administrative court.¹⁸

16. With regard to the inclusion in the scope of the Guidelines of cross-border cases only, such limitation is meant to exclude from scope purely domestic cases: the cross-border requisite should be interpreted broadly and as including all those cases that have a cross-border element, and not only those cases where the parties have their habitual residence in different States. For this reason, Article 2(3) of the Guidelines provides an autonomous definition of the term ‘cross border cases’.¹⁹

17. In consideration of the importance of – where possible – averting (rather than providing redress for) the violation of privacy rights, pursuant to Article 1(1) the scope of the Guidelines is extended to encompass both actual and threatened violations of privacy rights against individuals. During the discussions within the Committee, it was indicated that ‘threatened’ should be construed as ‘prospective’.

18. Against this backdrop, pursuant to Article 1(1) (and Article 2(4)) the Guidelines apply to compensatory damages, as well as injunctive relief and provisional measures. As a standalone remedy or in addition to compensatory relief, injunctions are of crucial importance in the protection of privacy rights since, by ordering the defendant to cease a specified act or behaviour and/or desist from it, they contribute to the preservation of the status quo or to the prevention of a threatened violation. Analogous considerations apply with respect to the inclusion in the scope of the Guidelines of provisional measures.²⁰

19. Pursuant to Article 1(2) the Guidelines apply to both contractual and non-contractual claims, in the traditional as well as in the digital and cyber framework. In fact, the Guidelines are primarily meant to cover tortious violations of privacy and data rights. However, they are also meant to cover violations arising in the context of contractual relations, especially between social media providers and users. In particular, the Committee aims to investigate whether and to which degree the occurrence of privacy and data rights violations in the cyber context shape and potentially modify the traditional definition and articulation of contractual and non-contractual violations and related remedies.²¹

20. Questions of legal standing, especially with respect to non-contractual claims (respectively, between users; between users and non-users; between users and Internet/social media providers; between non-users (or potential users) and Internet/social media providers), are of particular relevance. This is evidenced, for instance, by the recent litigation on collective redress;²² on the liability, for the processing of personal data, of the administrator fan page hosted on a social network and the concept of controller’s responsibility;²³ on the unauthorised collection of data from non-users through the use of so-called ‘datr’ cookies and social plug-

¹⁸ See, for instance, Articles 77 and 79 GDPR.

¹⁹ By regulating the case of torts claim governed by the law of a territorial unit of multi-state legal orders, Article 17 provides further assistance in this context (see infra).

²⁰ See more in detail the commentary under Article 2(4) of the Guidelines.

²¹ In this framework, questions such as collective redress and protection of weaker parties (consumers and minors) will also be examined.

²² CJEU, Case C-40/17, *Fashion ID* (currently pending); Case C-498/16, *Maximilian Schrems v. Facebook Ireland Ltd*, EU:C:2018:37.

²³ CJEU, Case C- 210/16, *Wirtschaftsakademie Schleswig-Holstein*, EU:C:2018:388; Case C-40/17, *Fashion ID* (currently pending).

ins;²⁴ as well as on the ‘find friends’ feature used by Facebook to automatically generate invitations to all the contacts of a user without obtaining the recipients’ (potential-users) consent.²⁵

21. Contractual issues pertain, in particular, to the relationship between Internet providers and users. In this context, questions of party autonomy and limits thereto are compelling, as demonstrated by the latest developments in this area. The Committee has not decided whether a specific head of jurisdiction regarding contractual claims should be included in the Guidelines. However, choice of court agreements will be specifically addressed by the Guidelines. Therefore, the definition of the scope of the Guidelines clarifies that contractual claims are included.²⁶

22. By providing that claims made by, or the liability of, administrative authorities acting in the exercise of their public powers are excluded from the scope of the Guidelines, Article 1(3)(a), reinforces and clarifies the exclusion, provided at paragraph 1 of the same provision, of any claim other than civil claims from the scope of the Guidelines.

23. Personality rights and intellectual property rights are linked by an inherent contiguity. Such contiguity stems from the fact that both categories of rights protect intangible property and both contemplate a form of appropriation of one’s personality. Since intellectual property rights are traditionally registered in national registers, they are governed by the principle of territoriality. Consequently, Article (1)(3)(b) excludes registered rights from the scope of the Guidelines.²⁷ In fact, personality rights such as privacy, while linked to the person (and to his or

²⁴ See *Nederlandstalige Rechtbank van Eerste Aanleg Brussel*, 9 November 2015, *Debeuckelaere*, 15/57/C. Id., 16 February 2018, 2016/153/A.

²⁵ BGH, 14 January 2016 – I ZR 65/14. NJW 2016, 3445-3453. See also J. von Hein and A. Bizer, ‘Social Media and the Protection of Privacy: Current Gaps and Future Directions in European Private International Law, International Journal of Data Science Analytics, Special Issue 2018.

²⁶ For instance, confirming the relevance of this issue and the adaptations and adjustments that are progressively taking place in this context, Facebook recently updated its terms of service to include the following clause: ‘If you are a consumer and habitually reside in a Member State of the European Union, the laws of that Member State will apply to any claim, cause of action, or dispute you have against us that arises out of or relates to these Terms or the Facebook Products (“claim”), and you may resolve your claim in any competent court in that Member State that has jurisdiction over the claim. In all other cases, you agree that the claim must be resolved in a competent court in the Republic of Ireland and that Irish law will govern these Terms and any claim, without regard to conflict of law provisions’. Terms of service last updated on 19 April 2018, available at <https://www.facebook.com/legal/terms/update?ref=old_policy>. With many thanks to Professor Marta Requejo Isidro for sharing this information.

²⁷ See the work of the Committee on Intellectual Property and Private International Law available at the Committee’s page at www.ila-hq.org/index.php/committees. See, in particular, Third Committee Report (2016), Articles 1-2 of the Guidelines, outlining the scope of the Committee and defining intellectual property rights as copyright and related rights, patent, utility model, plant breeder’s right, industrial design, layout-design (topography) of integrated circuits, trademark, geographical indication and similar rights. For a comment underscoring the different nature of intellectual property rights from personality rights, see *ivi*, p. 11. On the core distinction between personality and intellectual property rights see also CJEU, Case C-523/10, *Wintersteiger*, EU:C:2012:220, paras 24-25 (citing AG Cruz Villalón’s Opinion in *eDate Advertising*, Joined Cases C-509/09 and C-161/10, EU:C:2011:192, para. 20, observing that, contrary to personality rights, which are protected in all Member States, the protection afforded by the registration of a national mark is, in principle, limited to the territory of the Member State in which it is registered, so that, in general, its proprietor cannot rely on that protection outside the territory) and para. 27. See also CJEU, Case C-170/12, *Pinckney*, EU:C:2013:635, paras 36-37.

her centre of interest), are not registered. Therefore, territoriality does not provide a suitable connecting factor for the protection of these rights.²⁸

Article 2

Definitions

(1) For the purposes of these Guidelines, the notion of privacy refers to an individual's rights to: (a) image and identity; (b) the seclusion of personal space; (c) reputation; (d) the processing of personal data; and (e) the confidentiality of personal communication.

(2) For the purposes of these Guidelines, individuals include companies and other bodies, corporate or unincorporated, insofar as privacy rights are accorded to them.

(3) For the purposes of these Guidelines, cross-border cases are cases which have connections with more than one State.

(4) For the purposes of these Guidelines, remedies include but are not limited to:

- (a) damages;
- (b) injunctive relief;
- (c) order of access to data;
- (d) order to correct data;
- (e) order to erase data;
- (f) order to block usage of data;
- (g) order to publish judicial decisions;
- (h) order for an apology;
- (i) right to reply.

24. Article 2 aims to provide clarification in respect of certain terms used in the Guidelines and to avoid reference to national law or other instruments in the interpretation of such terms, to the benefit of predictability and legal certainty.

25. A uniform concept of 'privacy' did not emerge from the National Reports. Absent a common concept of privacy,²⁹ the provision at Article 2(1) endorses an open approach and puts

²⁸ On the mosaic principle see *infra* at para. 75.

²⁹ See J.Q. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty', 113 *Yale Law Journ.* 1151 (2004). See also the 'Summary of the Human Rights Council panel discussion on the right to privacy in the digital age' in the Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, 19 December 2014, at 6. See, finally: D.J.

forth an autonomous and comprehensive definition of privacy which embraces both the narrow understanding, found in the United States, of privacy as a means to protect liberty and namely on the protection against intrusion in one's private space,³⁰ and a broader concept of privacy, which is proper of the continental legal systems and identifies privacy as a means to protect one's dignity and personhood.³¹ Privacy is also derived from the protection of private and family life in international human rights instruments.

26. The provision at Article 2 does not prejudice the question of which rights in fact exist and how these rights are viewed in the legal systems,³² and leaves these issues to the substantive applicable law.

27. The right to image and identity (Article 2(1)(a)) includes the right of an individual to control the use of the individual's name, image, likeness, or other unequivocal aspects of the individual's identity, including thoughts, feelings, personal experiences, geo-location information, and biometric data (including fingerprints, face and hand geometry, retina

Solove, 'Conceptualizing Privacy', 90 Cal. Law Rev. 1087 (2002); Id., "'I've Got Nothing to Hide" and Other Misunderstandings of Privacy', 44 San Diego Law Rev. 745 (2007).

³⁰ Although privacy is not protected by name in the Constitution of the **United States**, the U.S. Supreme Court has interpreted many of the amendments constituting the Bill of Rights to protect various elements of privacy. These include an individual's right to be free from unreasonable searches and seizures by the government (*Katz v. United States*, 389 U.S. 347 (1967)); the right to make decisions about issues involving 'fundamental' individual liberty interests such as contraception (*Griswold v. Connecticut*, 381 U.S. 479 (1965)); abortion (*Roe v. Wade*, 410 U.S. 113 (1973)), marriage, pro-creation, child rearing, and sexual intimacy (*Lawrence v. Texas*, 539 U.S. 558 (2003)); the right not to disclose certain information to the government (*Whalen v. Roe*, 429 U.S. 589 (1977)); the right to associate free from government intrusion (*NAACP v. Alabama*, 357 U.S. 449 (1958)); and the right to enjoy one's own home free from intrusion by the government (*Stanley v. Georgia*, 394 U.S. 557 (1969)), sexually explicit mail (*Rowan v. Post Office*, 397 U.S. 728 (1970)) or radio broadcasts (*Federal Communications Commission v. Pacifica Found*, 438 U.S. 726 (1978)) or others who would disrupt one's solitude (*Frisby v. Schultz*, 487 U.S. 474 (1988); *Carey v. Brown*, 447 U.S. 455 (1980)).

³¹ See, e.g., in **Germany**: *Entscheidungen des Bundesgerichtshofs in Zivilsachen* (BGHZ) 13, 334 = 7 NJW 1404 (1954); *Bundesverfassungsgerichts* (BVerfG) 119, 1 at para. 70 = 39 IIC 606, para. 70 (2008); see also *Marlene Dietrich*, Bundesgerichtshof 1 Blätter für Zürcherische Rechtsprechung (ZR) 49/97 (1 December 1999); in **France**: *Dumas v. Lifbert*, Cour d'appel (CA) Paris, 25 May 1867, 13 A.P.I.A.L. 247 (1867); CA Paris 8.7.1887, Ann. prop. ind. 1888, 287; *Tribunal de grande instance* (TGI) Seine (réf.) 2.11.1966, JCP 1966, II, 14875; CA Paris 7.6.1988, D. 1988, inf. rap., 224; *Conseil constitutionnel*, judgment No 94-352 DC of 18 January 1995 and judgment 99-416 DC of 23 July 1999; in **Spain** see the joint reading of Articles 10 and 18 of the Constitution and STC 53/1985. Possibly influenced by the European continental approach, Article 5, X of the Federal Constitution in **Brazil** recognizes the right to private life, intimacy, honour and image as fundamental rights. Similarly, in the **Republic of Korea** the Constitutional Court has recognized privacy as a right which is derived from the right to private life (Article 17) and the right to dignity and the pursuit of happiness (Article 10).

³² Until recently in **English law** there was no general tort of violation of privacy (see, e.g., *Wainwright v. Home Office* [2004] 2 AC 406; *Kaye v. Robertson* [1991] FSR 62). English courts developed and adapted the law of confidentiality and progressively shaped of a novel cause of action, i.e. the misuse of private information, to protect one aspect of invasion of privacy and to comply with the Human Rights Act 1998 (*Campbell v. MGN Limited* [2004] United Kingdom House of Lords (UKHL) 22; *Douglas v. Hello!* (No 3) [2006] Queen's Bench (QB) 125, at para. 53; *A v. B plc* [2003] QB 195 at para. 4). While it was recently ruled that misuse of private information is a civil wrong without any equitable characteristics and may be construed as a tort for jurisdictional purposes, this rule is specifically tailored to apply limited to the context of service of proceedings out of the jurisdiction. *Google Inc. v. Judith Vidal-Hall* [2015] England and Wales Court of Appeal (EWCA) Civ. 311, esp. para. 43. A similar situation occurs in **Canada**, where only recently the Ontario Superior Court decision expanded on the newly created tort claim of 'invasion of privacy' or 'intrusion upon seclusion' (see *Jones v. Tsige*, 2012 Ontario Court of Appeal (ONCA) 32 (Canadian Legal Information Institute - CanLII)) by creating a new tort of 'public disclosure of private facts'. See *Jane Doe 464533 v. N.D.*, 2016 ONSC 541 (CanLII).

recognition and voice). Notably, the increasing sophistication of facial recognition and other biometric technology is raising remarkable privacy challenges. Biometric privacy is proving to be a current subject of litigation, especially in the form of class actions: for instance, claims have been brought under Illinois and California law, respectively, against Facebook, Google and others alleging that the companies' face-scanning practices violate Illinois and California's unique biometric privacy law (which prohibits private companies from collecting biometric identifiers, including scans of facial geometry, without obtaining people's written consent).³³ Similar complaints have been brought (especially in the employment context) alleging that companies failed to provide notice or obtain consent before collecting individuals' fingerprints.³⁴ Additionally, information collected using cookies (often employed to track individuals' Internet surfing habits and news reading habits for advertising or other marketing purposes) has been found to constitute private or personal information.³⁵

28. The right to image and identity is designed to protect one's legal right to control both the commercial and non-commercial use of one's identity. In this context, the right to control the commercial use of one's identity (so-called 'right of publicity') is an area where the protection of privacy may overlap with that of intellectual property rights (which are excluded from the scope of these Guidelines according to Article 1(3)(c)).³⁶ In fact, among the legal rights that can be used to protect various aspects of an individual's image and personality are those stemming from (tort law and data protection law, but also from) copyright and trademarks law as well as from advertising standard codes. According to the Committee's approach, the decisive difference lies in the registration of a personality right. These Guidelines only address unregistered rights.³⁷

29. The right to the seclusion of personal space (Article 2(1)(b)) focuses, in particular, on the protection from unauthorised intrusions against an individual's personal space and bodily autonomy. 'Seclusion of personal space' is meant to extend to the one's private physical but also digital space, property and body. Private digital space encompasses an individual's private space in the cyberspace and electronic area, such as a user's Internet Protocol (IP) or cloud storage space. Governmental intrusions against an individual's personal space and bodily autonomy are in principle excluded from the scope of the Guidelines, provided the State (including a government, a governmental agency or any person acting for a State) acts in its sovereign capacity ('*acta iure imperii*') (see supra, Article 1(1) and 1(3)(a)).

30. The National Reports suggest a common definition of defamation (encompassing libel and slander) as any allegation or imputation of a fact made public that disparages the reputation of an individual to whom the fact is ascribed. While some legal systems characterize defamation and the right to reputation as falling within the scope of privacy, others do not on the grounds

³³ See *Patel v. Facebook*, 2018 WL 1050154 (N.D. Cal. Feb. 26, 2018); *Joseph Weiss v. Google Inc.*, No. 1:16-cv-02870, N.D. Ill., 2017 U.S. Dist. LEXIS 27276; *Rivera v. Google Inc.*, 238 F.Supp.3d 1088 (N.D. Ill. 2017); *Monroy v. Shutterfly Inc.*, No. 16-cv-10984 (N.D. Ill. Sept. 15, 2017); *In re Facebook Biometric Information Privacy Litigation*, 185 F.Supp.3d 1155 (N.D. Cal. 2016) *Norberg v. Shutterfly, Inc.*, No. 1:15-cv-5351 (N.D. Ill. June 17, 2015); *Martinez et al. v. Snapchat Inc.*, No. 2:16-cv-05182 (C.D. Cal.); *Licata v. Facebook, Inc.*, Nos. 3:15-cv-03748, 3:15-cv-03749, and 3:15-cv-03747 (N.D. Cal. 2015).

³⁴ See, e.g., *Baron v. Roundy's Supermarkets, Inc.*, No. 17-03588 (N.D. Ill. May 11, 2017).

³⁵ *Google Inc. v. Judith Vidal-Hall* [2015] EWCA Civ. 311. See also *Nederlandstalige Rechtbank van Eerste Aanleg Brussel*, 9 November 2015, *Debeuckelaere*, 15/57/C. Id., 16 February 2018, 2016/153/A.

³⁶ In this respect see also the Committee on Intellectual Property and Private International Law, Report presented at the Washington Conference (2014), at 12.

³⁷ See supra, para. 23.

that the object of the claims is different (a violation of privacy rights involves the unauthorised dissemination of truthful information whereas defamation entails the dissemination of information which is tainted by some degree of falsehood).³⁸ In keeping with its desire to provide for a comprehensive protection of privacy in private international and procedural law, there was support in the Committee to adopt a broad definition of privacy and include violations to the right to reputation in the scope of the Committee's inquiry (Article 2(1)(c)).

31. The protection of personal data is included in the scope of the Guidelines.³⁹ Taking inspiration from the definitions provided under the GDPR, the Committee agreed that 'personal data' may be defined as 'any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.⁴⁰ The term 'processing' may be construed to indicate 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.⁴¹

32. The right to the confidentiality of personal communication (Article 2(1)(e)) is a fundamental precondition for free flow of ideas and information and for the establishment and existence of a democracy.⁴² For the purposes of the Guidelines such right is included in the notion of privacy and extended to all forms of communication and correspondence, including in electronic form.

33. According to Article 2(2), individuals include 'companies and other bodies, corporate or unincorporated, insofar as privacy rights are accorded to them'. Consequently, for the purposes of the Guidelines the term 'individuals' includes legal entities, and not only natural persons. In

³⁸ A common feature portrayed by the National Reports of the continental **European States** is the steady reference to honour as being the object of protection of the laws against defamation. While in the **United Kingdom** and in the **United States** defamation is not considered to fall within the scope of privacy, the other National Reports inform that in their jurisdictions defamation is considered as both a civil and a criminal offence against one's privacy.

³⁹ See CJEU, Case C-131/12, *Google Spain SL*, EU:C:2014:317. Similarly, in October 2017 the Full Court of the Supreme Court of **Australia** upheld the decision that Google Inc. was liable for the defamatory content of the hyperlinks and paragraphs in search results on the claimant's name. *Google Inc. v. Duffy* ([2017] SASFC 130). An analogous matter is pending on appeal before the High Court of Australia in *Trkulja v. Google*, case M88/2017.

⁴⁰ See esp. Article 4(1) GDPR. See also the Brazilian Bill of Data Protection Act (Bill No 5276/2016 currently pending approval), which sets a tentative definition of personal data: 'data related to an identified or identifiable person, including identification numbers, locational data or electronic identifiers whenever those relate to a person' (Article 5, Section I, Bill of Data Protection Act). See also Art. 2 of the Modernised Convention 108 (CM/Inf(2018)15-final).

⁴¹ See esp. Article 4(2) GDPR. See also Art. 2 of the Modernised Convention 108 (CM/Inf(2018)15-final).

⁴² For instance, see for **France** Articles 226-15 and 432-9 of the criminal code and Article L 33-1 of the Code of postal and electronic communications; for **Germany** Sec. 1 *Grundgesetz* (GG) and Sec. 201 and 202 of the *Strafgesetzbuch* (StGB); Article 18(3) of the **Spanish Constitution**; Article 36 of the **Croatian Constitution**; Article 15 of the **Italian Constitution**; Article V of the **Brazilian Constitution**; see also Article 8 of the European Convention on Human Rights. In the **United States**, the right to the secrecy of letters and correspondence is derived through litigation from the Fourth Amendment to the U.S. Constitution: *Ex parte Jackson*, 96 U.S. 727, 733 (1877).

particular, the notion of ‘individual’ is extended also to entities that are not technically legally formulated to include partnerships and non-profit organizations.

34. With regard to the inclusion of legal persons in the notion of ‘individual’, the Committee noted that domestic laws may diverge as to whether legal persons are assigned privacy rights. As the National Reports demonstrate, while most legal systems warrant certain personality rights to legal entities (and, in particular, rights protecting the reputation), this issue lacks a uniform approach.⁴³ Nonetheless, the inclusion of legal entities in the notion of individual for the purposes of the Guidelines is justified on the grounds that the differences in the national laws should be immaterial and should not affect the (abstract) provisions on jurisdiction. Namely, the Guidelines do not preclude ‘a priori’ courts from establishing jurisdiction over claims brought by legal persons for the violation of personality rights: rather, they leave the question to be decided on the merits in accordance with the law applicable to the single case.

35. In particular, the Committee recalled the argument whereby, rather than as an end in itself, personality rights may be understood as instrumental for the effective protection of other fundamental rights. As remarked by Advocate General of the EU Court of Justice Bobek in his Opinion in *Bolagsupplysningen*, the protection of the personality rights of legal persons is instrumental to the realisation of other rights those persons enjoy, such as the right to property, or the freedom to conduct business. In this respect, ‘the violation of a company’s personality rights consisting in harm to their good name and reputation will directly translate into the infringement of their economic rights. Thus, the effective protection of those economic rights (that legal persons certainly enjoy) also requires the protection of their personality rights’.⁴⁴

36. Furthermore, the argument that a distinction between natural and legal persons should be introduced on the grounds that natural persons – unlike legal persons – should benefit from the protection afforded to weaker parties is not supported, especially with regard to jurisdiction over online violations of personality rights. As eloquently observed, again, by AG Bobek in his Opinion in *Bolagsupplysningen*, ‘The Internet, for better or for worse, completely changed the rules of the game: it democratised publication. In the age of private websites, self-posting, blogs, and social networks, natural persons may very easily distribute information concerning any other person, whether they are natural or legal, or public authorities. Within such technical settings, the initial idea that might have governed the early rules on harm caused by defamatory publications, and which assumed that the claimant is likely to be a weak individual whereas the defendant is a (professional) publisher, falls entirely to pieces’.⁴⁵

⁴³ E.g., in **France**, pursuant to Law 6 January 1978, the protection of one’s privacy is limited to natural persons. *Conseil d’Etat*, 15 February 1991, No. 68639, *Paris Church of Scientology*; *Id.*, 22 May 1995, No. 151288, *Midi-Pyrénées South PTT Union*. However, the law on defamation protects both legal persons and natural persons, and the right of reply may be exercised by a corporation. Act No. 82-652 of 29 July. 1982, s. 6, I, para. 1; L. Dumoulin, ‘Les droits de la personnalité des personnes morales’, 1 *Revue des sociétés* 2006, point 19. In **Spain**, courts have denied a fundamental right to privacy to public legal persons (STC 107/1988, of June 8). Legal persons are afforded protection for their privacy rights in **Croatia** (see the Croatian Constitutional Court U-III – 1558/2000 of February 19, 2004). In **England**, libel and malicious falsehood re construed to protect the reputation and the economic interests of legal entities: see *Tesla Motors Ltd v. BBC* [2013] EWCA Civ. 152; *Marathon Mutual Ltd v. Waters* [2009] EWHC 1931 (QB).

⁴⁴ Case C-194/16, *Bolagsupplysningen*, EU:C:2017:554, at paras 49 and 52 et seq.

⁴⁵ *Id.*, at para. 67. Concurring with the AG in the same case, see CJEU, EU:C:2017:766 ruling that Article 7(2) of Regulation (EU) No 1215/2012 is to be interpreted as meaning that a legal person alleging that its personality rights

37. Article 2(3) lays down a notion of ‘cross border cases’ that helps clarify the limitation of scope to cross-border cases under Article 1(1). Such requisite should be subject to a broad interpretation to encompass all those cases that have a cross-border element, and not only those cases where the parties have their habitual residence in different States. Some issues remain, however open. For instance, is the mere availability of information on the Internet sufficient to satisfy the cross-border requirement? Would the case be construed as cross border if two individuals, habitually residing in Germany, communicate in German via a social media platform: one of them posts defamatory statements against the other, and comments are subsequently posted by another user from another country?⁴⁶ Is the cross-border requirement satisfied in an action for liability arising from the operation of an Internet site, if both the defendant’s whereabouts and the location of the server hosting the Internet site in question are unknown?⁴⁷

38. As concerns the types of remedies and relief, Article 2(4) further clarifies the statement under Article 1(1) that ‘compensatory and injunctive relief as well as provisional measures’ fall within the scope of the Guidelines. It provides a list of remedies that not meant to be exhaustive.⁴⁸ The fact that a remedy is contained in this list means that it is covered by the Guidelines, but does not mean that it will necessarily be available in a particular case.

39. As regards, in particular, damages, the Committee has indicated that both material and immaterial damages are included in the Guidelines.⁴⁹ In particular, damages include pecuniary damages for actual losses and moral damages (where afforded in accordance with the law governing the damages).⁵⁰

40. Injunctive (including provisional) relief is included in the list at Article 2(4) in light of the sheer relevance that it may have in the context of remedies against the violation of privacy and personal data.⁵¹ In fact, markedly in the field of the protection of personal data, injunctions

have been infringed by the publication of information on the Internet can, in respect of the entirety of the harm sustained, bring proceedings before the courts of the Member State in which its centre of interests is located.

⁴⁶ This was the case in *Sieben Tage in Moscow* decided by the BGH, 29 March 2011 – VIZR 111/10. NJW, 2016, 3445-3453, showing that language plays a considerable role in this context.

⁴⁷ See, for instance, CJEU, Case C-292/10, *G v. Cornelius de Visser*, EU:C:2012:142 indicating that such occurrence should be sufficient in order to guarantee effective access to justice. The issue will be further discussed by the Committee.

⁴⁸ On the rights and remedies of the data subject, see also Arts 9 and 12 of the Modernised Convention 108 (CM/Inf(2018)15-final).

⁴⁹ In this regard, see also Article 82(1) of the GDPR stating that ‘Any person who has suffered material or nonmaterial damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered’.

⁵⁰ It emerges from the National Reports that all the jurisdictions surveyed afford pecuniary damages for actual losses suffered as a result of privacy violations. Moral damages against privacy violations are awarded in several jurisdictions (**Brazil, Croatia, France, Italy, Spain**) to cover against distress/moral damages; in **Australia**, under the Uniform Defamation Act moral damages are capped: s 35. In **Germany**, they pursue not only the aim of compensating, but also that of gratifying the plaintiff and deterring such future demeanours by the defendant. See *Herrenreiter*, BGH - NJW1958, 82. However, in Germany moral damages do not qualify as punitive damages and they may be awarded only if the detriment is sufficiently serious and if there is no other way to compensate it. On punitive damages see more in detail, infra.

⁵¹ Injunctions to prevent and/or terminate the infringement of privacy rights are commonly available in the civil law jurisdictions: cease and desist orders – along with the other provisional measures and seizures – are available in **Brazil, Belgium, Croatia, France, Germany, Italy** and **Spain**. See *Practice Guidance: Interim Non-Disclosure Orders*, issued by the Master of the Rolls, [2012] 1 WLR 1003. 366. **U.S. courts**, on the other hand, appear

in the form of orders of access to data, rectification, cancellation and block usage of data give the data subject the power to protect personal information and exercise an effective control.

41. The right to access data (Article 2(4)(c)) is reminiscent of Article 15 GDPR, which assigns the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data. However, a recent U.S. judgment in this area of the law is particularly noteworthy in that it gave a company the right to access the data that Internet users post on their user-page on a social media platform (LinkedIn). In fact, a U.S. federal judge recently ruled that Microsoft Corp's (MSFT.O) LinkedIn unit cannot prevent a start-up from accessing public profile data, in a test of how much control a social media site can wield over information its users have deemed to be public. LinkedIn invoked a federal anti-hacking law in telling the plaintiff (hiQ) to cease the tracking. LinkedIn also installed technical blocks to prevent the plaintiff from accessing otherwise publicly available information on LinkedIn users. In his preliminary injunction the judge's gave LinkedIn a day to remove those blocks.⁵²

42. The right to the rectification of data (Article 2(4)(d)) gives the right to obtain from the controller the rectification of inaccurate personal data concerning the data subject itself. For instance, an employee may request and obtain that the medical report, carried out by a medical practitioner at the request of the employer and contents of which the employee considers to be inaccurate, be rectified to reflect the accurate description of the employee's particular circumstances.

43. The right to the erasure of data (Article 2(4)(e)) gives the right to obtain the cancellation or removal of personal data concerning him. In this respect, in January 2018 a case was settled in a highly publicised legal action relating to the publication of an inappropriate photograph of a Northern Irish 14 year old girl, posted on a Facebook shame page. While the case was settled and only limited information is available, Facebook maintained the position that the picture was taken down as soon as notification of the data subject's request to have the data erased was received. The victim's right to have her personal data erased from the Facebook shame page would no doubt have featured as an important legal point in the case, in which the victim was seeking damages for the misuse of her personal data. With regard to data unlawfully collected on the Internet, in February 2018 the Dutch Chamber of the Court of First Instance in Brussels ordered Facebook to delete all the data concerning Belgian citizens obtained illegitimately through the use of so-called 'datr' cookies, which allowed Facebook to collect information also with regard to the Belgian citizens who were not Facebook users. The Court ruled that Facebook's processing of personal data of both Facebook users and non-Facebook users for tracking purposes by means of cookies, social plug-ins and pixels, violates the Privacy Act and Cookie Act.⁵³

generally hesitant to issue injunctions and issue them only to avoid irreparable injury or if monetary damages are inadequate. *See, e.g., Walgreen Co. v. Sara Creek Property Co.*, 966 F.2d 273 (7th Cir. 1992) (the court reluctantly granted injunction because of difficulty of calculating money damages).

⁵² *hiQ Labs, Inc. v. LinkedIn, Corp.*, Case No 17-c-03301-EMCV, U.S. District Court for the Northern District of California, 14 August 2017. An appeal was filed on 5 September 2017 and is pending before the U.S. Court of Appeals for the Ninth Circuit.

⁵³ *Nederlandstalige Rechtbank van Eerste Aanleg Brussel*, 16 February 2018, *Debeuckelaere*, 2016/153/A.

44. A renowned ruling in the context of the right to the erasure of data is represented by the decision of the CJEU in *Google Spain*.⁵⁴ After stating that Google qualifies as a ‘controller’ pursuant to the (then applicable) Data Protection Directive,⁵⁵ the Court ruled that personal data must be retained for limited periods (namely, only for as long as it is relevant) and that, beyond such period, the data subject enjoys the right to have the data removed. In particular, the judgment requires the search engine to, under certain circumstances, block access to pages that ‘appear to be inadequate, irrelevant or no longer relevant or excessive... in the light of the time that had elapsed’.⁵⁶ Even accurate data which was initially legally published can be de-listed, the Court said, since such data can ‘in the course of time become incompatible with the directive’.⁵⁷ However, in its 2017 ruling in *Manni*, the CJEU limited this right and held that the right to be forgotten cannot be generally applied to a company register (though the Court did suggest that there may be some very limited circumstances where limitations might be imposed on access to personal data held on such a register).⁵⁸

45. Orders to block usage of personal data (Article 2(4)(f)) are becoming increasingly frequent in connection with methods and devices used to track the online behaviour of people (users and non-users), even if they are not logged on to a given site. In fact, as the following cases illustrate, placing cookies and invisible pixels on third party web sites allows to track down a user’s activity, also when the user is not logged on to the website that placed the cookie. Furthermore, depending on the ‘smart device’ employed, the tracking may be extended also to the online activity of non-users. For instance, this was the case in the first segment of the claim mentioned supra and brought before the Dutch Chamber of the Court of First Instance in Brussels: in this first part of the procedure, the Court issued a provisional measure ordering Facebook to cease collecting (and sharing with potential advertisers, and media content providers) data from non-users through the use of ‘datr’ cookies.⁵⁹ On a separate note, many reported cases before the English courts concern applications to renew or set aside interim injunctions, often granted initially without notice to the defendant, restraining the publication of private information. Such injunctions may be granted against persons unknown, or against the world.⁶⁰

⁵⁴ CJEU, Case C-131/12, *Google Spain SL*, EU:C:2014:317.

⁵⁵ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (now superseded by the GDPR), [1995] OJ L 281/31.

⁵⁶ CJEU, Case C-131/12, *Google Spain SL*, EU:C:2014:317, at para. 93.

⁵⁷ *Id.*, paras 93-94.

⁵⁸ CJEU, Case C-398/15, *Manni*, EU:C:2017:197, esp. paras 55-56. Manni, an Italian, challenged the availability of his personal data recorded in a local company register, alleging that this information – which disclosed that he had been the administrator of another company that went bankrupt – was damaging his current business. Observing that Italian company law did not impose any period for which data had to be retained, the CJEU reasoned that it was ‘impossible... to identify a single time limit, as from the dissolution of a company, at the end of which the inclusion of such data in the register and their disclosure would no longer be necessary’. This led the CJEU to hold that ‘Member States cannot... guarantee that the natural persons... have the right to obtain, as a matter of principle, after a certain period of time... the erasure of personal data concerning them, which have been entered in the register pursuant to the latter provision, or the blocking of that data from the public’.

⁵⁹ *Nederlandstalige Rechtbank van Eerste Aanleg Brussel*, 9 November 2015, *Debeuckelaere*, 15/57/C.

⁶⁰ *Venables v. News Group Newspapers* [2001] Fam 430; *X v. Persons Unknown* [2007] EWHC 2783 (QB); *TUV v. Person or Persons Unknown* [2010] EWHC 853 (QB). In 2010, a number of high-profile cases raised concerns about the practice of the courts of granting ‘super injunctions’, also restraining disclosure of the fact of grant of the

46. Orders to publish judicial decisions and for an apology (Article 2(4)(g)-(h)) provide a form of immaterial redress, in particular in the context of the violation of privacy rights. The right of reply (Article 2(4)(i)) generally carries the right to defend oneself against public criticism in the same venue where it the criticism was conveyed. It is usually applied in the context of print-media (newspapers) but can also be applied to webpages. The right of reply is distinct from the order for an apology, which entails that the publisher itself revoke the original statement.⁶¹

47. Punitive damages are not part of the list of remedies put forth at Article 2(4). In this respect, the Committee has taken note of the fact that the treatment warranted to punitive damages may differ significantly from legal system to legal system.⁶² In light of the non-exhaustive nature of the list, this exclusion is not conclusive and the recourse to such damages is simply left to the law applicable to the case. However, the Committee is mindful that the question of punitive damages will have to be taken in account in the Committee's future activity on the recognition and enforcement of judgments.

injunction itself (*LNS v. Persons Unknown* [2010] EWHC 119 (QB), [2010] EMLR 16), but such injunctions are now considered only in exceptional cases as departures from the general principle of open justice.

⁶¹ According to the National reports, the right of reply is commonly granted in the different jurisdictions, albeit with different strength. While in **Brazil** the right of reply benefits from no less than constitutional protection, in Croatia, France and Germany it is statutorily guaranteed. In **Germany** and **Spain**, however, a reply is only allowed with in response to factual statements, whereas it is not made available with respect to value judgments or opinions. In **England**, attempts to introduce the general right of reply were unsuccessful. However, there are statutory or self-imposed rules that are similar to or require the recognition of the right of reply. In the **U.S.**, on the other hand, the right of reply is acknowledged, but it has been at times substantially curtailed and suppressed by the courts on the principle that, under the First amendment to the U.S. Constitution, a State cannot tell a newspaper what it shall print. See *Miami Herald Publishing Co. v. Tornillo*, 418 U.S. 241 (1974).

⁶² With specific regard to punitive damages, the National Reports portray a heterogeneous situation. While in the U.S. courts may award punitive damages for the breach of privacy rights if the defendant's behaviour is so egregious or its resulting cost so high that the court deems it necessary to deter and sanction such behaviour, in continental Europe this option is not granted. E.g., in **Australia**, **Croatia**, **France**, **Italy** and **Spain** the principle of full compensation is applied and punitive damages are not awarded. As mentioned supra, in **Germany**, moral damages pursue not only the aim of compensating, but also that of gratifying the plaintiff and deterring such future demeanours by the defendant. See *Herrenreiter*, BGH NJW 1958, 82. However, in Germany moral damages do not qualify as punitive damages and they may be awarded only if the detriment is sufficiently serious and if there is no other way to compensate it. In general, under **English law** punitive damages are available in tort claims which involve an unlawful exercise of power by a public official, or where a tortfeasor has intentionally or recklessly profited from their wrongdoing in a way which exceeds the loss suffered by the claimant, or where otherwise authorised by statute. See *Rookes v Barnard* (No. 1) [1964] AC 1129. Either could include defamation cases, although a recent study suggests that punitive damages are (contrary to popular belief) in fact rarely awarded in defamation cases. See J.Goudkamp and E. Katsampouka, 'An Empirical Study of Punitive Damages' (2018) 38 Oxford Journal of Legal Studies 90. In English law breach of privacy, on the other hand, is closely related to breach of confidence, which is not a claim in tort but in equity, and there is authority to suggest that punitive damages are not available for such claims: see <http://www.bailii.org/ew/cases/EWHC/QB/2008/1777.html>.

B – JURISDICTION

Article 3

Jurisdiction at the defendant's habitual residence

- (1) The defendant may be subject to the jurisdiction of the courts of the State in which it is habitually resident.
- (2) For the purposes of these Guidelines, apart from in the context of Article 10(2), the habitual residence of a corporation includes:
 - (a) the State of the place of incorporation;
 - (b) the State of the principal place of business.
- (3) For the purposes of these Guidelines, the habitual residence of a corporation includes a State other than those under Article 3(2)(a) or (b) with which the defendant has essentially equivalent contacts.

48. Pursuant to Article 3, the courts of the State of the defendant's habitual residence may assert jurisdiction over the defendant, irrespective of whether the claims are related to the defendant's activities in the forum State.

49. Article 3(1) lays down the principle whereby the defendant should be subject to the jurisdiction of the courts of the State of the defendant's habitual residence. With regard to natural persons, the Guidelines do not provide an autonomous interpretation of the term 'habitual residence'. While according to regional and international instruments such concept is frequently left to be interpreted in accordance with the law of the forum,⁶³ the question arises as to whether this solution is actually appropriate with respect to an international instrument. While in the regional context, for instance, of the European Union, the difference in the laws of the Member States in this regard was noted but the conclusion was reached that 'the national courts have no difficulties in applying their definition of domicile',⁶⁴ with respect to an international instrument the question – and absent the mutual trust that characterizes the relationship between EU

⁶³ See for instance, the 2005 Hague Convention on Choice of Court Agreements, which defines 'residence' with regard to an entity or person other than a natural person at Article 4(2) but leaves the definition of residence of a natural person to the *lex fori*. Along the same lines, although with respect to the concept of 'domicile', see the Brussels I *bis* Regulation (Article 62). See also the commentary to Article 59 of the Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, signed in Lugano on 30 October 2007 ('2007 Lugano Convention') in the Explanatory Report by F. Pocar [2009] OJ C 319/01, para. 26, relaying that 'While it recognised the potential benefits of a common definition, the working party preferred to leave to national laws the task of defining the meaning of domicile in terms of the length of time the defendant had been in the territory, if such a definition was found to be necessary'. However, for an approach which is more inclined towards an autonomous definition, see Regulation (EU) No 650/2012 of the European Parliament and of the Council of 4 July 2012 on jurisdiction, applicable law, recognition and enforcement of decisions and acceptance and enforcement of authentic instruments in matters of succession and on the creation of a European Certificate of Succession ('Succession Regulation'), [2012] OJ L 201/107, esp. recitals 23-24.

⁶⁴ B. Hess, T. Pfeiffer, P. Schlosser, 'Report on the Application of Regulation Brussels I in the Member States' Study JLS/C4/2005/03 ('Heidelberg Report') (2007), para. 186.

Member States – an autonomous definition of the habitual residence of a natural person may, in fact, enhance transparency and predictability.

50. For the purposes of Article 3(1), the habitual residence should reveal a close and stable connection of the defendant with the forum State. In particular, to determine the habitual residence of a natural person an overall assessment of the circumstances of the individual preceding the facts and at the time of the claim should be performed, considering all the relevant factual elements, and notably the duration and regularity of the individual's presence in the forum State and the conditions and reasons for that presence. In some cases, identifying the individual's habitual residence may prove complex: this could be the case, for instance, where the individual relocates abroad for professional or economic reasons, sometimes for a prolonged period of time, but maintains a close and stable connection with his or her State of origin. In such case, and depending on the circumstances of the case, the individual could be considered still to have the habitual residence in his or her State of origin in which the centre of interests of his/her family and his/her social life is located. Other complex cases may arise where the individual lives in several States alternately or travels from one State to another without settling permanently in any of them. In this case, if the individual is a national of one of those States, his or her nationality could be considered as a special factor in the overall assessment of all the factual circumstances for the purposes of establishing jurisdiction in accordance with Article 3(1).⁶⁵

51. Article 3(2) provides an autonomous definition of 'habitual residence of a corporation' for the purposes of the Guidelines. Notably, under Article 3(2) the place of 'habitual residence of a corporation' includes (a) the State of the place of incorporation, and (b) the State of the principal place of business. This definition of place of 'habitual residence of a corporation' is meant to accommodate the different nuances that characterize the understanding of a corporation's place of habitual residence for the purposes of establishing jurisdiction. The place of incorporation embodies a criterion which is quite stable and may not easily be changed. The notion of 'principal place of business' is a factual notion and indicates the place where the main, i.e. the chief and most important, business activities are located. The Guidelines do not provide a hierarchy between such criteria: the criteria operate on an equal footing and are exhaustive. While the fact that this definition is articulated in two alternative criteria extends the competent fora, the fact that the criteria indicated in the two prongs are exhaustive narrows the jurisdiction to courts of States with which the corporation has its most significant ties, to the benefit of transparency and predictability.

52. Article 3(3) introduces a supplementary definition of habitual residence of a corporation. This provision, and markedly the use therein of the term 'essentially equivalent', aims at comprising the U.S. approach to this matter and accommodate, in particular, the wording used by the U.S. Supreme Court in its decision in *Bauman*.⁶⁶ Like *Morrison*⁶⁷ and *Kiobel*,⁶⁸ *Bauman* was a 'foreign cubed' case, in which a foreign plaintiff sued a foreign defendant based on conduct that occurred in a foreign country. Finding that considerations of international rapport reinforced the determination that subjecting Daimler to the jurisdiction of courts in California would not

⁶⁵ Similarly, see also the Succession Regulation, at recitals 23-24.

⁶⁶ *Daimler AG v. Bauman*, 134 S. Ct. 746 (2014). See, in part., L.J. Silberman, 'Daimler v. Bauman: A New Era for Judicial Jurisdiction in the United States', 16 Yearbook of Private Int'l Law 1 (2014-2015).

⁶⁷ *Morrison v. National Australia Bank*, 561 U.S. 247 (2010).

⁶⁸ *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659 (2013).

accord with the ‘fair play and substantial justice’ due process demands, in *Bauman* the U.S. Supreme Court ruled that courts may exercise jurisdiction over a defendant ‘to hear any and all claims against it’ only when the defendant’s affiliations with the forum State ‘are so constant and pervasive as to render it essentially at home in the forum State’.⁶⁹ Mindful of such wording, the supplementary definition provided at Article 3(3) is aimed at comprising in the ‘habitual residence of a corporation’ also instances that go beyond the definitions put forth at Article (2)(a)-(b), provided the defendant’s contacts with the forum State are so significant and stringent that, for jurisdictional purposes, they render the forum State ‘essentially equivalent’ to the defendant’s home.⁷⁰ In so doing, the Court indicated that the fact that a corporation does substantial business in a State is not by itself sufficient to confer that State’s courts with jurisdiction over the corporation.

53. Article 3 does not touch upon the national rules of venue: accordingly, venue remains subject to the national law of the State of the defendant’s habitual residence.

54. The Committee discussed whether there should be forum non conveniens exceptions to the general principle that the defendant should be subject to the jurisdiction of the courts of the State of the defendant’s habitual residence. While the Committee decided to put the question on hold for the time being, there was general consensus that a cooperation / coordination mechanism between courts would prove beneficial and should be taken into consideration.

Article 4

Jurisdiction based on conduct

- (1) A person may be sued in the courts of the State where the act or omission directly causing the harm occurred, irrespective of where the damage arose.
- (2) A person may also be sued at the plaintiff’s centre of main interest, unless the defendant could not have reasonably foreseen substantial consequences of his or her act or omission occurring in that State. The person’s main centre of interest is presumed to be at his or her place of habitual residence.
- (3) A person may also be sued in the State to which the publication in question is principally directed, taking into account, in particular,
 - (a) the language of the publication;
 - (b) the content of the publication;
 - (c) the physical location of the intended audience.

⁶⁹ 134 S. Ct. 751 (2014) (internal quotation marks and brackets omitted). Emphasis added.

⁷⁰ However, against this backdrop, the Committee has taken note of the Court’s statement in footnote 19 of the decision: such statement may be read to indicate that, in a case such as the one examined, jurisdiction may only be established in a place that is unique and ascertainable and that only in exceptional cases would such jurisdiction be possible outside of the paradigm basis according to which all-purpose fora are a corporation’s place of incorporation and principal place of business.

55. Article 4 regulates jurisdiction over non-contractual claims. Non-contractual claims are characterized by the absence of obligations freely assumed by one party towards another and by a possible breach of rules of law. Such claims are at the core of privacy violations, both in the traditional setting and in the area of digital interconnectivity. In particular, in the area of digital interconnectivity tortious breaches may stem from the unauthorised collection and processing of personal data, including the case where the processing of personal data takes place subsequent to the data subject's withdrawal of consent. Data breaches are recurrent in particular with respect to 'smart' devices that collect personal data such as IP addresses, zip codes, product model numbers, hardware and software versions, chipset IDs, region and language settings, browsing and content-viewing histories and share that information with interested third parties.⁷¹ This is notorious with respect to search engines, web browsers, and apps. However, it is true also of all appliances that require an account: for instance, a smart TV (especially if it comes with a camera or a voice recognition microphone) can be a means to collect and share data, including channel information, broadcast source data, TV platform information and even data from a connected USB. Likewise, an operating system can keep tabs and collect data in order to serve ads.

56. While the provision at Article 3 is meant to apply to both contractual and non-contractual claims, and it applies irrespective of whether the claims are related to the defendant's activities in the forum State, Article 4 provides additional fora (which are characterized by a significant proximity of the claim with the forum, as further explained *infra*) where the plaintiff may bring a non-contractual claim, provided such claim falls within the scope of the Draft Guidelines and provided the specific criteria put forth in the provision are met.

57. Pursuant to Article 4(1) 'A person may be sued in the courts of the State where the act or omission directly causing the harm occurred, irrespective of where the damage arose'. In accordance with this provision, both acts or omissions are relevant for jurisdictional purposes. An act entails the undertaking of a specific dynamic conduct: for instance, the unauthorized circulation of untruthful information on an individual by releasing it to the press, or through television broadcasting or, again, by posting it on a social media platform may satisfy this requirement, as does the unauthorised collection of data from non-users through the use of digital devices, e.g., cookies and social plug-ins.⁷² On the other hand, the failure of the administrator of an Internet forum to remove the damning and untruthful information posted by one user against another individual amounts to an omission for the purposes of this provision. An omission also occurs, for instance, when the law imposes on a person the duty to take adequate action and redact the name or personal data of an individual from a given document which is meant to undergo a certain degree of circulation, but the person fails to comply with such duty.⁷³ Failure

⁷¹ See D.P. Stewart, 'The Approach of North American Courts towards the Internet', in *Human Rights, the Digital Society and Law: A Research Companion* (draft; forthcoming, 2019).

⁷² See *Nederlandstalige Rechtbank van Eerste Aanleg Brussel*, 9 November 2015, *Debeuckelaere*, 15/57/C. Id., 16 February 2018, 2016/153/A. See also BGH, 14 January 2016 – I ZR 65/14. NJW 2016, 3445-3453.

⁷³ This would be the case, for example, where the a plaintiff filed a claim before a federal court in the United States but disregarded the rule which provides, in relevant part, that a party or non-party making an electronic filing (as well as a paper filing) that contains another individual's Social Security number, taxpayer identification number, or birth date, or the name of a person known to be a minor or a financial account number shall redact such sensible and personal information from the filing. In particular, the plaintiff may include, unless the court otherwise orders, only: (1) the last four digits of the Social Security number and taxpayer identification number; (2) the year of the individual's birth; (3) the minor's initials; and (4) the last four digits of the financial account number. See Federal Rule of Civil Procedure 5.2.

to comply with this duty, which is meant to protect the defendant's personal data, gives rise to the plaintiff's liability for the damages caused by this omission.

58. For Article 4(1) to apply, the act or omission must 'directly' cause the harm. Accordingly, for the purposes of establishing jurisdiction a direct 'causal nexus' – a reasonable and direct causal relationship – must link the act or omission with the harm: in particular, the harm must directly, immediately, and naturally flow from the act or omission. For instance, the online posting of incorrect or defamatory statements is an act that may cause direct harm to an individual's reputation and business: as such, it may qualify for the purposes of this provision.

59. On the other hand, according to Article 4(1) the criterion of the State of the place where the damage arises may not be used to establish jurisdiction under the first paragraph.⁷⁴ In particular, this choice accommodates the rules adopted in some legal systems which, absent further stringent contacts, do not find it constitutionally proper to establish jurisdiction over an out-of-State defendant in the State of the place where the damage arose. For instance, in the United States the U.S. Supreme Court has constantly ruled that specific personal jurisdiction comports with due process only where 'the defendant's suit-related conduct' creates 'a substantial connection with the forum state' and that the mere fact that the damage arose in a State fails to satisfy such requirement.⁷⁵

60. By relying on a single jurisdictional connection and confining the jurisdiction to the State where the act or omission 'directly' occurred, Article 4(1) favours predictability: in fact, the defendant – with whom lies the control over the act or omission that directly gives rise to the harm – may reasonably be expected to be able to identify *ex ante* such place and may therefore foresee being sued in the courts of such place.

61. Article 4(1) does not affect the national rules of venue: accordingly, venue remains subject to the law of the forum State.

62. Pursuant to Article 4(2) a person may also be sued 'at the plaintiff's centre of main interest, unless the defendant could not have reasonably foreseen substantial consequences of his or her act occurring in that State'. This provision moves from the assumption that the State to which the holder of personality rights is more significantly connected by reason of personal and professional ties is also the place in which he or she suffers the most extensive and serious harm as a result of the personality right violation.⁷⁶ Notably, this provision points to the place where

⁷⁴ However, it should be noted that relevance to the place of damage may stem from Article 4(2), provided that 'the defendant could not have reasonably foreseen substantial consequences of his or her act occurring in that State'.

⁷⁵ See *Walden v. Fiore*, 134 S. Ct. 1115, 1121-22 (2014); see also *J. McIntyre Machinery, Ltd. v. Nicastro*, 564 U.S. 873, 881 (2011) (plurality opinion) holding that, because a machinery manufacturer never engaged in activities in New Jersey with the intent to invoke or benefit from the protection of the state's laws, New Jersey lacked personal jurisdiction over the company under the due process clause, regardless of the fact that the damage was sustained in New Jersey.

⁷⁶ CJEU, Joined Cases C-509/09 and C-161/10, *eDate Advertising*, EU:C:2011:685, esp. paras 48-49. See also ECtHR, *Arlewin v. Sweden* (judgment of 1 March 2016, Application No 22302/10), para. 73 holding that Sweden had an obligation, under Article 6 of the European Convention on Human Rights (ECHR), to provide a Swedish national residing in Sweden with an effective access to court in a defamation claim over a TV program broadcasted by a London-based company, but targeting mostly, if not exclusively, a Swedish audience. See Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos 11 and 14, 4 November 1950, ETS 5, available at: <<http://www.refworld.org/docid/3ae6b3b04.html>>.

the courts are presumably best placed to assess and understand fully the conflict between the interests involved in the claim.

63. Article 4(2), second sentence, puts forth an autonomous concept of ‘centre of main interest’ in the part where it defines such place as that of the plaintiff’s habitual residence. In particular, the place of the plaintiff’s habitual residence is commonly the place where the plaintiff has established its most significant connections. It is also a place where the alleged perpetrator may foresee that harm might occur as a result of his or her conduct and, accordingly, where he or she may reasonably foresee being sued. For instance, deciding on a libelous article written and edited by the defendants in Florida, the U.S. Supreme Court ruled in *Calder* that jurisdiction was proper in California based on the ‘effects’ of the defendants’ Florida conduct in California. As the Court held, the defendants were in a position to reasonably foresee being sued in California on the grounds that the allegedly libelous story concerned the California activities of a California resident (a television entertainer). As the Court noted, the petitioners (both employed by the Florida-based newspaper that published the article) wrote and edited an article (for which most of the research was done in Florida) that they knew would potentially have an impact upon the California-based plaintiff.⁷⁷

64. However, a plaintiff may also have the centre of his or her main interests in a State other than the one of habitual residence. Accordingly, in Article 4(2) the definition that identifies the plaintiff’s centre of main interest in the plaintiff’s place of habitual residence is drafted as a presumption and is rebuttable: the seized court will assume that a person’s centre of main interest is located in the place of the person’s habitual residence, unless proof to the contrary is provided. This may be the case where factors – such as the pursuit of a professional activity in a State other than the one to which the plaintiff is linked by his or her most significant family ties or the one in which the plaintiff is incorporated– establish the existence of a particularly close connection with another State.⁷⁸ This latter State may be the place where the plaintiff suffers the most extensive and serious harm as a result of the violation, and it may embody the centre of his or her main interests for the purposes of the provision. In light of the plaintiff’s significantly close link (and, once again, subject to the exception put forth in the second sentence of Article 4(2)), this place is also readily ascertainable by the perpetrator, who should then be in a position to foresee being sued there.

65. To strengthen foreseeability and to balance any residual unpredictability that may arise from identifying the relevant jurisdictional factor in the plaintiff’s centre of main interest, the second part of the first sentence of Article 4(2) adds the condition whereby the plaintiff’s centre of main interest operates as a ground to establish jurisdiction ‘unless the defendant could not have reasonably foreseen substantial consequences of his or her act occurring in that state’. This provision is meant to capture, in particular, the foreseeability requirement that is at the core of the due process analysis in the United States. Notably, pursuant to the U.S. Supreme Court’s reading of the due process clause, for jurisdiction to be constitutionally proper it is critical ‘that

⁷⁷ *Calder v. Jones*, 465 U.S. 783 (1984), esp. 786. See also *supra*, fn. 4.

⁷⁸ CJEU, Case C-194/16, *Bolagsupplysningen*, EU:C:2017:766, paras 33 and 41-43, where in an action for rectification of that information, removal of incorrect comments and compensation in respect of all the damage sustained, the center of interests of a company incorporated under Estonian law was identified by the Court in Sweden as the place where the company’s commercial reputation was most firmly established and, as such, where the damage caused by online material occurred most significantly.

the defendant's conduct and connection with the forum are such that he should reasonably anticipate being haled into court there'.⁷⁹

66. The provision does not affect the national rules of venue: accordingly, venue remains subject to the law of the forum State.

67. Article 4(3) establishes the jurisdiction of the courts of the State where the publication in question is principally directed. The term 'publication' is to be construed as any means by which an individual (the defendant) makes something known to someone other than the plaintiff. This includes oral and written transmission: it covers any type of interaction that makes use of the spoken or written word, included but not limited to cyber- and digital-communications.

68. To establish jurisdiction, this provision mandates that the publication in question be 'principally directed' to the forum State. To establish an objective connection for the purposes of this provision it is not sufficient that the information be accessible from a State: to the contrary, it is necessary that a given State (and the individuals therein: i.e., readers/listeners/social media users and/or followers) be the principal target of the communication.⁸⁰ Accordingly, the courts of the State in which the information is received can assert jurisdiction in accordance with this provision only if it may be inferred from the act of communicating that the act was meant to principally (but not necessarily exclusively) target recipients in that State.⁸¹

69. In a list that is meant to be illustrative and not exhaustive, the provision states that, to assess the State to which the publication is principally directed, aspects such as the language of the publication, the content of the publication or the physical location of the audience may be taken into account. The language of the publication, especially when it is not a language commonly used in many States or at the international level, may clearly serve as an indication of intent to target a given audience. For instance, in *Sieben Tage in Moscow* the Bundesgerichtshof ruled that accepting jurisdiction would be improper in a case of disparaging comments posted online in Russian and in Cyrillic alphabet (thus hardly accessible to the average German reader) over events occurred in Moscow.⁸² Along the same lines, the CJEU ruled in *Football Dataco Ltd* that the circumstance that data placed online by a company which provides results and other statistics relating, inter alia, to English league matches live via the Internet is accessible to Internet users in the United Kingdom in English (a language which is not the one used in the

⁷⁹ See *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286 (1980), esp. 295-299; see also *Calder v. Jones*, 465 U.S. 783 (1984), esp. 786.

⁸⁰ See, for instance, *Young v. New Haven Advocate*, 315 F.3d 256 (4th Cir. 2002) holding that a court in Virginia cannot constitutionally exercise jurisdiction over the Connecticut-based newspaper defendants because they did not manifest an intent to aim their websites or the posted articles at a Virginia audience. The fact that the newspapers' websites could be accessed anywhere, including Virginia, does not by itself demonstrate that the newspapers were intentionally directing their website content to a Virginia audience. 'Something more than posting and accessibility is needed to "indicate that the [newspapers] purposefully (albeit electronically) directed [their] activity in a substantial way to the forum state", i.e., Virginia'.

⁸¹ See, for instance, BGH, 25 October 2016 – VI ZR 678/15 ruling that, pursuant to Article 5 (3) of the 2007 Lugano Convention, German courts had jurisdiction to issue an injunction for the violation of personal rights sought by the wife of the retired racing driver Michael Schumacher, who is a German citizen residing in Switzerland, against the website of a Swiss broadcaster (namely, www.srf.ch).

⁸² *Sieben Tage in Moscow*, BGH, 29 March 2011 – VIZR 111/10. NJW, 2016, 3445-3453. Cf., in particular, J. von Hein and A. Bizer, 'Social Media and the Protection of Privacy: Current Gaps and Future Directions in European Private International Law, International Journal of Data Science Analytics, Special Issue 2018.

Member State from which the provider pursues its activities), might, be supporting evidence for the existence of an approach targeting in particular the public in the United Kingdom.⁸³

70. As concerns the content of the publication, in *Sieben Tage in Moscow* the Bundesgerichtshof also found that the fact that the disputed post concerned events that had taken place in Moscow should be read in support of the publication being principally directed to Russia.⁸⁴

71. As regards the physical location of the audience, in *Football Dataco Ltd* the CJEU further held that the circumstance that the data available on the server included data relating to English football league matches showed an intention on the part of the provider to attract the interest of the public in the United Kingdom and may constitute evidence of targeting.⁸⁵

72. The criteria at subparagraphs (a)-(c) may also be used concurrently as was the case in *Arlewin v. Sweden*, where the European Court of Human Rights (ECtHR) ruled that requiring a Swedish national to bring defamation proceedings in the United Kingdom following an allegedly defamatory TV program broadcasted by a London-based company, but targeting mostly, if not exclusively, a Swedish audience, was not reasonable and violated Article 6(1) of the European Convention on Human Rights (ECHR). Noting that the content, production and broadcasting of the television program as well as its implications had very strong connections to Sweden and very little to the United Kingdom (the television program had been produced in Sweden, in Swedish and was sponsored by Swedish advertisers; the program was sent from Sweden via satellite to a London-based company which broadcast and transmitted it to viewers in Sweden), the Court ruled that the Sweden had an obligation under Article 6 ECHR to provide the applicant with an effective right of access to court.⁸⁶

73. Unlike the ground of jurisdiction at Article 4(1), the ground of jurisdiction at paragraph 3 applies regardless of where the act or omission directly causing the harm occurred. And unlike the ground put forth at paragraph 2, which focuses on the plaintiff's centre of main interest, the ground at paragraph 3 examines solely whether the defendant principally targeted its message to an audience in a given State. The ground of jurisdiction at paragraph 3 is the expression, at once, of flexibility and of a focussed approach. It is meant to introduce additional flexibility to the rigidity of the two grounds of jurisdiction established at Article 4(1)-(2). However, it 'controls' such flexibility by mandating that the publication be 'principally directed' to the forum State, as such ensuring foreseeability for and fairness to the defendant. Such ground of jurisdiction is tailored to extend the jurisdiction and provide additional alternative fora to the plaintiff that has suffered damage in a forum other than the ones identified in accordance with Article 4(1)-(2). However, it controls, in particular, the potential that the Internet has to subject its users to

⁸³ CJEU, Case C-173/11, *Football Dataco Ltd*, EU:C:2012:642, para. 42. See also the CJEU in Case C-194/16, *Bolagsupplysningen*, EU:C:2017:766, para. 11, relaying that the Harju Court of First Instance in Estonia had declined jurisdiction over an action for removal and rectification of online damaging content posted on the website of a trade association incorporated under Swedish law on the grounds that the information and comments at issue were published in Swedish and, without a translation, they were incomprehensible to persons residing in Estonia. As the CJEU ultimately also found (albeit without making direct reference to the language issue) the fact that the website at issue was accessible in Estonia could not automatically justify an obligation to bring a civil case before an Estonian court.

⁸⁴ *Sieben Tage in Moscow*, BGH, 29 March 2011 – VIZR 111/10. NJW, 2016, 3445-3453.

⁸⁵ CJEU, Case C-173/11, *Football Dataco Ltd*, EU:C:2012:642, para. 40.

⁸⁶ ECtHR, *Arlewin v. Sweden* (judgment of 1 March 2016, Application No 22302/10), para. 72.

limitless jurisdiction, or jurisdiction in every forum where the offending material can be accessed.

74. The provision does not affect the national rules of venue: accordingly, venue remains subject to the law of the forum State.

75. With respect to non-contractual jurisdiction, a solution such as the one put forth with the ‘mosaic principle’ – which was applied by the CJEU in *Shevill*⁸⁷ in an action seeking compensation for non-material damage allegedly caused by a defamatory article published in the printed press, and which states that the plaintiff may bring a claim in the State in which the plaintiff is known, but only in respect of damage caused in that State – was deemed by a clear majority of the Committee as unsuited to the goal of foreseeability and not fitted to the needs, in particular, of the Internet, where the dissemination of information is instantaneous and ubiquitous. Given the difficulty to limit an injunction to a certain territory, especially with vis-à-vis Internet violations, a clear majority of the Committee further observed that the ‘mosaic principle’ is unsuited also with respect to injunctive relief.⁸⁸

Article 5

Branch jurisdiction/Establishment

[]

Article 6

Co-defendants; counter-claim

[]

Article 7

Choice of court agreements

[]

⁸⁷ CJEU, Case C-68/93, *Fiona Shevill*, EU:C:1995:61, esp. paras 29-31.

⁸⁸ In this regard, see CJEU, Case C-194/16, *Bolagsupplysningen*, EU:C:2017:766, para. 48, where the Court ruled that, in the light of the ubiquitous nature of the information and content placed online and the fact that the scope of their distribution is, in principle, universal, an application for the rectification of the information and the removal of the comments is a single and indivisible application and may, consequently, only be made before a court with jurisdiction to rule on the entirety of an application for compensation for damage.

Article 8

Jurisdiction for follow-on lawsuits

[]

C – APPLICABLE LAW

1. Non-Contractual Obligations

Article 9

Party Autonomy

(1) The parties may, in accordance with Article 18, agree to submit non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation, to the law of their choice:

(a) by an agreement entered into after the event giving rise to the damage occurred; or

(b) also by an agreement concluded before the event giving rise to the damage occurred,

(i) if all the parties to this agreement are pursuing a commercial activity; or,

(ii) notwithstanding Article 10, with regard to the violation of privacy committed among users of social media, if the law chosen corresponds to that governing the contract which both parties have concluded with the same Internet service provider, and the non-contractual obligation arises out of activities falling under this contract.

(2) To the extent that the law applicable to a non-contractual obligation has not been chosen in accordance with paragraph 1, the law governing the obligation shall be determined in accordance with Articles 10 to 13.

76. Party autonomy is established as a fundamental principle of attachment not only for contracts,⁸⁹ but for non-contractual obligations as well, in order to respect the parties' common

⁸⁹ On party autonomy for contractual obligations see Art. 14.

intentions and to foster legal certainty.⁹⁰ Article 9 must be read in conjunction with Article 18, which lays down general principles of party autonomy that apply both to torts and contracts.

77. Article 9 is based on a modern and liberal approach to party autonomy for non-contractual obligations, allowing a choice of the applicable law both *ex post* and, provided certain conditions are met, *ex ante*. Article 14 of the Rome II Regulation served as an example.

78. According to Article 9(1)(a), an *ex post* agreement on the applicable law is possible for all parties; weaker parties, such as consumers, are not excluded because the threat of abuse of an inferior negotiating position is minimized in case of a choice made *post factum*.⁹¹ After the tortious event has occurred, even consumers should be aware of the potentially dangerous implications of choosing the applicable law – at least, they have a strong incentive to seek competent legal advice.

79. It is not necessary that the agreement after the event be made before the court. For instance, the parties are allowed to agree on the applicable law in an out-of-court settlement as long as the choice is made expressly or clearly demonstrated by the circumstances of the case.⁹²

80. Commercial activity in the sense of Article 9(1)(b)(i) is not limited to persons who qualify as merchants under domestic laws but includes liberal professions (e.g., doctors, lawyers) as well. The goal is to protect legally unsophisticated parties from a choice-of-law clause with unforeseeable effects. Accordingly, employees fall in the scope of protection. On the other hand, occasional C2C transactions are excluded from the scope of the provision.⁹³ The criterion of a ‘commercial activity’ is related to a specific transaction and not to a personal status; thus, such criterion makes clear that even a trader or a professional is protected if he or she is acting outside the scope of his or her trade or profession. For transactions that serve both private and business purposes, an *ex ante* choice of law is only excluded if the commercial purpose is of clearly minor importance.⁹⁴ Moreover, a consumer who deceives the other party by posing as a trader or a professional deserves no protection.⁹⁵

81. The non-contractual obligation to which the chosen law shall apply must be closely connected to the commercial activity in question.

82. In the case of choice of law in a contract concluded before the event, it is recommendable to include potential non-contractual obligations because the substantive laws of different States are characterized by significant divergences as far as the proper boundaries between tort and

⁹⁰ Party autonomy for violations of personality rights is typically only allowed within limits in the existing choice-of-law provisions: notably, an agreement may only be concluded after the tortious event has occurred. Art. 42 of the Introductory Law to the **German** Civil Code allows an agreement on the applicable law *ex post* generally for all non-contractual obligations without any requirements regarding formality and thus appears to be the most liberal rule. In **France**, for instance, a choice *ex post* may only point to the *lex fori* (see *Cour de Cassation*, decision No. 85-18.715 of 19 April 1988, *Roho*). The **Japanese** Article 21 AGRAL allows an *ex post* agreement as long as it is not of prejudice to the rights of a third party. However, several jurisdictions (**Brazil**, **Greece**, **Portugal**, **Spain**, the **United Kingdom**, and the **United States**) do not allow party autonomy in this area of the law.

⁹¹ See with further references J. von Hein, ‘Art. 14 Rome II’, in Calliess (ed.) *Rome Regulations* (2nd ed., 2015), mn. 18.

⁹² See Article 18 of these Guidelines for the validity of agreements.

⁹³ This may be the case, for instance, when two consumers agree that one of them is allowed to use pictures of the other one for his or her private profile in a social network.

⁹⁴ CJEU, Case C-464/01, *Gruber ./. BayWa*, EU:C:2005:32, para. 39-45 regarding Art. 13-15 of the Brussels Convention.

⁹⁵ BGH VIII ZR 91/04, NJW 2005, 1045.

contract law are concerned. Thus, parties who want to avoid a protracted litigation on issues of characterization are well advised to choose the law applicable not only to their contractual obligations, but to their non-contractual obligations as well. Usually, the law chosen for contractual obligations should already be applicable by way of an accessory connection (Article 12). Such a connection, however, is subject to the court's discretion, so that only a choice of law clause that applies to non-contractual obligations, as well, can ensure an adequate degree of legal certainty.

83. Article 9(1)(b)(ii) reacts to the development, generally occurring in an online context and especially in social media, whereby users might violate each other's personality as equals.⁹⁶ In order to avoid giving preference to either the perpetrator or the victim, these Guidelines provide for a law which is neutral to both parties, i.e. the law governing the contract that both parties have concluded as users with the same social media provider.⁹⁷ Since the same law is applicable to the provider's relation with both the plaintiff and the defendant – provided the choice of law in that relationship is valid –, it may be appropriate to apply this law to any kind of litigation arising between these two users as well, at least if they voluntarily choose this law for violations of privacy and rights relating to personality, including defamation. This approach might increase the importance of the defamation law in force at the provider's seat. However, this solution offers a law which is neutral to both claimant and defendant and is based on a voluntary connection. If the parties share a common habitual residence (Article 10), the latter connecting factor would have priority. In this case, both parties already have a significant relationship with the same law (the one of common habitual residence); thus, there is no practical need for allowing them to choose a 'neutral' law. Moreover, if both parties share their habitual residence in the same country, they will usually litigate in this State. In this scenario, a parallelism between jurisdiction and the applicable law will enhance procedural economy.

84. Article 9(2) states the prevalence of party autonomy over objective connections.

Article 10

Common Habitual Residence

(1) Where the person claimed to be liable and the person sustaining damage both have their habitual residence in the same country at the time when the violation of privacy or rights relating to personality, including defamation, occurs, the law of that country shall apply.

(2) The habitual residence of companies and other bodies, corporate or unincorporated, within the meaning of this article, shall be the place of central

⁹⁶ For a thorough discussion of the relationship between users of social networks and the implications for the identification of the applicable law on defamation cases see A. Mills, 'The law applicable to cross-border defamation on social media: whose law governs free speech in 'Facebookistan'?', 7 *Journal of Media Law* (2015), 1-35.

⁹⁷ Such a solution might be attractive, for instance, in groups serving the exchange of ideas and opinions in social networks. Users of such a group could set up rules of behaviour for the debate including a choice of law for any questions of liability between the users.

administration. Where the event giving rise to the damage occurs, or the damage arises, in the course of operation of a branch, agency or any other establishment, the place where the branch, agency or any other establishment is located shall be treated as the place of habitual residence.

(3) The habitual residence of a natural person acting in the course of his or her business activity shall be his or her principal place of business.

85. The common habitual residence is an objective criterion that is neither connected to the place of acting nor to the place where the harm was suffered. Rather, it is related to personal characteristics of both parties involved. Both parties will be more familiar with the law of the country in which they habitually reside than with any other law.

86. This rule is familiar to many European codifications on tort law.⁹⁸ It is an expression of an economic rationale because, usually, parties who share a common habitual residence will litigate in the country where they live. This solution reduces litigation costs and fosters a more efficient court administration.

87. The common habitual residence prevails over the other objective connections found in Article 11. This is justified by the especially close connection created by the common habitual residence.

88. Whereas habitual residence for jurisdictional purposes (Article 3(2)) may encompass more than one place between which the plaintiff may choose, a choice of law rule requires a narrower definition in order to designate a single applicable law. Thus, in line with Article 23(1) Rome II Regulation, Article 10(2) of these Guidelines refers to a corporation's central administration. 'Central administration' refers to company's main organization which can be identified by the location of the head offices and by the place where the fundamental decisions are being taken.⁹⁹ The statutory seat and the place of business are not relevant.¹⁰⁰ The special rule for branches, agencies and any other establishments is typically corresponds with the expectations of the other party.

⁹⁸ In some legal orders, the prevalence of the common habitual residence over other objective connections is stated explicitly; e.g. in Art. 40 (2) of the Introductory Law to the **German** Civil Code, in Art. 45(3) of the **Portuguese** Código Civil (common nationality or common habitual residence) or in Art. 20 of the **Japanese** AGRAL. In **Italy**, Article 62(2) of Law No 218/1995 provides that '[s]hould tortious liability concern only nationals of one State, and all are residents of that State, the law of that State shall apply'. In other legal systems, the common habitual residence may be taken into consideration in the context of the search of the proper law of the tort (**Greece**) or as part of a flexible exception (**United Kingdom**). In **Brazil**, the fact that both parties share common habitual residence may generally be relevant in the determination of applicable law, although not when personality rights are at stake. The prevalence of the common habitual residence generally for non-contractual obligations is also provided for in Art. 4(2) Rome II Regulation (which is not applicable to non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation according to Art. 1(2)(g)), but might be considered a general legal principle in European conflict of laws on non-contractual obligations.

⁹⁹ D. Baetge, 'Art. 23 Rome II', in Calliess (ed.) *Rome Regulations* (2nd ed., 2015), mn. 11.

¹⁰⁰ The CJEU repeatedly stated in different contexts that the place of incorporation is generally of low relevance to the identification of the real geographical centre of a company due to the fact that within the EU that place can be chosen without any real activity within that Member State; see e.g. Case C-194/16, *Bolagsupplysningen*, EU:C:2017:766, para. 41; Case C-230/14, *Weltimmo*, EU:C:2015:639, para. 29.

89. With regard to natural persons, the Draft Guidelines do not provide an autonomous interpretation of the term ‘habitual residence’. Such concept is therefore to be interpreted in accordance with the generally accepted understanding of this term.¹⁰¹

Article 11

Lex loci delicti commissi

(1) Notwithstanding Article 10, a court having jurisdiction under Article 3 shall apply the law of the State where the act or omission directly causing the harm occurred, irrespective of where the damage arose. The injured person may demand, however, that the law of the State where he has his or her main centre of interest be applied instead, if the act or omission in question was principally directed to this State.

(2) Notwithstanding Article 10, the courts shall, in exercising their jurisdiction under Article 4, apply their own law.

90. Article 11 contains two different objective connections for different heads of jurisdiction. Article 3 provides for the general jurisdictional rule *actor sequitur forum rei*; thus, this place is not justified by a special connection to the facts of the case. Consequently, a close connection between a specific legal system and the case at hand has to be found at the level of choice of law (Article 11(1)). Article 4, in contrast, already provides a kind of close connection so that a different treatment pursuant to Article 11(2) is justified.

91. In combination with the provisions on jurisdiction, the applicable law according to Article 11 is the law of the State where the act or omission directly causing the harm occurred. The comparative approach showed that in many legal systems, both jurisdiction and choice-of-law rules for personality cases were based on some variant of *lex loci delicti*.¹⁰² This normally leads to a parallelism of jurisdiction and choice-of-law, i.e. courts usually apply the *lex fori*.¹⁰³

¹⁰¹ For a thorough discussion, see P. Beaumont & J. Holliday, ‘Recent Developments on the Meaning of “Habitual Residence” in Alleged Child Abduction Cases’, in M. Župan (ed.), *Private International Law in the Jurisprudence of European Courts – Family at Focus* (2015), 37-56; M.-P. Weller & B. Rentsch, “‘Habitual Residence’: A Plea for “Settled Intention””, in: S. Leible (ed.), *General Principles of European Private International Law* (2016), 171-187.

¹⁰² The Committee’s survey on the national rules for jurisdiction and choice-of-law rules for violations of personality rights indicates that the basic rule in torts, which is decisive due to the lack of specific rule for personality violations, including defamation and data protection, is to apply the *lex loci delicti* (law of the State where the event causing the damage took place). When the place of acting and the place of the damage are split – typically in cases of violation of personality rights –, the legal systems show different solutions: some favour the place of acting (**Portugal**, mostly **Greece** and **Spain**), others decide depending on the circumstances of the individual case, with a tendency to prefer the *lex fori* or the law more favourable to the victim. In **Germany** and **Italy**, the victim may choose between the law of the place of damage and of the place of the acting

¹⁰³ Most legal systems theoretically allow for courts to apply a law that differs from the substantive *lex fori*. However, the observation of the courts’ decisions in various States show that it is almost always that the *lex fori* will be applied what is closely connected to the rules on jurisdiction. For instance, it is quite rare for the **English** courts

92. When the claim was brought before the courts at the defendant's habitual residence according to Article 3(1) and there is neither an agreement on the applicable law nor a common habitual residence, the typically closest connection is with the place where the act or the omission occurred. Insofar, Article 11(1) is to be interpreted in accordance with Article 4(1). However, this defendant-friendly solution should be balanced by allowing the plaintiff to opt for the law of the State where he/she has his/her main centre of interest to be applied instead. This solution prevents a circumvention of otherwise applicable laws if the act or omission in question was principally directed to the latter State. By limiting the law that might be chosen to just one State, this approach avoids the difficulties inherent in the *Shevill* doctrine (see supra at paragraph 75).

93. When the claim was brought under the provisions of Article 4, however, a close connection was already created; in the case of Article 4(1) and (2), applying the *lex fori* means indirectly – by the choice of court – applying the *lex loci delicti* as well. Explicitly providing the application of the *lex fori* is a rather untypical approach in conflict of laws, but has several advantages: it reduces the time and cost of litigation, it produces a judgment of higher quality, and it promotes foreseeability of result for defendants. The disadvantage of promoting forum shopping is minimized by the harmonization of the rule on jurisdiction.

94. The main reason to directly apply the *lex fori* is that, contrary to other areas of law, personality rights are significantly influenced by constitutional values. Thus, applying the *lex fori* reduces the need to resort to public policy.

Article 12

Escape clause and accessory connection

Where it is clear from all the circumstances of the case that the obligation is manifestly more closely connected with a country other than that indicated in Articles 10 or 11, the law of that other country shall apply. A manifestly closer connection with another country might be based in particular on a pre-existing relationship between the parties, such as a contract, that is closely connected with the obligation in question, unless such an accessory connection would amount to an evasion of Article 9.

95. The escape clause seeks to resolve the tension between the requirement of legal certainty, on the one hand, and the need to do justice in individual cases, on the other. Articles 10 and 11 determine the applicable law by identifying the typically closest connection. However, in exceptional cases, the closest connection might be the law of another country. Thus, the judge may have recourse to an escape clause in order to achieve justice in a conflict-of-law sense for

to apply foreign law to defamation claims, as most claims in the English courts relate to English publications only, and claimants often seek injunctive relief rather than compensatory damages (and thus do not try to establish the worldwide extent of the damage to their reputation). However, in theory, the double actionability rule does not prevent courts from applying foreign rules which are more restrictive than English law.

the individual case. This approach thus creates a flexible framework of conflict-of-law rules. Moreover, it enables the court seized to treat individual cases in an appropriate manner.

96. The escape clause also enables the judge to return to the law applicable pursuant to Article 11 in cases where the parties' common habitual residence (Article 10) is superseded by additional factors that lead to a closer connection to the former law.¹⁰⁴ This might be the case, for example, when the common habitual residence of the parties has been chosen for reasons unrelated to a deeper social integration (e.g. tax evasion) and bears no close relation to the violation of a personality right.

97. The use of the escape clause must be an exception, as made clear by the wording 'manifestly more closely connected'.¹⁰⁵ Thus, a judge must always start by determining the applicable law under Article 10 and 11 before exercising his or her discretion as to whether this law should be displaced in an exceptional case. Nevertheless, a court may, for the sake of procedural economy and common sense, leave open the issue of exactly localizing the place under Article 11 in complex scenarios when it is clear that such a place would be displaced anyway because of a contract between the parties justifying an accessory connection. In particular, the accessory connection is a valuable tool with regard to tortious claims of users against the providers of Internet services, because it makes difficult issues of localizing exactly the place of damages in cyberspace moot.

98. An accessory connection might be possible due to a pre-existing contract between the parties that stands in a close relation to the tort and is a factor that a court has to take into account in exercising its discretion concerning the existence of a manifestly closer connection. This is *inter alia* justified by the usual expectation of the parties especially when the applicable law to the contract is determined by a choice-of-law agreement. The main purpose of such a rule is to avoid conflicts of characterization that might arise because various substantive laws draw the line between contractual and non-contractual obligations in a different way. Apart from that, an accessory connection will frequently offer a unitary solution in cases where a multitude of victims is injured who do not share a habitual residence with the tortfeasor but who are linked to him by contracts governed by the same law. The technique of an accessory connection is well-known and found in several European codifications.¹⁰⁶

99. The accessory connection, however, must not be used to circumvent the limitations on choice of law stated in Article 9. Thus, if a user of a social network acting for private purposes and a social media provider agreed on the law applicable to their contractual relations within the

¹⁰⁴ Cf., with further references, J. von Hein, 'Art. 4 Rome II', in Calliess (ed.) *Rome Regulations* (2nd ed., 2015), mn. 44; also: R. Plender and M. Wilderspin, *The European Private International Law of Obligations* (4th ed., 2015), mn. 18-108.

¹⁰⁵ For the parallel rule in Art. 4(3) Rome II Regulation see e.g. R. Plender and M. Wilderspin, *The European Private International Law of Obligations* (4th ed., 2015), mn. 18-105.

¹⁰⁶ The accessory connection is provided in Art. 4(3) Rome II Regulation which is not applicable to the violations of privacy and personality rights. For this area, the technique of accessory connection is explicitly provided in **Germany** (Art. 41(2) Introductory Law to the German Civil Code) and **Japan** (Art. 20 AGRAL). In the **United Kingdom**, sec. 12 of the PIL (MP) Act 1995 allows the court to take into account a wide range of factors in determining whether "it is substantially more appropriate for the applicable law" to be a law other than the law of the place of the tort. The courts have held that this includes consideration of the law governing a contract between the parties, if the claim in tort arises out of the contract (see e.g. *Trafigura Beheer BV v Kookmin Bank Co* [2006] EWHC 1450 (Comm)). However, other legal systems do not accept a influence of a pre-existing relationship on the applicable law non-contractual obligations (**Greece, Italy, Portugal, Spain, USA**).

borders of Article 14 and 16, that law cannot be applied to torts because it would constitute an *ex ante* indirect choice of law. The accessory connection is hence especially relevant for the relation between social media providers or publishers and victims pursuing a commercial activity.¹⁰⁷

100. In addition, an accessory connection may come into play between social media users if they have not made an explicit choice of law agreement pursuant to Article 9(1)(b). In this regard, the fact that the users are linked to the social media providers by contracts governed by the same law may establish at least a kind of factual relationship justifying an accessory connection of tortious claims.¹⁰⁸

Article 13

Right of reply

The right of reply against a publisher, broadcaster or Internet service provider regarding the content of a publication or broadcast and regarding the violation of privacy or of rights relating to the personality resulting from the handling of personal data is exclusively governed by the law of the country in which the publisher, broadcaster or Internet service provider has its habitual residence.

101. The right of reply is closely linked to a State's media law and should thus not be imposed by a foreign law.

102. The right of reply comprises the victim's right to publically defend herself or himself against the harmful publication or broadcast in the same place and form of publication like the harming one. Such relief should be granted swiftly and is interim in nature. Such rights must typically be enforced in the State of the publisher's habitual residence; thus, the enforcement can be realized easier and faster when a foreign judgment is in accordance with the enforcement State's law.

103. The habitual residence is defined according to Article 10(2) and (3). For the purposes of these Guidelines, it is irrelevant whether a State qualifies the right of reply as private law or public law.

¹⁰⁷ An example might be a dispute between a celebrity who agrees with a magazine on the publication of a 'home story' containing certain private information for profit. If the magazine subsequently publishes more intimate details than were agreed on, thus violating the personality rights of its contracting party in this context, an accessory connection of tortious claims to the law governing the 'home story' contract is justified.

¹⁰⁸ See J. von Hein and A. Bizer, 'Social Media and the Protection of Privacy: Current Gaps and Future Directions in European Private International Law', *International Journal of Data Science Analytics*, Special Issue 2018.

2. Contractual Obligations¹⁰⁹

[Article 14

Party Autonomy for contractual obligations

A contract shall be governed by the law chosen by the parties in accordance with Article 18. The Hague Principles on Choice of Law in International Commercial Contracts may give further guidance in interpreting the present Guidelines as well.]

[Article 15

Applicable law in the absence of choice

(1) To the extent that the law applicable to the contract has not been chosen in accordance with Article 14 and without prejudice to Articles 16, the contract shall be governed by the law of the country where the party required to effect the characteristic performance of the contract has his or her habitual residence.

(2) Where it is clear from all the circumstances of the case that the contract is manifestly more closely connected with a country other than that indicated in paragraph 1, the law of that other country shall apply.]

[Article 16

Consumer contracts

(1) A contract concluded by a consumer with a professional shall be governed by the law of the country where the consumer has his or her habitual residence, provided that the professional:

(a) pursues his or her commercial or professional activities in the country where the consumer has his habitual residence, or

(b) by any means, directs such activities to that country or to several countries including that country,

and the contract falls within the scope of such activities.

(2) Notwithstanding paragraph 1, the parties may choose the law applicable to a

¹⁰⁹ The Committee Officers wish to convey that the provisions on contractual obligations were drafted by them, and have not yet been adopted by the Committee. This proposal is based on the Regulation No 593/2008 on the law applicable to contractual obligations (Rome I) of the European Union, which may serve as an example for unified conflict-of-law provisions in this area, and needs to be further discussed by the Committee.

contract which fulfils the requirements of paragraph 1, in accordance with Article 14. Such a choice may not, however, have the result of depriving the consumer of the protection afforded to him by provisions that cannot be derogated from by agreement by virtue of the law which, in the absence of choice, would have been applicable on the basis of paragraph 1.

(3) If the requirements in points (a) or (b) of paragraph 1 are not fulfilled, the law applicable to a contract between a consumer and a professional shall be determined pursuant to Articles 14 and 15.]

3. General Provisions on the Applicable Law

Article 17

Renvoi

The application of the law of any country specified by these Guidelines means the application of the rules of law in force in that country other than its rules of private international law.

104. Article 17 aims to clarify the scope of the application of foreign law due to the articles in these Guidelines.

105. *Renvoi* is the phenomenon that the application of a foreign law including that State's private international law may refer back to the *lex fori* or to a third State's law.¹¹⁰ To avoid these consequences, Article 17 excludes *renvoi* with the result that the law found by the provisions of these Guidelines will be the substantive law applicable to the case at hand.¹¹¹

106. Allowing *renvoi* would be counterproductive to the objective of these Guidelines to foster international harmony of decisions by creating internationally unified conflict-of-law rules. The highly elaborated and differentiated solutions in these Guidelines aim to offer a modern approach taking into account the alleged interests of the parties involved. The acceptance

¹¹⁰ Cf. J. von Hein, *Renvoi* in European Private International Law, in: S. Leible (ed.), *General Principles of European Private International Law* (2016), 227-273.

¹¹¹ This solution corresponds with the current situation in almost all legal systems that were accessible for the committee by questionnaire in the field of violations of personality rights, including defamation and data protection. Exceptions to this results can be found under further conditions in **Germany**, **Portugal** and in some States in the **US**. The exclusion of *renvoi* corresponds with most international instruments on the applicable law (e.g. Art. 20 Rome I Regulation, Art. 24 Rome II Regulation, Art. 12 Hague Protocol on the Law Applicable to Maintenance Obligations, Art. 17 Hague Convention on the Law Applicable to Succession). See also M. Sonnentag, '*Renvoi*', *Encyclopedia of Private International Law* (2017), 1541-1542.

of other conflict-of-law rules having effect by allowing *renvoi* would belittle the achieved solutions.

107. When a court develops a tailor-made solution in an individual atypical case by applying the general escape clause (Article 12), a possible remission by the foreign legal system would contradict the effort to find the closest connection for the case at hand.

108. When parties choose the applicable law according to Article 9 or Article 14, they usually expect the chosen substantive law to be applied. Thus, *renvoi* would reduce predictability and legal certainty – the main reasons for parties to agree on the applicable law. For the very rare case that the parties expressly allow *renvoi*, an exception to this Article may be made.¹¹²

Article 18¹¹³

General Principles of Party Autonomy

(1) A choice of the applicable law shall be made expressly or clearly demonstrated by the circumstances of the case and shall not prejudice the rights of third parties. The parties may at any time agree to subject their legal relationship to a law other than that which previously governed it. Any change in the law to be applied that is made after the legal relationship came into existence shall not prejudice its formal validity or adversely affect the rights of third parties.

(2) Where all the elements relevant to the situation at the time when the event giving rise to the damage occurs are located in a country other than the country whose law has been chosen, the choice of the parties shall not prejudice the application of provisions of the law of that other country which cannot be derogated from by agreement.

(3) Where all the elements relevant to the situation at the time when the event giving rise to the damage occurs are located in one or more of the Member States of a Federal State or a Regional Economic Integration Organisation, the parties' choice of the law applicable other than that of a Member State shall not prejudice the application of provisions of Federal or regionally unified or harmonized law which cannot be derogated from by agreement.

(4) The existence and validity of the consent of the parties as to the choice of the applicable law shall be determined in accordance with the provisions of the chosen law, unless this would have the result of depriving a consumer of the protection afforded to him or her by mandatory provisions which, in the absence of choice, would have been applicable.

¹¹² Cf. Article 8 of the Principles on Choice of Law in International Commercial Contracts.

¹¹³ The content of this provision was originally approved by the Committee regarding party autonomy for non-contractual obligations. To extend the general part of the original version of Art. 9 to party autonomy for contractual obligations and to avoid repetitions, it has been moved to this newly created article as part of the general provisions on the applicable law. This new structure is a proposal of Committee's Officers and must still be discussed and approved by the Committee.

109. This provision offers further specifications regarding the validity and the material scope of a choice-of-law agreement according to Articles 9, 14 and 16. Choice of law agreements offer a high degree of legal certainty and can determine the applicable law independently from jurisdictional questions, provided that a State's private international law allows such agreements. Parties may choose a neutral law. The provisions on conflict of laws in these Guidelines, especially the escape clause, can require further and complicated investigations and hence must be balanced by giving parties the possibility of quickly resolving any dispute on the applicable law.

110. The parties are free to choose any State's law without further requirements like a special connection to the tort. This liberal attitude is justified because demanding a close connection between the chosen law and the non-contractual obligation would reintroduce precisely the legal uncertainty that the parties want to avoid by entering into a choice-of-law agreement. However, the eligible law is restricted to the law of States; thus, non-State-law, in particular rules on privacy elaborated by social media providers, may not be chosen.

111. Article 18(2) and (3) avoid the circumvention of a State or an organization's mandatory law. Non-binding provisions of a State's substantive law can be substituted by the chosen law.¹¹⁴ In the field of personality rights, however, openness of a State's law to party agreements is not very likely due to the high relevance of fundamental rights. In addition, in some legal systems (such as the EU) the protection of privacy and data protection may have constitutional status, and thus not be subject to derogation by private parties. An agreement on the choice of a foreign tribunal or on the applicable law does not alter the essentially domestic character of the situation.¹¹⁵ Paragraph (3) encompasses cases where the relevant factors are located not in a single, but also in more than one Member State of an organization like, for example, the European Union.

112. Article 18(4) ensures the predictability of the agreement's validity. An exception is necessary to protect consumers. Furthermore, recurring to the *lex fori* would endanger the goal of decisional harmony.

Article 19

Overriding Mandatory Provisions

(1) Nothing in these Guidelines shall restrict the application of the overriding mandatory provisions of the law of the forum.

[(2) When applying under these Guidelines the law of a country, the court may give effect to the overriding mandatory rules of any State with which the dispute has a close connection. In considering whether to give effect to those provisions, regard shall be had to their nature and purpose and to the consequences of their

¹¹⁴ These provisions have been created after the models of Art. 3(3) and (4) Rome I Regulation and Art. 14 (2) and (3) Rome III Regulation.

¹¹⁵ J. von Hein, 'Art. 14 Rome II', in Calliess (ed.) *Rome Regulations* (2nd ed., 2015), mn. 40.

113. This provision aims to balance out the multilateral approach of these Guidelines by allowing the application of internationally mandatory provisions. Since in Article 9 the Guidelines adopt a rather liberal approach toward party autonomy, safeguards such as the one offered at Article 19 become more important to avoid negative externalities. Especially in the field of protection of personality and of personal data, national laws have a high interest in applying their mandatory provisions.

114. In modern European doctrine and legislation, it is commonly accepted that a court has to apply internationally mandatory provisions of its own law irrespective of the law designated by regular conflicts rules.¹¹⁶ Such unilateralism can also be seen in the U.S.-style governmental interest analysis.¹¹⁷

115. Article 19 only applies to internationally mandatory rules: it does not apply to merely internally mandatory rules, which are covered by Article 18(2) and (3). National data protection laws are an important example of internationally mandatory rules.¹¹⁸ Internationally mandatory provisions are rules which are regarded as crucial by a country for safeguarding its public interests. The European Union's GDPR expresses its will to be applied independently from the law that is applicable in accordance with Article 3 GDPR.¹¹⁹

116. [(2): Besides the internationally mandatory provisions of the *lex fori*, the court applying these Guidelines might also consider applying internationally mandatory provisions of a foreign law. Excluding this option would be a too narrow approach that might threaten the international harmony of decisions which is the fundamental goal of these Guidelines. The necessity to apply mandatory provisions of third States in certain instances can be seen in the CJEU's judgment in *Nikiforidis*.¹²⁰ Moreover, the fact that the courts of a State consciously

¹¹⁶ M. Wilderspin, 'Overriding Mandatory Provisions', *Encyclopedia of Private International Law* (2017), 1330-1334.

¹¹⁷ For an analysis focused on Rome II, see Muir Watt, 'Rome II et les 'intérêts gouvernementaux': pour une lecture fonctionnaliste du nouveau règlement du conflit de lois en matière délictuelle', in: *Le Règlement Communautaire 'Rome II' sur la loi applicable aux obligations non contractuelles* (Corneloup and Joubert eds, 2008), 129.

¹¹⁸ E.g. Administrative Court of Schleswig (Germany), 14 February 2013 – 8 B 60/12; M. Brkan, 'Data Protection and Conflict-of-Laws', 2 *European Data Protection L. Rev.* (2016), 324 (333-336).

¹¹⁹ C. Kohler, 'Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union', *Rivista di diritto internazionale privato e processuale* (2016), 653 (661-662); J.D. Lüttringhaus, 'Das internationale Datenprivatrecht: Baustein des Wirtschaftskollisionsrechts des 21. Jahrhunderts', 117 *Zeitschrift für Vergleichende Rechtswissenschaft* (2018), 50 (73-74); M. Melcher, 'Es lebe das Territorialitätsprinzip?', in *Politik und Internationales Privatrecht* (Gössl et. al. (eds) 2017), 129 (139); P.A. de Miguel Asensio, 'Competencia y derecho aplicable en el reglamento general sobre protección de datos de la Unión Europea', 69 *Revista Española de Derecho Internacional* (2017), 75 (104).

¹²⁰ CJEU, case C-135/15, *Nikiforidis*, EU:C:2016:774. The European lawmaker originally included overriding mandatory provisions of third States in the draft for the Rome I Regulation but finally refrained from this option (see draft report of the European Parliament on the proposal for a regulation of the European Parliament and of the Council on the law applicable to contractual obligations (Rome I), 2005/0261(COD), p. 15). Hence, the CJEU decided that courts may not give effect to internationally mandatory provisions of states other than the ones mentioned in Art. 9 (2) and (3) Rome I (para. 49). However, the CJEU held that 'Article 9 of the Rome I Regulation

ignore overriding mandatory provisions of another State's law will lead to the non-recognition of an ensuing judgment.

117. The decision to apply foreign internationally mandatory provisions is at the court's discretion and should take into account the objectives of these Guidelines. Cases of violation of personality infringement, including defamation, often occur on the Internet. Frequently, the place where the allegedly infringing publication is stored might not coincide with the place whose law is applicable according to the provisions of these Guidelines. Applying, for example, the data laws of the State where the data is stored can increase the harmony of decisions; this is especially the case when the defendant brings parallel proceedings in that third State under data protection law.]

Article 20

Public Policy

The application of a provision of the law of any country specified by these Guidelines may be refused only to the extent that the effects of such an application are manifestly incompatible with the public policy (*ordre public*) of the forum, in particular with its fundamental principles as regards freedom of expression and information as well as the protection of privacy and human dignity.

118. This provision corresponds to the typical public policy clause in international conflict-of-law conventions and codifications.¹²¹ It serves to protect the fundamental values of the State of the applying court. In cases of violations of personality rights, including defamation and data protection, a State's fundamental principles are often concerned what raises the importance of this provision.

119. Public policy should not impede the aim of harmonisation of these Guidelines and must hence be used restrictively and only where a court's decision would otherwise contradict the fundamental principles of a State's substantive law in an unbearable way.

120. The legal consequences of invoking public policy are not yet resolved in the academic discourse.¹²² As this question is not specific to the violation of personality rights, it is not decided in these Guidelines.

does not preclude overriding mandatory provisions of a State other than the State of the forum or the State where the obligations arising out of the contract have to be or have been performed from being taken into account as a matter of fact, in so far as this is provided for by a substantive rule of the law that is applicable to the contract pursuant to the regulation' (para. 51).

¹²¹ E.g. Art. 11(3) of the Principles on Choice of Law in International Commercial Contracts; see also the overview of I. Thoma, 'Public Policy (*ordre public*)', *Encyclopedia of Private International Law* (2017), 1455-1456.

¹²² The question at stake is what the judge should apply instead of the refused foreign law. National provision typically avoid to clarify the legal consequences of invoking public policy. An exception can be found, for example, in **Italy** where Article 16 of Law No 218/1995 regulates the public policy exception, and it provides that "1. No

Article 21

Multi-State legal orders

(1) Where a State comprises several territorial units, each of which has its own rules of law in respect of violations of privacy, defamation or data protection, each territorial unit shall be considered as a country for the purposes of identifying the law applicable under these Guidelines.

(2) A State within which different territorial units have their own rules of law in respect of violations of privacy, defamation or data protection shall not be required to apply these Guidelines to conflicts solely between the laws of such units.

121. According to this provision, each territory of a multi-State legal order is treated like a country to identify the applicable law.¹²³ A multi-State legal order is composed of various territories that – at least partly – provide own set of rules. It is irrelevant whether the law consists of statutory or case law.

122. This provision extends the scope of these Guidelines to conflict of laws within multi-State legal orders (e.g. USA, UK, and Canada) and thereby excludes the application of internal conflict-of-law rules. However, it does not apply for merely internal conflicts. In consequence, choice-of-law agreements in the sense of Articles 9 or 14 can point directly to the law of a territory of a multi-State legal order.

D – RECOGNITION AND ENFORCEMENT OF JUDGMENTS

[]

foreign law shall be applied whose effects are incompatible with public policy (*ordre public*). 2. In that case, the applicable law shall be determined on the basis of other connecting factors possibly provided for with respect to the same matter. In the absence of other connecting factors, Italian law applies". Given that Law No 218/1995 usually provides for more than one connecting factor for each case, resort to *lex fori* is usually avoided in theory. On European PIL, see W. Wurmnest, 'Ordre Public (Public Policy)', in: S. Leible (ed.), *General Principles of European Private International Law* (2016), 305 (326 ff.).

¹²³ The solution to apply choice-of-law rules also with regard to States with more than one legal system instead of applying the internal conflict rules corresponds to most international instruments of applicable law in the field of torts and contracts, e.g. Art. 25 Rome II, Art. 22 Rome I, Art. 12 Hague Convention on the Law Applicable to Products Liability, Art. 12 Hague Convention on the Law Applicable to Traffic Accidents. For further analysis, see F. Eichel, References to Non-unified legal systems, in: S. Leible (ed.), *General Principles of European Private International Law* (2016), 275–303.

III. Conclusions and Future Steps

123. In an effort to standardize and rationalize an extensive and expanding area of the law, the Committee has worked to produce Guidelines that strike a fair balance between the importance of, on the one hand, safeguarding the legitimate interests of the defendants and, on the other hand, ensuring that access to justice be effectively and efficiently guaranteed.

124. The Committee is prepared to progress with its activity by further developing and expanding its draft Guidelines on jurisdiction and applicable law, and by tackling questions of recognition and enforcement of foreign judgments.

125. The Members of the ILA Committee on the Protection of Privacy in Private International and Procedural Law wish to extend their appreciation to the participants in the 78th ILA Biennial Conference and are grateful to receive comments and insights on the Committee's achievements to date.