

Jurisdiction, Conflict of Laws and Data Protection in Cyberspace

Report on the Conference held in Luxembourg on 12 October 2017, by Martina Mantovani, Research Fellow MPI Luxembourg

On 12 October 2017, the Brussels Privacy Hub (BPH) at the Vrije Universiteit Brussel and the Department of European and Comparative Procedural Law of the Max Planck Institute Luxembourg held a joint conference entitled “Jurisdiction, Conflicts of Law and Data Protection in Cyberspace”. The conference, which was attended by nearly 100 people, included presentations by academics from around the world, as well as from Advocate General Henrik Saugmandsgaard Øe of the Court of Justice of the European Union. The entire conference was filmed and is available for viewing on the YouTube Channel of the Max Planck Institute Luxembourg (first and second parts)

Participants were first welcomed by Prof. Dr. Burkhard Hess, Director of the MPI, and Prof. Dr. Christopher Kuner, Co-Director of the BPH. Both highlighted the importance of considering each of the discussed topics from both a European and a global perspective.

The first panel was entitled “Data Protection and Fundamental Rights Law: the example of cross-border exchanges of biomedical data – the case of the human genome”. The speaker was Dr. Fruzsina Molnár-Gábor of the Heidelberg Academy of Sciences and Humanities, who discussed the regulatory challenges arising in connection to the processing and transfer of biomedical data, including data exchanges between research hubs within the EU and to third-countries (namely the US). The need for innovative regulatory solutions, originating from a bottom-up approach, was discussed against the backdrop of the impending entry into force of the new EU General Data Protection Regulation (GDPR), whose Article 40 encourages the adoption of Codes of Conduct intended to contribute to the proper application of the Regulation in specific sectors. According to Dr. Molnár-Gábor, however, in order to establish an optimal normative framework for biomedical research, the regulatory approach should be combined with appropriate privacy-enhancing technologies and privacy-by-design solutions (such as the emerging federated clouds, the European Open Science Cloud, and data analysis

frameworks bringing analysis to the data). This approach should also be paired with the development of adequate incentives prompting non-EU established companies to express binding and enforceable commitments to abide by EU-approved Codes of Conduct. Her presentation demonstrated the basic problem of data protection and data transfer: The creation of appropriate and applicable legal frameworks often lags behind the necessarily more rapid pace of data exchange seen in successful scientific research.

The second panel was entitled “Territorial Scope of Law on the Internet”. According to Prof. Dr. Dan Svantesson of Bond University in Australia, the focus on territoriality, which characterises contemporary approaches to the solution of conflicts of laws, is the result of an inherent “territorial bias” in legal reasoning. A strict application of territoriality would however be destructive when dealing with cyberspace. Here, the identification of the scope of remedial jurisdiction should follow a more nuanced approach. Prof. Svantesson specifically focused on Article 3 of the new GDPR, which he deemed “too unsophisticated” for its intended purposes as a result of its “all-or-nothing approach”. In other words, either a data controller is subject to the Regulation in its entirety, or it is totally excluded from its scope of application. As an alternative, he proposed a layered approach to its interpretation, grounded in proportionality. The GDPR, he contended, should be broken down into different sets of provisions according to the objectives pursued, and each of these sets should be assigned a different extraterritorial reach. Against this backdrop, the spatial scope of the application of provisions pertaining to the “abuse prevention layer” may, and should, be different from that of the provisions pertaining to the “rights layer” or “the administrative layer”.

A response was made by Prof. Dr. Gerald Spindler of University of Göttingen, who conversely advocated the existence of an ongoing trend toward a “reterritorialization” of the Cyberspace, favoured by technological advance (geo-blocking, Internet filtering). This segmentation of the Internet is, in Prof. Spindler’s opinion, the result of a business strategy that economic operators adopt to minimise legal risks. As specifically concerns private international law rules, however, a tendency emerges towards the abandonment of “strict territoriality” in favour of a more nuanced approach based on the so-called market principle or “targeting”, which is deemed better adapted to the more permeable borders that segment cyberspace.

The third panel was entitled “Contractual Issues in Online Social Media”. The

speaker was Prof. Dr. Alex Mills of University College London. A thorough analysis of Facebook's and Twitter's general terms and conditions brought to light private international law issues stemming from "vertical contractual relationships" between the social media platform and final users. Professor Mills highlighted, in particular, the difficult position of social media users within the current normative framework. In light of the ECJ case-law on dual purpose contracts, in fact, a characterisation of social media users as "consumers" under the Brussels I bis and the Rome I Regulations may be difficult to support. Against this backdrop, social media users are left at the mercy of choice of court and choice of law clauses unilaterally drafted by social media providers. In spite of their (generally) weaker position vis-à-vis social media giants, European social media users will in fact be required to sue their (Ireland-based) contractual counterpart in Californian courts, which will then usually apply Californian substantive law. In addition to generating a lift-off of these transactions from EU mandatory regulation, these contractual clauses also result in an uneven level of protection of European social media users. In fact, Germany-based social media users seem to enjoy a higher level of protection than those established in other EU countries. Since the contract they conclude with the social media provider usually encompass a choice of law clause in favour of German substantive law, they may in fact benefit from the European standard of protection even before Californian courts.

Prof. Dr. Heike Schweitzer of Freie Universität Berlin, highlighted a fundamental difference between E-Commerce and social media platforms. While the former have an evident self-interest in setting up a consumer-friendly regulatory regime (e.g., by introducing cost-efficient ADR mechanisms and consumer-oriented contractual rights) so as to enhance consumer trust and attract new customers, the latter have no such incentive. In fact, competition among social media platforms is essentially based on the quality and features of the service provided rather than on the regulatory standard governing potential disputes. This entails two main consequences. On the one hand, from the standpoint of substantive contract law, "traditional" contractual rights have to adapt to accommodate the need for flexibility, which is inherent to the new "pay-with-data" transactions and vital to survival in this harshly competitive environment. On the other hand, from the standpoint of procedural law, it must be noted that within a system which has no incentive in redirecting disputes to consumer-friendly ADR mechanisms (Instagram being the only exception), private international law rules, as applied in

state courts, still retain a fundamental importance.

The final roundtable dealt with “Future Challenges of Private International Law in Cyberspace”. Advocate General Saugmandsgaard Øe discussed the delicate balance between privacy and security in the light of the judgment of the Court of Justice in the case C-203/15, *Tele2 Sverige*, as well as the specifications brought to the protective legal regime applicable to consumers by case C-191/15, *Verein für Konsumenteninformation v Amazon EU Sarl*. Prof. Kevin D. Benish of New York University School of Law illustrated the US approach to extraterritoriality in the protection of privacy, having particular regard to the recent *Microsoft* case (the U.S. Supreme Court recently granted certiorari). Prof. Dr. Gloria Gonzalez Fuster of Vrije Universiteit Brussels pointed to a paradox of EU data protection legislation, which, on the one hand, regards the (geographic) localisation of data as irrelevant for the purpose of the applicability of the GDPR and, on the other hand, establishes a constitutive link with EU territory in regulating data transfers to third countries. Finally, Dr. Cristina Mariottini, Co-Rapporteur at the ILA Committee on the Protection of Privacy in Private International and Procedural Law, provided an overview of the European Court of Human Rights’ recent case-law on the interpretation of Article 8 ECHR. Specific attention was given to the conditions of legitimacy of data storage and use in the context of criminal justice and intelligence surveillance, namely with respect to the collection of biological samples in computerised national databases (case *Aycaguer v. France*), the use as evidence in judicial proceedings of video surveillance footage (*Vukota-Bojic v. Switzerland*) and the telecommunication service providers’ obligation to store communications data (case *Breyer v. Germany* and case *C?alovic? v. Montenegro*, concerning specifically the police’s right to access the stored data).

Overall, the conference demonstrated the growing importance of private international and procedural law for the resolution of cross-border disputes related to data protection. The more regulators permit private enforcement as a complement to the supervisory activities of national and supranational data protection authorities, the more issues of private international law become compelling. As of today, conflict of laws and jurisdictional issues related to data protection have not been sufficiently explored, as the discussion on private law issues related to the EU General Data Protection Regulation demonstrates. With this in mind, both Brussels Privacy Hub and MPI have agreed to regularly organize conferences on current developments in this expanding area of law.