MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY

VOLUME 11 | NUMBER 1 | SUMMER 2017 | ISSN 1802-5943

PEER REVIEWED

GUEST EDITOR:

DAN JERKER B. SVANTESSON

CONTENTS:

REVOLIDIS | VAN CLEYNENBREUGEL
GONÇALVES | MAUNSBACH | OSULA
ZOETEKOUW | STADNIK | ŽOLNERČÍKOVÁ | BOGDAN

www.mujlt.law.muni.cz

Masaryk University Journal of Law and Technology
issued by Institute of Law and Technology
Faculty of Law, Masaryk University
www.mujlt.law.muni.cz

Official Partner (Slovakia)
AS Legal s.r.o., advokátska kancelária (www.aslegal.sk)
Hlučínska 1, 83103 Bratislava

Official Partner (Czech Republic)
ROWAN LEGAL, advokátní kancelář s.r.o. (www.rowanlegal.com/cz/)
Na Pankráci 127, 14000 Praha 4

Subscriptions, Enquiries, Permissions
Institute of Law and Technology, Faculty of Law, MU (cyber.law.muni.cz)

licensed as peer-reviewed scientific journal by the Research and Development
Council of the Government of the Czech Republic
listed in HeinOnline (www.heinonline.org)
listed in Scopus (www.scopus.com)
reg. no. MK ČR E 17653

MASARYK UNIVERSITY JOURNAL OF
LAW AND TECHNOLOGY

VOLUME **11** | NUMBER **1** | SUMMER **2017**

Dan Jerker B. Svantesson: Editorial **3**

LIST OF ARTICLES

Ioannis Revolidis: Judicial Jurisdiction over Internet Privacy Violations and the GDPR: a Case of "Privacy Tourism"? **7**

Pieter Van Cleynenbreugel: The European Commission's Geo-blocking Proposals and the Future of EU E-commerce Regulation **39**

Anabela Susana de Sousa Gonçalves: Choice-of-court Agreements in the E-Commerce International Contracts **63**

Ulf Maunsbach: The CJEU as an Innovator – a New Perspective on the Development of Internet Related Case-law **77**

Anna-Maria Osula, Mark Zoetekouw: The Notification Requirement in Transborder Remote Search and Seizure: Domestic and International Law Perspectives **103**

Ilona Stadnik: What Is an International Cybersecurity Regime and How We Can Achieve It? **129**

Veronika Žolnerčíková: ICANN: Transformation of Approach towards Internet Governance **155**

LIST OF COMMENTARIES

Michael Bogdan: The New EU Rules on Electronic Insolvency Registers **175**

DOI: 10.5817/MUJLT2017-1-1

EDITORIAL: TIME TO MOVE FORWARD ON INTERNATIONAL ICT LAW

by

DAN JERKER B. SVANTESSON*

Anyone studying the comparatively short history of the discipline we may refer to as information and communications technology (ICT) law will notice several trends. One such trend is that, where a new topic starts gaining attention, that attention is typically directed at the domestic context. For example, it is only relatively recently that the international dimensions of data privacy law have started to gain widespread attention, and areas such as cyber security are still mainly approached from a domestic perspective.

This is not to deny that there, already early on, is an awareness of the international dimensions. All I am suggesting here is that those international dimensions only gain widespread attention once the domestic perspective has been pursued. And maybe this is both natural and desirable. However, what is striking is the extent to which attention is now being directed at the international dimensions of various topics falling within the umbrella term of ICT law. In fact, I think we are now in a "*golden era*" for anyone who has an interest in the cross-section of ICT law and international law – be it public, or private, international law (to the extent that distinction still is valid).

In light of this, this special issue of the Masaryk University's flagship journal – the Masaryk University Journal of Law and Technology (MUJLT) – is definitely timely. And given the high quality of the contributions, and the interesting topics they address, I have no doubt that this issue will help progress the law on several vitally important topics. Because the time

* dasvante@bond.edu.au, Professor and Co-Director, Centre for Commercial Law, Faculty of Law, Bond University, Australia; Researcher, Swedish Law & Informatics Research Institute, Stockholm University, Sweden.

has come to take some serious steps forward on how we approach the international dimensions of ICT law.

Revolidis sets a high standard with his fascinating account of jurisdiction over privacy violations, with special focus on the impact of art. 79(2) of the General Data Protection Regulation, which opens this issue. This is followed by excellent contributions addressing diverse topics within the field of international ICT law. Van Cleynenbreugel discusses the European Commission's geo-blocking proposals and the future of EU e-commerce regulation, Gonçalves addresses choice-of-court agreements in international e-commerce contracts, and Maunsbach provides an innovative perspective on the development of Internet related case-law within the Court of Justice of the European Union. Thereafter, we see the fruits of the collaboration between Osula and Zoetekouw in the form of their article focused on the notification requirement embedded into the legal regimes regulating remote search and seizure. We then have Stadnik's exploration of international cybersecurity regimes and Žolnerčíková's account of ICANN's recent transformation. The issue ends with Bogdan's comment on the new EU Regulation No 2015/848 on Insolvency Proceedings (Recast) that create a system of national insolvency registers and establish a decentralized system for the interconnection of such registers by means of the European e-Justice Portal.

All the contributions that appear in this issue stem from two events held in November 2016. The first of those events is the 2016 rendition of the highly successful conference series on interdisciplinary cyberspace issues held annually at the Masaryk University. I take this opportunity to thank the organisers of Cyberspace 2016 and especially the participants in the international ICT law work stream.

The second of the events from which the contributions to the special issue stem is a workshop organised by the European Law Institute's Intellectual Property Law Special Interest Group together with the Centre for Commercial Law at Bond University. The workshop was held at the University of Vienna and was funded by the Australian Research Council (ARC) as part of a project – an Australian Research Council Future Fellowship – I held at the time which reassessed and re-evaluated how the concept of jurisdiction most appropriately can be applied in the Internet

era characterised by cloud computing, Web 2.0 and geo-location technologies. I thank all involved in the Vienna workshop.

I feel privileged to have had the opportunity to – for a second time – be the Guest Editor for a special issue of the MUJLT. I thank all who have worked on this issue, especially the Editor-in-Chief Radim Polčák, the Deputy Editor-in-Chief Jakub Harašta and, of course, the crucially important and superbly qualified authors.

Dan Jerker B. Svantessson
18 June 2017, Mudgeeraba, Australia

DOI: 10.5817/MUJLT2017-1-2

JUDICIAL JURISDICTION OVER INTERNET PRIVACY VIOLATIONS AND THE GDPR: A CASE OF "PRIVACY TOURISM"?

by

IOANNIS REVOLIDIS*

This paper discusses the impact of art. 79(2) of the General Data Protection Regulation (GDPR) in international litigation over online privacy violations. The first part introduces the tendency of the European legislator to treat private international law problems in the field of data protection as isolated and independent from the traditional secondary private international law acts. The second part analyses the current status quo of international jurisdiction over online privacy violations according to Regulation 1215/2012. After briefly examining the eDate and Martinez ruling (joined cases C-509/09 and C-161/10), it concludes that the Court of Justice of the European Union has stretched the jurisdictional grounds of art. 7(2) Regulation 1215/2012 too far in order to afford strong protection to data subjects. In that sense, it raises doubts on whether art. 79(2) was necessary. Following this conclusion, it tries to explore the uneasy relationship of GDPR art. 79(2) with the jurisdictional regime established under Regulation 1215/2012. Instead of an epilogue, the last part tries to make some reflections on the impact of GDPR art. 79(2) in privacy litigation cases involving non-EU parties.

KEY WORDS

Conflict of Laws, International Jurisdiction, Internet, Data Protection Law, Forum Shopping, Regulation (EU) 2016/679, Regulation 1215/2012

* ioannis.revolidis@iri.uni-hannover.de, Ioannis Revolidis has graduated from Faculty of Law, Aristotle University of Thessaloniki, Coordinator of the EULISP Master of Laws in IT/IP Law, research associate, legal and ethical framework of health research projects at Institute for Legal Informatics, Leibnitz, University Hannover.

1. INTRODUCTION

Conflict of laws problems related to data protection have already received a unique treatment from the European legislator during the adoption of the Data Protection Directive. The Data Protection Directive had been prepared during the 1980s and 1990s, namely during a time when the current Internet was still just at the beginning of its creation and of course not widely used. In the historical reality of the Data Protection Directive, the vast amount of international exchanges of personal information were, more or less, a theoretical and mostly unlikely scenario.[1]

Although created in such a historical background, the Data Protection Directive included provisions regulating the law applicable to transnational data flows. These were to be accommodated in article 4(1) of the Data Protection Directive which reads as follows:

> *"1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable; (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law; (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community […]".*

By the time of its adoption, article 4(1) covered many legislative gaps within the system of the protection of personal information in the EU. On the one hand, the major concern of the European legislator was to prohibit a situation where a data controller could avoid the implementation of any of the national data protection laws adopted by the Member States. By the time of the adoption of the Directive, the basic

[1] See on that Moerel, L. (2011) The long Arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide? *International Data Privacy Law*, 1(1) p. 28.

fear was that a data controller might relocate his/her activities outside of the EU, while still continuing to process personal information of EU citizens. The three indents of art. 4(1) were designed in order to cover the different aspects of that same danger:

- indent a) the situation where the data controller, while having its main seat outside the EU, still actively conducts business with EU citizens through an establishment within the EU,
- indent b) the situation where the data controller would be established in territories that geographically do not belong to the European continent, but are still controlled by Member States; in that case the directive aimed at clarifying that it will be applicable to the extent that under public international law, the legal order of a Member State would still regulate the issues of that territory,
- indent c) the situation where the data controller, having its main seat outside the EU, would still process personal information of EU citizens by using equipment located within a Member State, without necessarily retaining an establishment in an EU Member State.[2]

On the other hand, art. 4(1), although not primarily an instrument of private international law, *de facto* obtained such a role within the EU. At the time of its adoption, the basic European instrument regarding the law applicable in European transactions was the Rome Convention of 1980, which only referred to certain contractual obligations without being applicable to problems related to data protection law. Moreover, there was still no unified regime regarding non-contractual obligations, which represented the main corpus of international data flows. Art. 4(1) was thus called upon to determine the law applicable also in cases where the data flows were taking place purely between different Member States of the EU.[3]

The insertion of a specific conflict of laws regime within the Data Protection Directive was a major departure from the principle of country of origin that was predominant at similar legislative initiatives of the EU at the time.[4] One might find such a departure reasonable if account is to be

[2] Moerel, L. (2011) Back to basics: when does EU data protection law apply? *International Data Privacy Law*, 1(2) pp. 92-110, esp. pp. 94-97, offers a very detailed account of the rationale behind art. 4(1) of the Data Protection Directive. For an early account of the same see Bygrave, L. (2000) Determining Applicable Law pursuant to European Data Protection Legislation. *Computer Law & Security Report*, 16 ,pp. 252-257.

taken of the complex and hybrid nature of Data Protection rules,[5] which is inextricably linked to the very particular nature of data as the subject matter of legal regulation and the subsequent discussion whether data shall be provided for a specific set of rules rather than being covered by pre-existing and non-data specific regulations.[6]

In addition, the adoption of the Data Protection Directive was a step towards an enhanced protection of the fundamental right to privacy;[7] its adoption was inspired, in other words, from a clear mandate to expand the protection of human rights within the EU. During the same period, it was still open to debate whether EU private international law (both procedural and substantive) was taking a similar direction towards guaranteeing the basic freedoms and rights of EU citizens.[8] A special conflict of laws regime for data protection law was, thus, probably stemming from the anxiety of the European legislator to guarantee that the strong human rights mandate of the Data Protection Directive would not be compromised by the different priorities of EU private international law.

---

[3] One can in that context better understand the mandate of art. 4(1)(a): "*[…] when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable […]*". It is worth mentioning here that the Article 29 Working Party has also classified art. 4 as a genuine private international law rule for intra-European data flows. See WP 56, 30 May 2002, p. 6 where it is stated: "*[…] Concerning the situations within the Community, the objective of the directive is twofold: it aims at avoiding gaps (no data protection law would apply) and at avoiding multiple/double application of national laws. As the directive addresses the issue of applicable law and establishes a criterion for determining the law on substance that should provide the solution to a case, the directive itself fulfils the role of a so-called "rule of conflict" and no resource to other existing criteria of international private law is necessary (emphasis added)*".

[4] See for example art. 3 of the E-Commerce directive. For an analysis of the functioning of the principle of country or origin in E-Commerce see Savin, A. (2013) *EU Internet Law*. Cheltenham; Northampton: Edward Elgar, pp. 45-48.

[5] Svantesson, D.J.B. (2013) A "*layered approach*" to the extraterritoriality of data privacy laws. *International Data Privacy Law*, 3(4) pp. 278-286, concludes that even within the premises of private international law per se, the nature of data protection rules is complicated and suggests that one cannot always cover them with the same conflict of laws rule. He tries, therefore, to classify them in three basic distinct private international law categories and goes on to examine which rules fit the distinct character of different data protection rules better.

[6] For a recent debate on the issue, see Woods, A.K. (2016) Against Data Exceptionalism. *Stanford Law Review*, 68(4) pp. 729-789, who provides some elaborate argumentation against treating data under a data specific legal regime, while Svantesson, D.J.B. (2016) Against "Against Data Exceptionalism". *Masaryk University Journal of Law and Technology*, 10(2) pp. 200-211, argues for the opposite.

[7] See Directive 95/46/EC of the 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. Official Journal of the European Union (1995/L 281/31) 23 November. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN:PDF [Accessed 7 June 2017), recitals 7 and 8.

In the meantime, though, there has been a clear convergence of the aims of EU private international law and those of the Data Protection Directive. Already during the middle of the previous decade and in the shadow of the discussion for the adoption of a European Constitution,[9] the Council urged a clear strengthening of the human rights dimension of EU private international law,[10] while the Lisbon Treaty[11] signaled the formal adoption of the Charter of the Fundamental Rights as primary EU Law,[12] a step that radically changed the value system of EU private international law, making the protection of fundamental rights its main priority.[13]

One might, in that sense, argue that EU private international law was, especially after the adoption of the Lisbon Treaty, in a better position

[8] The Court of Justice was nonetheless trying already during the 80s to establish that EU private international law in general and the Brussels Convention in particular were aiming at strengthening the legal protection of EU citizens rather than just promoting the facilitation of the common market. See *Duijnstee v Goderbauer* [1983], case C-288/82, par. 11-12, where the Court stated: *"[…] According to the preamble to the Convention, the Contracting States, anxious to "strengthen in the Community the legal protection of persons therein established"*, considered that it was necessary for that purpose *"to determine the international jurisdiction of their courts, to facilitate recognition and to introduce an expeditious procedure for securing the enforcement of judgments, authentic instruments and court settlements". Both the provisions on jurisdiction and those on the recognition and enforcement of judgments are therefore aimed at strengthening the legal protection of persons established in the Community […]"*.

[9] For the background of this initiative see Pache, E. (2002) Eine Verfassung für Europa – Krönung oder Kollaps der europäischen Integration? *Europarecht*, 37 pp. 767-784.

[10] As it has been documented in the Council's Hague Programme: Strengthening Freedom, Security and Justice in the EU. *Official Journal of the European Union*, (2005/C 53/1) 03 March. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005XG0303(01)&from=EN:PDF [Accessed 7 June 2017], p. 2: *"[…] Fundamental rights, as guaranteed by the European Convention on Human Rights and the Charter of Fundamental Rights in Part II of the Constitutional Treaty, including the explanatory notes, as well as the Geneva Convention on Refugees, must be fully respected. At the same time, the programme aims at real and substantial progress towards enhancing mutual confidence and promoting common policies to the benefit of all our citizens. Incorporating the Charter into the Constitutional Treaty and accession to the European Convention for the protection of human rights and fundamental freedoms will place the Union, including its institutions, under a legal obligation to ensure that in all its areas of activity, fundamental rights are not only respected but also actively promoted […]"*.

[11] For a general account on the impact of the Lisbon Treaty on the Institutional values of the EU, see among others Dougan, M. (2008) The Treaty of Lisbon 2007: Winning Minds not Hearts. *Common Market Law Review*, 45(3) pp. 617-703, Harpaz, G. and Herman, L. (2008) The Lisbon Reform Treaty: Internal and External Implications. *European Journal of Law Reform*, 10(4) pp. 431-436, Terhechte, J.P. (2008) Der Vertrag von Lissabon: Grundlegende Verfassungsurkunde der europäischen Rechtsgemeinschaft oder technischer Änderungsvertrag? *Europarecht*, 43 pp. 143-190, Pech, L. (2011) The Institutional Development of the EU Post - Lisbon: A case of plus ca change…?, UCD Dublin European Institute Working Paper 11 – 5, December 2011, Goebel, R.J. (2011) The European Union and the Treaty of Lisbon. *Fordham International Law Journal*, 34(5) pp. 1251-1268.

[12] For the importance and impact of the primary EU status awarded to the Charter under the Lisbon Treaty see Landau, E.C. (2008) A New Regime of Human Rights in the EU? *European Journal of Law Reform*, 10(4) pp. 557 – 575, Pache, E. and Rösch, F. (2009) Die neue Grundrechtsordnung der EU nach dem Vertrag von Lissabon. *Europarecht*, 44 pp. 769 – 790, Lanaerts, K. (2012) Die EU – Grundrechtecharta: Anwendbarkeit und Auslegung. *Europarecht*, 47 pp. 3 – 18, Sarmiento, D. (2013) Who's afraid of the Charter? The Court of Justice, National Courts and the new Framework of Fundamental Rights Protection in Europe. *Common Market Law Review*, 50(3) pp. 1267-1304.

to accommodate the protection of personal data in cases of international data flows in a more comprehensive way.[14]

Such a line of thinking was not convincing either for the Court of Justice, which in the recent *VKI v. Amazon* case[15] confirmed the special role of art. 4(1) in determining the law applicable to a certain data processing activity independently from any stipulations found in the Rome I and II Regulations,[16] or for the European legislator, who isolated the private international law regime of EU Data Privacy law even further. Art. 3 of the General Data Protection Regulation (GDPR) is the spiritual successor of art. 4 of the Data Protection Directive, while art. 79(2) of the GDPR, which lies in the center of this contribution, is a novelty in terms of defining the judicial jurisdiction over violations of data protection law. Instead of leaving the issues of judicial jurisdiction to be determined by the Brussels Ia Regulation and the principles developed over the past decades from the Court of Justice in interpreting the latter, the GDPR went as far as to create a special jurisdictional regime for data privacy disputes.

---

[13] See the priorities set by the The Stockholm Programme — An open and secure Europe serving and protecting citizens. *Official Journal of the European Union* (2010/C 115/1) 05 May. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2010:115:FULL&from=en:PDF [Accessed 7 June 2017] p. 4, as well as the EU Justice Agenda for 2020, COM(2014) 144 final.

[14] Starting as early as the Brussels Convention of 1967, one might argue that EU private international law has accumulated a non-negligible experience in dealing with the cross-border dimension of the protection of fundamental rights.

[15] *Verein für Konsumenteninformation v. Amazon* [2016], Case C-191/15.

[16] *Verein für Konsumenteninformation v. Amazon* [2016], Case C-191/15, par. 73-80. That the Rome II Regulation is not applicable to data privacy issues is clear from art. 1(2)(g) of the that Regulation. The applicability of the Rome I Regulation in data privacy issues has not been explored by the Court prior to this case. The Court has not offered a clear justification why a clause determining the law applicable to a contract does not affect the data privacy issues attached to it. One might reasonably assume that this is related to the wide scope of application of art. 4(1) of the Data Protection Directive. It seems, namely, that art. 4(1) of the Data Protection Directive covers data privacy issues in their entirety, including the possibility of contractual determination of the law applicable. Since art. 4(1) of the Data Protection Directive does not provide for such a contractual determination of the law applicable, it must be concluded that such contractual clauses are simply not allowed and, therefore, the Rome I Regulation cannot be called into application. That view seems to be consistent with the major goal pursued by art. 4(1) of the Data Protection Directive, namely the non-circumvention of EU data privacy law by clauses that might designate as applicable the law of a country with less stringent data privacy stipulations. See in that line Kartheuser, I. and Klar, M. (2014) Wirksamkeitskontrolle von Einwilligungen auf Webseiten Anwendbares Recht und inhaltliche Anforderung im Rahmen gerichtlicher Überprüfungen. *Zeitschrift für Datenschutz*, 4(10) pp. 500-505. Piltz, C. (2012) Rechtswahlfreiheit im Datenschutzrecht? *Kommunikation & Recht*, 15(10) pp. 640-644, considers data protection law to fall within art. 9 of the Rome I Regulation (overriding mandatory provisions) and, therefore, also suggests that a contractual circumvention of art. 4(1) of the Data Protection Directive shall not be possible. Despite the interesting argumentation, this opinion cannot be accepted without reservations. In excluding data protection law from the scope of the Rome I Regulation, the Court of Justice did not argue along these lines.

The question whether such a specific jurisdictional regime was necessary and whether the established bases of jurisdiction provide for a reasonable and effective solution will be the subject of the analysis to follow.

2. IS ART. 79(2) OF THE GDPR NECESSARY?

2.1 THE SHEVILL IMPACT AND DOCTRINAL REACTIONS

A brief overview of the jurisdictional regime for online data privacy violations under the Brussels Ia Regulation must necessarily start from the decision of the Court of Justice of the European Union (CJEU) in the *Shevill* case.[17] Although the case does not per se refer to online violations of data protection, it is the first one where the CJEU was called upon to examine the functioning of the Brussels jurisdictional regime in a scenario of ubiquitous personality infringements. In sum, the case revolved around the complaint of Fiona Shevill, domiciled in England, against a newspaper established in France that published an article linking Fiona Shevill to a drug case. The bulk of the newspapers containing the article that Fiona Shevill found to be defaming for her was distributed in France (237.000 of them). A considerably lower number had been distributed in other Member States (15.500 of them), and eventually only 230 papers made it to England. Fiona Shevill decided to sue the French newspaper in England, and the main question that the CJEU had to tackle was whether, under the Brussels jurisdictional rules, the English Courts could indeed adjudicate over the dispute.

In resolving this problem, the CJEU remained consistent with its previous case law regarding international judicial jurisdiction over tort cases,[18] declaring once more that, apart from being allowed to sue at Courts of the domicile of the defendant,[19] the victim of an alleged tort shall be able to sue either in the place where the event giving rise to the damage took place or in the place where the damage occurred.[20] The Court went on to accept that this basic scheme shall remain applicable to personality

---

[17] *Fiona Shevill v. Presse Alliance SA* [1994], Case C-68/93.

[18] Most prominently the *Bier v. Mines de potasse d'Alsace* [1976], Case C-21/76.

[19] Art. 4 REGULATION (EU) No 1215/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast). *Official Journal of the European Union* (2012/L 351/1) 20 December. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R1215&from=EN:PDF [Accessed 7 June 2017].

[20] *Bier v. Mines de potasse d'Alsace* [1976], Case C-21/76, par. 14-19.

infringements committed via mass media publications,[21] even more so because in such cases the event giving rise to the damage, namely the publication of the infringing information, will usually (but not always) coincide the domicile of the defendant, thus stripping the victim of a potential jurisdictional basis.[22] By allowing the victim to sue in each country where the alleged infringing material was distributed, the Court tried to establish an additional forum that shall be in a (procedurally) better position to adjudicate over ubiquitous personality disputes than the Courts of the domicile of the defendant.[23] Based on this better procedural position, the Court limited the extent of the jurisdiction awarded to the forum of the place where the damaged occurred only within the limits of its own territory.

Whether one agrees with the outcome of the *Shevill* case[24], or not,[25] the dogmatic consistency of the ruling with the basic jurisdictional foundations of the Brussels regime cannot be disputed. In justifying the formulation of the jurisdictional basis at the courts of the country where the alleged victim suffered the damage in his/her personality rights, the Court explained that this extension of the available fora is justified by the axiom of sound administration of justice, which is the basic reason for the existence of the special rule of jurisdiction for tort cases (nowadays art. 7(2) of the Brussels Ia Regulation).[26]

The ruling of the CJEU in *Shevill* has functioned as the starting point of the discussion on how to treat, from an adjudicatory jurisdiction point of view, the problem of violations of personality rights via the Internet.

While all possible variations have been proposed in legal literature,[27]

---

[21] *Fiona Shevill v. Presse Alliance SA* [1994], Case C-68/93, par. 23.

[22] *Fiona Shevill v. Presse Alliance SA* [1994], Case C-68/93, par. 24-27.

[23] *Fiona Shevill v. Presse Alliance SA* [1994], Case C-68/93, par. 31.

[24] In that direction among others Huber, P. (1996) Persönlichkeitsschutz gegenüber Massenmedien im Rahmen des Europäischen Zivilprozeßrechts. *Zeitschrift für Europäisches Privatrecht*, 4(2) pp. 295-313, Wagner, G. (1998) Ehrenschutz und Pressfreiheit im europäischen Zivilverfahrens- und Internationalen Privatrecht. *Rabels Zeitschrift für ausländisches und internationales Privatrecht*, 62(2) pp. 243-285.

[25] Among others Coester-Waltjen, D. (1999) Internationale Zuständigkeit bei Persönlichkeitsrechtsverletzungen. In: Festschrift für Rolf A. Schütze, Munich: C.H. Beck, pp. 175-187.

[26] *Fiona Shevill v. Presse Alliance SA* [1994], Case C-68/93, par. 31.

[27] An exhaustive presentation of the different opinions expressed on the matter goes beyond the scope of the current contribution. For a neat summary of the academic proposals on how to treat personality torts over the Internet within the premises of the Brussels jurisdictional regime see Marton, E. (2016) *Violations of Personality Rights through the Internet: Jurisdictional Issues under European Law*. Baden-Baden: Nomos Verlag; Chawley Park, Cumnor Hill, Oxford: Hart Publishing, pp. 201-231.

from also upholding the *Shevill* case law for Internet related personality violations[28] to abandoning them in favour of a plaintiff's forum[29] or in favour of a targeting test,[30] it has not been disputed that the existing jurisdictional rules of the Brussels regime provided an adequate basis (even if modifications of the existing case law have been proposed as necessary) to accommodate online violations of personality rights, including privacy.[31]

2.2 UPDATING SHEVILL: EDATE AND MARTINEZ CASE LAW

The definitive answer on whether the Brussels jurisdictional regime can accommodate personality violations over the Internet has been given by the CJEU in the joined *eDate and Martinez* cases.[32]

Both cases share a privacy background. In *eDate*, a web portal established in Austria reported on a crime committed by a person domiciled in Germany. The person was convicted for the crime but has lodged an appeal against the conviction. In order to force the web portal to desist from reporting the issue, the person linked to the crime brought an action before the German courts, claiming that the web portal shall be forced to refrain from using his full name when reporting about him in connection with the crime committed. In *Martinez*, French actor Olivier Martinez and his father brought an action before the French courts against MGN, a company established in England, because in the website of the *Sunday Mirror*, operated by MGN, there was a report on their private lives accompanied by pictures without their consent.

The CJEU was thus given the chance to examine the applicability of its previous *Shevill* case law in an Internet context. Inspired by the findings of AG Cruz Villalón,[33] the Court found the *Shevill* case law not completely

---

[28] See for example Stone P. (2006) *EU Private International law. Harmonization of Laws*. 2nd ed. Cheltenham, UK; Northampton MA: Edward Elgar, 2006, pp. 93-94.

[29] Kubis, S. (1999) *Internationale Zuständigkeit bei Persönlichkeits- und Immaterialgüterrechtsverletzungen*. Bielefeld: Verlag Ernst und Werner Giesing, pp. 153-176.

[30] Most characteristically Reymond, M. (2013) Jurisdiction in case of personality torts committed over the Internet: a proposal for a targeting test. *Yearbook of Private International Law*, 14 pp. 205-246.

[31] In urging the European legislator to regulate in a more comprehensive way the private international law issues related to personality rights Hess, B. (2015) The Protection of Privacy in the Case Law of the CJEU. In: Burkhard Hess and Christina Mariottini (eds.) *Protecting Privacy in Private International and Procedural Law and by Data Protection*. Baden-Baden: Nomos Verlag, pp. 112-113, suggests that such a future regulation shall be tailored on the Brussels Ia Regulation and in the way the CJEU has interpreted its provisions.

[32] *eDate Advertising GmbH v. X and Olivier Martinez v. MGN Limited* [2011], joint Cases C-509/09 and C-161/10.

satisfactory for Internet related privacy violations.[34] It came to that conclusion after performing a scrutiny of the characteristics of online communications. Although printed mass media can also be distributed in a variety of countries, Internet publications, due to the incredible speed and geographical penetration of the dissemination, marginalise the significance of the place of distribution (named as a major connecting factor under the *Shevill* case law) and maximises the scale of the exposure of individuals to violations of their personality.[35]

In view of that, the Court performed a revision of the *Shevill* case law. After declaring that the particularities of Internet communications make necessary the existence of a jurisdictional basis, independent from the domicile of the defendant, where the victim of the alleged privacy violation can claim protection for the full scale of infringement, the Court decided that this place is to be found in the Member State of the "*centre of the interests*" of the alleged victim.[36]

In sum, after the *eDate and Martinez* decision, the alleged victim of an online privacy violation could sue the perpetrator in the following places:

- regarding the full extent of the damage in the Courts either of the domicile of the defendant/perpetrator[37] or in the Courts of the victim's/plaintiff's centre of interests, which in the majority of the cases (but not necessarily always) will coincide with the victim's/plaintiff's domicile;[38]
- in cases where the domicile of the defendant/perpetrator does not coincide with the place of distribution,[39] the victim/plaintiff can sue also in the courts of the Member State of the distribution for the full

[33] Opinion of AG Cruz Villalón in joint Cases *eDate Advertising GmbH v. X and Olivier Martinez v. MGN Limited* [2011], C-509/09 and C-161/10, par. 56-67. Although the Court did not exactly adopt the jurisdictional ground proposed by the AG Villalón, in adapting the *Shevill* case law for Internet related cases shared his view on the necessity of doing so.

[34] *eDate Advertising GmbH v. X and Olivier Martinez v. MGN Limited* [2011], joint Cases C-509/09 and C-161/10, par. 46.

[35] *eDate Advertising GmbH v. X and Olivier Martinez v. MGN Limited* [2011], joint Cases C-509/09 and C-161/10, par. 47.

[36] *eDate Advertising GmbH v. X and Olivier Martinez v. MGN Limited* [2011], joint Cases C-509/09 and C-161/10, par. 48.

[37] Under art. 4 of REGULATION (EU) No 1215/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast). Official Journal of the European Union (2012/L 351/1) 20 December. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R1215&from=EN:PDF [Accessed 7 June 2017].

extent of the damage;

- last, but not least, the victim can still make use of the *Shevill* case law, allowing him/her to sue in each country where his/her personal information has been illegally processed, albeit only to the extent of the damage suffered in each of these countries.

The decision created polarised reactions. Some commentators considered that it was a step in the right direction,[40] claiming that by creating a jurisdictional basis that allows the victim of an alleged online privacy violation to sue in the courts of the Member State in which the centre of his/her interests are located, it strikes a fairer balance between the victim and the perpetrator. Other commentators praised the readiness of the CJEU to adapt the jurisdictional provisions of the Brussels regime to the particularities of online communication,[41] while others were very sceptical towards it, raising a series of legitimate concerns.[42]

Indeed, the ruling of the CJEU in *eDate and Martinez* signals a stark departure from the very fundamental principles of the jurisdictional scheme of the Brussels Ia Regulation. Adapting the principles of a legal instrument per se shall not be viewed as a problem. What is really problematic with the *eDate and Martinez* decision is that it ignores the compelling reasons that led to the adoption of the jurisdictional principles that it has dismantled without providing convincing arguments that this should have been the case.

It must not be forgotten that the rules of jurisdiction of the Brussels Ia

---

[38] Pursuant to art. 7 (2) of REGULATION (EU) No 1215/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast). Official Journal of the European Union (2012/L 351/1) 20 December. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R1215&from=EN: pdf[Accessed 7 June 2017], as interpreted in the *eDate and Martinez* ruling.

[39] For example, a data controller with a statutory seat in Member State A illegally posts personal information of the victim via the website of a subsidiary company established in Member State B and running its website in that Member State (Member State B).

[40] Most notably, Hess, B. (2012) Der Schutz der Privatsphäre im Europäischen Zivilverfahrensrecht. *Juristen Zeitung*, 67(4) pp. 189-193.

[41] Bogdan, M. (2013) Website Accessibility as Basis for Jurisdiction Under the Brussels I Regulation in View of New Case Law of the ECJ. In: Dan Jerker B. Svantesson and Stan Greenstein (eds.) *Internationalisation of Law in the Digital Information Society*. Copenhagen: Ex Tuto Publishing, pp. 159-172, esp. p. 167.

[42] See among others Heinze, C. (2011) Surf global, sue local! Der europäische Klägergerichtsstand bei Persönlichkeitsrechtsverletzungen im Internet. *Europäische Zeitschrift für Wirtschaftsrecht*, 22(24) pp. 947-950, Mankowfski P. (2016) In: Ulrich Magnus and Peter Mankowfski (eds.) *Brussels Ibis Regulation-Commentary*. Köln: Verlag Dr. Otto Schmidt KG, pp. 323-328.

Regulation are based on the principle of "*actor sequitur forum rei*" established in art. 4 of that Regulation.[43] The adoption of "*actor sequitur forum rei*" was not a random choice but has a very strong justification dating back to the adoption of the Brussels Convention. The jurisdictional provisions of the Brussels regime and especially the jurisdictional basis of the domicile of the defendant share an existential bond with the provisions that refer to the recognition and enforcement of judgements.[44] Simply put, the simplification of the recognition and enforcement of foreign civil judgements between the Member States of the EU[45] is a clear procedural advantage of the plaintiff, who is the hopeful beneficiary of the recognition and enforcement. The "*actor sequitur forum rei*" principle aims to counterpoise this procedural advantage by offering a chance to the defendant to procedurally defend him/herself on equal terms,[46] given that in international litigation the risks for the procedural rights of the defence are higher than those in plainly domestic cases.[47]

---

[43] For the content and the meaning of the "*actor sequitur forum rei*" principle within the Brussels jurisdictional regime see Hess, B. (2010) *Europäisches Zivilprozessrecht*. Heidelberg: C.F. Müller Verlag, pp. 265-271.

[44] That this is indeed the case see Hallstein, W. (1964) Angleichung des Privat- und Prozessrechts in der Europäischen Wirtschaftsgemeinschaft. *Rabels Zeitschrift für ausländisches und internationales Privatrecht*, 28(2) pp. 211-231, esp. 223 where he notes: *„[…] Die Vereinfachung und Beschleunigung des Exequaturverfahrens allein war jedoch nicht ausreichend, um allen Anforderungen zu genügen, die an ein wirksames Verfahren der Rechtsverfolgung innerhalb eines einheitlichen Wirtschaftsraumes gestellt werden müssen. Man denke zum Beispiel an die Fälle, in denen die Vollstreckung im Anerkennungsstaat verweigert wird, weil in diesem Staat ein bereits ergangenes Urteil unvereinbar ist mit dem Urteil, um dessen Exequatur nachgesucht wird, oder weil im Anerkennungsstaat zwischen denselben Personen und in derselben Sache ein Verfahren schwebt. Wollte man die Zahl dieser Fälle verringern, so musste auch die territoriale Zuständigkeit durch das neue Abkommen unmittelbar geregelt werden […]*".

[45] Simplification that reached so far as to abolish the exequatur procedure from the Brussels Ia Regulation. See on that Kramer, X.E. (2013) Cross-Border Enforcement and the Brussels I-bis Regulation: Towards a New Balance between Mutual Trust and National Control over Fundamental Rights. *Netherlands International Law Review*, 60 pp. 343 – 373, Geimer, R. Unionsweite Titelvollstreckung ohne Exequatur nach der Reform der Brüssel I-Verordnung. In: Festschrift für Rolf A. Schütze, Munich: C.H. Beck, pp. 109 – 121, Isidro, M.R. On the Abolition of Exequatur. In: Burkhard Hess and Maria Bergström and Eva Stroskrubb (eds.) *EU Civil Justice: Current Issues and Future Outlook*, Oxford: Hart Publishing, pp. 283-298.

[46] In that sense the "*actor sequitur forum rei principle*" is the jurisdictional mirroring of the non-recognition ground referring to the judgements that are given in default of appearance of art. 45 Brussels Ia. See in that regard the ruling of the Court in *Autoteile v. Malhé* [1985], Case C-220/84, par. 15: *"[…] According to article 2, persons domiciled in a Contracting State are to be sued in the courts of that State. That provision is intended to protect the rights of the defendant; it serves as a counterpoise to the facilities provided by the Convention with regard to the recognition and enforcement of foreign judgements […]*".

[47] On that, see the Jenard, P. Report on the Convention on jurisdiction and the enforcement of judgments in civil and commercial matters. *Official Journal of the European Union* (1979/C 59/1) 05 March. Available from: http://aei.pitt.edu/1465/1/commercial_report_jenard_C59_79.pdf [Accessed 7 June 2017], p. 18.

Although that does not mean that the domicile of the defendant is the only jurisdictional base to be found in the Brussels Ia Regulation, it still puts that jurisdictional ground in the place of the basic rule.[48] Save for the exclusive jurisdictional bases of the Brussels Ia Regulation,[49] the domicile of the defendant shall be the starting point of any international dispute in the EU,[50] including those that refer to online violations of privacy. That very fact shall also guide the interpretation of the additional bases of jurisdiction, especially those located in art. 7, where the special jurisdiction for torts is also accommodated.

By this is meant that the interpretation of the jurisdictional bases located in art. 7 of the Brussels Ia Regulation shall be restrictive, so that they do not go beyond their true scope of application, as this is to be found in the reasons that justified their adoption.[51] As it is clear both from the recitals of the Brussels Ia Regulation[52] and from an unbreakable chain of CJEU decisions,[53] the reason for adopting art. 7 in general and the jurisdictional base for torts in art. 7(2) is not the protection of the victims of torts. Art. 7 is neutral when it comes to protecting the individual interests of the parties.[54] The real reason for adopting art. 7 was the efficacious administration of justice, based on the proximity

---

[48] See *Group Josi v UGIC* [2000], Case C-412/98, par. 35.

[49] Established in art. 24 of REGULATION (EU) No 1215/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast). *Official Journal of the European Union* (2012/L 351/1) 20 December. Available from:http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R1215&from=EN:PDF [Accessed 7 June 2017].

[50] The actor sequitur forum rei has even survived within the jurisdictional scheme of sections 3, 4 and 5 of REGULATION (EU) No 1215/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast). *Official Journal of the European Union* (2012/L 351/1) 20 December. Available from:http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R1215&from=EN:PDF [Accessed 7 June 2017], even if that happened in the form of equal alternative to the otherwise plaintiff favourable jurisdictional grounds established thereof.

[51] In that context see *Handte v Traitements* [1992], Case C-26/91, par. 14.

[52] Recitals 15 and 16 REGULATION (EU) No 1215/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast). *Official Journal of the European Union* (2012/L 351/1) 20 December. Available from:http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R1215&from=EN:PDF [Accessed 7 June 2017].

[53] Among others *Tessili v Dunlop* [1976], Case C-12/76, par. 13, *Dumez France v Hessische Landesbank* [1989], Case C-220/88, par. 17 and most notably *Besix v Kretzschmar* [2001], Case C-256/00, par. 31, where the Court stated: "*[…] The reason for the adoption of the jurisdictional rule … was concern for sound administration of justice and efficacious conduct of proceedings […]*".

[54] For that conclusion see Pointier, J.A. and Burg, E. (2004) *EU Principles of Jurisdiction and Recognition and Enforcement of Judgements in Civil and Commercial Matters according to the case law of the European Court of Justice*. The Hague: TMC Asser Press, p. 160.

of the bases of jurisdiction found in this article to the procedural elements of a certain case.[55] By inserting a non-existent element of protection of the plaintiff in art. 7 in *eDate and Martinez*, the CJEU went far further than the scope of this article without providing convincing reasons for doing so.

In addition, the fact that the adoption of the domicile of defendant as the basic rule of jurisdiction within the Brussels is directly connected with the idea of providing the procedural balance that was described above means that the plaintiff shall not, in principle, acquire any procedural advantages in the territory of adjudicatory jurisdiction. Favouring the plaintiff both in terms of adjudicatory jurisdiction, by uncontrollably creating *fora actoris*, and in terms of simplifying the recognition and enforcement of judgements would turn the Brussels Ia Regulation from an instrument that aims to facilitate the protection of human rights of all EU citizens to an instrument that protects only the rights of the plaintiffs.

There are many other points of the *eDate and Martinez* ruling that raise legitimate questions,[56] such as, for example, the additional problems that stem from the unreasonable multiplication of jurisdictional bases created by the CJEU. Not only forum shopping in disputes regarding online privacy violations is not only easier now, but one also cannot ignore the possibility of different Member State courts rendering contradictory decisions for the same subject matter, undermining legal certainty in the European judicial space.[57] Nonetheless, a detailed and exhaustive discussion of the vices and virtues of the *eDate and Martinez* ruling goes beyond the scope of the current contribution.

What is really important to take away from the brief examination of that case is that the CJEU was ready to go as far as to dismantle the basic jurisdictional principles of the Brussels Ia Regulation, and even risk the existence of legal certainty, in order to afford a strong protection

---

[55] That this is the underlying principle especially of art. 7 (2) see Kropholler, J. and Von Hein, J. (2011) *Europäisches Zivilprozessrecht-Kommentar zu EuGVO, Lugano-Übereinkommen 2007, EuVTVO, EuMVVO und EuGFVO*. Frankfurt am Main: Verlag Recht und Wirtschaft GmbH, p. 201.

[56] Dickinson, A. (2012) *By Royal Appointment: No Closer to an EU Private International Law Settlement?* [blog entry] 24 October. Conflict Of Laws.net. Available from: http://conflictof laws.net/2012/by-royal-appointment-no-closer-to-an-eu-private-international-law-settlement/ [Accessed 07 June 2017], has neatly summarized 7 points of critique for the ruling.

[57] Schmidt, J. (2015) *Rechtssicherheit im europäischen Zivilverfahrensrecht*. Tübingen: Mohr Siebeck, pp. 133-138 presents some interesting argumentation in that direction.

to the victims of online privacy violations. In view of the above, one might legitimately raise doubts on whether an additional jurisdictional rule for privacy violations, like the one established in art. 79(2) of the GDPR, was necessary.

2.3 AN UNEASY RELATIONSHIP

The question becomes even more reasonable if one examines the content of art. 79(2) of the GDPR,[58] which states:

> "*Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.*"

The very first point that makes the relationship of GDPR art. 79(2) with the Brussels Ia Regulation uneasy is the blurry scope of application of GDPR art. 79(2) of the GDPR does not include any indication on whether it repeals the jurisdictional provisions of the Brussels Ia Regulation or whether it just complements them. While an assumption on the basis of the axiom "*lex specialis derogat lege generali*" would militate in favour of the assumption that art. 79(2) replaces the jurisdictional rules of Brussels Ia for privacy violations, recital 147 of the GDPR puts such an assumption in question. In a rather sibyllic and cryptic manner, recital 147 of the GDPR states:

> "*Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council should not prejudice the application of such specific rules.*"

---

[58] REGULATION 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). *Official Journal of the European Union* (2016/L 119/1) 04 May. Available from: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf [Accessed 7 June 2017].

That seems to imply that art. 79(2) does not replace the jurisdictional grounds of the Brussels Ia Regulation, but rather that the two systems shall coexist, albeit not on an equal basis. While the jurisdictional rules of the Brussels Ia Regulation are still in force for online privacy violations, they will not be applied in all cases that they contradict the jurisdictional grounds of GDPR art. 79(2).[59] What can lead to a contradiction between art. 79(2) and Brussels Ia shall probably be examined on a case by case basis for each one of the individual jurisdictional grounds of the Brussels Ia Regulation. Apart from being a rather tedious task, discovering a contradiction between legal rules can also be proven very controversial. It is probably the CJEU that will be called upon to solve the problem in the future, but the doubts and uncertainty caused in the meantime might be detrimental to the administration of justice within the EU.

If, for example, the most obvious candidate for a parallel application with GDPR art. 79(2), namely art. 7(2) of the Brussels Ia Regulation, is to be considered, a very unpleasant scenario will automatically occur. If one looks at the interpretation of art. 7(2) of the Brussels Ia Regulation in the *eDate and Martinez* ruling, a contradiction between the two does not seem likely.[60] Applied together, these two provisions [GDPR art. 79(2) and Brussels Ia art. 7(2)] would create a multitude of different fora in favour of the data subject. In such a scenario, the data subject will be able to sue in regard to the full extent of the damage suffered, at his/her discretion, in one of the following places: before the courts of the Member State of the domicile of the controller or processor (under art. 4 of the Brussels Ia Regulation), before the courts of the Member State of the centre of the data subject's interests (under art. 7(2) as the latter was interpreted by the CJEU in *eDate and Martinez*), before the courts of the Member State of the establishment of the controller or processor (under art. 79(2) of the GDPR) or, finally, before the courts of the Member State of the data

[59] The German version of recital 147 makes use of the term "*nicht entgegenstehen*", which implies that the non-application of the Brussels Ia jurisdictional rules shall be the outcome of their contradiction with the jurisdictional rules of art. 79(2) GDPR. If the jurisdictional grounds of Brussels Ia are not contradictory to those of art. 79(2) GDPR, then they shall apply in parallel. See Werkmeister, C. (2017). In: Peter Gola (ed.) *Datenschutz-Grundverordnung VO (EU) 2016/679-Kommentar*. Munich: C.H. Beck, p. 730, who notes: *"[…] Erwägungsgrund 147 gibt vor, dass die allgemeinen Vorschriften über die Gerichtsbarkeit, wie sie etwa in der EuGVVO enthalten sind, der Anwendung der spezifischen Vorschriften nach der DS-GVO nicht entgegenstehen sollen. Sofern die besonderen Gerichtsstände nach der EuGVVO neben den Gerichtsständen nach Art. 79 Abs. 2 anwendbar bleiben, stehen diese den Vorgaben der DS-GVO jedenfalls nicht entgegen […]"*.

[60] Ibid.

subject's habitual residence (under art. 79(2) of the GDPR). In addition, the data subject will still be able to sue in each individual Member State were his/her data became illegally available, but only for the extent of the damage suffered in each state.

That such an unreasonably overextended jurisdictional privilege of the data subject will cause a long series of problems does not need much analysis. It is just an example of how unthoughtful the legislator has been in dealing with jurisdictional problems within the GDPR, while ignoring at the same time the decades old Brussels regime.

In order to avoid such or similar absurd jurisdictional outcomes as the one described above, it is submitted that a parallel application of GDPR art. 79(2) and Brussels Ia art. 7(2) shall be denied. The contradiction of Brussels Ia art. 7(2) with GDPR art. 79(2) might not be derived directly from their jurisdictional grounds but from their different underlying principles: if it still holds true that the purpose of art. 7(2) of the Brussels Ia Regulation is not to favour the plaintiff, but to foster the better administration of justice,[61] while on the contrary, art. 79(2) of the GDPR aims to empower the position of the data subject in terms of judicial jurisdiction,[62] one could admit that there is a certain degree of incompatibility between the two, given that their underlying principles are mutually exclusive and cannot be pursued at the same time. Indeed, if one aims to procedurally favour one of the parties, such an aim cannot be compromised with the aim to form neutral and generally fair procedural conditions and justice guarantees. In other words, doing too much justice for one of the parties automatically means that one cannot do justice for both. Art. 79(2) of the GDPR must necessarily prevail, as art. 7(2) would otherwise prejudice its application.

This incompatibility test based not on the jurisdictional grounds per se but on the underlying principles of the competing jurisdictional rules might offer general guidance in clarifying the scope of application of GDPR art. 79(2) and the jurisdictional grounds of Brussels Ia Regulation.

For example, another interesting scenario might be that the parties agree

[61] Supra notes 52, 53 and 54..

[62] That conclusion might be justified from a systematic interpretation of art. 79(2) of the GDPR. Art. 79 is located in chapter VIII of the GDPR, a chapter that aims to strengthen the legal protection of the data subjects in the EU and, therefore, it is not neutral in its assessment of the procedural interests of the parties. Simply put like all the other remedies of chapter VIII of the GDPR, art. 79 wants to empower the data subject in terms of enforcement of his/her rights derived from the GDPR.

to submit a data privacy dispute before a commonly designated court. Can Brussels Ia art. 25 and GDPR art. 79(2) be compatible? Are, in other words, jurisdictional clauses for data privacy disputes allowed? The underlying principle of art. 25 is to protect the contractual autonomy of the parties,[63] while GDPR art. 79(2) aims to empower the procedural position of the data subject. Empowered procedural position and contractual autonomy are not always incompatible, if one takes the example of how Brussels Ia has treated the jurisdictional clauses in consumer cases.[64] Despite the strong procedural protection awarded to consumers, jurisdictional agreements are, nonetheless, possible, albeit with certain formal and material limitations. Contractual autonomy is in this way not sacrificed in favour of procedural protection; it is just being put in a certain frame.[65] By the same token, one could argue that contractual autonomy shall not be deemed incompatible with strong data privacy protection, if jurisdictional agreements related to data privacy violations respect the limits set by the combined application of Brussels Ia art. 25 and GDPR art. 79(2). Art. 25 of Brussels Ia will provide the formal limits of such jurisdictional agreements (for example art. 25 will provide that jurisdictional agreements shall in general be in written form), while the limits that stem from GDPR art. 79(2) will refer to the content of such agreements. Jurisdictional agreements in data privacy cases shall namely not deprive the data subject of the jurisdictional grounds prescribed in GDPR art. 79(2).[66] In other words, jurisdictional agreements that favour the data subject by expanding the available (under GDPR art. 79(2) grounds of jurisdiction will still be permissible.

The same line of argumentation might also prove helpful in solving the problem of tacit prorogation of jurisdiction. The CJEU has made clear in its *Česká podnikatelská v. Michal Bilas* ruling[67] that a party might abolish his/her jurisdictional privileges through a tacit prorogation of jurisdiction.[68] That might be a dangerous precedent for data subjects, who unbeknownst

---

[63] See *Anterist v. Crédit Lyonnais* [1986], case C-22/85, par. 14.

[64] See art. 19 REGULATION (EU) No 1215/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast). *Official Journal of the European Union* (2012/L 351/1) 20 December. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R1215&from=EN:PDF [Accessed 7 June 2017].

[65] For the notion of framed autonomy in EU Civil Law see Reich, N. (2014) General Principles of EU Civil Law. Cambridge; Antwerp; Portland: intersentia, pp. 18-36.

[66] See Feiler, L. and Forgó, N. (2017) EU-Datenschutz-Grundverordnung-Kurzkommentar. Vienna: Verlag Österreich, p. 336.

[67] *Česká podnikatelská pojišťovna as, Vienna Insurance Group v. Michal Bilas* [2010], Case C-111/09.

to them might lose the protection of GDPR art. 79(2). In that case, party autonomy cannot be combined with the aim to procedurally favour the data subjects and, therefore, art. 26 of the Brussels Ia Regulation must be deemed incompatible with GDPR art. 79(2) and thus non-applicable on data privacy violations.

Further problems from the scope of application of GDPR art. 79(2) might arise not only from its compatibility (or lack of such) with the Brussels Ia jurisdictional regime but also from the general problems attached to the applicability of the GDPR overall. The GDPR delegates a non-negligible amount of issues to the national laws of the Member States.[69] That leads to the question whether GDPR art. 79(2) shall cover also such data privacy disputes that stem from national regulations or whether it shall be deemed non-applicable in such cases. If one gives gravity to the wording of art. 79(1) of the GDPR, art. 79 in toto seems to represent the civil procedural incarnation of the rights afforded to the data subjects through the GDPR,[70] but not to those afforded to them through Member State legislation. If that is true, then the jurisdictional grounds of GDPR art. 79(2) shall only come into play for violation of privacy rights that stem from the GDPR, but not for those privacy rights that stem from Member State legislation. Practically, that will create two tiers of jurisdictional grounds for data privacy violations in the EU: for data privacy rights that stem from the GDPR, data subjects will benefit from both the jurisdictional grounds of GDPR art. 79(2) and those of Brussels Ia, to the extent that they can be applied in parallel, while for data privacy rights that stem from national codifications the only set of jurisdictional rules available is that of the Brussels Ia. If the GDPR wanted to unify the level of protection across the EU Member States, GDPR art. 79(2) does not seem to be heading in that direction, as it creates two diverse types of data subjects: namely those that will benefit from the combined jurisdictional grounds of GDPR

[68] Safe for the jurisdictional grounds that are established in Brussels Ia Regulation art. 24. See *Česká podnikatelská pojišťovna as, Vienna Insurance Group v. Michal Bilas* [2010], Case C-111/09, par. 24-26.

[69] See in more detail Kühling, J. and Martini, M. (2016) Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht? *Europäische Zeitschrift für Wirtschaftsrecht*, 27(12) pp. 448-454.

[70] Art. 79(1) states: Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation (emphasis added).

art. 79(2) and Brussels Ia Regulation and those that can only resort to the Brussels Ia regulation. For legal practitioners across the EU, the constant question of which set of jurisdictional grounds shall be applicable will also not be a pleasant task.

The second point, beyond the scope of application, that makes the relationship of GDPR art. 79(2) and the Brussels Ia Regulation uneasy refers to the jurisdictional grounds established in the former. Art. 79(2) of the GDPR expands the dismantling of the basic jurisdictional principles of the Brussels Ia Regulation initiated by the CJEU with its decision in *eDate and Martinez*. Apart from being disproportionately favourable for the data subject/plaintiff,[71] the jurisdictional grounds provided for by art. 79(2) of the GDPR extend well beyond their Brussels Ia counterparts.

Instead of allowing the data subject to sue at the domicile of the defendant along the lines of Brussels Ia Regulation art. 4, GDPR art. 79(2) opens the doors of litigation before the courts of the Member State where the data controller or processor retains an establishment. If the rulings of the CJEU in *Google Spain*[72] and *Weltimmo*[73] have clarified something, that is the readiness of the Court not only to flexibly adapt its legal reasoning to Internet situations[74] but, most prominently, also its willingness to marginalise the nexus of the contacts of the establishment with a Member State for the purpose of extending the scope of data protection law.[75] In *Google Spain*, the Court went as far as to declare that

[71] It must be reminded here that while the GDPR is not neutral towards the interests of the parties when providing the data subjects the procedural remedies of art. 79, the Brussels Ia Regulation aims to establish a very delicate balance that shall keep the plaintiff and the defendant in an equal procedural footing when they are trying to judicially protect their fundamental rights. In terms of the Brussels Ia Regulation see Hess, B. (2015) Unionsrechtliche Synthese: Mindesstandards und Verfahrensgrundsätze im acquis communitaire/Schlussfolgerungen für European Principles of Civil Procedure. In: Matthias Weller and Christoph Althammer (eds.) *Mindesstandards im europäischen Zivilprozessrecht*. Tübingen: Mohr Siebeck, pp. 221-235, esp. 223 where he states: "*[…] ine eigenständige Prinzipienebene enthält das europäische Zivilverfahrensrecht jedoch bereits heute: Sie besteht zunächst auf der Ebene des Primärrechts in den Vorgaben der Marktfreiheiten und der Grundrechte … Bei der Interpretation der EU-Sekundärrechtsakte zum internationalen Zivilprozessrecht hat der Gerichtshof eigenständige Grundsätze und Regelungskonzepte entwickelt: effektiver Zugang zur Justiz, Beklagtenschutz im Zuständigkeitsrecht, Urteilsfreizügigkeit, wechselseitiges Vertrauen in die Justizsysteme anderer EU-Mitgliedstaaten […]*".

[72] *Google Spain SL v. Agencia Española de Protección de Datos* (AEPD) [2014], Case C-131/12.

[73] *Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság* [2015], Case C-230/14.

[74] For a positive assessment of that part of the Google Spain decision in that regard see the comment of Karg (2014) EuGH: Löschungsanspruch gegen Google-"Recht auf Vergessen". *Zeitschift für Datenschutz*, 4(7) pp. 350-361, esp. pp. 359-361.

[75] For a critical assessment see Kartheuser, I and Schmitt, F. (2016) Der Niederlassungsbegriff und seine praktischen Auswirkungen. Anwendbarkeit des Datenschutzrechtes eines Mitgliedstaats auf ausländische EU-Gesellschaften. *Zeitschrift für Datenschutz*, 6(4) pp. 155-159.

the establishment must not actively take part in data processing activities in order for EU data protection law to be applicable;[76] in *Weltimmo*, it substantially lowered the level of what constitutes "*effective and stable arrangements*" within a Member State and accepted that a mere website that addresses its activities to a Member State different than that of the domicile of the controller or processor can suffice for the existence of an establishment in the meaning of art. 4(1)(a) of the Data Protection Directive, even if the nexus of contacts between the website and the Member State are rather low.[77] There seems to be no doubt that the notion of establishment in GDPR art. 79(2) is taken from the same term used in GDPR art. 3, which itself is the direct descendant of art. 4(1)(a) of the Data Protection Directive that gave rise to the aforementioned case law and, subsequently, that it must be interpreted along the same lines.[78]

Translated in jurisdictional terms, the combined effect of the *Google Spain* and *Weltimmo* notion of establishment will create a questionable and probably dysfunctional jurisdictional environment: not only will forum shopping be maximised[79] but also the very broad interpretation of the notion of establishment by the Court will create an extremely remote or even trivial connection between the courts of the Member State that will be deemed as having adjudicatory power and the dispute over which they shall adjudicate, raising doubts about the quality of the final outcome of the decision. Decisions related to data privacy violations and issued by Member State courts designated through such weak jurisdictional grounds as the establishment of the data controller prescribed in GDPR art. 79(2) will still be qualified to circulate within the EU based on the privileged recognition and enforcement regime of the Brussels Ia Regulation. It must be reminded here that the privileged recognition and enforcement regime of the Brussels Ia Regulation is founded

---

[76] *Google Spain SL v. Agencia Española de Protección de Datos* (AEPD) [2014], Case C-131/12, par. 52-55.

[77] *Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság* [2015], Case C-230/14, par. 29-33.

[78] Recital 22 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). *Official Journal of the European Union* (2016/L 119/1) 04 May. Available from: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf [Accessed 7 June 2017]., Martini, M. (2017) In: Boris Paal and Daniel Pauly (eds.) *Datenschutz-Grundverordnung*. Munich, Germany: C.H. Beck, p. 720.

[79] Feiler, L. and Forgó, N. (2017) EU-Datenschutz-Grundverordnung-Kurzkommentar. Vienna: Verlag Österreich, p. 335.

on the respect of certain procedural guarantees in favour of the defendant, one of the most important being the procedural balance that the Brussels regime tries to secure by its, more or less, fair and reasonable jurisdiction rules. Given that the generous to the data subject/plaintiff jurisdictional grounds of GDPR art. 79(2) neutralise such jurisdictional guarantees as those achieved by the Brussels Ia jurisdictional regime, the circulation of judgements related to online data privacy violations will severely distort the trust of EU citizens in the administration of justice within the common judicial area, even if none of the refusal grounds of Brussels Ia Regulation art. 45 can be invoked. In addition, one cannot overlook the concerns raised by the unreasonable multiplication of jurisdictional grounds created by the possibility of a data controller or processor being established in more than one Member States, which will further undermine the notion of legal certainty within the judicial system of the EU.

The alternative jurisdictional ground of the habitual residence of the data subject provided for by GDPR art. 79(2) does little, if anything, to bring the jurisdictional grounds of that provision closer to the Brussels regime. By allowing the data subject to sue in the courts of his/her habitual residence GDPR art. 79(2) creates another plaintiff jurisdiction to the detriment of the "*actor sequitur forum rei*" principle that lies in the centre of the Brussels Ia jurisdictional scheme. Although such jurisdictional rules favourable to the plaintiff are not unknown to the system of the Brussels Ia Regulation,[80] one must always take into account the exceptional character of such plaintiff jurisdiction rules as well as the compelling reasons that justified their adoption. The jurisdictional privileges awarded to the insurance policy holder, employee and consumer are justified by their weak socio-economical position in relation to their contractual counterparts.[81] By improving their jurisdictional position, the Brussels Ia Regulation is trying to counterbalance the negotiating deficiency that is inherent for these particular stakeholders. While that might be true for several privacy cases as well, the wide definition

[80] See art. 11, art. 18 and art. 21 REGULATION (EU) No 1215/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast). *Official Journal of the European Union* (2012/L 351/1) 20 December. Available from:http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R1215&from=EN:PDF [Accessed 7 June 2017].

[81] See most characteristically *Société Bertrand v. Ott* [1978], Case C-150/77, par. 13 and among others Hill, J. (2008) *Cross-border Consumer Contracts*. Oxford; New York: Oxford University Press, pp. 75-76.

of the subject matter of data protection law can render almost everyone a data controller. That means that in a rather considerable number of privacy cases the parties will litigate from a socio-economical equal basis. It seems, thus, that the creation of a plaintiff jurisdiction for data subjects cannot be so easily justified.[82]

It shall also be mentioned that the insertion of a plaintiff jurisdiction based not on the data subject's domicile but on that of his/her habitual residence might also be proven controversial. Although an autonomous interpretation of the concept of habitual residence is not completely foreign to EU civil procedural law[83] and the CJEU might probably provide one in the context of GDPR art. 79(2) in the future, its flexible and wide nature will once again lower the nexus of contacts between a privacy case and the Member State where such a case shall be adjudicated. Simply put, establishing a habitual residence is easier than establishing a domicile and, subsequently, data subjects will once more benefit from a relaxed jurisdictional rule, without being sure that such a procedural advantage is completely justified.

3. INSTEAD OF AN EPILOGUE: A FEW LINES ON THE IMPACT OF GDPR ART. 79(2) IN NON-EU PARTIES

The previous analysis focused on the impact of the jurisdictional rules of GDPR art. 79(2) within the EU. It seems fair to conclude this contribution with a few lines on the possible impact of GDPR art. 79(2) outside of the EU.

The adoption of the GDPR signals, among many other things, an official declaration from the EU that its privacy regulatory model is aggressively claiming a wide extraterritorial application.[84]

Art. 3 offers an extended territorial scope to the GDPR,[85] especially in Internet related activities, and that extended territorial scope is also

[82] For a different assessment see Brkan, M. (2015) Data protection and European private international law: observing a bull in a China shop. *International Data Privacy Law*, 5(4) pp. 257-278.

[83] See for example the ruling of the CJEU in *A* [2009], Case C-523/07, par. 8. Martini, M. (2017) In: Boris Paal and Daniel Pauly (eds.) *Datenschutz-Grundverordnung*. Munich, Germany: C.H. Beck, pp. 720-721, after noting that the use of the term habitual residence in art. 79(2) GDPR has been rather careless ("*ohne Bedacht*"), goes on to suggest that its interpretation shall be conducted autonomously by the CJEU and in line with the interpretation of the same term found in Council Regulation (EC) No 2201/2003 of 27 November 2003 concerning jurisdiction and the recognition and enforcement of judgments in matrimonial matters and the matters of parental responsibility, repealing Regulation (EC) No 1347/2000. Official Journal of the European Union (2003/L 338/1) 23 December. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003R2201&from=EN: PDF [Accessed 7 June 2017].

afforded to the jurisdictional grounds of GDPR art. 79(2). Quite remarkably, while the Member States vehemently opposed the application of the Brussels Ia Regulation in non-EU cases,[86] they displayed a rare unanimity and raised no objections when the GDPR declared its own jurisdictional regime applicable to almost the entire Internet.[87]

One must not be surprised if legal orders that do not share the same privacy concerns as those dominant in the EU[88] react, not always positively, to such wide jurisdictional claims. The US might pose a good example in that regard. It is after all a commonality that the US has a distinct and, in many ways, different approach to data privacy in comparison to the EU.[89] In addition, the US retains a firm stance in defending their unique approach to judicial jurisdiction over Internet cases[90] that is not necessarily compatible with the Brussels regime[91] and even more so with the rules provided for in GDPR art. 79(2).

In the (concomitant with data privacy) field of defamation law the US has been rather proactive in defending their notion of freedom of speech over the preference that the European courts have shown for the right to personality. Their reaction was triggered by the unfortunate jurisdictional outcome in the *Bin Mahfouz v. Ehrenfeld* case.[92] In sum, Dr. Rachel Ehrenfeld,

---

[84] Kuner, C. (2014) The European Union and the Search for an International Data Protection Framework. *Groningen Journal of International Law*, 2(1) pp. 55-71, looks critical at the tendency of the EU to impose its privacy model on other jurisdictions instead of creatively contributing to the creation of better global privacy standards.

[85] See among others Klar, M. (2017) In: Jürgen Kühling and Benedikt Büchner (eds.) *Datenschutz-Grundverordnung-Kommentar*. Munich: C.H. Beck, pp. 99-123.

[86] See European Parliament, Session document, A7-0219/2010, pp. 3-15.

[87] Despite its crucial importance extraterritoriality has not raised any serious discussions during the preparation of the GDPR. For a similar assessment see Svantesson, D.J.B. (2013) *Extraterritoriality in Data Privacy Law*. Copenhagen: Ex Tuto Publishing, p. 106.

[88] Kuner, C. (2009) An international legal framework for data protection: Issues and prospects. *Computer Law & Security Review*, 25 pp. 307-317, offers a very good insight into the complexity created by a common international data privacy model and explores what are the mechanisms that can lead to a convergence of the different regional approaches.

[89] For a comparative approach to the US privacy model see Moshell, R. (2005) … And then there was one: The outlook for a self-regulatory United States amidst a global trend toward comprehensive data protection. *Texas Law Review*, 37 pp. 357-432, Whitman, J.Q. (2004) The Two Western Cultures of Privacy: Dignity versus Liberty. The *Yale Law Journal*, 113 pp. 1151-1221.

[90] For a well-founded doctrinal reaction to the overarching impact of the EU jurisdictional system see Bradford, A. (2012) The Brussels Effect. *Northwestern University Law Review*, 107(1) pp. 1-67.

[91] For a comparative view on the US and EU approaches to judicial jurisdiction over Internet related cases see Chen, C. (2004) United States and European Union Approaches to Internet Jurisdiction and their Impact on E-Commerce. *University of Pennsylvania Journal of International Economic Law*, 25(1) pp. 423-454.

[92] *Mahfouz & Ors v Ehrenfeld & Anor* [2005] EWHC 1156 (Q.B.).

an American writer, published a book on international terrorism in which she reported that Khalid bin Mahfouz, a Saudi billionaire, assisted al Qaeda to deliver the 9/11 attacks. Only 23 books of Dr. Ehrenfeld's have been distributed in England. Based on the distribution of these 23 books, Khalid bin Mahfouz brought a defamation action before the English courts. Even though bin Mahfouz was not an English citizen and despite the extremely small number of books distributed in that jurisdiction, the English courts decided that they had international jurisdiction to adjudicate. In a default judgement, since Dr. Ehrenfeld did not appear before the English courts, they awarded damages to bin Mahfouz and enjoined Dr. Ehrenfeld from further publishing the allegedly defamatory statements in England. Despite her efforts before the state Courts of New York, Dr. Ehrenfeld has been unable to invalidate the English decision.

The undeniably chilling effects of such libel tourism tactics[93] to the freedom of speech alerted the US legislator, and not long after the outcome of the *Ehrenfeld* case was finalised the US adopted the Speech Act[94]. Simply put, the Speech Act blocks the recognition and enforcement of foreign judgements, the content of which does not respect freedom of speech in a manner similar to that of the American Constitution.[95]

If the example of the Speech Act[96] is to remind us of something, it is the value of reasonable jurisdictional claims. While it has been substantially supported that enforceability in an international context shall not be strictly tied to jurisdictional claims,[97] the existential relationship between

---

[93] Hartley, T. (2010) "Libel Tourism" and Conflict of Laws. *International and Comparative Law Quarterly*, 59 pp. 25-38, explains neatly why private international law rules, including jurisdiction, shall secure a balance between freedom of speech and personality rights.

[94] Securing the Protection of our Enduring and Established Constitutional Heritage Act 2010. United States of America. Washington D.C.: 111th United States Congress. In English. Before the adoption of the Speech Act in Federal Level several US States have enacted similar legislation at a state level. See for example Libel Terrorism Protection Act enacted in the State of New York, 2008 N.Y. Laws ch. 66, § 3 [codified at N.Y. C.P.L.R. 302, 5304 (McKinney 2008)]. For an analysis of that act and the impact of libel tourism in the US see Feldman, M. (2010) Putting breaks on libel tourism: Examining the effects test as a basis for personal jurisdiction under New York's Libel Terrorism Protection Act. *Cardozo Law Review*, 31(6) pp. 2458-2489.

[95] For a brief analysis of the provisions of the Act see Congressional Research Service (2010), *The Speech Act: The Federal Response to "Libel Tourism"*. 16 September. Available from: https://fas.org/sgp/crs/misc/R41417.pdf [Accessed 7 June 2017] and in more detail Rosen, M. (2012) The Speech Act's Unfortunate Parochialism: Of Libel Tourism and Legitimate Pluralism. *Virginia Journal of International Law*, 53(1) pp. 99-126.

[96] The acronym of the act offers a good indication of its content. The full title is: Securing the Protection of our Enduring and Established Constitutional Heritage Act.

[97] Svantesson, D.J.B. (2015) A Jurisprudential Justification for Extraterritoriality in (Private) International Law. *Santa Clara Journal of International Law*, 13(2) pp. 517-571.

adjudicatory jurisdiction and international enforcement shall not be ignored.[98] The Speech Act is a good example of the negative impact of unreasonable jurisdiction claims, even if one remains adamant in questioning the value of international enforceability, since it has forced a jurisdiction traditionally friendly to foreign judgments such as that of the US[99] to become completely hostile and refuse to recognise and enforce a certain category of foreign judgments.

It seems that the European legislator has wilfully ignored the message delivered by the adoption of the Speech Act when preparing art. 79(2) of the GDPR. It remains to be seen if that was a wise decision.[100]

LIST OF REFERENCES

[1] Baumgartner, S. (2017) The External Dimensions of the European Law of Civil Procedure-A Transatlantic Perspective. In: Burkhard Hess (ed.) *Der Europäische Gerichtsverbund-Die internationale Dimension des europäischen Zivilverfahrensrechts*. Bielefeld: Verlag Ernst und Werner Gieseking GmbH, pp. 165-199.

[2] Bogdan, M. (2013) Website Accessibility as Basis for Jurisdiction Under the Brussels I Regulation in View of New Case Law of the ECJ. In: Dan Jerker B. Svantesson and Stan Greenstein (eds.) *Internationalisation of Law in the Digital Information Society*. Copenhagen: Ex Tuto Publishing, pp. 159-172.

[3] Bradford, A. (2012) The Brussels Effect. *Northwestern University Law Review*, 107(1), pp. 1-67.

---

[98] See Section 4102(b)(1) of the Speech Act which states: "*In general.--Notwithstanding any other provision of Federal or State law, a domestic court shall not recognize or enforce a foreign judgment for defamation unless the domestic court determines that the exercise of personal jurisdiction by the foreign court comported with the due process requirements that are imposed on domestic courts by the Constitution of the United States*".

[99] That the American courts show a deep respect in the principle of international comity and are usually open to recognize and enforce foreign judgements, as well as that the Speech act has changed that attitude see Baumgartner, S. (2017) The External Dimensions of the European Law of Civil Procedure-A Transatlantic Perspective. In: Burkhard Hess (ed.) *Der Europäische Gerichtsverbund-Die internationale Dimension des europäischen Zivilverfahrensrechts*. Bielefeld: Verlag Ernst und Werner Gieseking GmbH, pp. 165-199. He makes, therefore, the argument that this change of attitude after the Speech Act shall function as an incentive for an enhanced cooperation in the field of recognition and enforcement of judgments, via the Hague Judgements Project.

[100] Current indications do not support an optimistic assessment here. The press has already reported that after the adoption of the Speech Act, which currently only affects defamation but not data privacy cases, European lawyers are disguising defamation cases as privacy litigation in order to circumvent the application of the Speech ACT. See Roberts, J. (2016) Privacy Laws Pose New Threat to Free Speech [blog entry] 19 January. Fortune-Tech. Available from: http://fortune.com/2016/01/19/libel-privacy-tourism/ [Accessed 7 June 2017]. By making privacy litigation easier GDPR art. 79(2) might maximize the scale of "*Privacy Tourism*" and, therefore, force the US to react accordingly.

[4] [4] Brkan, M. (2015) Data protection and European private international law: observing a bull in a China shop. *International Data Privacy Law*, 5(4) pp. 257-278.

[5] Bygrave, L. (2000) Determining Applicable Law pursuant to European Data Protection Legislation. *Computer Law & Security Report*, 16, pp. 252-257.

[6] Chen, C. (2004) United States and European Union Approaches to Internet Jurisdiction and their Impact on E-Commerce. *University of Pennsylvania Journal of International Economic Law*, 25(1), pp. 423-454.

[7] Coester-Waltjen, D. (1999) Internationale Zuständigkeit bei Persönlichkeitsrechts-verletzungen. In: Festschrift für Rolf A. Schütze, Munich: C.H. Beck, pp. 175-187.

[8] Congressional Research Service (2010), The *Speech Act: The Federal Response to "Libel Tourism"*. 16 September. Available from: https://fas.org/sgp/crs/misc/R41417.pdf [Accessed 7 June 2017].

[9] Dickinson, A. (2012) *Royal Appointment: No Closer to an EU Private International Law Settlement?* [blog entry] 24 October. Conflict Of Laws.net. Available from: http:// www.conflictoflaws.net/2012/by-royal-appointment-no-closer-to-an-eu-private-international-law-settlement/ [Accessed 7 June 2017].

[10] Dougan, M. (2008) The Treaty of Lisbon 2007: Winning Minds not Hearts. *Common Market Law Review*, 45(3), pp. 617-703.

[11] EU Council. The Hague Programme: Strengthening Freedom, Security and Justice in the EU. *Official Journal of the European Union*, (2005/C 53/1) 03 March. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005XG0303 (01)&from=EN:PDF [Accessed 7 June 2017].

[12] EU Council. The Stockholm Programme — An open and secure Europe serving and protecting citizens. *Official Journal of the European Union* (2010/C 115/1) 05 May. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2010: 115:FULL&from=en:PDF [Accessed 7 June 2017].

[13] Feiler, L. and Forgó, N. (2017) EU-Datenschutz-Grundverordnung-Kurzkommentar. Vienna: Verlag Österreich.

[14] Feldman, M. (2010) Putting breaks on libel tourism: Examining the effects test as a basis for personal jurisdiction under New York's Libel Terrorism Protection Act. *Cardozo Law Review*, 31(6), pp. 2458-2489.

[15] Geimer, R. Unionsweite Titelvollstreckung ohne Exequatur nach der Reform der Brüssel I-Verordnung. In: Festschrift für Rolf A. Schütze, Munich: C.H. Beck, pp. 109-121.

[16] Goebel, R.J. (2011) The European Union and the Treaty of Lisbon. *Fordham International Law Journal*, 34(5), pp. 1251-1268.

[17] Hallstein, W. (1964) Angleichung des Privat- und Prozessrechts in der Europäischen Wirtschaftsgemeinschaft. *Rabels Zeitschrift für ausländisches und internationales Privatrecht*, 28(2), pp. 211-231.

[18] Harpaz, G. and Herman, L. (2008) The Lisbon Reform Treaty: Internal and External Implications. *European Journal of Law Reform*, 10(4), pp. 431-436.

[19] Hartley, T. (2010) „Libel Tourism" and Conflict of Laws. *International and Comparative Law Quarterly*, 59, pp. 25-38.

[20] Heinze, C. (2011) Surf global, sue local! Der europäische Klägergerichtsstand bei Persönlichkeitsrechtsverletzungen im Internet. *Europäische Zeitschrift für Wirtschaftsrecht*, 22(24), pp. 947-950.

[21] Hess, B. (2010) *Europäisches Zivilprozessrecht*. Heidelberg: C.F. Müller Verlag.

[22] Hess, B. (2012) Der Schutz der Privatsphäre im Europäischen Zivilverfahrensrecht. *Juristen Zeitung*, 67(4), pp. 189-193.

[23] Hess, B. (2015) The Protection of Privacy in the Case Law of the CJEU. In: Burkhard Hess and Christina Mariottini (eds.) *Protecting Privacy in Private International and Procedural Law and by Data Protection*. Baden-Baden: Nomos Verlag, pp. 112-113.

[24] Hess, B. (2015) Unionsrechtliche Synthese: Mindesstandards und Verfahrensgrundsätze im acquis communitaire/Schlussfolgerungen für European Principles of Civil Procedure. In: Matthias Weller and Christoph Althammer (eds.) *Mindesstandards im europäischen Zivilprozessrecht*. Tübingen: Mohr Siebeck, pp. 221-235.

[25] Hill, J. (2008) *Cross-border Consumer Contracts*. Oxford; New York: Oxford University Press.

[26] Huber, P. (1996) Persönlichkeitsschutz gegenüber Massenmedien im Rahmen des Europäischen Zivilprozeßrechts. *Zeitschrift für Europäisches Privatrecht*, 4(2), pp. 295-313.

[27] Isidro, M.R. On the Abolition of Exequatur. In: Burkhard Hess and Maria Bergström and Eva Stroskrubb (eds.) *EU Civil Justice: Current Issues and Future Outlook*, Oxford: Hart Publishing, pp. 283-298.

[28] Jenard, P. Report on the Convention on jurisdiction and the enforcement of judgments in civil and commercial matters. *Official Journal of the European Union* (1979/C 59/1) 05 March. Available from: http://aei.pitt.edu/1465/1/commercial_report_jenard_C59_79.pdf [Accessed 7 June 2017].

[29] Karg (2014) EuGH: Löschungsanspruch gegen Google-"Recht auf Vergessen". *Zeitschift für Datenschutz*, 4(7), pp. 350-361.

[30] Kartheuser, I and Schmitt, F. (2016) Der Niederlassungsbegriff und seine praktischen Auswirkungen. Anwendbarkeit des Datenschutzrechtes eines Mitgliedstaats auf ausländische EU-Gesellschaften. *Zeitschrift für Datenschutz*, 6(4), pp. 155-159.

[31] Kartheuser, I. and Klar, M. (2014) Wirksamkeitskontrolle von Einwilligungen auf Webseiten Anwendbares Recht und inhaltliche Anforderung im Rahmen gerichtlicher Überprüfungen. *Zeitschrift für Datenschutz*, 4(10), pp. 500-505.

[32] Klar, M. (2017) In: Jürgen Kühling and Benedikt Büchner (eds.) *Datenschutz-Grundverordnung-Kommentar*. Munich: C.H. Beck, pp. 99-123.

[33] Kramer, X.E. (2013) Cross-Border Enforcement and the Brussels I-bis Regulation: Towards a New Balance between Mutual Trust and National Control over Fundamental Rights. *Netherlands International Law Review*, 60, pp. 343-373.

[34] Kropholler, J. and Von Hein, J. (2011) *Europäisches Zivilprozessrecht-Kommentar zu EuGVO, Lugano-Übereinkommen 2007, EuVTVO, EuMVVO und EuGFVO*. Frankfurt am Main: Verlag Recht und Wirtschaft GmBH.

[35] Kubis, S. (1999) *Internationale Zuständigkeit Persönlichkeits- und Immaterial-güterrechtsverletzungen*. Bielefeld: Verlag Ernst und Werner Giesing.

[36] Kühling, J. and Martini, M. (2016) Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht? *Europäische Zeitschrift für Wirtschaftsrecht*, 27(12), pp. 448-454.

[37] Kuner, C. (2009) An international legal framework for data protection: Issues and prospects. *Computer Law & Security Review*, 25, pp. 307-317.

[38] Kuner, C. (2014) The European Union and the Search for an International Data Protection Framework. *Groningen Journal of International Law*, 2(1), pp. 55-71.

[39] Lanaerts, K. (2012) Die EU – Grundrechtecharta: Anwendbarkeit und Auslegung. *Europarecht*, 47, pp. 3-18.

[40] Landau, E.C. (2008) A New Regime of Human Rights in the EU? *European Journal of Law Reform*, 10(4), pp. 557-575.

[41] Mankowfski P. (2016) In: Ulrich Magnus and Peter Mankowfski (eds.) *Brussels Ibis Regulation-Commentary*. Köln: Verlag Dr. Otto Schmidt KG, pp. 323-328.

[42] Martini, M. (2017) In: Boris Paal and Daniel Pauly (eds.) *Datenschutz-Grundverordnung*. Munich, Germany: C.H. Beck, p. 720.

[43] Marton, E. (2016) *Violations of Personality Rights through the Internet: Jurisdictional Issues under European Law*. Baden-Baden: Nomos Verlag; Chawley Park, Cumnor Hill, Oxford: Hart Publishing.

[44] Moerel, L. (2011) Back to basics: when does EU data protection law apply? *International Data Privacy Law*, 1(2), pp. 92-110.

[45] Moerel, L. (2011) The long Arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide? *International Data Privacy Law*, 1(1), p. 28.

[46] Moshell, R. (2005) … And then there was one: The outlook for a self-regulatory United States amidst a global trend toward comprehensive data protection. *Texas Law Review*, 37, pp. 357-432.

[47] Pache, E. (2002) Eine Verfassung für Europa – Krönung oder Kollaps der europäischen Integration? *Europarecht*, 37, pp. 767-784.

[48] Pache, E. and Rösch, F. (2009) Die neue Grundrechtsordnung der EU nach dem Vertrag von Lissabon. *Europarecht*, 44 , pp. 769-790.

[49] Pech, L. (2011) The Institutional Development of the EU Post – Lisbon: A case of plus ca change…?, UCD Dublin European Institute Working Paper 11 – 5, December 2011.

[50] Piltz, C. (2012) Rechtswahlfreiheit im Datenschutzrecht? *Kommunikation & Recht*, 15(10), pp. 640-644.

[51] Pointier, J.A. and Burg, E. (2004) *EU Principles of Jurisdiction and Recognition and Enforcement of Judgements in Civil and Commercial Matters according to the case law of the European Court of Justice*. The Hague: TMC Asser Press.

[52] Reich, N. (2014) General Principles of EU Civil Law. Cambridge; Antwerp; Portland: intersentia.

[53] Reymond, M. (2013) Jurisdiction in case of personality torts committed over the Internet: a proposal for a targeting test. *Yearbook of Private International Law*, 14, pp. 205-246.

[54] Roberts, J. (2016) Privacy Laws Pose New Threat to Free Speech [blog entry] 19 January. Fortune-Tech. Available from: http://fortune.com/2016/01/19/libel-privacy-tourism/ [Accessed 7 June 2017].

[55] Rosen, M. (2012) The Speech Act's Unfortunate Parochialism: Of Libel Tourism and Legitimate Pluralism. *Virginia Journal of International Law*, 53(1), pp. 99-126.

[56] Sarmiento, D. (2013) Who's afraid of the Charter? The Court of Justice, National Courts and the new Framework of Fundamental Rights Protection in Europe. *Common Market Law Review*, 50(3), pp. 1267-1304.

[57] Savin, A. (2013) *EU Internet Law*. Cheltenham; Northampton: Edward Elgar.

[58] Schmidt, J. (2015) *Rechtssicherheit im europäischen Zivilverfahrensrecht*. Tübingen: Mohr Siebeck.

[59] Stone P. (2006) *EU Private International law. Harmonization of Laws*. 2nd ed. Cheltenham, UK; Northampton MA: Edward Elgar, 2006, pp. 93-94.

[60] Svantesson, D.J.B. (2013) A "layered approach" to the extraterritoriality of data privacy laws. *International Data Privacy Law*, 3(4), pp. 278-286.

[61] Svantesson, D.J.B. (2013) *Extraterritoriality in Data Privacy Law*. Copenhagen: Ex Tuto Publishing.

[62] Svantesson, D.J.B. (2015) A Jurisprudential Justification for Extraterritoriality in (Private) International Law. *Santa Clara Journal of International Law*, 13(2), pp. 517-571.

[63] Svantesson, D.J.B. (2016) Against "Against Data Exceptionalism". *Masaryk University Journal of Law and Technology*, 10(2), pp. 200-211.

[64] Terhechte, J.P. (2008) Der Vertrag von Lissabon: Grundlegende Verfassungsurkunde der europäischen Rechtsgemeinschaft oder technischer Änderungsvertrag? *Europarecht*, 43, pp. 143-190.

[65] Wagner, G. (1998) Ehrenschutz und Pressfreiheit im europäischen Zivilverfahrens- und Internationalen Privatrecht. *Rabels Zeitschrift für ausländisches und internationales Privatrecht*, 62(2), pp. 243-285.

[66] Werkmeister, C. (2017). In: Peter Gola (ed.) *Datenschutz-Grundverordnung VO (EU) 2016/679-Kommentar*. Munich: C.H. Beck, p. 730.

[67] Whitman, J.Q. (2004) The Two Western Cultures of Privacy: Dignity versus Liberty. The *Yale Law Journal*, 113, pp. 1151-1221.

[68] Woods, A.K. (2016) Against Data Exceptionalism. *Stanford Law Review*, 68(4), pp. 729-789.

DOI: 10.5817/MUJLT2017-1-3

THE EUROPEAN COMMISSION'S GEO-BLOCKING PROPOSALS AND THE FUTURE OF EU E-COMMERCE REGULATION

by

PIETER VAN CLEYNENBREUGEL*

As part of its Digital Single Market strategy, the European Commission envisages to take action aimed at eradicating the practice of blocking one's website to persons established or residing in a particular EU Member State. To that extent, a 2015 proposal for a regulation on the portability of online streaming services and a 2016 proposal for a regulation on geo-blocking outside the audio-visual context have been presented, the scope of which will be analysed in this paper.

Although the proposed Regulations would tackle topical problems in EU e-commerce and thus offer a necessary step forward in enhancing cross-border trade in the European Union, their envisaged regulatory approach raises important concerns from enforcement and rules' circumvention points of view.

Taking stock of those two concerns, the paper will reflect upon ways to mitigate their detrimental effects. Arguing that the geo-blocking proposals already contain the basic tools for such mitigation, the paper advocates the adoption of a more streamlined EU competition law and e-commerce regulation enforcement strategy, complemented by a "technologically more pro-active" EU law interpretation stance to e-commerce at the EU level.

KEY WORDS

Digital Single Market, E-commerce Regulation, Geo-blocking, Online Content Portability, Enforcement, Competition Law

* pieter.vancleynenbreugel@ulg.ac.be, Professor (chargé de cours) of European economic law, Liège Competition and Innovation Institute, Ph.D (KU Leuven), LL.M. (Harvard), Liège Competition and Innovation Institute Université de Liège, Université de Liège, Belgium.

1. INTRODUCTION

In May 2015, the European Commission set itself the ambitious goal to establish a Digital Single Market (DSM). Focused primarily on better access for consumers and businesses to online goods and services across Europe,[1] the Commission has proposed new legislation aimed at removing obstacles to free online cross-border trade. Key targets in this regard have been instances of geo-blocking, where access to goods or services is blocked for reasons of residence or nationality of (potential) customers. Seeking to eradicate such instances, the EU proposed two Regulations, one relating to audio-visual media and another more generally to most other goods and services. Although both proposed regulations differ in scope and ambition, they allow to understand how the EU envisages the Regulation of technology in the context of its DSM agenda.

In proposing both Regulations, the European Commission opted to proceed with a piecemeal approach to e-commerce regulation. Section 2 of this paper analyses and frames that approach. Following this analysis, section 3 will argue that, to the extent the Commission deems more regulation of e-commerce necessary, the envisaged piecemeal approach raises important concerns from an enforcement and a rules' circumvention point of view. Taking stock of those two concerns, section 4 will subsequently reflect upon ways to mitigate their detrimental effects. In doing so, it advocates the adoption of a more streamlined EU competition law – e-commerce regulation enforcement strategy, complemented more generally by a "*technologically more pro-active*" EU law interpretation strategy in the realm of e-commerce.

Before developing this argument, it is important to stress that the paper should not be understood as implicitly approving the Commission's regulatory approach as the only right one. The approach towards, and even the need for, EU e-commerce regulation can be contested in their own right indeed. Preferring not to enter into those debates here, all the more given that the EU institutions clearly prefer to move forward on this strategy, this paper's aim is rather to look for ways that can turn the Commission's preferred regulatory approach in a stronger and more sustainable one.

---

[1] European Commission (2015) a *Digital Single Market Strategy for Europe*. COM/2015/192 final, section 2. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN [Accessed 11 June 2017] (hereafter DSM Strategy).

2. THE COMMISSION'S GEO-BLOCKING PROPOSALS

Geo-blocking refers to a set of traders' practices consisting in the blocking of access to websites and other online interfaces and the rerouting of customers from one country version to another.[2] Those practices can take place in relation to both consumer goods and – most obviously – to digital content available in one Member State to which a customer residing in another Member State wants to gain access. In the latter case, digital content will be made unavailable to customers having their IP-address located outside the Member State concerned.[3] The prevalence this practice is problematic from the point of view of a European Union wanting to create and maintain an internal market characterised by the free flow of goods and services.[4]

Although existing EU law would already prohibit certain of those practices,[5] more tailored regulation was felt necessary to oblige traders to stop blocking access to their websites or online ordering systems. The European Union presented two specific proposals in that regard. Firstly, the Commission in December 2015 proposed a Regulation enabling subscribers to audio-visual streaming services to keep their subscription when temporarily residing in another Member State (2.1). Secondly, a May 2016 proposal would prohibit traders more generally to continue geo-blocking customers (2.2).

---

2 European Commission (2016) *Issues paper presenting initial findings of the e-commerce sector inquiry conducted by the Directorate-General for Competition*. SWD(2016) 70 final, recital 32 Available from: http://ec.europa.eu/competition/antitrust/e-commerce_swd_en.pdf [Accessed 11 June 2017] (hereafter referred to as geo-blocking initial findings report).

3 European Commission (2016) *Antitrust e-commerce sector inquiry finds geo-blocking is widespread throughout EU*. [press release] 18 March. Available from: http://europa.eu/rapid/press-release_IP-16-922_en.htm [Accessed 11 June 2017]. A final report, published on 10 May 2017, confirmed those findings. For that report, see European Commission (2017) *Final Report on the E-commerce Sector Inquiry*. COM(2017) 229 final. Available from: http://ec.europa.eu/competition/antitrust/sector_inquiry_final_report_en.pdf [Accessed 11 June 2017].

4 At the same time, however, geo-blocking often also serves as a tool to ensure compliance with nationally-structured copyright laws. See for that perspective already Trimble, M. (2012) the Future of Cybertravel. Legal implications of the evasion of geolocation. *Fordham Intellectual Property, Media and Entertainment Law Journal*, 22(3), p. 570. See also Trimble, M. (2016) Geoblocking, Technical Standards and the Law. In: R. Lobata and J. Meese (eds.) *Geoblocking and digital video culture*. Amsterdam: Institute of Network Cultures, p. 55.

5 Especially when the State obliges or enables directly traders to do so; in that case, the State would restrict the freedom to deliver goods or to provide services, prohibited by Articles 34 and 56 of the Treaty on the functioning of the European Union (TFEU). Article 101 TFEU would prohibit contracts between businesses containing geo-blocking clauses. In the same way, Article 102 TFEU would prohibit dominant business from engaging in such an abusive practice.

2.1 THE 2015 ONLINE CONTENT PORTABILITY PROPOSAL

In an attempt to avoid situations where consumers are confronted with inaccessible audio-visual content when travelling abroad within the European Union, the European Commission proposed an online content portability Regulation in December 2015.[6]

To that extent the proposed Regulation would require that online service providers enable their subscribers to use the service in the Member State of their temporary presence by providing them access to the same content on the same range and number of devices, for the same number of users and with the same range of functionalities as those offered in their Member State of residence. This obligation is mandatory and therefore the parties may not exclude it, derogate from it or vary its effect. Any action by a service provider which would prevent the subscriber from accessing or using the service while temporarily present in a Member State, for example restrictions to the functionalities of the service, would amount to an illegal circumvention of the portability rights guaranteed by the proposed Regulation.[7]

In very general terms, the proposed Regulation obliges a provider of an online content service to enable a subscriber who is temporarily present in a Member State to access and use the online content service in the same way as made possible in the home Member State.[8] More specifically, providers have to offer subscribers access to the same content on the same range and number of devices, for the same number of users and with the same range of functionalities as those offered in their Member State of residence.[9] The only exception to this obligation relates to the quality of the service offered. The services provider is not obliged to deliver the same quality of online deliveries as was the case in the home Member State, at least on condition that the subscriber is informed about

---

[6] European Commission (2015) *Proposal for a Regulation of the European Parliament and of the Council on ensuring the cross-border portability of online content services in the internal market*. COM/2015/627 final. Available from: https://ec.europa.eu/transparency/regdoc/rep/1/2015/EN/1-2015-627-EN-F1-1.PDF [Accessed 11 June 2017] (hereafter portability proposal). See also Peifer, K.-N. (2016) the Proposal of the EU Commission for a Regulation on Ensuring the Cross-Border Portability of Online Content Services in the Internal Market. In: A. De Franceschi (ed.) *European Contract Law and the Digital Single Market. the Implications of the Digital Revolution*. Antwerp: Intersentia, p. 164.

[7] Recital 18 portability proposal.

[8] Article 3(1) portability proposal.

[9] Recital 18 portability proposal.

this quality difference.[10] In order to overcome copyright difficulties disputes, the proposed Regulation would establish that the provision, the access to and the use of such online content service should be deemed to occur in The Member State of the subscriber's residence.[11]

An online content service is defined more specifically as a service legally provided in a Member State qualifying as an audio-visual media service, i.e. a service which is under the editorial responsibility of a media service provider and the principal purpose of which is the provision of programmes, in order to inform, entertain or educate, to the general public by electronic communications networks or an audio-visual commercial communication.[12] According the European Commission, the proposal envisages above all

> "*video-on-demand platforms (Netflix, HBO Go, Amazon Prime, Mubi, Chili TV), online TV services (Viasat's Viaplay, Sky's Now TV, Voyo), music streaming services (Spotify, Deezer, Google Music) or game online marketplaces (Steam, Origin).*"[13]

Temporarily residing in that regard implies the presence of a subscriber in a Member State other than the Member State of residence, without that subscriber relinquishing his residence in the home Member State.[14]

The proposed Regulation would also cover any other service the main feature of which is the provision of access to and use of works, other protected subject matter or transmissions of broadcasting organisations, whether in a linear or an on-demand manner, which is provided to a subscriber on agreed terms either against payment or money or without payment or money yet after verification of the subscriber's residence.[15] An example of the latter could be a free YouTube-user profile upon completion of a registration form requiring the user to provide details about his location. Online content services which are provided without the payment of money and whose providers do not verify the Member State

---

[10] Article 3(2) portability proposal.

[11] Article 4 portability proposal.

[12] Article 2(e) portability proposal.

[13] European Commission (2017) *Digital Single Market: EU negotiators agree on new rules allowing Europeans to travel and enjoy online content services across borders*. [press release] 7 February. Available from: http://europa.eu/rapid/press-release_IP-17-225_en.htm [Accessed 11 June 2017].

[14] Article 2(d) portability proposal.

[15] Article 2(e) portability proposal.

of residence of their subscribers remains outside the scope of this Regulation.

The Regulation would not impose specific enforcement obligations on Member States' authorities in this regard. It nevertheless firmly states that any contractual provisions including those between holders of copyright and related rights, those holding any other rights relevant for the use of content in online content services and service providers, as well as between service providers and subscribers which do not guarantee such portability shall be deemed unenforceable.[16] The Regulation proposal adds to this that holders of copyright and related rights or those holding any other rights in the content of online content services may ask for verifications that the online content is used only by subscribers residing temporarily in another Member State.[17]

On 26 May 2016, the Council agreed on the principled approach taken in the Commission's proposal.[18] The European Parliament having taken a similar position on 29 November 2016,[19] the European Commission managed to reach an agreement on 7 February 2017 with the Council and The European Parliament to move forward the proposal on online content portability, transforming it in a directly applicable EU Regulation.[20] If and when adopted, the Regulation would be applicable to contracts concluded and rights acquired before the date of its application if they are relevant for the provision, the access to and the use of an online content service after that date.[21]

2.2 THE 2016 GENERAL GEO-BLOCKING PROPOSAL

In an attempt to remove existing barriers to cross-border online trading activities[22], the 2016 proposal envisages to capture all traders engaging

---

16 Article 5(1) portability proposal.

17 Article 5(2) portability proposal.

18 See Council of the European Union (2016) *Portability of digital content: Council agreement on main principles*. [press release 26 May]. Available from: http://www.consilium.europa.eu/en/press/press-releases/2016/05/26-portability-digital-content/ [Accessed 11 June 2017].

19 European Parliament (2016) *Watch your online films anywhere in the EU: MEPs back cross-border portability*. [press release] 29 November. Available from: http://www.europarl.europa.eu/news/en/news-room/20161128IPR53511 [Accessed 11 June 2017].

20 European Commission (2017) *Digital Single Market: EU negotiators agree on new rules allowing Europeans to travel and enjoy online content services across borders*. [press release] 7 February. Available from: http://europa.eu/rapid/press-release_IP-17-225_en.htm [Accessed 11 June 2017].

21 Article 7 portability proposal.

22 DSM Strategy, p. 5.

in cross-border geo-blocking practices. More particularly, it is meant to provide more opportunities for customers not being able to buy products and services from traders located in a different Member State or those being discriminated in accessing the best prices or sales conditions compared to nationals or residents of that Member State.[23] Remarkably, however, the proposal would exclude access to audio-visual content available in another Member State from its scope.[24] As a result, traders could still geo-block customers seeking to access an online content service in another Member State, based on their location or on their IP-address.

For geo-blocking practices falling within its scope, the proposed Regulation would not of itself oblige traders to engage in cross-border commerce. The proposal only seeks to enable or facilitate envisaged cross-border commercial transactions taking place by means of an online interface, i.e. any software, including a website and applications, operated by or on behalf of a trader, which serves to give customers access to the traders' goods or services with a view to engaging in a commercial transaction with respect to those goods and services.[25] Consumers or businesses established outside the European Union but being geo-blocked by an EU business would not be able to benefit from the scope of this Regulation.[26] As such, the prohibitions outlined in it only apply to situations in which a trader established in a Member State or a third country offering goods or services in a Member State to customers temporarily residing in that same state, customers established in another Member State, or residing in the same Member State yet having the nationality of another Member State.[27]

---

[23] Mazziotti, G. (2015), Is geo-blocking a real cause for concern in Europe? *EUI Law Working Papers*, (2015)43, pp. 8-11. Available from: http://cadmus.eui.eu/handle/1814/3808 [Accessed 11 June 2017].

[24] See Article 2(g) Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market. *Official Journal of the European Union* (2006/L376/36) 27 December. Available from: http://eur-lex.europa.eu/legal-content/En/TXT/?uri=celex%3A32006L0123 [Accessed 11 June 2017].

[25] Article 2(f), European Commission (2016)*Proposal for a Regulation of the European Parliament and of the Council on addressing geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulation (EC) no 2006/2004 and Directive 2009/22/EC*. COM (2016) 289 final. Available from: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-geo-blocking [Accessed 11 June 2017] (hereafter geo-blocking proposal).

[26] For an interesting comparison regarding geo-location as a jurisdictional starting point in EU cyberspace regulation, Svantesson, D.J.B. (2016) Nostradamus Lite – Selected speculations as to the future of internet jurisdiction, *Masaryk Journal of Law and Technology*, 10(1), p. 59.

[27] Article 1(2) geo-blocking proposal.

When using an online interface, traders shall not, through the use of technological measures or otherwise, block or limit customers' access to that interface for reasons related to the nationality, place of residence or place of establishment of the customer. Nor should they redirect customers to a version of their interface that is different, by virtue of its layout, use of language other characteristics that make it specific to customers with a particular nationality, place of residence or establishment, from the one which the customer originally wanted to access.[28] Such redirection can only take place with the customer's explicit consent; in that case, the original version of the interface has to remain easily accessible for that customer as well.[29] The obligation to refrain from geo-blocking would apply even when traders do not explicitly direct their activities to the territory where the customer concerned is located. However, Article 1, paragraph 5 of the proposed Regulation confirms that

> *"The mere fact that a trader acts in accordance with the provisions of this Regulation should not be construed as implying that he directs his activities to the consumer's Member State for the purpose of such application."*

This confirmation is important, as EU choice of law instruments generally determine that the law of the consumer's state of residence will be applicable in cross-border consumer contracts. As a result, the law of the seller would be applicable in transactions subject to this regulation but not specifically directed towards the Member State of the customer's residence.[30]

In the same vein, the trader cannot apply different conditions of payment where payments are made by means of electronic transfer

---

[28] Article 3(1) and (2) geo-blocking proposal.

[29] Article 3(2), second sentence geo-blocking proposal.

[30] Article 1(5) geo-blocking proposal. See also a newly proposed recital 10(a) by the European Parliament. On the notion of directing, see Article 6(1)(b) of Regulation 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I). *Official Journal of the European Union*(2008/L177/6) 4 July. Available from http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32008R0593 [Accessed 11 June 2017]. See also Article 17(1)(c) of Regulation 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. *Official Journal of the European Union* (2012/L 351/1) 20 December. Available from: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32012R1215 [Accessed 11 June 2017]. According to the Court of Justice, directing activities towards a Member State implies that the trader was envisaging doing business with consumers domiciled in one or more Member States, including the Member State of that consumer's domicile, in the sense that it was minded to conclude a contract with them, see CJEU, Joined Cases C-585/08 and C-144/09, *Pammer and Alpenhof*, para 92.

within the same payment brand.[31] The obligation to give access to the original interface is not absolute, however. Indeed, the proposed Regulation highlights that the trader is not obliged to grant access to its interface whenever this is necessary to ensure compliance with a legal requirement in EU law or in the laws of the Member States, in accordance with Union law.[32] In that case, the trader has to provide a clear justification for doing so in the language of the online interface that the customer originally sought to access.[33]

In addition to the generally applicable obligation to grant access to the online interface, the proposal also prohibits traders to apply different general conditions of access to their goods or services, for reasons related to the nationality or place of residence or establishment of the customer where the trader sells goods and those goods are not delivered cross-border directly to the Member State of the customer by the trader or on his behalf, where the trader provides electronically supplied services or where the services provided are supplied to the customer in the premises of the trader situated in a Member State other than that of the customer's nationality or place of residence.[34] In those circumstances, traders cannot justify a refusal to trade with a customer on the same terms and conditions as the ones applicable to those having the nationality of or residing in the same Member State.[35]

The Regulation also confirms that agreements imposing on traders obligations to act in violation of it in terms of passive sales (i.e. transactions initiated by the customer, the trader not actively recruiting its customers in another Member State) are considered to be automatically void.[36]

On 28 November 2016, the Council adopted a Common position regarding the Commission's proposal. According to the Council, the Regulation should prohibit only *unjustified* geo-blocking.[37] In its common position, the Council proposed more or less marginal

---

[31] Article 5 geo-blocking proposal.

[32] Article 3(3) geo-blocking proposal.

[33] Article 3(4) geo-blocking proposal.

[34] Article 4(1) geo-blocking proposal. The Regulation in this regard envisages hotel accommodation, sport events, car rental, and entry tickets to music festivals or leisure parks, see recital 20.

[35] Article 4(3) geo-blocking proposal nevertheless permits Member States to maintain fixed book prices as long as they are in compliance with EU law, as well as to maintain restrictions explicitly permitted as a matter of EU law. Beyond those restrictions, traders cannot justify themselves.

[36] Article 6 geo-blocking proposal.

modifications, without directly changing the ambit of the Commission's proposal. The European Parliament Internal Market and Consumer Protection Committee on 25 April 2017 adopted a common position, following which negotiations on a final text between the three institutions can take place.[38] The Parliament's Committee position above all seeks to stress the need to protect consumers, replaces the word 'nationality' by 'country of origin' and aims to make even clearer that traders respecting this obligation are not necessarily directing their activities to any part of the EU internal market for the purposes of determining the applicable Member State's consumer protection law.[39]

3. HEADING IN THE WRONG DIRECTION, PIECE BY PIECE?

Both sets of geo-blocking proposals reflect a prohibition-focused approach: to the extent that certain commercial practices limit or render more difficult cross-border trade in goods or services, EU law will take steps to prohibit it. Given that mere prohibitions do not as such result in more e-commerce, flanking policies are meant to encourage consumers to actually engage in more such transactions. That approach, also already reflected in the e-commerce Directive 2000/31[40], seemingly remains the preferable way forward in the realm of e-commerce regulation, contributing to enhanced European private law standards.[41]

---

[37] Council of the European Union (2016) *Proposal for a Regulation of the European Parliament and of the Council on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulation (EC) no 2006/2004 and Directive 2009/22/EC – general approach*. 2016/0152 (COD). Available from: http://data.consilium.europa.eu/doc/document/ST-14663-2016-INIT/en/pdf [Accessed 11 June 2017]. This document contains the modifications proposed by the Council.

[38] See European Parliament (2016) *Geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market*. 2016/0152(COD). Available from: http://www.europarl.europa.eu/oeil/popups/fiche procedure.do?lang=&reference=2016/0152(COD) [Accessed11 June 2017].

[39] See to that extent, modifications proposed to Articles 1(1), 1(5) and 2(2)(c) of the Commission's proposal.

[40] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. *Official Journal of the European Union* (2000/L178/1). Available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML [Accessed 11 June 2017]. Waelde, C. (2005), Article 3, ECD: Internal Market Clause. International Private Law, Consumers and the Net: a Confusing Maze or a Smooth Path Towards a Single European Market? In: L. Edwards (ed.) *the New Legal Framework for E-Commerce in Europe*. Oxford: Hart Publishing, pp. 3-30.

Although the need for more specific EU regulation of e-commerce deserves to be questioned as such[42], this paper would like to argue that, even when one assumes that some kind of regulatory intervention is needed indeed in this field, the approach chosen by the European Commission can be criticised from two angles. Those angles relate to the enforcement limits (3.1) and seemingly increased circumvention risks (3.2) exacerbated by the proposed e-commerce regulations in general and the geo-blocking proposals in particular.

3.1 ENFORCEMENT LIMITS

The mere adoption of portability rights or online trade restrictions' prohibitions does not in itself guarantee the removal of obstacles to a DSM and the concomitant increase in cross-border trade. Effective e-commerce regulation also requires targeted supervision and enforcement actions, guaranteeing that the EU law provisions adopted are implemented in a coherent fashion across the different Member States. In that respect, both geo-blocking proposals, although showing concern for such enforcement, are too limited in scope and scale for them to be able to fulfil the ambitions of a streamlined common DSM agenda set at the European Union level.

The 2015 portability proposal only explains that contractual limitations to subscription portability are prohibited, leaving it to the Member States to enforce that provision. The 2016 geo-blocking proposal requires more oversight in terms of compliance. Designated Member State enforcement bodies will have to ensure compliance with the Regulation.[43] In that respect, the European Commission obliges Member States' competent consumer protection authorities to have minimum enforcement powers to tackle intra-Union consumer law violations. Those powers should include the possibility to request information regarding traders from online platforms, to close down a website, domain or similar digital site, service

---

[41] Micklitz, H. W. (2016) The economic efficiency rationale and European private law. In: G. Comparato, H. W. Micklitz and Y. Svetiev (eds.) *European regulatory private law – Autonomy, competition and regulation in European private law*. Florence: EUI Law Working Papers 2016(6), p. 59. Available from: http://cadmus.eui.eu/handle/1814/40376 [Accessed 11 June 2017].

[42] Brotman, S.N. (2016) the European Union's Digital Single Market Strategy: A conflict between government's desire for certainty and rapid marketplace innovation? *Centre for Technology Innovation at Brookings Working Papers*, pp. 1-7. Available from: https://www.brookings.edu/wp-content/uploads/2016/07/digital-single-market.pdf [Last accessed 11 June 2017].

[43] Article 7(1) geo-blocking proposal.

or account or a part of it, including by requesting a third party or other public authority to implement such measures or the possibility to impose penalties on traders.[44] The authorities should be able either directly to impose those sanctions or apply to competent Member State courts to do so.[45] The European Parliament proposes to add that the sanctions are to be communicated to the Commission, which is to make them publically available on its website.[46] as a result, the existing consumer protection authorities in Member States would receive specific powers aimed at preventing and penalising geo-blocking practices prohibited by the envisaged Regulation.

Despite those modest enforcement initiatives, the scope for uniform or coordinated enforcement of EU geo-blocking regulation, and more generally DSM regulation, is likely to remain limited in two ways.

Firstly, the particular nature of the EU legal order implies that Member States remain responsible for the enforcement of EU legal provisions, even when covered by a directly applicable Regulation. The fact that different authorities will have to interpret and apply the same provisions, gives rise to diverging interpretations and enforcement strategies. As those authorities are independent from direct oversight by EU institutions, they may determine, to the extent permitted by Member States' law, their own enforcement priorities.[47] As a result, the enforcement of DSM provisions may not be ranked as high as their adoption has been among EU policymakers. On top of that, the differentiated structure of different Member States' authorities may have an impact on the resources devoted in different Member States to implement and enforce the EU DSM provisions. As a result, the application and enforcement of EU law provisions cannot be guaranteed in a consistent way. In order to tackle those defects, the establishment of a consumer protection coordination network offers a step towards some convergence in enforcement practices. However, this network does not in itself guarantee that more coherence

[44] Article 8(2), European Commission (2016)*Proposal for a Regulation of the European Parliament and of the Council on cooperation between national authorities responsible for the enforcement of consumer protection laws*. COM/2016/283 final. Available from: http://ec.europa.eu/consumers/consumer_rights/unfair-trade/docs/cpc-revision-proposal_en.pdf [Accessed 11 June 2017] (hereafter consumer enforcement proposal).

[45] Article 9(1) consumer enforcement proposal.

[46] Article 7, paragraph 2a, geo-blocking proposal, amendment proposed by the European Parliament.

[47] Wils, W. (2011) Discretion and Prioritisation in Public Antitrust Enforcement, in Particular EU Antitrust Enforcement, *World Competition*, 34(3), pp. 357-360.

in enforcement priorities can be attained, all the more since the European Commission is not directly injecting enforcement priorities in this network, in contrast with a similar network in EU competition law enforcement.[48]

Secondly, enforcement at Member State level does not necessarily take place by one single enforcement body or authority. As a result, different actors may be involved at the enforcement level, even within one and the same Member State. The EU regulatory framework does not impede this phenomenon, but rather confirms it. In the context of the 2016 geo-blocking proposal, it has to be reminded that consumer protection authorities taking sanctions against unjustified geo-blocking practices only have powers in relation to trader-consumer relationships. Member States' authorities will not be able to target those practices. Either the courts or specific authorities, set up in accordance with Member States' own rules and practices, will be tasked to enforce the EU law provisions in that context.

It can therefore be concluded that both the geo-blocking proposals in particular and the DSM agenda more generally fail to pay sufficient attention to the need for a coordinated enforcement system. In order to guarantee that the EU law provisions covered in the geo-blocking Regulations would be enforced truly, attention to such enforcement venues is more than necessary. In just subscribing to the existing weak coordinated consumer protection coordination framework, the geo-blocking proposals fail to take into account the need for a truly EU enforcement approach in this domain. Given that other sectors are characterised by such a coordinated enforcement approach, its absence is a consequence of political unwillingness rather than a lack of competence to set up a more coordinated enforcement mechanism.

3.2 INCREASED CIRCUMVENTION RISKS?

The geo-blocking proposals, and the regulatory approach they reflect, are presented as consistent with earlier legislation and therefore justified and desirable as a way forward.[49] Nearly exclusive attention to consistency with other legal instruments has the perverse effect of increasing risks

[48] Betlem, G. (2007), Public and private transnational enforcement of EU consumer law. In: W. van Boom and M. Loos (eds.) *Collective enforcement of Consumer Law. Securing compliance in Europe through private group action and public authority intervention*, Groningen: Europa Law Publishing, pp. 37-62.

[49] Portability proposal, pp. 2-3 and geo-blocking proposal, pp. 2-3.

for rules' circumvention. DSM regulation appears to be especially prone to those risks.

In confirming that proposed geo-blocking regulations are consistent with other existing regulatory instruments, the European Commission seems to be convinced sufficiently that the regulation will work in practice as well. Somewhat paradoxically, however, despite or maybe because of the quasi-exclusive attention to macro-level consistency with the general objectives of the establishment of the EU internal market, the EU legislator runs the risk of neglecting fundamental circumvention risks associated with this type of regulation.

The geo-blocking proposals vividly illustrate those risks, as they tackle only a few situations, leaving all non-covered types of geo-blocking like practices outside the scope of EU law. It should be remembered in this respect, that EU internal market law prohibits in principle all state-imposed restrictions, but leaves untouched private actions limiting access to a market in another Member State. Absent regulatory intervention, those private actions remain unaffected by EU law. This is most clear in the geo-blocking proposals. Firstly, the data portability proposal would only permit subscribers to take their content with them. Any non-subscribed content could still be blocked since it would not be covered by the Regulation. Secondly, the proposed Regulation would target online sales of goods and services except for those exempted from the scope of application of the services Directive. In doing so, the proposal envisages a specific situation where obstacles created by private traders are prohibited as a matter of EU secondary legislation, yet also threatens to introduce a distinction between situations where customers can rely on those provisions and all situations (such as access to audio-visual media in the absence of a subscription) not covered by the Regulation. In the same way, the simple refusal to use certain payment brands may result in the exclusion of certain traders' practices from the scope of the same Regulation. In not wishing to cover the entire spectrum of e-commerce transactions that could be subjected to geo-blocking, the EU does facilitate circumvention, inviting traders to reflect about practices not technically falling within the scope of the envisaged Regulations, yet having the same effects in practice. The chosen regulatory approach in tackling geo-blocking is therefore, by its very nature, selective and prone to keep certain obstacles to e-commerce in place.

It can therefore be concluded that justifying the proposed Regulations as being consistent with other legal rules detracts attention from the actual circumvention risks they harbour and that remain unaddressed in this respect. To the extent that EU legislation intervenes to prohibit certain actions or to remove certain obstacles maintained by private actors, albeit in a consistent way, only those actions covered by legislation will be prohibited. Other types of private actions will remain legal, even though their effects may be very similar to the ones prohibited. In that understanding, it would pay off more than ever for traders to make sure they fall outside the narrow scope of the envisaged Regulations in order to continue their geo-blocking practices. Not offering payments through certain brands already suffices in that respect and would be perfectly legal.

4. TOWARDS MORE SUSTAINABLE EU E-COMMERCE REGULATION?

The enforcement limits and rules' circumvention risks outlined in the previous section showcase the principal defects associate with the EU's regulatory approach implementing the DSM agenda. Despite those shortcomings, however, the geo-blocking proposals also reflect the nucleus of two legal-political strategies which, whilst not overcoming them, could at least mitigate the detrimental effects of a lack of coordinated enforcement and a narrow focus. Taking those strategies more seriously, it will be submitted, will allow those effects to be less prominently present in the application and implementation of those legal instruments.

This section identifies where elements of those legal-political strategies can be detected in the geo-blocking proposals' context and how more explicit attention to them can alleviate limited enforcement and narrow focus concerns. In that regard, this section particularly argues that a more streamlined EU competition and e-commerce regulation enforcement strategy (4.1), complemented by a more technologically more pro-active EU law interpretation stance (4.2) could in themselves already partly address the concerns voiced in the previous section. Given the presence – albeit somewhat implicit – of both strategies in the geo-blocking proposals, it would be rather easy to give a more prominent place to them when continuing to design and implement the DSM regulatory framework.

4.1 STREAMLINING EU COMPETITION LAW AND E-COMMERCE REGULATION ENFORCEMENT STRATEGIES

In addressing geo-blocking practices, the Commission's proposals demonstrate how EU internal market regulation and EU competition law can interact and complement each other. That possibility of complementarity could be elaborated further in order to address some of the enforcement concerns underlying the EU's DSM regulatory approach.

The relationship between internal market regulation and competition law has been considered traditionally as one of complementarity and separateness; Articles 101 and 102 TFEU in principle only target private action, whereas internal market law regulates public authorities' action.[50] At the same time, EU competition law only envisages an *ex post* intervention in the assessment of anticompetitive practices engaged in by or between private actors.[51] Agreements have to have been concluded or abusive behaviour has to be engaged in prior to the European Commission or national competition authorities taking action in those domains. In addition, those authorities only intervene Given the *ex post* and case-by-case focus of EU competition law, it would not be surprising that the EU legislature would like to intervene by prohibiting certain practices deemed anticompetitive in an *ex ante* fashion. *Ex ante* regulatory intervention in those circumstances is seen as a way to complement the existing Treaty competition law prohibitions, covering situations not directly covered by them, or to directly target the behaviour of non-dominant undertakings. In addition, the EU institutions could further clarify the competition law provisions by means of EU internal market secondary legislation in a particular economic sector, such as e-commerce.[52]

It will not be surprising that both geo-blocking proposals reflect this complementarity relationship. Both proposals have been made in the light of a competition law inquiry into the e-commerce sector, which has permitted to detect the prevalence of geo-blocking practices, both relating

---

[50] Mataija, M. (2016) *Private Regulation and the Internal Market. Sports, Legal Services, and Standard Setting in EU Economic Law*. Oxford: Oxford University Press, p. 119.

[51] Council Regulation 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty. *Official Journal of the European Union* (2003/L 1/1). Available from: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32003R0001 [Accessed 11 June 2017].

[52] Ackermann, T. (2010), Vodafone: Price Regulation as a Substitute for Intervention under Article 102 TFEU. *Journal of European Competition Law & Practice*, 1(5), p. 428.

to audio-visual contents and to the sales of goods and services.[53] Directly addressing those concerns, the 2015 data portability proposal envisages the non-enforceability of contractual clauses between copyright holders and online service providers restricting data portability. In doing so, this Regulation would confirm that any such contractual clause is to be considered contrary to Article 101 TFEU. In the same way, unilateral business practices escaping from competition law scrutiny are prohibited by the 2016 geo-blocking proposal. In addition, Article 6 of that proposal declares void all geo-blocking agreements restricting passive sales. Whilst the Commission proposed an absolute prohibition of such clauses, the Council and Parliament propose to amend this provision by stating that only those clauses that could not be justified by Article 101(3) TFEU or by Regulation 330/2010 exempting vertical agreements from the Article 101(1) TFEU prohibition would be considered void.[54] In being formulated in this way, both proposals clearly clarify or complement the application of competition law provisions in specific contexts.

The implicit acknowledgement of the complementarity of competition law and internal market regulation in both proposals constitutes a starting point for a more developed and focused enforcement strategy capable of mitigating enforcement limits identified in this respect. As EU competition law's attention clearly also goes to e-commerce practices, it can be expected that both the European Commission and the Member States' competition authorities will consider contractual and abusive geo-blocking practices as an enforcement priority. To the extent that this is the case, e-commerce cases will likely be brought before those authorities in the years to come. In this setting, it would not be entirely unimaginable to entrust, at Member States' level, national competition authorities also with the enforcement of geo-blocking practices which escape strictly from the scope of application of EU competition law. In some Member States such as the Netherlands, the United Kingdom or Poland,[55] competition and consumer protection law are already being enforced by one and the same authority. In the alternative, it would seem relatively

[53] Geo-blocking initial findings report, note 4.

[54] Newly proposed Article 6(2) geo-blocking proposal. Commission Regulation 330/2010 of 20 April 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices. *Official Journal of the European Union* (2010/L102/1). Available from: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32010R0330 [Accessed 11 June 2017].

easy to propose, through the intermediary of the European Competition Network (ECN) chaired by the European Commission[56], the prioritisation and coordination, at Member States' level, of geo-blocking cases not technically falling within the scope of EU competition law. From that point of view, the European Commission could indirectly yet effectively offer guidelines to those national authorities on how to prioritise and set up coordination memoranda with other authorities tasked with the enforcement of EU competition law. Whilst not resolving all enforcement limits accompanying the EU's DSM regulatory approach, streamlining by intermediary of the ECN would permit to at least bring to the forefront the need for coordinated enforcement and to streamline the Regulation's application above and beyond the specific context of anticompetitive behaviour at the level of the Member States.

The suggestions outlined here would require no direct legislative intervention. Quite on the contrary, relying on the existing coordinated enforcement structure accompanying EU competition law enforcement, the European Union could nudge Member States' competition authorities in either taking the lead in or coordinating with other enforcement agencies. Whilst imperfect, implementing such cooperation mechanisms would at the very least ensure that some of the limited enforcement concerns can be overcome by putting in place enhanced Member State cooperation mechanisms. Given the potential anticompetitive effects of copyright, it could even be envisaged that this streamlining strategy could also take place in relation to the enforcement of other future DSM regulation instruments.

4.2 TOWARDS "TECHNOLOGICALLY MORE PRO-ACTIVE" EU LAW INTERPRETATIONS?

One of the major issues with regulating digital transactions and commercial practices is that technological developments generally precede legislative responses. Legal rules are generally adopted in response to technological

[55] The Dutch Consumer and Markets authority (ACM), https://www.acm.nl [Accessed 11 June 2017], the U.K. Competition and Markets Authority (CMA), https://www.gov.uk/government/organisations/competition-and-markets-authority [Accessed 11 June 2017] and the Polish Office of Competition and Consumer Protection (UOKIK), https://uokik.gov.pl/home.php [Accessed 11 June 2017].

[56] On that network, see Gerard D. (2011) the ECN – Network antitrust enforcement in the European Union. In: I. Lianos and D. Gerard (eds.) *Research Handbook on EU competition law*., Cheltenham: Edward Elgarpp. 181-226.

challenges and the DSM regulatory approach is not different in this regard. Both geo-blocking Regulation proposals directly respond to concerns voiced in market and competition law studies, permitting to conclude that geo-blocking was still very prevalent across the European Union. At the same time, however, the geo-blocking proposals not only respond to certain technological challenges recognised, but also seek to establish a regulatory framework that would be fit for future e-commerce transactions. With this in mind, both proposals define online content service or online interfaces in a very general and broad fashion, permitting not only traditional websites or subscription services to be taken into account, but also cloud services and other online or digital venues in relation to which commercial transactions can take place.[57] On top of that, the 2016 proposal envisages a review four years after its entry into force and every five years thereafter.[58] The first review will especially have as its goal to evaluate whether access to audio-visual services at large should be granted in this respect.[59] As such, it is clear that the Commission shows to care about pro-actively regulating a technological field that is in development and that may result in new instances of geo-blocking currently not encountered or envisaged in practice.

Paying attention to future developments when developing market regulation permits to avoid or at least address as quickly as possible the circumvention of legal rules and to guarantee the responsiveness of regulation to challenges posited in a given context.[60] The Commission's willingness to engage in a review of the geo-blocking legislation envisaged is therefore laudable and would permit to code in certain. At the same time, however, the mere review and re-opening of policy discussions on the aptitude of the envisaged Regulation does not permit truly to set up a framework that responds directly to new challenges posed by technological innovations. Such a framework would require traders to "*code in*" from the outset an attitude that prevents geo-blocking from being introduced in interfaces that are presently unknown but may

[57] Article 2(e) portability proposal and Article 2(f) geo-blocking proposal.

[58] Article 9(1) geo-blocking proposal, and the modification from two to four years proposed by the Council.

[59] Article 9(2) geo-blocking proposal.

[60] See Ayres, I. and Braithwaite J. (1995) *Responsive Regulation – Transcending the Deregulation Debate*. Oxford: Oxford University Press.

soon conquer the market.[61] By defining broadly the notion of interface, the Commission can in some way already attain this goal.

However, that in itself is not sufficient. If the Commission, and by extension, the other EU institutions are taking seriously the adoption of digital markets regulation that envisages to apply the same principles of non-discrimination to online interfaces in interfaces that have not been proposed or constructed, more tailored immediate action would be advisable to the extent that the adoption of updated regulations would take too much time. In that respect, it is submitted that it will pay off to ensure that interpretative guidelines are in place informing those new interfaces of their obligations the moment those new interfaces begin to be active on the European market. Even though such guidelines are not binding – and a contrary interpretation of the legislation underlying them can be given indeed by the Court of Justice[62] – they would at least give some *prima facie* expectations as to the applicability of the geo-blocking or more general DSM regulatory frameworks to those new interfaces. Such a pro-active interpretative guidelines action could in that regard contribute to avoiding rules' circumvention in this particular context. The adoption of such guidelines would not require immediate legislative intervention, but only requires the Commission to be vigilant as to the potential application of its existing regulatory framework to new technological developments. In doing so, the Commission could take into consideration an approach already voiced by the Court of Justice in its *Ker-Optika* judgment, following which any restriction on cross-border ecommerce is almost automatically to be considered a restriction on the free movement of goods rather than a selling arrangement not covered by the Article 34 TFEU prohibition.[63] Taking a similar stance and adopting concrete ways forward inspired by such case law could help already in developing this more pro-active stance.

5. CONCLUSION

This paper analysed both geo-blocking proposals and the typical features of the EU's regulatory approach they reflect. Paying attention to the scope

[61] For that perspective, Lessig, L. (1999) *Code and other laws of Cyberspace*. New York: Basic Books, pp. 6-7.

[62] e.g. CJEU, Case C-360/09, *Pfleiderer*. para 21.

[63] CJEU, C-108/09, *Ker-Optika*, para 69.

and limits of both proposals, the paper identified the ways in which the EU seeks to prohibit different geo-blocking practices. Despite being a laudable effort to stimulate e-commerce, it was submitted that the geo-blocking proposals are characterised by a limited enforcement and narrow consistency focus, which would potentially facilitate their circumvention in practice. At the same time, however, they harbour features for a more coordinated enforcement strategy as well as a technologically pro-active regulatory focus. Although imperfect, acknowledging more explicitly those features in practice would serve to alleviate concerns voiced over the limited practical impact of the geo-blocking proposals and, more generally, the EU's DSM regulatory framework. This paper outlined ways to make those features more explicit, without necessarily having to amend the legislative framework in force, in an attempt to downplay the enforcement limits and circumvention risks otherwise associated with the EU's regulatory approach.

LIST OF REFERENCES

[1] Ackermann, T. (2010), Vodafone: Price Regulation as a Substitute for Intervention under Article 102 TFEU. *Journal of European Competition Law & Practice*, 1(5), pp. 426-428.

[2] Ayres, I. and Braithwaite J. (1995) *Responsive Regulation – Transcending the Deregulation Debate*. Oxford: Oxford University Press.

[3] Betlem, G. (2007), Public and private transnational enforcement of EU consumer law. In: W. van Boom and M. Loos (eds.) *Collective enforcement of Consumer Law. Securing compliance in Europe through private group action and public authority intervention*, Groningen: Europa Law Publishing, pp. 37-62.

[4] Brotman, S.N. (2016) the European Union's Digital Single Market Strategy: a conflict between government's desire for certainty and rapid marketplace innovation? *Centre for Technology Innovation at Brookings Working Papers*, pp. 1-7. Available from: https://www.brookings.edu/wp-content/uploads/2016/07/digital-single-market.pdf [Last accessed 11 June 2017].

[5] Council of the European Union. (2016) *Portability of digital content: Council agreement on main principles*. [press release 26 May]. Available from: http://www.consilium.europa.eu/en/press/press-releases/2016/05/26-portability-digital-content [Accessed 11 June 2017].

[6] Council of the European Union. (2016) *Proposal for a Regulation of the European Parliament and of the Council on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulation (EC) No. 2006/2004 and Directive 2009/22/EC – general approach*. 2016/0152 (COD). Available from: http://data.consilium.europa.eu/doc/document/ST-14663-2016-INIT/en/pdf [Accessed 11 June 2017].

[7] European Commission. (2015) *A Digital Single Market Strategy for Europe*. COM/2015/192 final, section 2. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/uri=CELEX:52015DC0192&from=EN [Accessed 11 June 2017].

[8] European Commission. (2015) *Proposal for a Regulation of the European Parliament and of the Council on ensuring the cross-border portability of online content services in the internal market*. COM/2015/627 final. Available from: https://ec.europa.eu/transparency/regdoc/rep/1/2015/EN/1-2015-627-EN-F1-1.PDF [Accessed 11 June 2017].

[9] European Commission. (2016) *Issues paper presenting initial findings of the e-commerce sector inquiry conducted by the Directorate-General for Competition*. SWD(2016) 70 final, recital 32. Available from: http://ec.europa.eu/competition/antitrust/e-commerce_swd_en.pdf [Accessed 11 June 2017].

[10] European Commission. (2016) *Proposal for a Regulation of the European Parliament and of the Council on addressing geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulation (EC) no 2006/2004 and Directive 2009/22/EC*. Available from: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-geo-blocking [Accessed 11 June 2017].

[11] European Commission. (2016) *Proposal for a Regulation of the European Parliament and of the Council on cooperation between national authorities responsible for the enforcement of consumer protection laws*. Available from: http://ec.europa.eu/consumers/consumer_rights/unfair-trade/docs/cpc-revision-proposal_en.pdf [Accessed 11 June 2017].

[12] European Commission. (2016) *Antitrust e-commerce sector inquiry finds geo-blocking is widespread throughout EU*. [press release] 18 March. Available from: http://europa.eu/rapid/press-release_IP-16-922_en.htm [Accessed 11 June 2017].

[13] European Commission. (2017) *Digital Single Market: EU negotiators agree on new rules allowing Europeans to travel and enjoy online content services across borders*. [press release]

7 February. Available from: http://europa.eu/rapid/press-release_IP-17-225_en.htm [Accessed 11 June 2017].

[14] European Commission. (2017) *Final Report on the E-commerce Sector Inquiry*. Available from: http://ec.europa.eu/competition/antitrust/sector_inquiry_final_report_en.pdf [Accessed 11 June 2017].

[15] European Parliament. (2016) *Watch your online films anywhere in the EU: MEPs back cross-border portability*. [press release] 29 November. Available from: http://www.europarl.europa.eu/news/en/news-room/20161128IPR53511 [Accessed 11 June 2017].

[16] Gerard D. (2011) The ECN – Network antitrust enforcement in the European Union. In: I. Lianos and D. Gerard (eds.) *Research Handbook on EU competition law.* Cheltenham: Edward Elgarpp. 181-226.

[17] Lessig, L. (1999) *Code and other laws of Cyberspace*. New York: Basic Books.

[18] Mataija, M. (2016) *Private Regulation and the Internal Market. Sports, Legal Services, and Standard Setting in EU Economic Law*. Oxford: Oxford University Press

[19] Mazziotti, G. (2015), Is geo-blocking a real cause for concern in Europe? *EUI Law Working Papers,* (2015)43. Available from: http://cadmus.eui.eu/handle/1814/38084 [Accessed 11 June 2017].

[20] Micklitz, H. W. (2016) The economic efficiency rationale and European private law. In: G. Comparato, H. W. Micklitz and Y. Svetiev (eds.) *European regulatory private law – Autonomy, competition and regulation in European private law*. Florence: EUI Law Working Papers 2016(6). Available from: http://cadmus.eui.eu/handle/1814/40376 [Accessed 11 June 2017].

[21] Peifer, K.-N. (2016) the Proposal of the EU Commission for a Regulation on Ensuring the Cross-Border Portability of Online Content Services in the Internal Market. In: A. De Franceschi (ed.) *European Contract Law and the Digital Single Market. The Implications of the Digital Revolution*. Antwerp: Intersentia, pp. 163-172.

[22] Svantesson, D.J.B. (2016) Nostradamus Lite – Selected speculations as to the future of internet jurisdiction, *Masaryk Journal of Law and Technology*, 10(1), pp. 47-72.

[23] Trimble, M. (2012) the Future of Cybertravel. Legal implications of the evasion of geolocation. *Fordham Intellectual Property, Media and Entertainment Law Journal*, 22(3), pp. 567-655.

[24] Trimble, M. (2016) Geoblocking, Technical Standards and the Law. In: R. Lobata and J. Meese (eds.) *Geoblocking and digital video culture*. Amsterdam: Institute of Network Cultures, pp. 54-63.

[25] Waelde, C. (2005), Article 3, ECD: Internal Market Clause. International Private Law, Consumers and the Net: a Confusing Maze or a Smooth Path Towards a Single European Market? In: L. Edwards (ed.*) the New Legal Framework for E-Commerce in Europe*. Oxford: Hart Publishing, pp. 3-30.

[26] Wils, W. (2011) Discretion and Prioritisation in Public Antitrust Enforcement, in Particular EU Antitrust Enforcement, *World Competition*, 34(3), pp. 353-382.

DOI: 10.5817/MUJLT2017-1-4

CHOICE-OF-COURT AGREEMENTS IN THE E-COMMERCE INTERNATIONAL CONTRACTS

by

ANABELA SUSANA DE SOUSA GONÇALVES*

The choice-of-court agreements are a common practice in the e-commerce international contracts. In the European Union, the choice-of-courts agreements find their legal framework in Article 25 of Regulation No. 1215/2012 of the European Parliament and of the Council, of 12 December 2012, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I bis). The purpose of this paper is to analyse the current legal framework, in the European Union, of the jurisdiction agreements in international contracts concluded in e-commerce, comparing it to the previous one, and taking into consideration the interpretative options of the European Union Court of Justice (ECJ).

KEY WORDS

Brussels I bis Regulation, Choice-of-court Agreements, E-commerce Contracts, International Contracts

1. BRUSSELS I *BIS* REGULATION

The choice-of-courts agreements in the context of international contracts find their legal framework in *Regulation No. 1215/2012 of the European Parliament and of the Council, of 12 December 2012, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters* (Brussels I *bis*).[1] So, it is necessary, briefly, to determine the scope of application of this Regulation.

* asgoncalves@direito.uminho.pt, Professor Private Law Department Law School - University of Minho, Portugal.

The Brussels I *bis* Regulation is one of the most important milestones of the policy of the European Union (EU) of judicial cooperation in civil matters,[2] and unifies, within the EU, the rules of jurisdiction (from Article 4 to Article 35), and the rules about recognition and enforcement of judgments and the recognition and enforcement of authentic instruments and court settlements (Article 36 and Article 60).

Brussels I *bis* Regulation governs civil and commercial matters, according to the provisions of Section 1, Article 1, being excluded from its scope those issues listed in Section 1 and 2 of the same legal provision, as: status and legal capacity of natural persons; rights in property arising out of a matrimonial relationship and comparable relationships; maintenance obligations, resulting from family relationship, parentage, marriage or affinity; wills and successions; bankruptcy; revenue, customs and administrative matters; the liability of the State for acts and omissions in the exercise of State authority.

The existence of international elements in the situation is required to the application of the Brussels I *bis* Regulation, since the Regulation does not apply to purely internal situations.[3] Thus, it will be applicable to those contracts which are in contact with more than one legal system.

Regarding the spatial scope of application, the international jurisdiction rules of the Brussels I *bis* Regulation has its application in those situations in which the defendant has its domicile in one of the Member-States (Article 4, Section 1). Otherwise, the national jurisdiction rules of the Member-States will be applicable, except in the situations identified in Article 6, Section 1: in cases of consumer contracts (Article 18, Section 1);

---

[1] It is true that there are special rules in relation to choice-of-courts agreements regarding insurance contracts (Article 15), consumers contracts (Article 21) and employment contracts (Article 23), which have in account the need to protect the weaker party of the contract. However, these special regimes are excluded from the scope of this study.

[2] About the politicy of judicial cooperation in civil matters see Gonçalves, A.S.S. (2016) 'Cooperação Judiciária em Matéria Civil' in Direito da União Europeia, Elementos de Direito e Política da União, ed. Alessandra Silveira, Mariana Canotilho, Pedro Madeira Froufe, Almedina, Coimbra, pp. 339-391.

[3] Condition claimed in Jenard Report and in Schlosser Report, as well as in several ECJ decisions: Jenard, P. (1999) *Report on the Convention, of 27 September 1968, regarding the judiciary competence and enforcement of judgements in civil and commercial matters* JO C 189, p. 8; Schlosser, P. (1990) *Report on the Convention on the Association of the Kingdom of Denmark, Ireland and the United Kingdom of Great Britain and Northern Ireland to the Convention on jurisdiction and the enforcement of judgments in civil and commercial matters and to the Protocol on its interpretation by the Court of Justice* JO C 189, § 21; ECJ, *Andrew Owusu v. N. B. Jackson, acting under the commercial name Villa Holidays Bal-Inn Villas*, Case (2005) C-281/02, de 1.3.2005, § 25, still regarding the *Brussels Convention, of 27 September 1968 regarding the judiciary competence and enforcement of judgements in civil and commercial matters* (Brussels Convention), among others.

employments contracts (Article 21, Section 2); exclusive jurisdiction (Article 24); and choice-of-court agreements (Article 25). In the cases mentioned, there can be jurisdiction of the Member-States` courts, regardless the place of residence of the defendant. In turn, the recognition and enforcement rules will apply to the judgments issued by the Member-States' courts included within the material scope of application of Brussels I *bis,* according to its Article 36. The Regulation also applies to the recognition and enforcement of authentic instruments and court settlements originated from one the Member States in other Member States within its material scope of application, according to Articles 58 and 59.

Brussels I *bis* Regulation is in force since 10 January 2015 (Article 81) and has repealed *Regulation No. 44/2001, of 22 December 2000, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters*, known as Brussels I[4] (Article 80).[5]

The choice of jurisdiction agreement is a common practice in international contracts concluded in e-commerce, and Brussels I *bis* establishes in Article 25 its legal framework. The purpose of this study is to analyse that legal framework comparing it to the previous one, and taking into consideration the interpretative options of the ECJ.

2. CHOICE-OF-COURT AGREEMENTS

The choice-of-court agreements are regulated in Article 25 of Brussels I *bis* Regulation, allowing the parties, by agreement, to assign jurisdiction in legal disputes in civil and commercial matters to a court or courts of a Member-State. As in the previous drafting (Article 23 Regulation No. 44/2001), this is a expression of the principle of freedom of choice by the parties, allowing them to choose a court or courts of a Member-State to settle future disputes, or a dispute that has already taken place, having the selected court exclusive jurisdiction to decide, unless otherwise agreed by the parties (Article 23, Section 1). Therefore, in harmony

[4] Regulation No. 44/2001 came into force in 1 March 2002, according to its Article 76, being determinate, in Article 66, Section 1, that the provisions in this regulation are applicable to legal proceedings instituted or to documents formally drawn up or registered as authentic instruments after its entry into force, and has superseded between Member-States the Brussels Convention, adopting its structure and, in great part, its text (article 68).

[5] About the main modifications introduced by Brussels I bis to the previous Regulation, see Gonçalves, A.S.S. (2014) *A Revisão do Regulamento Bruxelas I Relativo à Competência Judiciária, ao Reconhecimento e à Execução de Decisões em Matéria Civil e Comercial' in Estudos em Comemoração dos 20 Anos da Escola de Direito da Universidade do Minho.* ed. Mário Monte et al., Coimbra Editora: Coimbra, pp. 39-59.

with the principle of freedom of choice, the selected court should settle the dispute, excluding the jurisdiction of any other court that might have jurisdiction according to the rules of the Regulation.[6]

However, to the validity of the choice-of-court agreement, certain requirements were established in Article 23, Section 1, to ensure legal certainty and to guarantee that the parties have given their consent.[7] It was necessary that one of the parties had its domicile within the territory of a Member-State and, as a substantive condition, the object of the agreement must concern a particular legal relationship.[8] As formal requirements, the agreement should have to be concluded: in writing or verbally, with written confirmation; in a form which accords with practices which the parties have established between the parties; or in a form according to the usage in international trade or commerce, of which the parties know or should know and which in such commerce or trade is widely known to, and regularly observed by parties in contracts of the same type involved in the specific trade or commerce in question. Section 2 of Article 23 determined that any communication by electronic means which could allows a durable record of the agreement was equivalent to a written contract. One of the objectives of the formal requirements of Article 23 was to ensure the existence of the agreement between the parties, which was

> *"[...] justified by the concern to protect the weaker party to the contract by avoiding jurisdiction clauses, incorporated in a contract by one party, going unnoticed."*[9]

So the consensus between the parties must be clearly and precisely demonstrated in the choice of jurisdiction agreement, and the substantial and formal requirements guarantee that.

Article 25, Sections 1 and 2 of Brussels I *bis* Regulation, retains the same text of the previous provision of Article 23, but with one major change:

---

[6] The importance of freedom of choice principle in jurisdiction rules results from recital 11 and is recognised by the ECJ, as becomes clear in the case *Refcomp SpA v. Axa Corporate Solutions Assurance SA and others* (2013) Case C- 543/10, 7. Feruary, § 26.

[7] ECJ, *Trasporti Castelletti Spedizioni Internazionali SpA v. Hugo Trumpy SpA.Castelletti* (1999) C-159/97, 16.March, § 34; *Francesco Benincasa and Dentalkit Srl*, (1997) C-269/95, 03 July, § 25; *Hőszig Kft. v. Alstom Power Thermal Services* (2016) Case C222/15, 07.July § 32.

[8] ECJ, *Profit Investment Sim SpA, in liquidation v. Stefano Ossi et. al.* (2016) C-366/13, 20 April, § 23; *Hőszig Kft. v. Alstom Power Thermal Services* (2015) Case C222/15, § 33.

[9] ECJ, *Hőszig Kft. v. Alstom Power Thermal Services*, Case C222/15, § 33. See also, ECJ, *Trasporti Castelletti Spedizioni Internazionali SpA v. Hugo Trumpy SpA.Castelletti*, C-159/97, § 24.

a jurisdiction agreement, regardless the domicile of the parties, can, now, be settled, not being needed, as in the previous drafting, that one of the parties has its domicile in a Member-State (Article 25, Section 1).

Another relevant change in the writing of Article 25, comparing to the previous draft, concerns the validity of the jurisdiction agreement, on which the ECJ had already dwell on. In the case *Francesco Benincasa v. Dentalkit Srl*[10], after defining that the objective of a jurisdiction agreement is the precise and clear designation by the parties of the court that has exclusive jurisdiction (except otherwise agreed), the ECJ considered that the judicial security, resulting form that agreement, would be impaired if one of the parties could evade to what was agreed, alleging the nullity of the entire contract in which that clause is inserted. Therefore, the validity of both must be analysed autonomously, as we are before two agreements that should be treated in an independent way.[11] In the same process, ECJ decided that the nullity of the contract, where the jurisdiction agreement was inserted, should be assessed by the court stipulated for in that agreement.[12] Well, it is this independence of the jurisdiction agreement, regarding the other provisions of the contract, and the prohibition of challenging the validity of that clause based, only, in the contract invalidity, that Article 25, Section 5 establishes.

Brussels I *bis* Regulation, also solved an issue, whose solution was not clear in the previous text, where certain questions aroused. Several authors[13] questioned on what would be the law that should assess the substantial validity of the jurisdiction agreement. Article 25, Section 1 of Brussels I *bis* Regulation, seems to indicate that the substantial validity must be assessed according to the law of the court of the Member-State that has jurisdiction, according to the choice-of-court agreement (as it is confirmed by recital 20).

---

[10] Process C-269/95, 20.2.1997, *CJ* 1997, p. I-3767.

[11] Magnus, U. (2012) *Prorogation of jurisdiction* in Brussels I Regulation, ed. U. Magnus and P. Mankowski, Sellier European Law Publishers:Munich, pp. 500-501; Visher, F. (2004) *Der Einbezug deliktischer Ansprüche in die Gerichtsstandsvereinbarung für den Vertrag* in Festschrift für Erik Jayme I, ed. Heinz-Peter Mansel *et al*., Sellier European Law Publishers: München, p. 995.

[12] *Francesco Benincasa contra Dentalkit Srl* (1995) C-269/95, p. I-3767.

[13] V. Gaudemet-Tallon, H. (2002) *Compétence et Exécution des Jugements en Europe, Règlement no. 44/2001, Conventions de Bruxelles et de Lugano.* 3rd ed., Montchrestien, L.G.D.J., Paris, pp. 93, indicating some solutions for the resolution of this problem, as the query of the law of the appointed court and the law of the excluded court, about the validity of the clause; Magnus, U. (2012) *Prorogation of jurisdiction.* Cit., pp. 473-474, 476-478, differentiating the several substantive questions which might arise related to the jurisdiction agreement; Stone, P. (2008) *EU Private International Law, Harmonization of Laws.* Edward Elgar Publishing, Cheltenham – UK: Northampton – USA, p. 168.

What must be understood as law, for the purposes of this rule, is clarified in recital 20, as including the conflict of law rules of the legal order of the Member-State appointed court.[14] It seems that this option of the Brussels I *bis* Regulation is in line with the autonomous treatment given to the jurisdiction agreement and with the drafting of Article 5, Section 1 of the *Hague Convention, of 30 June 2005, on Choice-of-Court Agreements*, achieving the compatibility between the two legislative texts.[15]

In what concerns the interpretation of the content of a jurisdiction clause, it is not necessary that the chosen court can be identified only by its wording. According to the ECJ

> *"it is sufficient that the clause state the objective factors on the basis of which the parties have agreed to choose a court or the courts to which they wish to submit disputes which have arisen or which may arise between them."*[16]

In addition, those factors, which have to be sufficiently accurate to allow the court seised to determine its jurisdiction, may be result of particular circumstances of the case.[17]

Finally, under Article 26, Section 1, it is considered to exist a tacit choice-of-court agreement, when the action is brought into the courts of a Member-State which does not have jurisdiction according to the jurisdiction rules of the Regulation, but before which a defendant enters an appearance (except if the objective of that appearance is to challenge the jurisdiction

---

[14] Hypothesis already admitted by some doctrine, regarding the assessment of the consent declaration: see e.g. Gaudemet-Tallon, H. (2002) L*es Conventions de Bruxelles et de Lugano*, Cit., p. 93; Magnus, U. (2012) *Prorogation of jurisdiction*, Cit., pp. 477-478; Stone, P. (2008) *EU Private International Law,* p. 168. Cfr. About this question, in the revision of the Regulation, Beraudo, J-P. (2013) *Regards sur le nouveau règlement Bruxelles I sur la compétence judiciaire, la reconnaissance et l´execution des décisions en matière civile et commerciale.* Clunet, Vol. 3, p. 749; Hay, P. (2013) *Notes on the European Union´s Brussels-I "Recast" Regulation. The* European Legal Forum, Vol. 1, p. 3; Nuyts, A. (2013) *La refonte du règlement Bruxelles I.* RCDIP, Vol. 1, pp. 55-57; Ratkovic, T. and Rotar, D.Z. (2013) *Choice-of-Court Agreements Under the Brussels I Regulation (Recast).* JPIL, Vol. 9 (2), pp. 251-259.

[15] As it is referred in the proposal of the European Commission (2010) *Proposal for a Regulation of the European Parliament and of the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.* COM 748 final, Brussels, p.10.

[16] *Hőszig Kft. V Alstom Power Thermal Services*, Case C222/15, § 43.

[17] Ibid. In that case, the agreement clause did not refer expressly to the courts of a Member State, but to the courts of the capital of a Member State (Paris) and the law of that State was also chosen by the parties as law of the contract. So, the ECJ considered that this jurisdiction clause fulfilled the requirements of precision demanded by the rule. It held that jurisdiction clause referring to the courts of a city of a Member State should be interpreted has referring implicitly but necessarily to the system of jurisdiction rules of that Member State: *ibid,* § 48-49.

of the court or if there is exclusive jurisdiction granted to another court by virtue of Article 24).

3. JURISDICTION AGREEMENTS IN E-COMMERCE CONTRACTS

Having settled the formal and substantial validity requirements to which a jurisdiction agreement must obey, it is relevant, now, to look upon the choice-of-court agreements in international e-commerce contracts, since the selection of the court that has jurisdiction is a common practice in e-commerce contracts.

As previously seen, nowadays the assignment of jurisdiction to a court or courts of a Member-State can be done even if both parties do not have domicile in one Member-State (Article 25, Section 1). The substantial validity of the jurisdiction agreement shall be ascertained according to the law of the Member-State of the court that has jurisdiction, in accordance with the choice-of-court agreement (Article 25, Section 1). Regarding the formal requirements, they are settled in the subparagraphs of Article 25, Section 1 and they can be applied alternatively, as previously said. The goal of formal requirements has to do with the need to safeguard the actual existence of the consent of the parties.[18]

From the formal requirements needed for the conclusion a jurisdiction agreement, the one that might be more difficult to accomplish in e-commerce, is the requirement foreseen in Article 25, Section 1 (a), which demands that the parties express their consent through a writing or verbal way, with a subsequent written confirmation.[19] In e-commerce contracts, the jurisdiction agreements are commonly included in general conditions of contracting, and the acceptance is done through the *click-wrapping* technique. The question is, under these circumstances, how to satisfy the formal validity requirement foreseen in Article 25, Section 1 (a) of Brussels I *bis* Regulation, not forgetting that the choice-of-court

[18] As it has been stated by ECJ, e.g. *Powell Duffryn plc and Wolfgang Petereit*, Case C-214/89, 10.03.1992, § 26; *Galeries Segoura SPRL v. Société Rahim* (1976) Case C-25/76, 14. February, § 6.

[19] Fausto Pocar has also the same opinion regarding Article 23, Section 2, of the Lugano Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, which has the same drafting as Article 23 of the Regulation No. 44/2001: Pocar, F. (2009) *Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, signed in Lugano on 30 October 2007 — Explanatory report.* JO C, 319, § 109.

agreement ascribes, unless otherwise contracted, exclusive jurisdiction to the chosen court (Article 25, Section 1).

First of all, it should be considered if a jurisdiction agreement established in general conditions referred by the contract is lawful. The ECJ has already held that such a clause is lawful if the contract signed includes an express reference to general conditions which include a jurisdiction clause.[20] However, the reference should be express, so that it

> *"[...] can be controlled by a party applying normal diligence and […] that the general conditions containing the jurisdiction clause was actually communicated to the other contracting party."*[21]

Secondly, it is important to consider Section 2 of Article 25, which clarifies that written form is the one that corresponds to *any communication by electronic means which provides a durable record of the agreement.* The explanation of this legal provision is found on the 2001 version of Brussels I Regulation: it is as a way to adapt the rule regarding jurisdiction agreements to e-commerce contracts. In the proposal of the European Commission, which introduces the rule, it can be read that

> *"[…] the need for an agreement "in writing or evidenced in writing" should not invalidate a choice-of-forum clause concluded in a form that is not written on paper but accessible on screen."*[22]

It results from the writing of the legal provision that the electronic communication, through which the jurisdiction agreement was settled, shall allow a durable record, which can be better achieved when communications between the parties, are done through e-mail, since, in this case, the electronic communication, where the jurisdiction agreement is stated, can be stored in the mail box, in the computer, in an external hard drive or can even be printed, as a last resource, allowing a durable record.

A situation that presents further complications to analyse is the one in which the contract is concluded on-line, on a website, being

---

[20] ECJ, *Trasporti Castelletti Spedizioni Internazionali SpA v. Hugo Trumpy SpA.Castelletti*, C-159/97, § 13; ECJ, Profit Investment Sim SpA, in liquidation v. Stefano Ossi et. al., C-366/13, § 26; *Hőszig Kft. v. Alstom Power Thermal Services*, Case C 222/15, § 39.

[21] *Hőszig Kft. v. Alstom Power Thermal Services*, (2016) Case C222/15, 7 July, § 40. Cfr., ECJ, *Estasis Saloti di Colzani (1976)* Case 24/76, 14. December, § 12.

[22] European Commission (1999) *Proposal for a Council Regulation (EC) on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.* Brussels, 14. 7. 1999, p. 18.

the jurisdiction agreement integrated in the general conditions of contracting, whose acceptance is done through a simple *"click"* in an acceptance message appearing on screen. In these cases, is the requirement of a *communication by electronic means which provides a durable record* of *the agreement* met?[23]

To answer this question, it is relevant to analyse ECJ decision, *Jaouad El Majdoub v. CarsOnTheWeb.Deutschland GmbH*[24], where a contract concluded on the Internet was at stake, in which no consumers were involved and that was concluded through the click-wrapping technique. *Jaouad El Majdoub* acquired an electric vehicle, at a favourable price, in *CarsOnTheWeb website*,[25] having the contract, subsequently, been cancelled by the seller because, allegedly, some damages have been detected in the vehicle at the time of its preparing to delivery. Non-accepting this unilateral behaviour of the seller, the buyer addressed himself to the German court, country where *CarsOnTheWeb* has its domicile, questioning the behaviour of that seller and requesting the compliance of the mentioned contract. Indeed, according to the general rules of Brussels I *bis* Regulation, namely its Article 4, Section 1, that court would have jurisdiction, according to the principle of the defendant´s domicile.[26] Note that the Regulation defines, on an autonomous way, the domicile of legal persons in its Article 63, as being the place where they have its statutory seat, its central administration or its principal place of business.[27]

In turn, the seller questioned the jurisdiction of the German court, alleging that in the general conditions of the contract concluded on the Internet, and accessible on the website used by the buyer, there was an jurisdiction agreement in favour of a Belgium court. *CarsOnTheWeb* also plead that the co-contractor of this contract, who should have been sued, was its parent-company established in Belgium, fact known to the buyer,

---

[23] It is excluded from this hypothesis those situations in which what appears on the screen corresponds to a mere invitation to a contract (in the sense that the page clarifies the conditions in which the trader is willing to contract) and in which the user is the one accessing the *website* and the one that starts the negotiating process, through certain behaviours which suggest the willingness of a legal binding, proceeding the responsible for the page to the subsequent acceptance of the submission, normally by *e-mail*.

[24] Case C-322/14 (2015), 21. May.

[25] In this case the contract was concluded online.

[26] The case was decided based on the Regulation No 44/2001, being the general rule established in Article 2, Section 1.

[27] Primitive Article 60 of the Regulation No. 44/2001.

since he had asked the Belgian parent-company the issuing of an invoice (request that was attended, with the identification of this company and its location) and the price of the vehicle was paid through a deposit in a Belgian account.[28]

The buyer questioned the formal validity of the jurisdiction agreement which was integrated in the general conditions of the contract, because he considered that the written form required and foreseen in the Regulation had not been complied, since the general conditions of the sell did not automatically open, nor at the moment of registration, nor at the moment of the buying operation. Instead, it was necessary to select a filed indicating "*click here to visualize the general conditions of supplying and payment"* in a new window.

From the case resulted also that the potential buyer would have to, expressly, accept those general conditions of the contract, by ticking in a box for that, before proceeding to a purchase. However, that behaviour did not, automatically, lead to the opening of the document which contained the general conditions of the seller, being, therefore, essential an additional click in an existing specific hyperlink.

The ECJ started by restate that the objective of the formal requirements, regarding the celebration of jurisdiction agreements, is to ensure the consensus of the parties, which happened in this case, because the buyer ticked in the existing box for that effect in the website, accepting the general conditions of the contract.[29] Furthermore, it was necessary to clarify the concept *communication by electronic means which provides a durable record of the agreement*. The ECJ had in account that the objective of the rule would be to equate to the written form, certain electronic communications aiming

[28] This information raises an important question, which was not object of assessment by the ECJ, because the jurisdiction agreement was considered valid. However, if it was not the case, it would be necessary to determine if the defendant should be *CarsOnTheWeb*, with its domicile in Germany, and to whom the website belonged and through which the contract was concluded, or if should be its parent-company, with its domicile in Belgium. Although this question is not included in the object of this study, if the contract was concluded with *CarsOnTheWeb*, as it seems resulting from the case, this one should be the defendant and, according to the general rule of Article 4 of Brussels I *bis* Regulation (previous Article 2, Section 1), the German court would be the competent one to assess the substantial request. It is clear that this conclusion depends on who is identified in the contract concluded, as a party in the contract, element that is not clarified in the case. However, this conclusion would arise the question of the need of an international elements in the legal relationship, as a necessary condition for the application of Brussels I *bis* Regulation, since the plaintiff had his residence in Germany. In the case the payment is done in an account located in Belgium, which means that, the obligation of compliance of the contract by the buyer, *i,e. The* payment of the price, is done in Belgium.

[29] ECJ, *Jaouad El Majdoub v. CarsOnTheWeb.Deutschland GmbH*, Case C-322/14, § 31.

to simplify the conclusion of electronic contracts, assuming that the accessible information through a screen is transmitted.[30] It is possible to establish here a parallelism with Article 224, Section 1, 1st part of the Portuguese Civil Code regarding the declaration of the will of negotiation which has a recipient: it becomes effective when the recipient acknowledges or comes into its possession, meaning that it is in condition of been known by him (Article 224, Section 3, a *contrario sensu*). The idea is the same, however, with the necessary adjustments to the contracting techniques by electronic means: the information which is available on a screen will be, indeed, known to the receiver or it is in condition to be known by him, if he chooses to. So, the possibility of registration ensures evidence of knowledge or the possibility of knowledge of the jurisdiction agreement, before the conclusion of the contract and the consequent acceptance of it with the conclusion of the electronic contract.

Therefore, according to ECJ

> *"in order for electronic communication to offer the same guarantees [as written communications], in particular as regards evidence, it is sufficient that it is "possible" to save and print the information before the conclusion of the contract."*[31]

So, the acceptance by *"clicking"* technique, allows recording and printing the general conditions of the contract before its conclusion, if the parties chooses to, not being necessary, for them to automatically open, at the moment of registration on the website or at the moment of buying.[32] in this particular case, the conclusion of the contract would involve a click-wrapping technique, which allowed the recording of the general conditions of the contract before its conclusion, by selecting a field that would open an access hyperlink to those conditions, being, therefore, satisfied the requirement of Article 25, Section 1(a).

Thus, to meet the condition of written validity established in Article 25, Section 1 (a), in electronic contracts, it is not necessary that an actual and permanent registration of the jurisdiction agreement occurs, but only the possibility to do a durable register of that agreement, either by printing,

---

30 ECJ, *Jaouad El Majdoub v. CarsOnTheWeb.Deutschland GmbH*, Case C-322/14, § 36.

31 Ibid.

32 CJEU, *Jaouad El Majdoub v. CarsOnTheWeb.Deutschland GmbH*, Cit., § 39.

either by digital recording, before the conclusion of the contract, which ensures the actual knowledge or possible knowledge of the jurisdiction agreement.

4. CONCLUSION

The purpose of this study was to analyse the legal framework of the jurisdiction agreement in international contracts concluded in the e-commerce. The choice of jurisdiction is a common practice in these contracts and, according to Brussels I *bis* Regulation, this agreement can be done, even when both parties are not domiciled in one Member-State (Article 25, Section 1).

The substantial validity of the jurisdiction agreement shall be assessed according to the law of the Member-State of the court that has jurisdiction, as stated by the jurisdiction agreement (Article 25, Section 1). On the other hand, the formal requirements are foreseen within the several subparagraphs of Article 25, Section 1, alternatively, aiming the safeguard of the actual existence of a consent between the parties. The formal requirement, which seems to be more difficult to accomplish in e-commerce, is the request that the conclusion of the agreement shall be in writing or verbally, with written confirmation [Article 25, Section 1(a)], as in electronic contracts, the jurisdiction agreements are commonly integrated in the general conditions of the contract, being that acceptance done through the click-wrapping technique.

Article 25, Section 2, which was introduced as a solution aiming the e-commerce contracts, clarifies that the written form equates to any *communication by electronic means which provides a durable register of the agreement*. So, it was necessary to ascertain if in contracts concluded on-line, whose acceptance is made through a simple *"click"* in an acceptance message appearing on screen, the requirement for a *communication by electronic means which provides a durable register of the agreement* is met and if it equates to a written form. After the analysis of ECJ recent jurisprudence, in the case of *Jaouad El Majdoub v. CarsOnTheWeb.Deutschland GmbH*, it can be concluded that, for the written validity requirement established on Article 25, Section 1(a) to be met in electronic contracts, it is not necessary that an actual durable register of the jurisdiction agreement exist, but only the possibility to do a durable register of that agreement, either by printing, either by digital recording

before the conclusion of the contract. That possibility of register ensures the actual knowledge or possibility of knowledge of the jurisdiction agreement.

LIST OF REFERENCES

[1] Beraudo, J-P. (2013) *Regards sur le nouveau règlement Bruxelles I sur la compétence judiciaire, la reconnaissance et l´execution des décisions en matière civile et commerciale.* Clunet, Vol. 3, pp. 741-763.

[2] European Commission (2010) *Proposal for a Regulation of the European Parliament and of the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.* COM 748 final, Brussels, pp. 1-105.

[3] European Commission (1999) *Proposal for a Council Regulation (EC) on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.* Brussels, 14. 7. 1999, COM 348 final, pp. 1-17.

[4] Gaudemet-Tallon, H. (2002) *Compétence et Exécution des Jugements en Europe, Règlement No. 44/2001.* Conventions de Bruxelles et de Lugano, 3rd ed., Montchrestien, L.G.D.J., Paris.

[5] Gonçalves, A.S.S. (2014) a *Revisão do Regulamento Bruxelas I Relativo à Competência Judiciária, ao Reconhecimento e à Execução de Decisões em Matéria Civil e Comercial*' in *Estudos em Comemoração dos 20 Anos da Escola de Direito da Universidade do Minho.* ed.] Mário Monte et al., Coimbra Editora: Coimbra, pp. 39-59.

[6] Gonçalves, A.S.S. (2016) *Cooperação Judiciária em Matéria Civil' in Direito da União Europeia,Elementos de Direito e Política da União, ed. Alessandra Silveira, Mariana Canotilho, Pedro Madeira Froufe.* Almedina: Coimbra, pp. 339-391.

[7] Hay, P. (2013) *Notes on The European Union´s Brussels-I "Recast" Regulation.* The European Legal Forum, Vol. 1, p. 3, pp. 1-8.

[8] Jenard, P. (1999) *Report on the Convention, of 27 September 1968, regarding the judiciary competence and enforcement of judgements in civil and commercial matters.* JO C 189, pp. 1-65.

[9] Magnus, U.(2012) *Prorogation of jurisdiction* in *Brussels I Regulation.* ed. U. Magnus and P. Mankowski, Sellier European Law Publishers, Munich, pp. 436-514.

[10] Nuyts, A. (2013) *La refonte du règlement Bruxelles I.* RCDIP, Vol. 1, pp. 1-63.

[11] Pocar, F. (2009) *Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, signed in Lugano on 30 October 2007 — Explanatory report.*

JO C, 319, pp. 1-56.

[12] Ratkovic, T. and Rotar, D.Z. (2013) *Choice-of-Court Agreements Under the Brussels I Regulation (Recast).* JPIL, Vol. 9 (2), pp. 245-268.

[13] Schlosser, P. (1990) *Report on the Convention on the Association of the Kingdom of Denmark, Ireland and the United Kingdom of Great Britain and Northern Ireland to the Convention on jurisdiction and the enforcement of judgments in civil and commercial matters and to the Protocol on its interpretation by the Court of Justice.* JO C 189, pp. 1- 81.

[14] Stone, P. (2008) *EU Private International Law, Harmonization of Laws.* Edward Elgar Publishing, Cheltenham – UK: Northampton – USA.

DOI: 10.5817/MUJLT2017-1-5

THE CJEU AS AN INNOVATOR – A NEW PERSPECTIVE ON THE DEVELOPMENT OF INTERNET RELATED CASE-LAW

by

ULF MAUNSBACH*

In this paper I will use concepts from innovation theory to analyse the work of the Court of Justice of the European Union in its important role as sole interpreter of EU law. In that regard, I define 'innovator' as one that facilitates use of new or existing inventions. Thus innovation is portrayed as a process in which several actors may contribute and where it all starts with an invention (the solution) and it ends with the innovation (the process of making use of the invention). The Court of Justice of the European Union may be an inventor in as much as it is allowed to invent solutions in order to solve new or existing problems, and it may be innovative in as much as it hands down judgments that shall be followed (i.e. it makes use of the invention).

The substance of the paper deals with case-law from the Court of Justice of the European Union in the field of cross-border infringements. The cases will be analysed in relation to the idea that legal decision-making can be described as an innovative process. An approach like this makes it possible to draw conclusions regarding the Court of Justice of the European Unions ability to innovate. It will be apparent that the Court is primarily concerned with so called reactive innovation (i.e. innovation that builds on existing knowledge). Only in exceptional circumstances do we find examples where the Court has proved to conduct in proactive innovation (i.e. inventing and applying new solutions) and this may, according to the author, prove to be a preferred standard. Better to drive safely than to drive in the ditch.

* Ulf.Maunsbach@jur.lu.se, Associate Professor of Law, University of Lund, Sweden.

KEY WORDS

Legal Innovation, Private International Law, Jurisdiction, EU Law, Court of Justice of the European Union (CJEU)

1. INTRODUCTION

If law were described as a construction that had the ability to be innovative, as I think it should be, the actors in the legal market – using innovation theory terminology – are important entrepreneurs and a necessary driving force in the innovation process.[1] Among such actors are the courts, and in the realm of EU law, the most important is the Court of Justice of the European Union (CJEU).

The CJEU, with its monopoly on interpretation of EU law and its capacity to hand down judgments that shall be followed by courts in Member States may be defined as both a potential inventor and a potential innovator. It may be an inventor in as much as it is allowed to solve problems with new solutions (e.g. invent new solutions to new or existing problems), and it may be innovative in as much as it hands down judgments that are decisive, e.g. there is a guarantee that the new suggested solution will be used by others, which generally is a central prerequisite for innovation.[2]

In this paper, I have no ambition to develop the idea to describe legal decision-making in terms of innovation, but I will use concepts from innovation theory to analyse the work of the CJEU in its important role as sole interpreter of EU law. In that regard, I define "*innovator*" as one that facilitates use of new or existing inventions. Thus innovation is portrayed as a process in which several actors may contribute and where it all starts with an invention (the solution) it ends with the innovation (the process of making use of the invention).

In relation to innovative legal decision-making, I have previously argued in favour of an approach that accentuates that the better innovator may be the actor that possesses the ability to listen, i.e. pick up inventive solutions

---

[1] See e.g Schumpeter, J.A. (1934) the Theory of Economic Development. Harvard University Press.; Rosenberg, N. and Birdzell, L.E. (1986) *How the West Grew Rich – the Economic Transformation of the Industrial World*. Basic Books.; Salzberger, Eli M., (ed.) (2012) *Law and Economics of Innovations*. Edward Elgar.

[2] See Maunsbach, U. (2017) *How to Facilitate Legal Innovations - Like Home Cooking with a Twist* [Online]. Owen Dixon Society eJournal. Available from: http://epublications.bond.edu.au/odsej/10 [Accessed 12 June 2017].

among the actors in the legal market and make use of them, rather than the actor that possesses the ability to invent. Irrespective of the efficiency aspect – that it is an advantage to benefit from the work already done by others – it is clear that the inventor ought to be separated from the innovator. Although these two quite frequently coincide – the inventor and the innovator might very well be the same actor – it is essential to stress that their skills differ. The inventor needs to be creative and focused (even narrow minded), whereas the innovator, as already stated, needs to listen, be open-minded and be ready to make use of inventive solutions irrespective of their origin.

Henceforth case-law from the CJEU in the field of cross-border infringements will be analysed in relation to the idea that legal decision-making can be described as an innovative process. An approach like this not only provides the author with a possibility to go through a number of cases that have already been studied exhaustively, it also (and hopefully more importantly) makes it possible to draw new conclusions in relation to CJEU actions regarding this important institution's ability to innovate. It also allows for some conclusions as to whether or not the CJEU is building on existing knowledge or inventing new solutions, i.e. if innovations from the CJEU are reactive or proactive.

From this starting point, I have decided to take a new look at the increasing case-load that deals with Internet related infringements (of different sorts). The aim in this paper is to shed new light on the on-going development and, if possible, to say something about the innovativeness in relation to how the CJEU is approaching problems related to the Internet. While analysing cases, I will primarily focus on the court's assessment of jurisdiction, i.e. how the court is interpreting different rules in the Brussels Ia regulation,[3] and not include various aspects that regard the interpretation of rules in other instruments. Particular attention will be paid to the CJEU's argument in relation to how Internet related problems are supposed to be handled, not only including arguments

[3] In this paper I will generally refer to Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels Ia Regulation), although most of the case-law analysed are actually interpreting its predecessor, Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. as regards the issues that are being dealt with in this paper the substantive rules are the same in both Regulations and I have therefore, throughout the paper, consistently taken the liberty of updating cases with references to the corresponding articles of the new regulation.

it aims at answering but also the questions that are actually dealt with in the case. Put differently, I will try to identify the solutions that are put forward by the CJEU, acknowledging the fact that the analytical framework is decided by the preliminary questions and that some of the reasoning is *obiter dictum*.

The structure of the paper is straight forward. I will start out with a presentation of the decided cases so far (until December 2016). Cases have been chosen due to their relevance in relation to the fact that they relate to problems as to jurisdiction in Internet related cases. I will cover the cases in chronological order starting with the *Pammer & Alpenhof* case of 7 December 2010 and ending with the Concurrence case of 21 December 2016.[4]

The purpose of the presentation is to pinpoint how the CJEU is addressing Internet related problems present in each case, and throughout the analysis I will keep to the following structure. Starting in Chapter Two, I will first specify the point of law that is relevant in the case. To a large extent, the national courts decide this inasmuch as it is the courts of the Member States that actually formulate the questions that need to be answered. It may, however, be necessary to clarify and/or rewrite the original questions, and it will be necessary to skip questions that aim at issues outside the scope of this paper. Secondly, I want to clarify the rule of law that may be derived from the case. This is, in the best of worlds, something directly provided for in the judgment, and I will primarily, for obvious reasons, derive my rules of law from this source. It may, however, be necessary to analyse the rule of law in light of the reasoning, and it will prove possible to rewrite the judgment into more abstract rules. Finally, I will focus on the mode of procedure, e.g. how the CJEU have actually approached the Internet challenge. It is primarily during this last stage of the presentation that it will be possible to say something about the innovativeness of the CJEU, although this

[4] Case covered in this survey are: C-144/09 & C-585/08 (*Pammer and Alpenhof*), 7 December 2010 (Grand Chamber), EU:C:2010:740; C-509/09 & C-161/10 (*E-date and Martinez*), 25 October 2011 (Grand Chamber), EU:C:2011:685; C-523/10 (*Wintersteiger*), 19 April 2012 (First Chamber), EU:C:2012:220; C-173/11 (*Dataco*), 18 October 2012 (Third Chamber), EU:C:2012:642; C-170/12 (*Pinckney*), 3 October 2013 (Fourth Chamber), EU:C:2013:635; C-387/12 (*Hi Hotel*), 3 April 2014 (Forth Chamber), EU:C:2014:215; C-360/12 (*Coty Germany*), 5 June 2014 (Forth Chamber), EU:C:2014:1318; C-441/13 (*Hejduk*), 22 January 2015 (Forth Chamber), EU:C:2015:28; C-322/14 (*El Majdoub*) 21 May 2015 (Third Chamber), EU:C:2015:334 and Case C-618/15 (*Concurrence*) on 21 December 2016 (Third Chamber), EU:C:2016:976.

analysis is primarily saved for the last section of the paper, Chapter Three, during which a concluding analysis will be presented.

2. AN INNOVATION ANALYSIS OF CJEU CASE-LAW

2.1 *PAMMER & ALPENHOF*

2.1.1 POINT OF LAW

On 7 December 2009, the Grand Chamber of the CJEU delivered its judgment in the joined *Pammer & Alpenhof* case.[5] In this landmark case, the CJEU had, for the first time, the opportunity to interpret the meaning of "*directed activities*" in relation to website activities within the frames of Article 17(1)c of the Brussels Ia Regulation. The case dealt with two similar situations. In the *Pammer* case, it was an Austrian consumer who was arguing for jurisdiction in Austria in relation to a dispute with a trader in Germany that according to the plaintiff (the consumer) had directed online activities to Austria in a way that made Article 17(1)c applicable. In the *Alpenhof* case, it was the other way around. A trader in Austria initiated proceedings in Austria against a consumer from Germany, who counterclaimed that there was no jurisdiction in Austria due to the fact that the trader had directed online activities towards Germany. By doing so, the same provision was made applicable (Article 17(1)c) with the consequence that the German consumer should benefit from the protecting rule in Article 18, stating that a consumer always can demand that a case against the consumer is to be tried in a court in the country of the consumers domicile. Both cases dealt with activities conducted on the Internet and the core issue was the interpretation of Article 17(1)c in the Brussels Ia Regulation and the prerequisite

> *"directing commercial or professional activities to the Member State of the consumers domicile"*.

The point of law of relevance dealt with in this case may consequently be stated in the following way: how is Article 17(1)c in the Brussels Ia Regulation and the expression

> "*directing commercial or professional activities to the Member state of the consumers domicile"*

[5] *Peter Pammer v. Reederei Karl Schlüter GmbH & Co KG and Hotel Alpenhof GesmbH v. Oliver Heller* (2010) joined cases C-585/08 and C-144/09, Court of Justice of the European Union (Grand Chamber), 7 December.

to be interpreted in relation to online activities? an alternative way of expressing this would be whether it is sufficient to be online or if some other website activities are necessary in order for a trader´s action to be regarded as directed to the Member State of the consumer's domicile in a way that makes the consumer-protection rules in the Brussels Ia Regulation applicable.[6]

2.1.2 RULE OF LAW

The rule of law that can be derived from the judgment in the *Pammer & Alpenhof* case may be framed as follows: if a trader is offering goods or services for online sales, the prerequisite "*directing professional activities*" in Article 17(1)c of the Brussels Ia Regulation is not satisfied merely due to the accessibility of the trader's website; but if it is apparent from the trader's, or an intermediary's, overall website activity that the trader was envisaging doing business (i.e. conclude contracts) with consumers in the Member State of the consumer's domicile, the requirements are satisfied.

The closer assessment as regards the prerequisite "*directing professional activities*" is for the national courts to ascertain, i.e. whether the overall website activity in case is sufficient for it to be regarded as "*directed activity*". The CJEU provides some additional help in as much as the judgment includes a non-exhaustive list of matters that may be evidence in support of a finding that a trader's activity is directed to the Member State of the consumer's domicile. The list comprises more or less obvious matters, and it highlights the importance of prior international trade, use of language and use of currency. It also places importance on more Internet-related matters like the use of country specific top-level domains and marketing activities by way of Internet referencing services.

2.1.3 MODE OF PROCEDURE

In its reasoning the CJEU is more elaborate than in the judgment. In relation to the list of factors that may constitute evidence regarding directed activities, the CJEU differentiates between "*patent evidence*" and other items

[6] *Peter Pammer v. Reederei Karl Schlüter GmbH & Co KG and Hotel Alpenhof GesmbH v. Oliver Heller* (2010) joined cases C-585/08 and C-144/09, Court of Justice of the European Union (Grand Chamber), 7 December. § 47.

of evidence. Patent evidence would, for example, be if it is mentioned on the trade's website that the trader is offering its goods or services in the consumer's Member Sate or if the trader has had expenditure for marketing activities in the consumer's Member State. Other items of evidence are such that, in combination with each other, may lead to the conclusion that a trader's activities are directed to another Member State. The list in the judgment includes examples from the latter group but not examples of patent evidence. Presumably this is due to the fact that patent evidence is regarded as obviously influential.[7]

The *Pammer & Alpenhof* case is a landmark case in as much as it discusses how directed professional activities are to be interpreted for the first time. In its reasoning, the Grand Chamber is attentive to specific Internet-related circumstances, and it acknowledges that the vulnerability of consumers increases due to the development of Internet communication.[8] Simultaneously, the CJEU shows an understanding as regards the fact that commercial online activities are ubiquitous and consequently globally assessable; it may prove difficult to delimit access to online offers, not least in light of the fact that there are mandatory requirements regarding some information that needs to be provided in the case of services offered online.[9] as a result, the trader must have manifested its intention to conduct business with the consumer in order to make Article 17(1)c applicable.

The *Pammer & Alpenhof* case may be framed as an innovative case, in as much as it shows that the CJEU possesses the ability to be attentive – adopting functional principles – in relation to a new problem, i.e. to what extent Internet related activities can be regarded as directed to a specific Member State. In this regard, this case, and the rule of law that may be derived from it, could be defined as a case that illustrates that the CJEU is reactive in its capacity as innovator. It actually strives to solve a new problem – by addressing the problem of how Internet related activities are supposed to be demarcated – but the solution is not an invention; it is rather

---

7 *Peter Pammer v. Reederei Karl Schlüter GmbH & Co KG and Hotel Alpenhof GesmbH v. Oliver Heller* (2010) joined cases C-585/08 and C-144/09, Court of Justice of the European Union (Grand Chamber), 7 December. § 81–83.

8 Ibid., § 62.

9 Ibid., § 68 and 78, with further reference to Article 5(1)c Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-commerce Directive). *Official Journal of the European Union* (2000/L 178/1) 17 July. Available from: http://data.europa.eu/eli/dir/2000/31/oj [Accessed 12 June 2017].

an interpretation based on existing knowledge applied in relation to a new problem.

2.2 *EDATE AND MARTINEZ*

2.2.1 POINT OF LAW

Almost one year later, on 25 October 2011, the Grand Chamber had the opportunity to add to the knowledge as regards Internet related activities in its judgment in the joined *eDate & Martinez* cases.[10] Both cases deal with Internet-related defamation where the action – the event that gave rise to damage – was located in one country and potential damages in another. In both cases, the plaintiff sued on basis of the special jurisdictional rule in Article 7(2) of the Brussels Ia Regulation, but not in the country where the tortious action took place and not in the country where the defendants were domiciled. In the *eDate* case, proceedings were brought before a court in Germany in relation to actions that took place on a website in Austria, and in the *Martinez* case proceedings were brought before a French court in relation to actions that took place on a website in the UK. In both cases, questions arose as to whether this special rule on international jurisdiction in Article 7(2) was applicable.

In addition to this question, the *eDate* case also includes a question as to applicable law and how the e-commerce directive is supposed to be interpreted. For the purpose of this paper, however, I will focus on the question regarding jurisdiction.

The point of law – with relevance for this study – in both cases is how the expression "*the place where the harmful event occurred or may occur*", in Article 7(2) of the Brussels Ia Regulation, is to be interpreted in the case of an alleged infringement of personality rights by means of content placed online on an Internet website.

2.2.2 RULE OF LAW

The CJEU provides an answer narrowed down to the specific situation that is relevant for a person in the event of an alleged infringement of personality rights by means of content placed online on an Internet website. In this specific situation, the rule of law is that a person who

[10] *eDate Advertising GmbH v. X and Olivier Martinez, Robert Martinez v. MGN Limited* (2010) joined cases C-509/09 and C-161/10, Court of Justice of the European Union (Grand Chamber), 25 October.

considers that his/her rights have been infringed may bring an action for liability under Article 7(2) in respect of all the damage caused before the courts of the Member State in which the centre of his/her interest is based.

This ruling, seen in light of prior case-law, means that Article 7(2) provides for three separate jurisdictional heads. The first two are derived from prior case-law.[11] Firstly, the plaintiff may bring an action before the courts of the Member State in which the publisher of the defamatory content is established. Secondly, the plaintiff may, instead of an action for liability in respect of all the damage caused, bring an action before the courts of each Member State in the territory of which content placed online is or has been accessible. This latter group of courts have jurisdiction only in respect of the damage caused in the territory of the Member State of the court seized. The third option is the inventive addition that is introduced by the *eDate & Martinez* case, namely a possibility for the plaintiff to bring an action covering all damage caused before the courts of the Member State in which the centre of the plaintiffs' interests is based.

2.2.3 MODE OF PROCEDURE

In this case, the CJEU is indeed both an inventor and innovator. The introduction of a third jurisdictional head based on the plaintiff's centre of interest is a novel solution. It is likely that inspiration is derived from similar solutions in common-law, where "*centre of interest theories*" are quite common[12] – but the way the CJEU is tailoring this idea in relation to online infringements of personality rights must be regarded as an invention. The reasoning in this regard is expressly emphasising the ubiquitous nature of the Internet. It initially departs from the *Shevill* case – in which the second jurisdictional head of Article 7(2) was defined – and it is concluded that the two connecting criteria in the *Shevill* case would provide the victim with a possibility to bring an action for damages against the publisher either before the courts of the Member State of the place where the publisher of the defamatory publication is established, which

[11] See further *Handelskwekerij G. J. Bier BV v. Mines de potasse d'Alsace SA* (1976) case C-21/76, Court of Justice of the European Union, 30 November. EU:C:1976:166. And *Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v. Presse Alliance SA* (1995) case C-68/93, Court of Justice of the European Union, 27 March.

[12] See e.g. Shapira, A., the *Interest Approach to Choice of Law*, Martinus Nijhoff, 1970.

have jurisdiction to award damages for all of the harm caused by the defamation, or before the courts of each Member State in which the publication was distributed and where the victim claims to have suffered injury to his reputation, which have jurisdiction to rule solely in respect of the harm caused in the State of the court seised.[13]

The CJEU then concludes that the Internet reduces the usefulness of the criterion defined in the *Shevill* case. It may prove difficult to delimit damage to a specific Member State when information is placed online, taking account to the ubiquitous nature of the Internet, and the risk of serious harm.[14] The CJEU is specifically emphasising

> "*the serious nature of the harm which may be suffered by the holder of a personality right who establishes that information injurious to that right is available on a world-wide basis.*"

It is in reaction to these considerations that the CJEU decides that it is necessary to invent a new jurisdictional head within the frames of Article 7(2).

Consequently, the *eDate & Martinez* case includes an inventive aspect that makes this case an example where the CJEU may be said to adhere to proactive innovation rather than reactive.

2.3. *WINTERSTEIGER*

2.3.1 POINT OF LAW

After the two landmark cases in 2010 and 2011, responsibility for the further development of case-law was handed over to the separate chambers of the CJEU. Consequently, on 19 April 2012, the First Chamber delivered its judgment in the case of *Wintersteiger*.[15] The dispute regards use of the Austrian, nationally registered, trademark "*Wintersteiger*". The Austrian proprietor of that trademark brought an action before an Austrian court, claiming that the defendant, a company residing

---

[13] *eDate Advertising GmbH v. X and Olivier Martinez, Robert Martinez v. MGN Limited* (2010) joined cases C-509/09 and C-161/10, Court of Justice of the European Union (Grand Chamber), 25 October. § 42, with further reference to *Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v. Presse Alliance SA* (1995) case C-68/93, Court of Justice of the European Union, 27 March. § 33.

[14] *eDate Advertising GmbH v. X and Olivier Martinez, Robert Martinez v. MGN Limited* (2010) joined cases C-509/09 and C-161/10, Court of Justice of the European Union (Grand Chamber), 25 October. § 45–47.

[15] *Wintersteiger AG v. Products 4U Sondermaschinenbau GmbH.* (2012) case C-523/10, Court of Justice of the European Union (First Chamber), 19 April.

in Germany, had infringed the Wintersteiger trademark by use of keyword advertising placed on the google.de website and that the use in question made Article 7(2) of the Brussels Ia Regulation applicable. The defendant contested jurisdiction arguing that advertisement on a website registered under a national top-level domain is directed to users in that country only.

Hence the question that eventually came before the CJEU regards what criteria are to be used to determine jurisdiction under Article 7(2) of Brussels Ia Regulation to hear an action relating to an alleged infringement of a nationally registered trademark through the use of a keyword identical to that trademark on the website of an Internet search engine operating under a top-level domain different from that of the Member State where the trademark is registered.[16]

2.3.2 RULE OF LAW

In relation to this question the rule of law that may be derived from the judgment of the CJEU may be framed as follows: when an actor places keyword advertising on a website identical to a trademark registered in a Member State, the top-level domain under which the website is registered has no influence on the question as to jurisdiction under Article 7(2) of Brussels Ia Regulation. Thus, an action relating to infringement in such a case may be brought before either the courts of the Member State in which the trademark is registered or the courts of the Member State of the place of establishment of the advertiser.

Put differently the CJEU acknowledges the first two jurisdictional heads of Article 7(2), but it disregards the third possibility that was provided by the *eDate & Martinez* case.

2.3.3 MODE OF PROCEDURE

In its reasoning the CJEU develops rather extensively why the circumstances in the case differ from those in the *eDate & Martinez* case, and it concludes that infringements of personality rights differ in important aspects from nationally registered trademarks. Personality rights are protected in all Member States, whereas nationally registered trademarks are protected in one country only and a proprietor of such a right cannot rely on protection outside the territory of the protecting country.[17] It is thus

[16] Ibid., § 17.
[17] Ibid., § 22–25.

logical, according to the CJEU, that the protecting country is the only place where damage in relation to infringement of a national trademark can take place and, therefore, courts in that country are best able to assess the infringement claim. Consequently the second jurisdictional head, based on damage, of Article 7(2) is applicable in the case and, in contrast to the situation in the *Shevill* case – taking account to the fact that a national trademark is limited to the territory of the protecting country – a court under that jurisdiction, as a matter of fact, will be competent to try all the damages that occur whereas there is no possibility that a nationally registered trademark can be harmed outside of the protecting country.

In relation to the first jurisdictional head of Article 7(2), based on the action – i.e. the event giving rise the damage – the CJEU focus on the activities performed by the advertiser. It is, according to the CJEU,

> "*the activation by the advertiser of the technical process displaying, according to pre-defined parameters, the advertisement which it created for its own commercial communications which should be considered to be the event giving rise to an alleged infringement, and not the display of the advertisement itself.*"[18]

In support of this finding, the CJEU refers both to prior case-law and the objective of foreseeability arguing that

> "*the place of establishment of that server cannot, by reason of its uncertain location, be considered to be the place where the event giving rise to the damage occurred […].*"[19]

The finding in the *Wintersteiger* case is rather reactive than proactive, and it is a case that fully supports the idea that intellectual property rights are territorial and hence best adjudicated in the country of protection.

---

[18] *Wintersteiger AG v. Products 4U Sondermaschinenbau GmbH*. (2012) case C-523/10, Court of Justice of the European Union (First Chamber), 19 April. § 34.

[19] Ibid., § 35–36. See also *Google France SARL and Google Inc. v. Louis Vuitton Malletier SA; Google France SARL v. Viaticum SA and Luteciel SARL and Google France SARL v. Centre national de recherche en relations humaines (CNRRH) SARL and Others* (2010) joined cases C-236/08, C-237/08 and C-238/08, Court of Justice of the European Union, (Grand Chamber), 23 March 2010.

2.4 *DATACO*

2.4.1 POINT OF LAW

The next relevant case to mention, after the *Wintersteiger* case, is the Third Chamber's judgment in the *Dataco* case.[20] The judgment was delivered on 18 October 2012, and it is worth mentioning in relation to the Brussels 1a Regulation, although this case primarily concerns applicable law. The dispute regards certain rights in relation to a database containing data collected from on-going football matches. The proprietor of this database, a UK-based company Football Dataco, claimed that the Swiss/German Company Sportsradar had infringed Football Dataco's rights and brought infringement actions before a UK court. In relation to the dispute at hand, there was two questions: one that related to the interpretation of the database directive and the concept of extraction and re-utilisation and one general question regaring where such an act takes place. In the following, I will concentrate my analysis on this latter question.

Thus the question that will be dealt with regards cross-border use of proprietary data and where such use takes place in situation where the information is stored on a server in one country and made available in another. This question relates in general terms to the wider issue how Internet-related acts are to be delimited and in that regard the problem is similar to the discussion about "*directed professional activities*" in the *Pammer & Alpenhof* case.

The point of law that is relevant in this part of the judgment can be phrased as follows: in a situation when someone located in one Member State extracts information stored on a server in another Member State, is the act of extraction taking place in the Member State where the server is located, in the Member State where the information is made available, or in both those States?[21]

2.4.2 RULE OF LAW

In relation to this question, the CJEU delivers a rather open-ended and inventive rule of law. It states that the act of extraction takes place, at least, in the Member State where the information is made available, where there is evidence from which it may be concluded that the act

[20] *Football Dataco Ltd and Others v. Sportradar GmbH and Sportradar AG* (2012) case C-173/11, Court of Justice of the European Union (Third Chamber), 18 October.

[21] Ibid., § 18

discloses an intention on the part of the person performing the act to target members of the public in that Member State. This rule of law is inventive in as much as it introduces "*intention*" as a pre-requisite for the localisation of use in a specific territory and it is open-ended in as much as it does not specify the closer meaning what "*intention to target*" may be, although some guidance is provide for in the reasoning.

The CJEU refers to the *Pammer & Alpenhof* case and suggest a similar list of criteria that may indicate intention, namely that there is evidence that business is conducted with users in the territory and whether country specific language is used. However, the examples are, in contrast to the list in the *Pammer & Alpenhof* case, not included in the judgment but provided in the reasoning *obiter dicta*.[22] It is also worth noticing that this judgment primarily deals with the issue whether UK database protection is applicable and not to what extent UK-courts have jurisdiction to hear the case, although the CJEU acknowledges that the question of localisation of a tortious act is liable to have an influence also on the question of jurisdiction.[23]

2.4.3 MODE OF PROCEDURE

The reasoning in the *Dataco* case follows rather closely the reasoning in the *Pammer & Alpenhof* case and the findings from this case is applied to a situation in which there are no objective to protect weak party interest. Specific account is taken of the ubiquitous nature of a website, and it is confirmed that the mere fact that a website is accessible in a particular national territory is not a sufficient basis for the localisation of an tortious act in that territory in relation to questions as regards applicable national law. If the mere fact of being accessible were sufficient, the CJEU concludes that there is a risk that certain conducts would wrongly be subject to the application of national laws that should not apply.[24]

Overall the reasoning in the *Dataco* case is attentive to Internet-related problems, and in this regard the judgment may be defined as proactive rather than reactive.

---

[22] *Football Dataco Ltd and Others v. Sportradar GmbH and Sportradar AG* (2012) case C-173/11, Court of Justice of the European Union (Third Chamber), 18 October. § 41–42.

[23] Ibid., § 30.

[24] Ibid., § 35–38.

2.5 *PINCKNEY*, *HI HOTEL*, *COTY GERMANY* AND *HEJDUK*

2.5.1 POINTS OF LAW

Following the Third Chamber's decision in the Dataco case, the Forth Chamber delivered a series of judgments regarding the closer meaning of Article 7(2) of the Brussels Ia Regulation in relation to different sorts of infringements: the *Pinckney* case on 3 October 2013,[25] the *Hi Hotel* case on 3 April 2014,[26] the *Coty Germany* case on 5 June 2014[27] and the *Hejduk* case on 22 January 2015.[28]

In these cases, there are a similar questions as regards international jurisdiction when the infringement claim is brought before courts in other Member States than the ones in which the tortious act took place.

In the *Pinckney* case, a composer (and proprietor of copyright) brought an infringement action before a French court against an Austrian actor who had reproduced CDs that had been marketed and sold online by UK companies. During the proceeding, the defendant contested that there was international jurisdiction in France; the question arose as to whether Article 7(2) of the Brussels Ia Regulation must be interpreted as meaning that where there is an alleged infringement of a copyright which is protected by the Member State of the court seised, that court has jurisdiction to hear an action to establish liability brought by the author of a work against a company established in another Member State, which has reproduced that work on a material support which is subsequently marketed by companies established in a third Member State through an Internet site which is also accessible in the Member State of the court seised.[29]

In the *Hi Hotel* case, different claims regarding copyright infringement were brought before a court in Germany (Cologne) by a photographer who had transferred rights to a number of photos of various rooms in a French hotel (Hi Hotel in Nice) under a transfer agreement that limited the use of the photos to Hi Hotel only. The photos later appeared in a book,

---

[25] *Peter Pinckney v. KDG Mediatech AG* (2013) case C-170/12, Court of Justice of the European Union (Forth Chamber), 3 October.

[26] *Hi Hotel HCF SARL v. Uwe Spoering* (2014) case C-387/12, Court of Justice of the European Union (Forth Chamber), 3 April.

[27] *Coty Germany GmbH v. First Note Perfumes NV* (2014) case C-360/12, Court of Justice of the European Union (Forth Chamber), 5 June.

[28] *Pez Hejduk v. EnergieAgentur.NRW GmbH* (2015) case C-441/13, Court of Justice of the European Union (Forth Chamber), 22 January.

[29] *Peter Pinckney v. KDG Mediatech AG* (2013) case C-170/12, Court of Justice of the European Union (Forth Chamber), 3 October. § 22.

published by a German publisher, that was available in a bookshop in Cologne and consequently proceedings were brought there. The defendant contested jurisdiction and argued that it possibly had made the photos available to the publisher's subsidiary in Paris and that it potentially was the subsidiary that passed them on to its German sister company. From the case it is apparent that there are several supposed perpetrators of the damage allegedly caused. On the basis of these conditions the point of law in relation to the proceedings is if Article 7(2) of the Brussels Ia Regulation should be interpreted as meaning that jurisdiction may be established with respect to one of those perpetrators who did not act within the jurisdiction of the court seised.[30]

In the *Coty Germany* case, proceedings were brought before a German court against a Belgian wholesaler who had sold perfumes through an intermediary in Germany that was claimed to infringe trademark rights in Germany. Due to the fact that the trademark in question was an EU trademark, protected under the EU trademark Regulation (which also regulates the competence of EU trademark courts)[31], the question that became relevant in relation to international jurisdiction in Germany regarded separate claims based on national German laws regarding unfair competition. Such claims are not covered by the EU trademark regulation, and consequently there is nothing in the EU trademark Regulation that prevents those claims from being brought before a court that is competent under the Brussels Ia Regulation. The point of law that will be further discussed is whether Article 7(2) must be interpreted as meaning that, in the event of an allegation of unlawful comparative advertising or unfair imitation of a sign protected by a EU trademark, prohibited by the law against unfair competition of the Member State in which the court seised is situated, that provision attributes jurisdiction to hear an action for damages based on that national law against one of the presumed perpetrators who is established in another Member State and is alleged to have committed the infringement in that State.[32]

---

[30] *Hi Hotel HCF SARL v. Uwe Spoering* (2014) case C-387/12, Court of Justice of the European Union (Forth Chamber), 3 April. § 23.

[31] See further Council Regulation (EC) No. 207/2009 of 26 February 2009 on the Community trademark (codified version) (EU-trademark Regulation). *Official Journal of the European Union* (2009/L 78/1) 24 March. Available from: http://data.europa.eu/eli/reg/2009/207/oj [Accessed 12 June 2017].

[32] *Coty Germany GmbH v. First Note Perfumes NV* (2014) case C-360/12, Court of Justice of the European Union (Forth Chamber), 5 June. § 39.

And finally, in the *Hejduk* case, claims regarding copyright infringement were brought before an Austrian court against a German defendant who had published photos on a German website supposedly not directed at Austria. The point of law was whether Article 7(2) must be interpreted as meaning that, in the event of an allegation of infringement of rights related to copyright which are guaranteed by the Member State of the court seised, that court has jurisdiction to hear an action for damages in respect of an infringement of those rights resulting from the placing of protected photographs online on a website accessible in its territorial jurisdiction.[33]

Simply put, the point of law in these four cases regards how acts that constitute distance delict, e.g. tortious act that takes place in one jurisdiction and that have effect in another, are to be handled within the frames of Article 7(2) of the Brussels Ia Regulation; it is therefore appropriate to summarise the findings in one general rule of law.

2.5.2 RULES OF LAW

Read together, the rule of law that may be derived from these four cases may be framed as follows: Article 7(2) provides for international jurisdiction based on the fact that damage occurred in the Member State of the court seised, and that court will be competent as regards damage that occurs in that country following an infringement conducted by a defendant domiciled in another Member State who has made copyright or trademark protected works assessable from the state of the court seised, irrespective of the fact that the defendant did not act in that state. In this regard, it is irrelevant if the defendant acted through intermediaries in other Member States. If jurisdiction is based on the occurrences of damages, the only prerequisite that is relevant is whether or not damage may occur in the Member Sate of the court seised, and regarding online infringement, it is sufficient for international jurisdiction under Article 7(2) if protected works has been made accessible in the country of the court.

2.5.3 MODE OF PROCEDURE

In their reasoning, the Fourth Chamber relates to the Shevill case in its assessment of jurisdiction under Article 7(2). The third jurisdictional head that was introduced in the e*Date & Martinez* case is not applicable,

[33] *Pez Hejduk v. EnergieAgentur.NRW GmbH* (2015) case C-441/13, Court of Justice of the European Union (Forth Chamber), 22 January. § 15.

nor is the discussion regarding intention to target from the *Dataco* case. Instead the Fourth Chamber confirms the idea that infringement claims based on national rights are best adjudicated in a court where the damage occurred (in a court where the act took place – which in the four cases coincides with the courts of the defendant's domicile).

In this regard, the judgments from the Fourth Chamber are obvious examples of reactive innovation where the CJEU is applying existing knowledge to further develop that understanding of Article 7(2).

2.6 *EL MAJDOUB*

2.6.1 POINT OF LAW

The next Internet-related case of relevance is the *El Majdoub* case, which was delivered by the Third Chamber on 21 May 2015.[34] The dispute regarded an agreement to purchase an electric car which, after the conclusion of the sales contract, was cancelled. The parties to the dispute had dissenting opinions as regarded the reasons for the cancellation, and the purchaser (a car dealer established in Cologne) brought action before a court in Krefeld (Germany) regarding the transfer of ownership of the vehicle in question. In that situation, the defendant (the seller) claimed that there was no jurisdiction. The principal argument in support of that claim was that a prorogation clause conferring jurisdiction on a court in Leuven (Belgium) was included in the general terms and conditions for Internet sales transactions and that this clause was applicable in the case due to the fact that the purchase was made from the sellers website, from which the terms and conditions was presented by way of a pop-up window that appeared and had to be clicked on in order to complete the purchase (i.e. click wrap agreement).

The question arose whether or not the terms and conditions (including the prorogation clause) had been validly incorporated into the sale agreement. In Article 25(2) of the Brussels Ia Regulation, it is made clear that a written prorogation clause provides for jurisdiction and that

> *"any communication by electronic means which provides a durable record of the agreement shall be equivalent to writing."*

[34] *Jaouad El Majdoub v. CarsOnTheWeb.Deutschland GmbH* (2015) case C-322/14, Court of Justice of the European Union (Third Chamber), 21 May.

Thus, the point of law that became relevant in the *El Majdoub* case was whether Article 25(2) of the Brussels Ia Regulation must be interpreted as meaning that the method of accepting general terms and conditions of contract for sale by "*click-wrapping*", concluded electronically, containing an agreement conferring jurisdiction, constitutes a communication by electronic means capable of providing a durable record of that agreement within the meaning of that provision.[35]

2.6.2 RULE OF LAW

As a response to the question raised, the CJEU gave a rather straight forward answer. The rule of law derive from the case is that Article 25(2) must be interpreted as meaning that the method of accepting the general terms and conditions of a contract for sale by "*click-wrapping*", concluded by electronic means, which contains an agreement conferring jurisdiction, constitutes a communication by electronic means which provides a durable record of the agreement within the meaning of that provision, where that method makes it possible to print and save the text of those terms and conditions before the conclusion of the contract.[36]

2.6.3 MODE OF PROCEDURE

The El Majdoub case concerns a novel question, and in that regard the case is a landmark case addressing a new Internet-related question for the first time. This may explain why the CJEU is rather developed in its reasoning. It starts out with a clear reference to the old Brussels Convention[37] and the fact that Article 25(2) was included in the first Brussels Regulation for a reason [at the time the rule was placed in Article 23(2)], namely to take account to the development of new methods of communication.[38] It then places importance on the wording and uses a literal interpretation to reach the conclusion that Article 25(2) is about providing a possibility, not a requirement that there should be a physical record of the agreement.[39]

---

35 Ibid., § 20.

36 Ibid., § 40.

37 1968 Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters (Consolidated version), *Official Journal of the European Union* (1998/C 27/1) 26 January. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:1998:027:TOC [Accessed 12 June 2017].

38 *Jaouad El Majdoub v. CarsOnTheWeb.Deutschland GmbH* (2015) case C-322/14, Court of Justice of the European Union (Third Chamber), 21 May. § 32.

39 Ibid., § 33–34.

In this regard, Article 25(2) differs from seemingly similar provisions regarding protection of consumers in respect of distance contracts, e.g. Article 5(1) of Directive 97/7/EC,[40] which expressively states that the consumer must receive written confirmation.[41] Due to the fact that there is no expressed consumer protection objective in relation to the application of Article 25(2), case-law regarding the application of directive 97/7/EC is not relevant in relation to the understanding of Article 25(2) of the Brussels Ia Regulation.[42]

In reaching the conclusion that there should be no requirement that there are written records of a potential agreement on jurisdiction, only a possibility to record a durable evidence of that agreement, I would describe the reasoning and the rule of law in this case as reactive even though it deals with a novel issue. It should be acknowledged that the CJEU establishes a new standard for click-wrap agreements, but they do not invent the idea that a click-wrap solution could amount to a binding agreement; they rather reason in relation to existing knowledge and apply that knowledge in relation to a new problem, hence an example of reactive rather than proactive innovation.

2.7 *CONCURRENCE*

2.7.1 POINT OF LAW

The final case that will be covered in this paper is the Third Chamber's judgment on 21 December 2016 in the *Concurrence* case.[43] In this case a French retailer, Concurrence, brought action against Samsung as regarded a selective distribution agreement that prevented Concurrence from selling Samsung products through its website. Concurrence questioned the legality of this part of the agreement, with reference to the fact that several other retailers where allowed to conduct online sales. In the dispute before the French court, Concurrence brought actions in relation to both Samsung, regarding the selective distribution agreement, and against several branches

[40] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts. *Official Journal of the European Union* (1997/L 144/19) 4 June. Available from: http://data.europa.eu/eli/dir/1997/7/oj [Accessed 12 June 2017].

[41] *Jaouad El Majdoub v. CarsOnTheWeb.Deutschland GmbH* (2015) case C-322/14, Court of Justice of the European Union (Third Chamber), 21 May. § 37–38.

[42] Ibid., § 38.

[43] *Concurrence Sàrl v. Samsung Electronics France SAS and Amazon Services Europe Sàrl* (2016) case C-618/15, Court of Justice of the European Union (Third Chamber), 21 December.

of Amazon with the view to obtain an order requiring the withdrawal of any offers for sale of Samsung products directed to the French market that affected Concurrence position as distributor of those products. The lower instances dismissed the claims against Amazon due to lack of jurisdiction and the case was appealed to the Court of Cassation which decided to stay proceedings and forward a preliminarily question to the CJEU.

The point of law relevant in the case may be framed as follows: how shall Article 7(2) of Brussels Ia Regulation be interpreted for the purpose of conferring the jurisdiction given by that provision to hear an action to establish liability for infringement of the prohibition on resale outside a selective distribution network resulting from offers, on websites operated in various Member States, of products covered by that network.[44]

2.7.2 RULE OF LAW

In response to the questions asked, the Third Chamber provides a judgment that comprises a rule of law that states that Article 7(2) of Brussels Ia Regulation must be interpreted, for the purpose of conferring the jurisdiction given by that provision to hear an action to establish liability for infringement of the prohibition on resale outside a selective distribution network resulting from offers, on websites operated in various Member States, of products covered by that network, as meaning that the place where the damage occurred is to be regarded as the territory of the Member State which protects the prohibition on resale by means of the action at issue, a territory on which the appellant alleges to have suffered a reduction in its sales.[45]

2.7.3 MODE OF PROCEDURE

This case is closely linked to the line of case-law already derived from the CJEU, and it supports the idea that courts in countries in which tortious effect occurs will always be component to try claims regarding that effect. It has been emphasised in relation to infringements of intellectual property rights, in relation to unfair marketing activities and now in relation to loss in sales as regards claims based on arguments related to acts of unfair competition and selective distribution arrangements. In this

[44] Ibid., § 24.
[45] Ibid., § 35.

regard, this is a case that confirms the strict application of Article 7(2) in as much as it places importance on the difference between the place where action was committed and the place where damaged occurs; courts in this latter place are best equipped to assess claims in relation to the damage that occurred in that country. Hence, the Third Chamber in this case proves to adhere to reactive innovation.

3. CONCLUSIONS

After having assessed the Internet related cases chosen for this paper, with the ambition to penetrate the findings in light of innovation theory, it is now time to draw some tentative conclusions.

One observation would be that the CJEU is reactive rather than proactive. Among the cases dealt with in this paper only two can be defined as proactive, the *eDate & Martinez* case from the Grand Chamber and the *Dataco* case from the Third Chamber, in as much as the CJEU in those two cases actually invented new solutions. Interestingly enough it is apparent that these inventive solutions has not yet been confirmed and applied in later case-law. In contrast to this, it may be stated that reactive cases are more frequently followed. This may be explained by the obvious reason that it is more appropriate to deliver a judgment that is in line with prior case-law than it is to start from a blank sheet and invent a new solution. It may also be stated that there are reasons to be cautious in relation to inventiveness, due to the fact that inventive solutions are less likely to be accepted as a logical continuation of the legal development.

Another reflection in relation to the proactive solution that was chosen in the *Dataco* case is that this case actually deals with choice of law rather than jurisdiction. In this regard, it can be concluded that there are more profound reasons to be cautious as to the interpretation of rules regarding jurisdiction, due to the fact that it is inappropriate to investigate substantive issues at the jurisdictional stage of the proceedings, which may be required if the circumstances of the case are to be assessed in a proactive way. The fact that the issue in the *Dataco* case related to the application of national (substantive) law may be the primary reason that explains why the Third Chamber dared to invent a new solution.

As regards the organisation of the CJEU in different chambers, it can furthermore be concluded, perhaps not surprisingly, that inventiveness and proactive innovation primarily seems to reside in the Grand Chamber

and that the separate chambers, with the exception of the Third Chamber, adhere to reactive innovation in as much as they are more literal in their approach to the problems at hand and more faithful to prior case-law.

From this analysis a cautious conclusion may be drawn in relation to a plaintiff that is about to bring proceedings before a court. It matters how the claims are framed. If the plaintiff wants to plead for new inventions, it may prove problematic if the preliminary question regards jurisdiction, and if that is the case, the remaining hope for an inventive solution is that the CJEU decides to answer the question at hand with a judgment from the Grand Chamber. if the ambition is to urge for inventiveness, which by no reason must be a preferred choice, there seems to be better odds to get a proactive judgment if the preliminary questions deals with substantive law. In this regard, it may be stated that the parties to a dispute, irrespective of the fact that it is the national courts that formulate preliminary questions, have an influence over the proceedings by the way they actually formulates their claims.

A final conclusion, in line with the theme of this paper, would be that the analysis confirms that the CJEU is predominantly reactive in its approach to innovation. When it has challenged the conventions – and adhered to proactive innovation – it has seemingly delivered less influential judgments. This conclusion supports the idea that courts shall primarily be reactive and listening – and that there is a danger if courts adhere to untamed inventiveness. Better to listen to the development and adhere closely to a logical line of cases bearing in mind that it is sensitive to speed up the legal development. In this regard, legal developments, according to the CJEU, resemble a slogan that would be fit for a Volvo: *drive safe*.

LIST OF REFERENCES

[1] *Concurrence Sàrl v. Samsung Electronics France SAS and Amazon Services Europe Sàrl* (2016) case C-618/15, Court of Justice of the European Union (Third Chamber), 21 December.

[2] *Coty Germany GmbH v. First Note Perfumes NV* (2014) case C-360/12, Court of Justice of the European Union (Forth Chamber), 5 June.

[3] *eDate Advertising GmbH v. X and Olivier Martinez, Robert Martinez v MGN Limited* (2010) joined cases C-509/09 and C-161/10, Court of Justice of the European Union (Grand Chamber), 25 October.

[4] *Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v. Presse Alliance SA* (1995) case C-68/93, Court of Justice of the European Union, 27 March.

[5] *Football Dataco Ltd and Others v. Sportradar GmbH and Sportradar AG* (2012) case C-173/11, Court of Justice of the European Union (Third Chamber), 18 October.

[6] *Google France SARL and Google Inc. v. Louis Vuitton Malletier SA; Google France SARL v. Viaticum SA and Luteciel SARL and Google France SARL v. Centre national de recherche en relations humaines (CNRRH) SARL and Other*s (2010) joined cases C-236/08, C-237/08 and C-238/08, Court of Justice of the European Union, (Grand Chamber), 23 March 2010.

[7] *Handelskwekerij G. J. Bier BV v. Mines de potasse d'Alsace SA* (1976) case C-21/76, Court of Justice of the European Union, 30 November.

[8] *Hi Hotel HCF SARL v. Uwe Spoering* (2014) case C-387/12, Court of Justice of the European Union (Forth Chamber), 3 April.

[9] *Jaouad El Majdoub v. CarsOnTheWeb.Deutschland GmbH* (2015) case C-322/14, Court of Justice of the European Union (Third Chamber), 21 May.

[10] Maunsbach, U. (2017) *How to Facilitate Legal Innovations - Like Home Cooking with a Twist* [Online]. Owen Dixon Society eJournal. Available from: http://epublications.bond.edu.au/odsej/10 [Accessed 12 June 2017].

[11] *Peter Pammer v. Reederei Karl Schlüter GmbH & Co KG and Hotel Alpenhof GesmbH v. Oliver Heller* (2010) joined cases C-585/08 and C-144/09, Court of Justice of the European Union (Grand Chamber), 7 December.

[12] *Peter Pinckney v. KDG Mediatech AG* (2013) case C-170/12, Court of Justice of the European Union (Fourth Chamber), 3 October.

[13] *Pez Hejduk v. EnergieAgentur.NRW GmbH* (2015) case C-441/13, Court of Justice of the European Union (Fourth Chamber), 22 January.

[14] Rosenberg, N. and Birdzell, L.E. (1986) *How the West Grew Rich – the Economic Transformation of the Industrial World*. Basic Books.

[15] Salzberger, Eli M., (ed.) (2012) *Law and Economics of Innovations.* Edward Elgar.

[16] Shapira, A. (1970) *The Interest Approach to Choice of Law*. Martinus Nijhoff.

[17] Schumpeter, J.A. (1934) *The Theory of Economic Development*. Harvard University Press.

[18] *Wintersteiger AG v. Products 4U Sondermaschinenbau GmbH*. (2012) Case C-523/10, Court of Justice of the European Union (First Chamber), 19 April.

DOI: 10.5817/MUJLT2017-1-6

THE NOTIFICATION REQUIREMENT IN TRANSBORDER REMOTE SEARCH AND SEIZURE: DOMESTIC AND INTERNATIONAL LAW PERSPECTIVES[*]

by

ANNA-MARIA OSULA[**], MARK ZOETEKOUW[***]

Modern criminal investigations increasingly rely on evidence that is not in a tangible format and can no longer be assumed to be located close to the locus delicti or the perpetrator. This article focuses on the notification requirement embedded into the legal regimes regulating one of the available investigative measures employed to access data stored in digital devices – remote search and seizure. The article will first analyse whether there is an obligation under international law to notify the other state about such a transborder investigative measure. Then we will compare the notification requirements for remote search and seizure in three countries' domestic law: in Estonia, the Netherlands and the United States. Finally, we will draw conclusions on the principal challenges related to the implementation of the notification requirement under the domestic regulation. These involve balancing, on the one hand, the difficulties in identifying the location and the identity of the possible suspect and, on the other hand, the need to provide the involved individuals' protection as guaranteed by the principles of fair trial and effective remedy.

[*] Both authors have contributed equally to this article. The views expressed herein are those of the authors and do not reflect the policy or the opinion of any other entity.

[**] Anna-Maria Osula, Ph.D., is a researcher at NATO CCD COE, Estonia and a lecturer at Tallinn Univeristy of Technology, Estonia.

[***] Mark Zoetekouw is a Ph.D. researcher at Utrecht University, the Netherlands and senior Legal Advisor Cybercrime & Digital Technology at the Dutch National Police.

KEY WORDS

Remote Search and Seizure, Notification, Fair Trial, Effective Remedy, Law Enforcement

1. INTRODUCTION

Modern criminal investigations increasingly rely on evidence that is not in a tangible format and can no longer be assumed to be located close to the locus delicti or the perpetrator. Instead, evidence may be stored in electronic devices located in foreign territories or in cloud service providers' servers. Furthermore, due to the Internet's decentralised nature and easily accessible anonymising tools, the exact location of the evidence may not be able to be determined at all.

However, these technological developments for storing and transmitting data and tools enabling the anonymisation of one's identity and footprints in the virtual world should not handicap the efforts of law enforcement (LE) in investigating crime. In the arms race between LE and criminals, LE must be equipped with effective investigative tools to counter such complex circumstances.

This article focuses on one of the available investigative measures employed to access data stored in digital devices: remote search and seizure. Traditionally, search and seizure represents a coercive power used for accessing and seizing tangible items. In the context of digital evidence and depending on the peculiarities of domestic legal regimes, search and seizure may also be used for accessing, copying and seizing data stored in domestically located devices situated on the premises specified in a search warrant. Remote search and seizure signifies searches that are either undertaken by extending the original search and seizure to devices accessible from the originally searched device (and these accessible devices may also be located outside the original premises of the search) or by remotely conducting search and seizure from other (such as the LE's own) devices.

Both – accessing data from the initially searched devices on the premises of the search or from LE's own devices – are increasingly employed in practice by LE notwithstanding whether the physical location of the data (storage) has been identified, or not.

The possible extraterritorial reach of such investigative measures has raised questions regarding their overall legality under international law.[1] Instead of revisiting this debate, the article will focus on something that has received much less attention: the obligation of notifying the involved parties about a search that has taken place.

This obligation is commonly enshrined in the domestic regulation of criminal procedure with the general aim to respect the principles of effective remedy and fair trial as set out in art. 13 and art. 6 of the European Convention of Human Rights (ECHR).[2] It is generally accepted that providing notice of a search is an obligation of investigative bodies, prosecutors' offices or courts.[3] One of the goals of notification is to explain to the participants of the proceedings the objective of the investigative measure and the rights and obligations of the involved parties, thereby granting everyone whose rights and freedoms have been violated the right of recourse to the courts.[4] Such access to the courts would be effectively non-existent if knowledge of the execution of the measure were to remain unknown to the involved parties.

In some countries, remote access to data may alternatively or additionally be regulated under surveillance activities. Similarly, in these

---

1 E.g. Goldsmith, J. (2001) *The Internet and the Legitimacy of Remote Cross-Border Searches*. University of Chicago Law School, Chicago Unbound. Available from: http://chicagounbound.uchicago.edu/cgi/viewcontent.cgiarticle=1316&context=public_law_and_legal_theory [Accessed 8 March 2017]; Koops, B.-J. and Goodwin, M. (2014) *Cyberspace, the Cloud, and Cross-Border Criminal Investigation*. Tilburg University, Tilburg Institute for Law, Technology, and Society, WODC. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2698263 [Accessed 8 March 2017]; Osula, A.-M. (2015) *Transborder Access and Territorial Sovereignty.* Computer Law & Security Review, 31(6); Zoetekouw, M. (2016) *Ignorantia Terrae Non Excusat*. Available from: https://english.eu2016.nl/documents/publications/2016/03/7/c-mzoetekouw---ignorantia-terrae-non-excusat---discussion-paper-for-the-crossing-borders---jurisdiction-in-cyberspace-conference-march-2016---final [Acessed 8 March 2017]; see also Svantesson, D. (2016) Preliminary Report: Law Enforcement Cross-Border Acces to Data, pp. 4-5, 9. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874238 [Accessed 8 March 2017].

2 Council of Europe, *European Convention on Human Rights*, 1950.

3 See e.g. *Kriminaalmenetlusseadustik (Code of Criminal Procedure), RT I 2003, 27, 166; RT I, 31.12.2016, 46*. Estonia: Riigi Teataja. In Estonian. § 8(1). Also see art. 94 *Wetboek van Strafvordering (Dutch Criminal Procedure Code, DCPC hereafter)*, the Netherlands. In Dutch. For particularly search and seizure of goods and art. 125i jo. 125m DCPC for "*seizing*" data. The legal history on art. 126bb DCPC, while not immediately applicable to search and seizures, offers much insight into the status of notification in Dutch law in general. See footnote 8 and sub-section 3.2.2.

4 E.g. *Eesti Vabariigi põhiseadus (Constitution of the Republic of Estonia),* RT 1992, 26, 349; RT I, 15. 5. 2015, 2. Estonia: Riigi Teataja. In Estonian. § 15(1); Kergandberg, E. and Pikamäe, P. (2012) *Kriminaalmenetluse seadustik: kommenteeritud väljaanne (Code of Criminal Procedure: Commented Edition)*. Tallinn: Juura, p. 271. See e.g. 'Appeal against Activities of Investigative Body or Prosecutor's Office' Division 5 in Estonia, Kriminaalmenetlusseadustik (Code of Criminal Procedure), footnote 3.

cases the requirement of (eventual) notification is also an undisputed element of the legal regime which in addition to the already quoted basic rights touches upon the inviolability of private and family life,[5] human dignity[6] and the general right to access information held by government agencies and local authorities.[7]

But how is the requirement of notification carried out during remote search and seizure? When accessing data stored on the territory of the other state, would domestic, or international law require the notification of the other state or would such behaviour be rather regarded as a polite gesture? In particular, do the traditional means of notification that have been used to inform the suspect regarding e.g. searching his/her house suffice in the context of remote searches? How does and should domestic regulation balance on the one hand the difficulties in identifying the location and the identity of the possible suspect, and on the other hand, the need to provide the involved individuals' protection as guaranteed by the principles of fair trial and effective remedy?

In order to answer these questions, the article will first look into the notification issue from the perspective of international law. The article will then turn to analysing three examples of domestic regulation in countries where the reforms of codes of criminal procedure are in different stages. Firstly, Estonia is a case study of a domestic approach where the traditional search and seizure regime is not yet taking into account the possibility of remote search and seizure and therefore illustrates well the shortcomings of the traditional notification requirements. Secondly, the Netherlands showcases a regulation which already considers the peculiarities of remote search and seizure, but is nevertheless undergoing substantial reforms. Thirdly, the United States (US) recently passed amendments to its Federal Rules of Criminal Procedure which now also address search and seizure in situations where the location of the data has been concealed. Based on the comparison of these three examples we

[5] Eesti Vabariigi põhiseadus, footnote 4, § 26.

[6] Eesti Vabariigi põhiseadus, footnote 4, § 10.

[7] Eesti Vabariigi põhiseadus, footnote 4, § 44(3). See also exceptions to the general right; see also Kergandberg and Pikamäe, footnote 4, p. 328. *Grondwet (The Dutch Constitution), the* Netherlands. In Dutch. Article 110 charges the government to be transparant in the excution of its tasks. See also for specific rules, The *Wet Openbaarheid Bestuur (Governance Transparency Act),* the Netherlands. In Dutch. While the Dutch Constitution does grosso modo to provide the same basic rights as the Estonian Constitution, because of particularities of Dutch law (and the system being moderately monistic in nature) reference will more likely be made to treaties such as the ECHR to achieve the same effects.

will draw conclusions on the principal challenges related to the domestic regulation of notification of search and seizure and examine whether notification of a foreign state is, or should be considered obligatory in the case of transborder search and data seizure.

2. NOTIFICATION IN INTERNATIONAL LAW

Reservations about the possible impact of territorial sovereignty are one of the main issues holding back a wider agreement on the use of remote investigative measures such as remote search and seizure, or "*transborder access*" in terms of art. 32(b) of the Council of Europe (CoE) Convention on Cybercrime.[8] Notification of the state on whose territory the investigatory measure is affected or ends up being affected might appease some of these reservations. However, does such an obligation exist under international law? Who decides who is notified of what and at what point in time?

The drafters of the CoE Convention on Cybercrime discussed the requirement of notification as part of the established search and seizure regime. They noted that while not obligatory for the Parties of the Convention, some states may consider the notification requirement as an essential feature of the search and seizure measure with the general aim to distinguish between (generally non-surreptitious) computer search of stored data and (covert) interception of data in transmission in their domestic legislation.[9] As such a notification prior to the search may prejudice the investigation, the legislator was suggested to consider notifying the persons concerned after the search has been carried out.[10] Due to the difficulties in determining the physical location of the data to be searched (or more specifically the storage medium upon which it resides), it might be problematic to identify who ought to be notified at all. But no attention was given to that topic at the time.

---

[8] Council of Europe, Convention on Cybercrime, ETS No. 185.

[9] Council of Europe (2001) *Explanatory Report to the Convention on Cybercrime (ETS No. 185)*. Sec. 204. Available from: https://rm.coe.int/CoERMPublicCommonSearchServices/ Display DCTMContentdocumentId=09000016800cce5b [Accessed 8 March 2017]. The requirement of notification was also discussed at the G8 in 1999 but never made it to the actual wording of art. 32(b). See Council of Europe (2012) *Transborder Access and Jurisdiction: What Are the Options?*, pp. 6-7. Available from: https://rm.coe.int/CoERM PublicCommonSearch Services/DisplayDCTMContentdocumentId=09000016802e79e8 [Accessed 8 March 2017].

[10] Council of Europe, *Explanatory Report to the Convention on Cybercrime (ETS No. 185)*, footnote 9, sec. 204.

In fact, the explanatory notes to the convention make it very clear that the issue of notification is left for domestic legislation. One of the most prominent examples of domestic regulation including the requirement to notify another state about the remote search and seizure of data stored in its territory can be found in the Belgium Code of Criminal Procedure (BCCP). BCCP art. 39bis § 3 (previously art. 88ter) allows under certain conditions the public prosecutor (previously: investigative judge) to issue a warrant to extend a computer search to a computer system or part thereof, even if it is located in a place other than the location of the initial search performed. If the data is not situated in domestic territory, it can only be copied (and not, for instance, made inaccessible), and the public prosecutor should communicate this information to the Department of Justice, who shall inform the competent authorities of the state concerned if it can be identified.[11] However, since practice has shown that it is very difficult to determine the exact location of the data, the possibility of informing the other state has been rarely exercised, even if the provision is used often for accessing data not stored domestically.[12] Confusingly, given the text of BCCP art. 88ter (old) and art. 39bis (current), Belgium practitioners in several meetings[13] have seemed to posit an approach going beyond this. The (paraphrased) reasoning then seemed to be that if the information is accessible from the Belgium territory, its seizure is not considered extraterritorial even if the data is stored abroad as the act of seizing is executed domestically. In other words, it is the place of the LE officer acting or "*looking*" that is apparently considered the sole location of the act – disregarding the fact that the data was retrieved for viewing or copying from "*elsewhere*".

We have found no basis in international law for a specific obligation to notify the other state about a transborder investigative measure even if considerations of comity may be proposed as a reason for states to notify nevertheless. This would still not, however, imply that transborder investigative measures would be legal by default. Rather, we believe that a unilateral notification, whether before, or after the search, would not

[11] *Code d'Instruction Criminelle (Belgium Code of Criminal Procedure*), Livre Premier, Belgium. In French. Art 39bis § 3.

[12] Interview with Mr. Geert Schoorens, Federal Prosecutor's Office of Belgium, 2015. Quoted in Osula, A.-M. (2016) *Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study*. International Journal of Law and Information Technology 24(4), pp. 365-366.

[13] Amongst those: the Council of Europe Octopus 2015 meeting and the Crossing borders: Jurisdiction in Cyberspace conference of 7-8 March 2016.

impact the assessment of the legality of the transborder investigative measure. Nevertheless, while bearing no apparent legal weight under international law, the gesture of notification may be beneficial for the diplomatic relationship between countries.

3. NOTIFICATION IN DOMESTIC LAW

3. 1 ESTONIA

3.1.1 REMOTE SEARCH AND SEIZURE IN DOMESTIC LAW

In Estonia, the principal provision regulating traditional search and seizure powers is Code of Criminal Procedure (CoCP) § 91. Due to the coercive nature of the search and seizure powers, it is considered as possibly one of the most serious violations of the principle of the inviolability of the home[14] and secrecy of communication.[15]

The provision prescribes that search and seizure must be conducted for the purposes outlined in law and its objective is to locate an object to be confiscated or used as

> *"physical evidence, a document, thing or person necessary for the adjudication of a criminal matter, property to be seized for the purposes of compensation for damage caused by a criminal offence or of confiscation, or a body, or to apprehend a fugitive in a building, room, vehicle or enclosed area."*[16]

While it can generally be concluded from case law and legal commentary that evidence in digital form is accepted in courts like any "*tangible*" evidence,[17] it is not evident whether CoCP § 91 would also cover the search of the devices found on the premises subject to a search warrant.[18] Since the provision has been interpreted as to not allow

---

[14] Eesti Vabariigi põhiseadus, footnote 4, § 33; Kergandberg and Pikamäe, footnote 4, p. 268.

[15] Eesti Vabariigi põhiseadus, footnote 4, § 43; Lõhmus, U. (2014) *Põhiõigused kriminaalmenetluses (Fundamental Rights in Criminal Procedure*). 2nd ed. Tallinn: Juura, p. 312.

[16] Kriminaalmenetlusseadustik (Code of Criminal Procedure), footnote 3, § 91(1), § 64(3).

[17] Estonian CoCP does not specifically include the concept of digital evidence but *lex lata* has been interpreted to also cover evidence in digital form. CoCP's lack of clarity regarding digital evidence has been subject to critique in recent research. See e.g. Ginter, J. et al (2013) *Analüüs isikute põhiõiguste tagamisest ja eeluurimise kiirusest kriminaalmenetluses (Analysis of Ensuring Fundamental Rights and the Speed of Preliminary Investigation in Criminal Procedure)*, pp. 148-151. Available from: http://www.kriminaalpoliitika.ee/en/analuus-isikute-pohioiguste-tagamisest-ja-eeluurimise-kiirusest-kriminaalmenetluses [Accessed 8 March 2017]. See also Osula, Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study, footnote 12, pp. 356-359.

[18] Lõhmus, footnote 15, pp. 312-313.

the digital environment or a computer system as an objective of a search,[19] it is doubtful whether the current CoCP § 91 alone can, in addition to seizing the device where the data is stored, also be applied for searching the data located on the device.

However, when applied together with "*Inspection*" [CoCP § 83, § 86(2)], it is clear that CoCP § 91 may be used to access data stored on electronic devices.[20] For example, in circumstances where an immediate examination of the evidence found on the search premises is not reasonable due to the amount of data and the time needed for listing all the documents in the search protocol, LE can decide that the evidence should be seized for later inspection.[21] Inspection can be used for collecting

> "*information necessary for the adjudication of a criminal matter, detect the evidentiary traces of the criminal offence and confiscate objects which can be used as physical evidence*",

and objects for inspection can include a

> "*document, other evidence or any other object or physical evidence.*"[22]

Nevertheless, it is unclear whether CoCP § 91 alone or in conjunction with CoCP § 83, § 86(2) would offer legal bases for remotely accessing and seizing data, or whether the CoCP surveillance activities[23] should be employed instead. Hopefully the ongoing CoCP reform[24] will clarify the current ambiguity of domestic regulation and thereby offer better protection against possible breach of basic rights.[25]

3.1.2 NOTIFICATION REQUIREMENT FOR REMOTE SEARCH AND SEIZURE IN DOMESTIC LAW

As explained, the Estonian law does not clearly regulate remote search and seizure. Therefore it is not evident what the notification requirement

---

[19] Kergandberg and Pikamäe, footnote 4, p. 269; Lõhmus, footnote 15, p. 313.

[20] Kergandberg and Pikamäe, footnote 4, p. 269.

[21] Kergandberg and Pikamäe, footnote 4, p. 253.

[22] Kriminaalmenetlusseadustik (Code of Criminal Procedure), footnote 3, § 83(1)-(2).

[23] Kriminaalmenetlusseadustik (Code of Criminal Procedure), footnote 3, chap. 31.

[24] Estonia, *Justiitsministeerium, Kriminaalmenetlusõiguse revisjoni lähteülesanne (Initial Task of the Revision of the Law of Criminal Procedure)*, 2015. Available from: http://www.just.ee/sites/www.just.ee/files/kriminaalmenetluse_revisjoni_lahteulesanne.pdf [Accessed 8 March 2017].

[25] Lõhmus, footnote 15, pp. 310, 313.

for remote search and seizure would entail. However, if we take the traditional search and seizure as an example, we would turn to CoCP § 91(7). It prescribes that a search warrant has to be presented for examination to the person

> "*whose premises are to be searched or to his or her adult family member or a representative of the legal person or the state or local government agency whose premises are to be searched.*"

The search warrant identifies what is being searched for, what the objectives of the search are, the reasons for the search as well as the place where the search is conducted [CoCP § 91(4)]. The warrant will have to be signed by the individual to whom the warrant is presented [CoCP § 91(7)]. In the current wording, it appears to be difficult to directly apply the notification requirement in remote search and seizure circumstances, especially with regards to the requirement of signing the warrant, as LE officials carrying out remote searches do generally not come into direct contact with the involved individual.

Remarkably, the regulation does not prescribe an option to delay the notification for search and seizure, such as is possible under the surveillance activities regime. With regard to the latter, a general legal obligation exists to notify

> "*the person with respect to whom the surveillance activities were conducted and the person whose private or family life was significantly violated by the surveillance activities and who was identified in the course of the proceedings*".[26]

This notification explicitly includes explaining the procedure for appeal.[27] However, CoCP § 126^{13}(2) allows a surveillance agency, with the permission of a prosecutor, not to give notification of conduct of surveillance activities if this may

> "*significantly damage the criminal proceedings; significantly damage the rights and freedoms of another person which are guaranteed by law or endanger another person, or endanger the confidentiality of the methods and tactics of a surveillance agency, the equipment or police agent used*

[26] Kriminaalmenetlusseadustik (Code of Criminal Procedure), footnote 3, § 126^{13}(1).
[27] Kriminaalmenetlusseadustik (Code of Criminal Procedure), footnote 3, § 126^{13}(7).

in conducting surveillance activities, of an undercover agent or person who has been recruited for secret cooperation."

The rest of CoCP § 126[13] regulates the conditions for extending the period of non-notification.

3.1.3 NOTIFICATION REQUIREMENT IN THE CASE OF "LOSS OF LOCATION"

Given the traditional focus on tangible items and the overall critique towards the need to update the current search and seizure regime, the circumstances where it is not possible to identify the location of the data to be remotely searched, are not addressed in current regulation. According to practitioners, no specific internal guidelines exist which would help to clarify the details of undertaking remote search and seizure in case of "*loss of location*".[28] It has been suggested that such guidelines should be established and different options for going forward should be examined and assessed domestically, taking into account both national and international restrictions. Any possible extraterritorial reach of the search (or another investigative measure) should be legally justified, though no specific proposals have been made. Circumstances, such as danger to life or "*loss of location*" under which remote access to data stored in another territory may be necessary, should be determined domestically and, if possible, agreed upon internationally.[29]

3.2 NETHERLANDS

3.2.1 REMOTE SEARCH AND SEIZURE IN DUTCH DOMESTIC LAW

In the Netherlands, search and seizure for LE purposes is regulated in the Dutch Criminal Procedure Code[30] (DCPC) art. 94-99 and art. 110. Depending on the infringement on the right to privacy inherent to that type of location,[31] the competent authority to lead or authorise the search ranges from any law enforcement officer via public prosecutor to investigation judge.

---

[28] Interview with Ms. Eneli Laurits, Estonian Public Prosecutor, 2015; Interview with Mr. Robert Laid, Estonian Assistant Prosecutor, 2015; Interview with Mr. Oskar Gross, Police and Border Guard Board, 2017. Quoted in Osula, A.-M. (2017) *Remote Search and Seizure of Extraterritorial Data*. University of Tartu Press, p. 60.

[29] Osula, Remote Search and Seizure of Extraterritorial Data, footnote 28, pp. 58-62.

[30] DCPC, footnote 3.

However, data in the Netherlands are regarded as non-objects which, bar a few exceptional circumstances based on jurisprudence,[32] for that reason cannot be stolen or fenced or seized by LE in the traditional sense of the law. Instead, they are considered a class of their own.[33] As (regular) seizure is a concept limited to physical objects, "*data seizure*" has received its own definition that allows for it to be taken into the possession or copied for law enforcement purposes.[34] For the purposes of this article we will call this "*data seizure*".[35]

Currently search and data seizure in the Netherlands is limited to situations where physical premises are searched with the express purpose of data seizure.[36] Computers or data storage devices, whether local or remote, are not considered "*premises*" and as such cannot be the target locations of a regular search and seizure.[37] If relevant to the investigation,

---

[31] Under Dutch law a general stratification is made with regards to the inherent privacy of certain locations. In general, homes are more private than a private building that in turn is more private than a vehicle and ultimately a public area. The minimum level of authority that should give the permission is tied to that general stratification.

[32] As a result of jurisprudence there is a category of data under Dutch law that is still considered to be objects. In order for this to happen data has to have similar characteristics to real objects. The most important one of these is the fact that in the case of transfer of an object from one person to another the former must necessarily lose possession of it. This is an uncommon characteristic for data as it can usually be shared and multiplied with losing control of the original data or reducing its quality. See *Runescape* (2012), Hoge Raad, ECLI:NL:HR:2012:BQ9251 and *Habbo Hotel* (2009), Rechtbank Amsterdam, ECLI:NL:RBAMS:2009:BH9789.

[33] Article 80quinquies *(Wetboek van Strafrecht, Dutch Criminal Code – DCC hereafter)*, the Netherlands. In Dutch, defines data "*as any representation of facts, concepts or instructions organised in an standardized format suitable for transfer, interpretation or processing by persons of automated works*" (read: computers, see also footnote 39). This may also include written and printed texts. This definition carries over into the DCPC, footnote 3, though this is not made explicit in the law.

[34] DCPC, footnote 3, art. 125i regulates the existence of this special data seizure as well as the conditions under which it may take place.

[35] A more correct translation – given the discussion in Dutch law about the difference in nature between goods and data – would probably "*securing of data*". For this article we will however use "*data seizure*".

[36] Although if a premise is searched under this power and potentially relevant computers or data storage found they may, under circumstances, still be physically seized for investigation. The Dutch legislator has however indicated that search and data seizure should be used unless taking the objects is absolutely necessary as a matter of subsidiarity. Differently put, as long as there is a reasonable option to take just the data, use of seizure of the data carrier is not allowed. There are of course also other ways for law enforcement to obtain relevant data, such as wiretaps (both voice and data) [DCPC, footnote 3, art. 126m / t / zg] and production orders for all manner of data [DCPC, footnote 3, art. 126n to 126ni] to almost any party in possession of such data.

[37] The law references back to the articles for physical seizure for conditions and competent authorities. DCPC, footnote 3, art. 126n to 126ni jo. DCPC, footnote 3, art. 96b, 97.

data may be seized subject to the same conditions and under the same competent authorities as regular objects.[38]

If devices are found during the execution of the search and data seizure which have access to data stored on remote "*automated works*",[39] those remote systems may be searched as well and any data required to "*uncover the truth*"[40] seized. A simple example of this might be a Network Attached Storage or "*standalone*" hard disks where daily backups of laptops are stored. One important limitation is that such remote data seizure may only take place to the extent that the persons working or residing in the physical place being searched have lawful access to (parts of) those remote systems. Differently put, if such persons have unlawful access to (parts of) such a remote machine, that machine may not be searched in the course of the search and data seizure execution. Currently the law does not specifically provide for remote access outside of the search location.[41]

3.2.2 NOTIFICATION REQUIREMENT FOR REMOTE SEARCH AND SEIZURE IN DOMESTIC LAW

Under Dutch law, notification is considered an essential part of civil rights and liberties and the obligation to notify involved parties after the use of investigatory measures in integrated throughout the DCPC. The Dutch legislator considers the duty to notify corollary to the right to effective remedy as guaranteed by art. 13 ECHR.

In principle, search and data seizure is done "*in the open*" like regular search and seizure. This means that in standard circumstances no attempt is made to (temporarily) hide the fact a search and data seizure took place. Contrary to most other investigatory powers, for which notification is regulated in art. 126bb DCPC, notification for search and data seizure is regulated separately, in art. 125m DCPC. If any data seizure has taken place, the article stipulates all "*involved parties*" should be notified in writing

[38] In practice this requirement is not followed too strictly; however, some sensible (possible) connection to the investigation should exist.

[39] This is the direct translation of the Dutch term defined in DCC, footnote 33, art. 80sexies. The definition also includes automation such as routers, smart watches etc. Under the new Computercriminaliteit III (Computercrime III) law proposal, the definition will be changed to be even more comprehensive. The term however, is clunky even in Dutch, so we will use more regular terms for the remainder of the article.

[40] Dutch police in an criminal investigation are tasked to uncover the truth whatever it may be.

[41] We may, however, soon see a testcase where the search is not formally closed and then "*continued*" from a remote location, the police station. It then becomes a remote remote search. It is unclear whether the judiciary would agree to this.

of the fact that search and data seizure took place as well as the general nature of the data seized data as long as this is reasonable possible.[42]

In principle all relevant parties[43] must, within reason, be notified of an investigatory measure. Information about the kind and general extent of data seized should be included in the notification as to allow involved parties to determine if and how much their rights may have been infringed. This does not create an obligation to provide a detailed list or description of all data seized.

The involved parties that should be notified are the suspect, the party responsible for the data and the rightful owner or user or inhabitant of the physical premises searched. However, notification of the suspect may be omitted if he will be made aware of the fact though the official documents in his case (which he will receive at the latest at the moment of his indictment).[44]

In deviation of the law regulating regular search and seizure the public prosecutor in charge of the data search and seizure, or the investigate judge if he was the authority executing the search, is explicitly given the legal possibility to postpone notification of all involved parties as long as the due course of the investigation would be negatively impacted due to notification as per art. 125m, lid 2 DCPC.

3.2.3 NOTIFICATION REQUIREMENT IN THE CASE OF "LOSS OF LOCATION"

Currently no particular legislation exists in the Netherlands to deal with the problem of "*loss of (knowledge of) location*".[45] As discussed above, the law does not expect "*unreasonable*" effort to notify. Not knowing who to address or where could clearly fall under this limitation. However from the legislative documents it is clear that cyberspace and a habitual situation of "*loss of location*" was not particularly on the legislators mind. The legislator seems to have assumed that any inadvertent cross-border

[42] The legislators intent here is not to overburden law enforcement with (neigh) impossible tasks such as for instance finding a suspect who has left for another country, current location unknown.

[43] Explicit reference is made in the legislatory documents to Recommendation R(95) 13 of the Council of Europe defining "*involved parties*" with regards to investigatory measures with regards to data, extending the parties to be notified from previous legislation.

[44] More detailed rules apply in particular circumstances, but are beyond the scope of this article.

[45] See Koops and Goodwin, footnote 1, pp. 8-9 for a distinction between the two. In practice both meanings are relevant.

search and data seizure would be an exception and employing the MLA procedures the traditional means to be employed.[46]

Habitual loss of location potentially adds a new relevant "*involved*" party to the mix, i.e. the state in which the remote data was (as determined eventually) seized. However, the legislator's intent to create a limited list of parties to be notified is clear in the legislative documents,[47] and foreign states are not on the list.

However, new law currently being developed is (likely) going to change relevant legislation with regards to search and data seizure.

The first of these law proposals is the Dutch Computer Crime III law proposal which was passed by the House of Commons in December 2016 and is currently awaiting continuation of the legislative process.[48] If this law passes, remote search and data seizure will no longer be tied to the search of physical locations. Instead systems or "*devices*" may be remotely targeted. After considerable debate, the power for remote search and seizure on systems or devices has been limited to crimes which carry a maximum penalty of eight years imprisonment minimum or crimes that will be specifically listed in lower regulation.[49] This is a significant increase from earlier plans[50] and together with other results from parliamentary

---

[46] See Tweede Kamer (2004/2005), *Kamerstukken II 2004/2005*, 26 671, nr. 10, p. 23. Available from: https://zoek.officielebekendmakingen.nl/kst-26671-10.pdf [Accessed 8 March 2017].

[47] Tweede Kamer, (1998/1999), *Kamerstukken II 1998/1999*, 26671, 3, p. 52. Available from: https://zoek.officielebekendmakingen.nl/kst-26671-3.pdf [Accessed 8 March 2017].

[48] All official documents pertaining to this law proposal can be found under parliamentary file number 34372. An overview of the current state of the law proposal as well as all official documents can be found at the site of 1e Kamer, where the proposal is currently awaiting being put on the agenda to be discussed. Eerste Kamer, *afdeling Inhoudelijke Ondersteuning en de unit Communicatie & Protocol*. Available from: https://www.eerstekamer.nl/wetsvoorstel/34372_computercriminaliteit_iii [Accessed 8 March 2017].

[49] Eerste Kamer (2015/2016), *Kamerstukken I 2015/2016, 34372*, A p. 5, art. 126nba (1), second section and under d. Available from: https://zoek.officielebekendmakingen.nl/kst-34372-A.pdf [Accessed 8 March 2017]; Tweede Kamer (2004/2005), *Kamerstukken II 2015/2016* Kamerstukken II 2015/2016, 34372, 4, p. 5. Available from: https://zoek.officiele bekendmakingen.nl/kst-34372-4.pdf [Accessed 8 March 2017]; Tweede Kamer (2004/2005), *Kamerstukken II 2015/2016* Kamerstukken II 2015/2016, 34372, 34, item 17. Available from: https://zoek.officielebekendmakingen.nl/kst-34372-17.pdf [Accessed 8 March 2017]; Tweede Kamer (2015/2016), *Kamerstukken II 2015/2016*, 34372, 34, item 25. Available from: https://zoek.officielebekendmakingen.nl/kst-34372-25.pdf [Accessed 8 March 2017]; Tweede Kamer (2004/2005), *Kamerstukken II 2015/2016*, Handelingen II, 2015/2016, 34372, 34, item 26, p. 17, 29, 42-44, 52. Available from: https://zoek.officielebekendmakingen.nl/kst-34372-26.pdf [Accessed 8 March 2017].

[50] See the Internet consultation on this law proposal: Kennis- en exploitatiecentrum Officiële Overheidspublicaties, *Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (Computercriminaliteit III).* Available from: https://www.internet consultatie.nl/computercriminaliteit/document/727 [Accessed 8 March 2017]. The proposed article was at that time known as 125ja Sv (DCPC).

proceedings dramatically reduces the number of situations in which such a remote search and seizure may be executed.

This new remote search and data seizure is classified as a "*special investigatory measure*". Notification for this new investigatory measure will therefore be regulated by art. 126bb DCPC, the general notification article for the Dutch special powers of investigation. The differences with the notification for art. 125m DCPC are limited, which is not surprising as the legislator explicitly took art. 126bb DCPC as the model for art. 125m DCPC.[51] The article will still not count "*foreign states*" under the "*parties involved*" that need to be notified, although extensive coverage in the legislative proceedings make it clear the government is aware of the issue.

The government has stated during the legislative process that the Netherlands, when engaging in (potentially) cross-border investigative activity, will in principle stop the activity and notify the state involved when the physical nexus of the activity becomes apparent and is outside Dutch territory. From the wording, however, it is clear that this is seen as a matter of comity and not of legal obligation.[52] According to the government, the possibility of "*loss of location*" and difficulties with the requirement of notification should not be an absolute barrier to (potentially) cross-border investigations.[53]

At the very least this seems to be a new direction that introduces a divide in the DCPC. For instance, current legislation for placing a wiretap on a phone when it is known to be active in the territory of another state or when this becomes apparent during the wiretap, would in principle require notification and consent of that state.[54]

A second relevant law proposal is a significant redraft of the complete DCPC. It is too early to talk about specific content and consequences of this proposal, since it is unlikely to enter into force before 2022 and its drafting is currently very much in initial stages. Nevertheless, the intent

---

[51] Tweede Kamer (2003/2004), *Kamerstukken II 2003/2004,* 29441, 3, p. 19. Available from: https://zoek.officielebekendmakingen.nl/kst-29441-3.pdf [Accessed 8 March 2017].

[52] Tweede Kamer (2015/2016), *Handelingen II 2015/2016, 34372, 34, item 26*, pp. 42, 43, 45. Available from: https://zoek.officielebekendmakingen.nl/h-tk-20162017-34-26.pdf [Accessed 8 March 2017].

[53] Tweede Kamer (2015/2016), *Handelingen II 2015/2016, 34372, 34, item 26*, p. 45. Available from: https://zoek.officielebekendmakingen.nl/h-tk-20162017-34-26.pdf [Accessed 8 March 2017].

[54] DCPC, footnote 3, art. 126ma.

of the legislator, as apparent from the first draft put up for Internet consultation,[55] does not seem to indicate significant changes to the general ideas behind notification, nor do the plans seem to include notification of a foreign state when an investigation turns cross-border beyond any such requirements already existent in current law.

3.3. UNITED STATES

Rule 41 of the Federal Rules of Criminal Procedure (FRCP) regulates the procedures for obtaining a search warrant in federal court. The US has recently amended FRCP Rule 41 so that it now also allows for remote search warrants as well as physical search warrants. Under the amended FRCP Rule 41, a judge can now issue warrants to gain "*remote access*" to computers "*located within or outside that district"* in cases in which the

> "*district where the media or information is located has been concealed through technological means"*

and a search of multiple computers in numerous districts would be allowed.[56] From the reading of the new text of the law, which allows to target data when the location of the data is unknown, it follows that possible extraterritoriality cannot be always avoided.

---

[55] See Ministerie van Veiligheid en Justitie, *Memorie van Toelichting: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek*. Available from: https://www.rijksoverheid.nl/documenten/kamerstukken/2017/02/07/memorie-van-toelichting-vaststellingswet-boek-2-van-het-nieuwe-wetboek-van-strafvordering-het-opsporingsonderzoek [Accessed 8 March 2017] – preliminary numbering (these numbers will change in a later stage of the legislative procedure) section 7.3.1/art. 2.7.3.1.1, pp. 184-188. Confusingly, as these legislative processes are running parallel, this proposal is not taking into account the changes due to be made through the Wet Computercriminaliteit III yet.

[56] The previous wording of Rule 41 entailed a territorial limitation to the locations within the district. See United States Courts (2016) *Current Rules of Practice & Procedure, Criminal Rules 4, 41, and 45, Redline of Amended Rules, Including Committee Notes* pp. 10-14. Available from: http://www.uscourts.gov/file/21315/download [Accessed 8 March 2017]. See also US Government's comments on extraterritoriality at United States Department of Justice (2013) *Mythili Raman Letter to Advisory Committee on the Criminal Rules.* Available from: http://justsecurity.org/wp-content/uploads/2014/09/Raman-letter-to-committee-.pdf [Accessed 8 March 2017].

The amendments were target to a substantial criticism,[57] cautioning that such transborder access would result in serious diplomatic consequences,

> "*with short-term FBI investigations undermining the long-term international relationship building of the US State Department"*

and possible quick escalation of responses.[58]

In terms of notification, FRCP Rule 41 (f)(1)(c) prescribes that, in case of remote search and seizure,

> "*the officer must make reasonable efforts to serve a copy of the warrant and receipt on the person whose property was searched or who possessed the information that was seized or copied"*.

The means of accomplishing the notification may among others include electronic means, reasonably calculated to reach that person. Such wording has received critique as it does not set an absolute obligation to provide the notice but instead requires the officer to make "*reasonable efforts"*, thereby casting doubt to the "*constitutional adequacy"* of the warrant.[59] Professor Orin Kerr has warned that since a remote search is essentially a secret search, there is nothing about the search itself to provide notice, and therefore this may signify a shift from a standard of notice searches to a standard of delayed notice (aka "*sneak and peek"*) searches.[60]

---

[57] E.g. Rule 41 Coalition Letter (2016). Available from: https://noglobalwarrants.org/assets/Rule41CoalitionLetter.pdf [Accessed 8 March 2017]; Reitman, R. (2016) *With Rule 41, Little-Known Committee Proposes to Grant New Hacking Powers to the Governmen*t, Electronic Frontier Foundation. Available from: https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government [Accessed 8 March 2017]; Tor Project Blog (2016) *Day of Action: Stop the Ch*anges to Rule 41. Available from: https://blog.torproject.org/blog/day-action-stop-changes-rule-41 [Accessed 8 March 2017] inviting the US Congress to support the "*Stop Mass Hacking Act*".

[58] Pilkington, E. (2014) *FBI Demands New Powers to Hack into Computers and Carry out Surveillance.* [Online] The Guardian. Available from: http://www.theguardian.com/us-news/2014/oct/29/fbi-powers-hacking-computers-surveillance [Accessed 8 March 2017]. Read more at e.g. Thompson II, R. (2016) *Digital Searches and Seizures: Overview of Proposed Amendments to Rule 41 of the Rules of Criminal Procedure*. Congressional Research Service. Available from: https://www.fas.org/sgp/crs/misc/R44547.pdf [Accessed 8 March 2017]; Osula, Transborder Access and Territorial Sovereignty, footnote 1, p. 731.

[59] American Civil Liberties Union, *ACLU Comment on the Proposed Amendment to Rule 41 Concerning Remote Searches of Electronic Storage Media* (2014) p. 15. Available from: https://www.aclu.org/sites/default/files/assets/aclu_comments_on_rule_41.pdf [Accessed 8 March 2017] quoting *United States v. Freitas*, 800 F.2d 1451,1456 (9th Cir. 1986) [citing *Berger v. New York*, 388 U.S. 41, 60 (1967)].

[60] United States Courts (2014). Advisory Committee on Rules of Criminal Procedure - April 2014., p. 252. Available from: http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-april-2014 [Accessed 8 March 2017].

Another concern was that the new wording gives LE the option to leave the notice at the third-party service providers as the (legal) person whose property was searched. However, this would not guarantee the actual target of the search to get the notice, thereby leaving him/her without the possibility to challenge the search warrant.[61]

The government's response to the above-mentioned critique explained that the wording of the provision was chosen to provide a parallel system to notices in physical searches where similarly, in case of not being able to deliver a notice to the person from whom, or from whose premises, the property was taken, the copy of the warrant and receipt may be left at the place where the officer took the property.[62] Upon government's request, the notice may be delayed "*only if authorised by a statute"* [Rule 41 (f) (3)].[63]

There have also been proposals from academics suggesting that in case it would inadvertently turn out that the subject of the search is located outside the territory of the US, the foreign government should be immediately notified and general information about such searches and their circumstances reported and made public to the extent possible, unless there are grounds to believe that that such notification would significantly jeopardize the investigation.[64] Currently, such an option is not foreseen in the law.

4. DISCUSSION

This article compared three countries' domestic regulation of the notification requirement under the remote search and seizure regime. The regulation of notification in none of these countries has been free from critique and as can be seen below may differ significantly.

	Netherlands	United States	Estonia
Regulation of search and seizure of digital evidence	DCPC art. 94, 94a, 95-97, 110, 125i, 125j, Awbi art. 2-6, 10	FRCP Rule 41	Somewhat unclear but generally CoCP § 91 and CoCP § 83, § 86(2)

[61] ACLU suggests that notice should be given to both. American Civil Liberties Union, footnote 59, p. 16.

[62] United States Courts (2015). Advisory Committee on Rules of Criminal Procedure - May 2015, p. 93. Available from: http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-may-2015 [Accessed 8 March 2017].

[63] See generally, Thompson II, footnote 58, p. 10.

[64] Daskal, J. (2016) *Rule 41 Has Been Updated: What's Needed Next* [Online] Just Security. Available from: https://www.justsecurity.org/35136/rule-41-updated-needed/ [Accessed 8 March 2017].

Regulation of remote search and seizure	DCPC 125i, 125m, 125j	FRCP Rule 41	Not explicitly regulated
Notification requirement	DCPC 94 (3) (providing a description of assets seized), 125m, Awbi art. 11	FRCP Rule 41 (f)(1)(c) "*must take reasonable efforts*"	CoCP § 91(7) but does not take into account the characteristics of remote search and seizure
Possibility to delay the notification of search and seizure	DCPC 125m (only for search and data seizure 125i DCPC cases), Awbi art 11 (2)	FRCP Rule 41 (f)(3)	Not regulated under the search and seizure regime but mentioned under surveillance activities

Tab. 1: Comparison of the domestic regulation of the Netherlands, United Nations and Estonia

Firstly, we observe that the increasingly occurring circumstances of "*loss of location*" are making it difficult for the legislator to directly employ the traditional notification regime designed for searching and seizing tangible items. Examples were presented in this article where the notification of the involved parties would require signing the warrant which may be challenging in situations where LE does not have direct contact with the individuals in question. Particularly, we would like to point out the difficulties in defining "*reasonable effort*" which needs to be made by the LE in identifying the individual to be notified. On the one hand, a relatively low threshold of the "*effort*" would probably speed up the investigation, but at the same time would not aim to grant the widest possible protection for the actual targets of the search. On the other hand, too high of a threshold would saddle LE with an unmanageable task as well as (depending on domestic regulation) increase the risk of procedural errors. The more detailed meaning of "*reasonable effort*" will probably develop with emerging case law.

Secondly, we can see that countries are having trouble in identifying the "*involved parties*" whose rights may have been infringed upon and who should therefore be notified about the employment of the investigative measure. In the cases of the Netherlands and the US, the issue has been under discussion, whereas in Estonia the legal debate has not yet reached these questions as part of the on-going CoCP reform. We believe that the standard approach should be the requirement to notify person in overall control of the computer system which was remotely searched or data to be

targeted by the remote search and seizure. If the actual target of the search cannot be reasonably identified, a third party service provider may be notified instead. Notification of all parties of whom relevant data was found during the search could be considered as an option but should not be a legal obligation as this may place to great a burden on the investigation.

Thirdly, we suggest including an explicit possibility of a delayed notice for the notification requirement of the remote search and seizure regime, such as foreseen by the Dutch and US legislation. This option may be connected with specific exigent circumstances and should be accompanied with further regulation on the conditions for postponing the notification as not to allow for avoiding the notification requirement altogether.

Fourthly, we conclude that despite all countries being aware of the fact that remote search and seizure may add foreign states to the list of parties whose rights have been infringed upon, only Belgium law currently requires the foreign state, within reason, to be notified. Failure to do so however is not considered a critical breach of law as apparent from case law.[65] It has also been suggested that prior notification to the other state is not desirable due to uncertainty and potential delay.[66]

It follows then that none of the researched states seem to think of notification of a foreign state as a matter of obligation under international law. Instead it is seen, at most, as a matter of comity, regardless of domestic regulation or lack thereof. The authors have not found any indications that the researched countries are deviant from the norm in this respect.

Looking from an international law perspective, and avoiding going into the details of the debate of legality of extraterritorial remote search and seizure, the authors have found no indication of an obligation to notify the other state about a transborder remote search and seizure targeting data stored on the territory of that state. In fact, the CoE Convention on Cybercrime has left the matter explicitly to domestic law.

Finally, we underline that the notification regime, despite the challenges set out above must remain as an integral part of the remote search and seizure regime due to the need to protect the principles of fair trial and effective remedy. Countries should consider options for making

[65] Hof van Beroep Brussel 26-06-2008, vol. 6, Tijdschrift voor Strafrecht: jurisprudentie, nieuwe wetgeving en doctrine voor de praktijk, 2008, 26th june, p. 467.

[66] New Zealand and Law Commission (2007) *Search and Surveillance Powers.* Wellington. p. 228. Available from: http://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20R97.pdf [Accessed 8 March 2017].

the notification of other states more feasible under the circumstances of "*loss of location*". One option would be to develop a shared platform, or use an existing one, between cooperative states where information regarding transborder investigative measures could be shared, if needed, in retrospect.

5. CONCLUSION

Despite the requirement for notification being widely accepted as part of traditional search and seizure, following this obligation in the context of remote search and seizure is not an easy task for LE. On the international level, the notification of foreign states about remote search and seizure of data located on their territory, if they can even be identified, is at the time being a matter of comity and not a legal obligation. Domestically, traditional search and seizure regimes may not be equipped with flexible options for notifying individuals who are not present at the premises of the search or who cannot be easily identified. "*Loss of location*" that may occur, for example, due to the employment of anonymising tools, is challenging the notification requirement even further by possibly making the identification of the individual targeted by the search unfeasible at all. However, given that notification serves as an important tool for the targeted individual by way of protecting his/her right for a fair trial and effective remedy, the legislator should not abandon the requirement as part of remote search and seizure but instead use the reasonable effort approach.

LIST OF REFERENCES

[1] Advisory Committee on Rules of Criminal Procedure - April 2014, United States Courts. Available from: http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-april-2014 [Accessed 8 March 2017].

[2] Advisory Committee on Rules of Criminal Procedure - May 2015, United States Courts. Available from: http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-may-2015 [Accessed 8 March 2017].

[3] American Civil Liberties Union, *ACLU Comment on the Proposed Amendment to Rule 41 Concerning Remote Searches of Electronic Storage Media* (2014), p. 15. Available from: https://www.aclu.org/sites/default/files/assets/aclu_comments_on_rule_41.pdf [Accessed 8 March 2017].

[4] Hof van Beroep Brussel 26-06-2008, vol. 6, Tijdschrift voor Strafrecht: jurisprudentie, nieuwe wetgeving en doctrine voor de praktijk, 2008, 26th june, p. 467.

[5] *Code d'Instruction Criminelle (Belgium Code of Criminal Procedure)*, Livre Premier, Belgium. In France.

[6] Council of Europe (2001) *Explanatory Report to the Convention on Cybercrime (ETS No. 185)*. Available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContentdocumentId=09000016800cce5b [Accessed 8 March 2017].

[7] Council of Europe (2012) *Transborder Access and Jurisdiction: What Are the Options?* Available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContentdocumentId=09000016802e79e8 [Accessed 8 March 2017].

[8] Council of Europe, Convention on Cybercrime, ETS No. 185.

[9] Council of Europe, European Convention on Human Rights, 1950.

[10] Council of Europe, Recommendation R(95) 13.

[11] Daskal, J. (2016) *Rule 41 Has Been Updated: What's Needed Next* [Online] Just Security. Available from: https://www.justsecurity.org/35136/rule-41-updated-needed/ [Accessed 8 March 2017].

[12] Eerste Kamer (2015/2016), *Kamerstukken I 2015/2016*, 34372, A p. 5. Available from: https://zoek.officielebekendmakingen.nl/kst-34372-A.pdf [Accessed 8 March 2017].

[13] Eerste Kamer, *afdeling Inhoudelijke Ondersteuning en de unit Communicatie & Protocol*. Available from: https://www.eerstekamer.nl/wetsvoorstel/34372_computercriminaliteit_iii [Accessed 8 March 2017].

[14] *Eesti Vabariigi põhiseadus (Constitution of the Republic of Estonia)*, RT 1992, 26, 349; RT I, 15. 5. 2015, 2. Estonia: Riigi Teataja. In Estonian.

[15] Estonia, Justiitsministeerium, *Kriminaalmenetlusõiguse revisjoni lähteülesanne (Initial Task of the Revision of the Law of Criminal Procedure)*, 2015. Available from: http://www.just.ee/sites/www.just.ee/files/kriminaalmenetluse_revisjoni_lahteulesanne.pdf [Accessed 8 March 2017].

[16] Ginter, J. et al. (2013) *Analüüs isikute põhiõiguste tagamisest ja eeluurimise kiirusest kriminaalmenetluses (Analysis of Ensuring Fundamental Rights and the Speed of Preliminary Investigation in Criminal Procedure)*. Available from: http://www.kriminaalpoliitika.ee/en/analuus-isikute-pohioiguste-tagamisest-jaeeluurimise-kiirusest-kriminaalmenetluses [Accessed 8 March 2017].

[17] Goldsmith, J. (2001) *The Internet and the Legitimacy of Remote Cross-Border Searches*. University of Chicago Law School, Chicago Unbound. Available from:

http://chicagounbound.uchicago.edu/cgi/viewcontent.cgiarticle=1316&contextpublic_law_and_legal_theory [Accessed 8 March 2017].

[18] *Grondwet (The Dutch Constitution)*, the Netherlands. In Dutch.

[19] Habbo Hotel (2009), Rechtbank Amsterdam, ECLI:NL:RBAMS:2009:BH9789.

[20] Interview with Mr. Geert Schoorens, Federal Prosecutor's Office of Belgium, 2015.

[21] Interview with Mr. Oskar Gross, Police and Border Guard Board, 2017.

[22] Interview with Mr. Robert Laid, Estonian Assistant Prosecutor, 2015.

[23] Interview with Ms. Eneli Laurits, Estonian Public Prosecutor, 2015.

[24] Kennis- en exploitatiecentrum Officiële Overheidspublicaties, *Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (Computercriminaliteit III)*. Available from: https://www.internetconsultatie.nl/computercriminaliteit/document/727 [Accessed 8 March 2017].

[25] Kergandberg, E. and Pikamäe, P. (2012) *Kriminaalmenetluse seadustik: kommenteeritud väljaanne (Code of Criminal Procedure: Commented Edition)*. Tallinn: Juura.

[26] Koops, B.-J. and Goodwin, M. (2014) *Cyberspace, the Cloud, and Cross-Border Criminal Investigation*. Tilburg University, Tilburg Institute for Law, Technology, and Society, WODC. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2698263 [Accessed 8 March 2017].

[27] *Kriminaalmenetlusseadustik (Code of Criminal Procedure)*, RT I 2003, 27, 166; RT I, 31. 12. 2016, 46. Estonia: Riigi Teataja. In Estonian.

[28] Lõhmus, U. (2014) *Põhiõigused kriminaalmenetluses (Fundamental Rights in Criminal Procedure)*. 2nd ed. Tallinn: Juura.

[29] Ministerie van Veiligheid en Justitie, *Memorie van Toelichting: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek*. (2017) Available from: https://www.rijksoverheid.nl/documenten/kamerstukken/2017/02/07/memorie-van-toelichting-vaststellingswet-boek-2-van-het-nieuwe-wetboek-van-strafvordering-het-opsporingsonderzoek[Accessed 8 March 2017].

[30] New Zealand and Law Commission (2007) *Search and Surveillance Powers.* Wellington. Available from: http://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20R97.pdf [Accessed 8 March 2017].

[31] Osula, A.-M. (2015) *Transborder Access and Territorial Sovereignty*. Computer Law & Security Review, 31(6).

[32] Osula, A.-M. (2016) *Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Stud*y. International Journal of Law and Information Technology 24(4).

[33] Osula, A.-M. (2017) *Remote Search and Seizure of Extraterritorial Data*. University of Tartu Press.

[34] Pilkington, E. (2014) *FBI Demands New Powers to Hack into Computers and Carry out Surveillance*. [Online] The Guardian Available from: http://www.theguardian.com/us-news/2014/oct/29/fbi-powers-hacking-computers-surveillance [Accessed 8 March 2017].

[35] Reitman, R. (2016) *With Rule 41, Little-Known Committee Proposes to Grant New Hacking Powers to the Government*, Electronic Frontier Foundation. Available from: https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government [Accessed 8 March 2017].

[36] Rule 41 Coalition Letter (2016). Available from: https://noglobalwarrants.org/assets/Rule41CoalitionLetter.pdf [Accessed 8 March 2017].

[37] Runescape (2012), Hoge Raad, ECLI:NL:HR:2012:BQ9251.

[38] Svantesson, D. (2016) *Preliminary Report: Law Enforcement Cross-Border Acces to Data*, pp. 4-5, 9. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874238 [Accessed 8 March 2017].

[39] *The Wet Openbaarheid Bestuur (Governance Transparency Act)*, the Netherlands. In Dutch.

[40] Thompson II, R. (2016) *Digital Searches and Seizures: Overview of Proposed Amendments to Rule 41 of the Rules of Criminal Procedure*. Congressional Research Service. Available from: https://www.fas.org/sgp/crs/misc/R44547.pdf [Accessed 8 March 2017].

[41] Tor Project Blog (2016) *Day of Action: Stop the Changes to Rule 41*. Available from: https://blog.torproject.org/blog/day-action-stop-changes-rule-41 [Accessed 8 March 2017].

[42] Tweede Kamer (2004/2005), *Kamerstukken II 2004/2005, 26 671, nr. 10*. Available from: https://zoek.officielebekendmakingen.nl/kst-26671-10.pdf [Accessed 8 March 2017].

[43] Tweede Kamer (2004/2005), *Kamerstukken II 2015/2016 Kamerstukken II 2015/2016, 34372*, 4. Available from: https://zoek.officielebekendmakingen.nl/kst-34372-4.pdf [Accessed 8 March 2017]

[44] Tweede Kamer (2004/2005), *Kamerstukken II 2015/2016 Kamerstukken II 2015/2016, 34372*, 34. Available from: https://zoek.officielebekendmakingen.nl/kst-34372-17.pdf [Accessed 8 March 2017].

[45] Tweede Kamer (2004/2005), *Kamerstukken II 2015/2016, Handelingen II, 2015/2016, 34372, 34.* Available from: https://zoek.officielebekendmakingen.nl/kst-34372-26.pdf [Accessed 8 March 2017].

[46] Tweede Kamer (2015/2016), *Handelingen II 2015/2016, 34372, 3*4. Available from: https://zoek.officielebekendmakingen.nl/h-tk-20162017-34-26.pdf [Accessed 8 March 2017].

[47] Tweede Kamer (2015/2016), *Kamerstukken II 2015/2016, 34372, 34.* Available from: https://zoek.officielebekendmakingen.nl/kst-34372-25.pdf [Accessed 8 March 2017].

[48] Tweede Kamer (1998/1999), *Kamerstukken II 1998/1999, 26671, 3*. Available from: https://zoek.officielebekendmakingen.nl/kst-26671-3.pdf [Accessed 8 March 2017].

[49] Tweede Kamer (2003/2004), *Kamerstukken II 2003/2004, 29441, 3*. Available from: https://zoek.officielebekendmakingen.nl/kst-29441-3.pdf [Accessed 8 March 2017].

[50] United States Courts. (2016) *Current Rules of Practice & Procedure, Criminal Rules 4, 41, and 45, Redline of Amended Rules, Including Committee Notes*. Available from: http://www.uscourts.gov/file/21315/ download [Accessed 8 March 2017].

[51] *United States v. Freitas*, 800 F.2d 1451,1456 (9th Cir. 1986).

[52] US Government's comments on extraterritoriality at United States Department of Justice (2013) Mythili Raman Letter to Advisory Committee on the Criminal Rules. Available from: http://justsecurity.org/wp-content/uploads/2014/09/Raman-letter-to-committee-.pdf [Accessed 8 March 2017].

[53] *Wetboek van Strafrecht (Dutch Criminal Code)*, the Netherlands. In Dutch.

[54] *Wetboek van Strafvordering (Dutch Criminal Procedure Code)*, the Netherlands. In Dutch.

[55] *Wetboek van Strafvordering*, the Netherlands. In Dutch.

[56] Zoetekouw, M. (2016) *Ignorantia Terrae Non Excusat*. Available from: https://english.eu2016.nl/documents/publications/2016/03/7/c-mzoetekouw---ignorantia-terrae-non-excusat---discussion-paper-for-the-crossing-borders---jurisdiction-in-cyberspace-conference-march-2016---final [Acessed 8 March 2017].

DOI: 10.5817/MUJLT2017-1-7

WHAT IS AN INTERNATIONAL CYBERSECURITY REGIME AND HOW WE CAN ACHIEVE IT?

by

ILONA STADNIK*

This article explores the two mainstream directions of debates about the possibility of establishing a kind of international cybersecurity regime. It develops the idea of different governance models based on sovereignty, on the one hand, and multistakeholderism on the other. The application of international relations theory helps to understand the current process and stalemate initiatives regarding state cooperation in this field. In addition, the author pays attention to the applicability of the constructivism framework to the understanding of cybersecurity threats and the elaboration of international norms applicable to cyberspace. Finally, the article concludes with the idea that the multistakeholder approach to norm-making may become a viable solution to the problem of constructing an international cybersecurity regime.

KEY WORDS

Cybersecurity, Information Security, Sovereignty, Multistakeholderism, Regimes, Constructivism, Securitization

1. INTRODUCTION

Security is a key concern for all states. In fact, many of today's technologies are a direct result of research and development in national defense industries. However, at times technological advancements in other fields impinge on states' security concerns. The revolution in Information and Communications Technologies (ICT) presents one such case. With the emergence of global cyberspace at the beginning of the 21st

* ilona.st94@gmail.com, Saint-Petersburg State University, School of International Relations, Russia.

century, national cybersecurity has raised its priority in foreign and domestic policies of states. Since there is no international regime governing cyberspace, like the regime of high seas or outer space, states have been increasingly finding themselves in conflict over the breach of cyberspace that they perceive as a threat to their national security.

Cyberspace has gained a great importance for human interactions as well as for a higher level – international relations. More importantly, the cyber domain is multi-faceted – the flow of information and actions runs between these two quite separate (in comparison with other domains) levels. It may become necessary to regulate cyberspace as outer space, sea and airspace to establish common "*rules of game*" and to avoid arbitrary and potentially harmful actions of states. Bilateral agreements between nations, sometimes called as "*cyberpacts*", have become a widespread practice of strategic defense and cooperation.[1] As we are witnessing a dangerous trend of cyberspace militarization, some experts argue that wars of future are cyberwars.[2] This statement falls in the discourse of war as

> "*not merely a political act, but also a real political instrument, a continuation of political commerce, a carrying out of the same by other means.*"[3]

A war is an act of violence, aimed at making the adversary to compel to someone's will. Clauzewitz argued that war among nation states always stemmed from political reasons. Violence used for waging wars tended to exploit new discoveries in science and technology to counteract adverse violence. Connecting this idea to cyberspace seems to be logical, however

---

[1] See for example: U.S. Department of Homeland Security. (2011) *United States and India Sign Cybersecurity Agreement.* [press release], 19 July. Available from: https://www.hsdl.org/?view&did=682137 [Accessed 25 March 2015]; *Soglashenie mezhdu Pravitel'stvom Rossijskoj Federacii i Pravitel'stvom Kitajskoj Narodnoj Respubliki o sotrudnichestve v oblasti obespechenija mezhdunarodnoj informacionnoj bezopasnosti*, 8 May 2015. Available from: http://government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf [Accessed 10 June 2015]; *UK Government. (2015). UK-China Joint Statement on building a global comprehensive strategic partnership for the 21st Century.* [press release], 22 October. Available from: https://www.gov.uk/government/news/uk-china-joint-statement-2015 [Accessed 25 March 2015]; White House. (2015). *President Obama and President X joint statement on cybersecurity.* [press release], 25 September. Available from: https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states [Accessed 25 March 2015].

[2] Clarke, R., Knake, R. (2010) *Cyber War: the Next Threat to National Security and What to Do about It.* New York: Harper Collins Publishers.

[3] Clausewitz, C; Howard, M., Editor and translator; Paret, P., Editor and translator (1989) [1832]. *On War*. Princeton, NJ: Princeton University Press.

there are a plenty of cyberskeptics who refuse to name future wars as cyberwars, because cyber attacks and computer operations may have only indirect potential for being physically violent, notwithstanding that they are kinds of classical hostile activities like espionage and sabotage.[4]

Militarization of cyberspace is a controversial and difficult for measuring process. The indirect indicators of militarization are instant messages from the media about an increase in expenses and development of military capabilities for cyberspace in different countries. Such capabilities include cyber offence and defense tools, involvement of IT specialists and programmers in defense strategies, creation of military units and commands responsible for cyberspace operations. In order to prevent the worst scenario and regulate the still unseen cyber arms race, there is a necessity to put much attention to the cyber dimension of international security.

The lack of a shared definition of what cyberspace and cybersecurity across the world is has led to a relatively slow negotiation process for the formation of an international cyberspace regime. The central theme of the contemporary debates is a future configuration of such an international regime. All parties involved in the issue can be roughly divided into two camps – adherents of the multistakeholder model (with equal participation of states, business and society in cyber governance issues) and supporters of the sovereignty-based model (with total government control over cyber infrastructure and information flows for security needs). This article focuses on analysis of ideas expressed by Russia, China, and the US in connection to possible cyber governance models, as these countries try to take the lead and put forward initiatives to the international community to promote their views and advance their interests. One of the factors that hampers inter-state dialog is the difference in interpretation of cybersecurity. On the one hand, it is about security of physical infrastructure – wired, fiber optic networks, routing equipment, storage systems and database servers; on the other, it may also encompass the security of information flows that circulate through this infrastructure. The last interpretation has direct implications for freedom of expression and access to information. These assumptions predominantly define

[4] See for example: Rid, T. (2013) *Cyber War Will Not Take Place*. New York: Oxford University Press.; Gartzke, E. (2013) the Myth of Cyber War. Bringing War in Cyberspace Back Down to Earth. *International Security*, Vol. 38, No. 2, pp. 41-73.

the features that underlie the governance models for the cyber domain and the participation of various stakeholders in particular.

2. GOVERNANCE MODELS

Very often scholars draw analogies between the cyber domain and the old domains of power such as the high seas, outer space or Antarctica because it is a "*global commons*". The "*commons*" refers to resources that are not excludable but rival in consumption. However, the "*technical*" status of cyberspace that allowed for naming it "*commons*" is not a defining feature for such a comparison. Instead, from a legal perspective, the most important unifying feature of these domains is that they are not currently partitioned and governed according to traditional Westphalian sovereignty – in other words,

> "*states enshrined the non-sovereign status of old domains in international treaties*".[5]

That is why we can single out some useful patterns for prospective global governance of cyberspace. Nevertheless, the analogy between cyber and old domains has its limits. The governance solutions were similar for the old domains — multilateral governance, governance by treaty, and certain demilitarization. But the cyber domain has distinct presets to be considered in the new governance model. These presets imply empowerment of private parties, governance through norms, and regulated militarization. The physical infrastructure level of cyberspace is located within national borders of states and often owned by private parties.[6] This fact prevents the usage of complete analogy between cyberspace and global commons.

According to Kristen Eichensehr, cyberspace has gone through several stages of cyber governance and its relations with sovereignty.[7] Since

---

[5] Eichensehr, K. (2015) The Cyber-Law of Nations. *Georgetown Law Journal*, 317. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2447683 [Accessed 7 December 2016].

[6] According to Youchai Benkler (2000), information environment is composed of three layers - "*the physical infrastructure layer*," the "*logical infrastructure layer*," and "*the content layer*." the physical layer includes infrastructure like cables, wires, and routers. The logical layer consists of software. Above both is the content layer, which includes "*the stuff that gets said or written within any given system of communication*". For the purposes of this article we consider cyberspace as a close concept to information environment.

[7] Eichensehr, K. (2015) The Cyber-Law of Nations. *Georgetown Law Journal*, 317. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2447683 [Accessed 7 December 2016].

the 1990s, cyber itself was seen as sovereign – users, not governments, designed rules of the Internet because cyberspace

"*needs and can create its own law and legal institutions*".[8]

An example of such self-governance is the domain name system (DNS), which evolved from decisions made by engineers and the practices of Internet service providers. The second stage began in the early 2000s, when states started to realize the potential of the Internet as well as challenges it brought along. It has become clear that a new regulation is needed to facilitate the use of the Internet and prevent crimes related to the abuse of the ICT. In addition, an idea emerged that states could regulate the Internet by controlling its underlying hardware within their national borders. However, two issues define the feasibility of control: whether such a control is important for a state in order to protect its political stability; whether costs of imposing such a control are worthy.[9] Finally, the 2010s are characterized by government-to-government debates over cyber governance, the agenda being much more comprehensive than transnational cybercrime issues.

The current debate among states turns upon a particular model for global cybersecurity. As mentioned in the introduction, the alternatives are sovereignty-based and multistakeholder models. To develop this idea further by applying terms from international law we can add important extensions to both models. Thus, cyberspace can be treated, on the one hand, as a sovereign territory, and as a global commons on the other. Each extreme option implies a particular type of a legal regime. Also, even where the concept of territorial sovereignty cannot be applied to the full extent (as is the case in cyberspace), global governance is still possible – an international regime for the high seas and outer space are the examples. Another important question that is open for cyberspace but resolved in aforementioned examples is the role of private parties in governance (see Tab.1).[10]

---

[8] Johnson, D., Post, D. (1996) Law and Borders—The Rise of Law in Cyberspace, *Stanford Law Review*, 48, Available from: https://cyber.harvard.edu/is02/readings/johnson-post.html [Accessed 12 March 2015].

[9] Goldsmith, J. (1998) *The Internet and the Abiding Significance of Territorial Sovereignty, Indiana Journal of Global Legal Studies*, 5, Issue 2. Available from: http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1130&context=ijgls [Accessed 15 March 2015].

[10] The compilation is based on Eichensehr, K. (2015) the Cyber-Law of Nations. *Georgetown Law Journal*, 317.

	High Seas	Outer Space	Antarctic	Cyberspace*			
				USA	Russia	China	"Third option"
Governance by	Multilateral treaty	Multilateral treaty	Multilateral treaty	Globally accepted norms	Multilateral treaty	Multilateral treaty	Globally accepted norms
Participation of private parties	NO	NO	NO	YES	NO	NO	YES
Regulation of military activity	Limitation to peaceful purposes	Restricted militarization Peaceful activity on celestial bodies	Demilitarized zone	Regulated militarization	Demilitarization	Limitation to peaceful purposes	Regulated militarization

Tab. 1: Visions of governance models

Any governance model is defined by two main factors – who participate in decision-making and who has an overall control over taking and implementing decisions. As it can be seen from the table above, the US, Russia, and China support different solutions for cyberspace. Russia and China endorse a multilateral model in which states interact with each other and make decisions about policy and permissible actions in the cyber domain. The state-based model opens the door to a greater regulation of information. This is the focus of the proposed "*Cyber Code of Conduct*" by members of the Shanghai Cooperation Organization.[11] The United States and its allies endorse a multistakeholder model where Internet governance includes "*all appropriate stakeholders*", such as a private sector, civil society, academia, and individuals, in addition to governments.[12] The application of the multistakeholder model excludes the existence of any international treaty by definition. However, the need to define the "*rules of the game*" requires elaboration of globally accepted norms. Finally, the "*third option*" represents pure private governance, which is close to the idea of cyber as sovereign described by J. Barlow in his declaration of independence of cyberspace.[13] This idea has roots in the history of Internet commercialization and its deployment in some countries without close

[11] United Nations General Assembly. (2011) *Letter dated 12 September 2011 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations. A/66/359*. New York. Available from: http://undocs.org/A/66/359 [Accessed 15 March 2015]; United Nations General Assembly. (2015) *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations. A/69/723*. New York. Available from: https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf [Accessed 15 March 2015].

[12] The White House. (2011) *The U.S. International Strategy for Cyberspace.* Washington D.C. Available from: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [Accessed 15 March 2015].

government attention at initial stages. It led to the prevalence of private parties or professional IT communities in the first stage of the "*rules-creation*" process. However, the recent increased involvement of governments in regulation and examples of "*Internet takeovers*" in authoritarian states do not allow for speaking about the viability of this governance option.

The multistakeholder approach deserves describing in more detail. The very notion of multistakeholderism is new to the international relations theory and is undergoing theorization. M. Raymond and L. DeNardis define multistakeholderism

> "*as two or more classes of actors engaged in a common governance enterprise concerning issues they regard as public in nature, and characterized by polyarchic authority relations constituted by procedural rules.*"[14]

By polyarchy they understand distribution of authority among a number of actors. Nevertheless, the distribution of authority is nominal in practice. The typology of stakeholder participation proposed by W. Drake reveals the level of involvement and, respectively, the distribution of authority. He distinguishes three types:[15]

- weak participation of non-state actors in government-led initiatives, limited ability to articulate their own position (as observers)
- limited capacity for participation in comparison with government representatives (as consulting experts in working groups)
- non-state actors act as equal peers with governments in the drawing up of the agenda, elaboration of rules, iterative consultations ("*strong multistakeholderism*")

Obviously, the last ideal type can hardly be found in practice,[16] and there are plenty of reasons for that. Firstly, inadequate participation of non-state

---

[13] Barlow, J. Electronic Frontier Foundation. (1996) *A Declaration of the Independence of Cyberspace*. [record] 8 February, Davos. Available from: https://www.eff.org/cyberspace-independence [Accessed 15 March 2015].

[14] Raymond, M., DeNardis, L. (2015) *Multistakeholderism: anatomy of an inchoate global institution*. International Theory,7, Issue 3 November, pp. 572-616. Available from: https://doi.org/10.1017/S1752971915000081 [Accessed 3 July 2016].

[15] Drake, W. (2011) Multistakeholderism: Internal Limitations and External Limits. In: Wolfgang Kleinwächter (ed.) *Discussion Paper Series No. 1, MIND #2 Internet Policy Making*. Berlin-Nairobi: Internet and Society Collaboratory.

stakeholders is sometimes caused by lack of resources to travel and participate on-site. W. Drake emphasizes the reluctance of industrial democracies to invest in multistakeholder initiatives in order to facilitate organizational expenses and travel support, together with unwillingness to provide political support. Also, there is a gap in nominal and effective participation due to the character of the multistakeholder process, which is very complex in terms of procedures and amounts of information and the number of issues that stakeholders are supposed to discuss. Despite the idea of comprehensive inclusion of all concerned parties, multistakeholderism is not cooperative for newcomers because the workflow is dispersed among the communities, making it difficult to see the connections to the global aim of the whole process. Ultimately, C. Trautmann puts forward the idea of strengthening multistakeholderism positions by connecting

> "*multistakeholder fora with traditional decision-making bodies: the latter's task would be to implement the principles crafted in the former.*"[17]

In this connotation, multistakeholderism seems to be rather a mode of "*decision-shaping*" than alternative decision-making.

3. GOVERNANCE MODELS

Turning back to the main question of the article – what is a cybersecurity regime? – we should explain what we understand under this notion. Regimes define the range of permissible actions by outlining explicit injunctions for actors. The most widely used definition of an international regime formulated by S. Krasner signifies that international regimes are

> "*implicit or explicit principles, norms, rules and decision-making procedures around which actors' expectations converge in a given area of international relations.*"[18]

---

[16] The IANA transition process may be acknowledged as illustration of strong multistakeholderism due to the ICANN policy of inclusion of governments, tech, business, and civil society in shaping the future of Internet governance.

[17] Trautmann, C. (2011) Multistakeholderism needs fundamental and decisive legitimation. In: Wolfgang Kleinwächter (ed.) *Discussion Paper Series No. 1, MIND #2 Internet Policy Making*. Berlin-Nairobi: Internet and Society Collaboratory.

[18] Krasner, S. (1982) Structural Causes and Regime Consequences: Regimes as Intervening Variables. *International Organization*, 2, Issue 36, Spring, pp. 185-205.

However, this definition is too broad; as J. Mearsheimer points out, such a formulation of a concept covers

> "*almost every regularized pattern of activity between states, from war to tariff.*"[19]

A more restricted definition treats regimes as multilateral agreements among states, which aim to regulate national actions within an issue-area.[20] Nevertheless, both definitions deserve our attention in equal terms. Current controversy and uncertainty for the international regime for cyberspace lies within a particular type of regime – norms, rules, and procedures that guide actors' behavior, or a more restricted multilateral treaty with fixed penalties for disobedience. Here we can draw parallels with governance models described in the previous part. The former is softer and makes sense for the multistakeholder approach, while the latter resembles sovereignty-based governance.

Since an international regime can be also viewed as a form of cooperation and coordination between actors, it is worth considering how the main IR paradigms depict coordination and cooperation in cyberspace.

Realists considered cooperation problems as essential to the international system because of their anarchic structure.[21] The security dilemma is one of the examples of the cooperation problem. A security dilemma means a situation where efforts of one nation to improve its security decrease the security of others. In response, another nation tries to enhance its own defense capabilities. Such consecutive steps result in an arms race, worsening of diplomatic relations, and even in an open conflict. For cyberspace, it can unfold in the form of a cyber arms race. Countries try to build up their offensive cyber capabilities as, for example, espionage through intrusion to computer networks and dissemination of malware for spying purposes.[22] Another important factor that hampers cooperation is a difficulty in distinguishing between offensive

---

[19] Mearsheimer, J. (1995) The False Promise of International Institutions. *International Security*, 19, Issue 3, Winter, pp. 5-49.

[20] Haggard, S., Simmons, B. (1987) Theories of international regimes. *International Organization*, 41, Issue 3, pp. 491- 517.

[21] Waltz, K. (1979) Theory of international politics. Reading, MA: AddisonWesley Pub. Co.

[22] Craig, A., Valeriano, B. (2016) Conceptualising Cyber Arms Races. In: N. Pissanidis, H. Rõigas, M. Veenendaal (Eds.) *8th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications.

and defensive weapons and policies of states. If we focus on "*cybersecurity dilemma*", the definition can be transferred with particular details. In this case, it means that efforts by one country to enhance the security of its cyber infrastructure decrease the cybersecurity of others. Cybersecurity can be achieved either through the development of offensive or defensive cyber warfare capabilities. An important addition is that cyber-attack is easier, faster, and cheaper than cyber-defense, because

> "*effective defense must be successful against all attacks, whereas an attacker needs to succeed only once.*"[23]

In other words, factors of time for envision of coming attack as well as physical buffer space to resist it (features of conventional kinetic warfare) do not work in cyberspace, thus making offense capabilities a priority. Moreover, the "*cybersecurity dilemma*" is also complicated by problems of definition (what constitutes a cyber weapon) and attribution (the source of an attack).

Thus, cooperation between states on cybersecurity depends on whether offensive and defensive cyber warfare weapons and policies can be distinguished one from another. Even if countries agreed on the definition of cyber weapon, it would be highly difficult to distinguish between offensive and defensive cyber capabilities. The majority of military unites, in the USA and China in particular, responsible for cybersecurity, possesses both offensive and defensive capabilities. Such capabilities may include technologies of dual use. Solutions for cooperation proposed by realists include a cyber arms control in the form of a treaty, but the definition and attribution problems together with the "*verifiability problem*" (compliance to the treaty) make it a difficult task. In other words, it is hard to imagine the emergence of an IAEA-like (International Atomic Energy Agency) organization for cyberspace as it was organized to control nuclear energy use.

Liberal theories put an emphasis on cheating and dividing gains among states for cooperation and coordination problems.[24] For example, coordination problems in technocratic areas of global governance are solved

---

[23] National Research Council, Computer Science and Telecommunications Board. (1999) *Realizing the Potential of C4I: Fundamental Challenges*. Washington, D.C.: National Academy Press.

[24] Snidal, D. (1985) The limits of hegemonic stability theory. *International Organization*, 39, Issue 4, pp. 579-614.

through the creation of specialized international organizations. For instance – the International Telegraph Union created in 1865 and later the International Telecommunications Union (ITU) for allocation of global radio spectrum and satellite orbits, development of technical standards for interconnectedness and setting International Telecommunication Regulations (ITRs). The revision of ITRs in 2012 turned a coordination problem into a cooperation one because a part of the member states refused to sign the new ITRs, considering that they imposed more governmental control over the Internet.[25] Some countries (Russia, China) advocate giving the ITU responsibilities to define policy for Internet governance that is currently distributed among different entities of private and non-commercial background.[26] Governance of distribution of Internet names and numbers together with the development of technical protocols can be firmly classified as an issue of low politics and involve coordination problems. But in recent years it was highly politicized and brought together with security concerns that the agreement on a particular equilibrium of governance model presents difficult negotiation problems.[27]

Liberalist thinkers argued that international institutions (including international rules, norms, principles, and decision-making procedures) can help to facilitate cooperation even in the face of a security dilemma.[28] International norms can play roles in both constraining state behavior and encouraging interstate cooperation. In the context of the IR theory, norms refer to

> "*collective understandings of the proper behavior of actors*".[29]

---

[25] International Telecommunications Union. (2012) *WCIT-12 Final Acts*. Dubai. Available from: www.itu.int/en/wcit-12/documents/final-acts-wcit-12.pdf [Accessed 19 April 2015].

[26] Kurbaljia, J. (2014) *Introduction to Internet governance.* 6th ed. Malta: DiploFoundation.

[27] ICANN is undergoing the process of its reorganizations towards more accountability and independence. Transition of the US National Telecommunications and Information Administration (NTIA) oversight role over IANA came to an end. It started in March 2014, and two years later a final proposal (elaborated upon with participation of all stakeholders) was introduced to the NTIA for consideration. The summer of 2016 was named the "*end of the era of American control over the Internet*".

[28] See for example: Keohane, R. (1984) *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press; Krasner, S. (1983) *International Regimes*. Ithaca: Cornell University Press; Axelrod, R. Keohane, R. (1986) *Cooperation Under Anarchy*. Princeton: Princeton University Press; Martin, L., Simmons, B. (1998) Theories and Empirical Studies of International Institutions. *International Organization*, 52, Issue 4, Autumn, pp. 729-757.

[29] Legro, J. (1997) Which Norms Matter? Revisiting the 'Failure' of Internationalism. *International Organization*, 51, Issue 1.

Although norms are not always codified in law, they often inspire or lead to the development of international law. Institutions can help create and foster norms, although norms can also develop at the domestic level and then "*diffuse*" throughout the international system.[30] As institutions serve as instruments through which states can achieve cooperation, they may impose constraints on a state behavior. But these constraints are usually accepted as the inevitable costs of cooperation.

Thus "*cybersecurity dilemma*" may potentially be resolved through the creation of international institutions. Moreover, liberalism acknowledges non-state entities as actors, so a possible international organization for maintenance of cybersecurity can be composed of states and non-state actors (represented by the IT industry, for example). Such option would enable participants to strengthen trust by revealing capabilities and methods to identify cyber war incidents and share defensive technologies. The IT industry can greatly contribute its expertise to foster trust and transparency. On the other hand, participation in such an organization will require members to share sensitive information about their cyber capabilities, which they are not willing to do, fearing it could weaken their relative positions. Simultaneously, cyber powers (like the US, for instance) would hardly be ready to join such an organization in an attempt to avoid any accountability for their offensive cyber capabilities and to keep their relative dominance in the cyber domain.

The constructivist approach pays attention to the perception of reality that defines the reason for cooperation between states on security issues. Although many constructivists do not contest the idea that there is a material basis to security threats, they argue that the labeling of diverse activities as threats to national security is a product of "*intersubjective interpretation*".[31] Hence, discursive practices of cyber threats formulation and perception play an important role.

Cybersecurity discourse is about more than one threat form, ranging from computer viruses and other malicious software to the cyber-crime activity and the categories of cyber-terror and cyber-war. Each sub-issue is

---

[30] Finnemore, M., Sikkink, K. (1998) International Norm Dynamics and Political Change. *International Organization*, 52, Issue 4.

[31] See for example: Dartnell, M. (2003) Weapons of Mass Instruction: Web Activism and the Transformation of Global Security. Millennium, 32, Issue 3, pp. 477-499; Hansen, L., Nissenbaum, H. (2009) Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 53, Issue 4, pp. 1155-1575.

represented and treated differently in the political process and at different points in time.[32] That is why the theory of securitization introduced by Buzan, Weaver and De Wilde can be useful to draw the link between a national security and cyber domain.[33]

> "*The question of when a threat becomes a national security threat depends on what type of threat it is, how the recipient perceives it.*"[34]

Securitization is a process of justifying a new security policy in several steps. Firstly, an actor (it can be a government or secondary actors) starts to voice serious concerns over a topic and formulates threats to a referent object (a nation, a state) that has to be protected. The second step is audience validation of a formulated threat as an existential threat. When the necessity is acknowledged, an actor starts to design required policies and actions needed to be taken to ensure security of the referent object. For constructivist studies, the scale of analysis matters a lot – actors and referent objects comprise a unique set of threats. Thus, securitization theory can help to trace back states' intentions by analyzing the language of the cybersecurity discourse. Moreover, the very word "*cybersecurity*" is replaced sometimes (or even disappears from the public discourse) by information security. Consequently, threat representations differ in a substantial way. Information security implies more sensitive issues for national security – threats acquire a psychological and ideological context – for instance, dissemination of harmful information that can destroy political stability and public order. The cyber/information security discourse differs a lot in Russia, China, and the US.[35]

The analysis of threat perceptions in Russia, China, and the US reveals common grounds in cyber threat perceptions for further cooperation

---

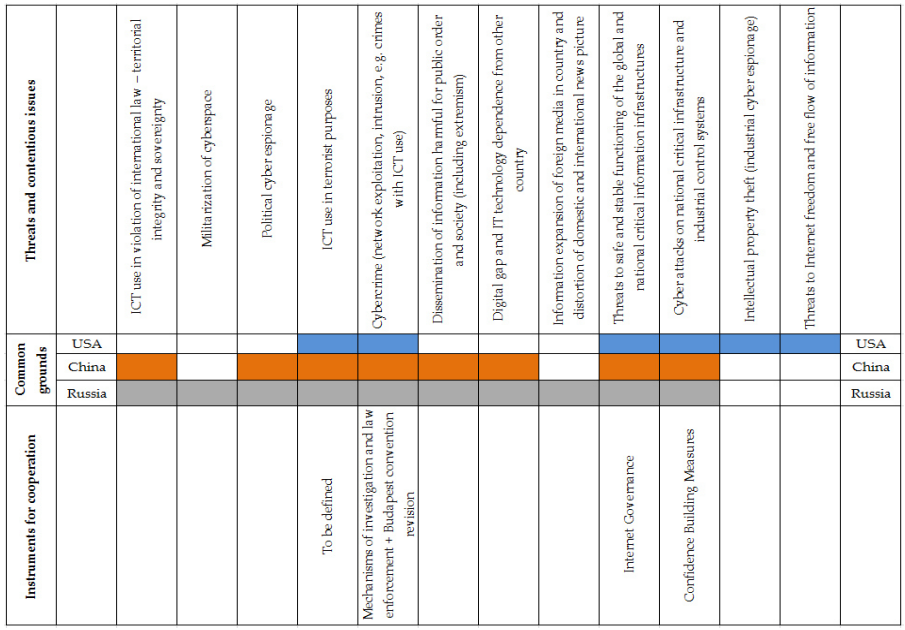
[32] Dunn Cavelty, M. (2013) From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review,* 15, Issue 1, March.

[33] Buzan, B., Waever, O. and De Wilde, J. (1998). *Security: a New Framework for Analysis*. Boulder, CO: Lynne Rienner.

[34] Buzan, B. (1991). *Peoples, States and Fear: an Agenda for International Security Studies in the Post-Cold War Era*, 2nd ed. Boulder, CO: Lynne Rienner.

[35] The Russian Government. (2016) *Doktrina Informacionnoi Bezoasnosti*. 5 December, Moscow. Available from: http://kremlin.ru/acts/bank/41460. [Accessed 10 February 2017]; the White House. (2011) the *U.S. International Strategy for Cyberspace*. Washington D.C. Available from: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [Accessed 10 February 2017]; Chang, A. (2014) *Warring State: China's Cybersecurity Strategy*. [online] 3 December, Center for a New American Security. Available from: https://www.cnas.org/publications/reports/warring-state-chinas-cybersecurity-strategy [Accessed 10 February 2017].

to mitigate the negative effect for a national security (see Tab.2).[36] Colored boxes indicate what threat or contentious issue is under the country's focus. The last row of the table emphasizes possible policy areas for global cooperation for the norm-making process.



Tab. 2: Common grounds for cooperation in combating cyber threats

Russia and China are closer to each other in threat perceptions. More importantly, they put an emphasis on sovereignty in cyberspace, while the US is concerned with network security and a free flow of information for economic and political reasons. However, there are issues that all three countries acknowledge as dangerous for a national security – ICT use for terrorist purposes, cybercrime, threats to safe and stable functioning of the global and national critical information infrastructures, and cyberattacks on the national critical infrastructure and industrial control systems. As cyberspace and the Internet are a transnational and single world domain (at least so far, keeping in mind the tendencies for Internet fragmentation), there is a need to elaborate global norms of behavior (applicable for non-state actors also) with national enforcement. The first steps are already taken for outlined issues: confidence-building

[36] Based on content analysis of national strategic documents. The complete list is introduced in references in the end of the article.

measures in cyberspace;[37] the Budapest convention to combat cybercrime;[38] Internet governance evolution; and the reform of ICANN. Yet, all stakeholders are still at odds with these issues.

4. CONSTRUCTIVISM FOR NORM-MAKING

In addition, the constructivist approach also can shed light on the norm-creation process. Constructivists have done a great deal of work attempting to explain the emergence of new international norms. The theory of strategic social construction proposed by M. Finnemore and K. Sikkink can help to answer the question of how the cybersecurity regime can be achieved.[39] Their proposed "*life cycle*" of norms consists of norm emergence, norm cascade, and internalization. Firstly, a norm emerges from the need for desirable behavior of stakeholders, but it never "*enters a normative vacuum*" and has to compete with other interests. Importantly, international organizations serve as a platform through which norms can be promoted, due to their expertise. We will develop the example of such norms' promotion for cyberspace later in this paragraph. Moreover, institutionalization of specific rules and principles through such organizations helps to clarify what constitutes the norm and its violation. Further steps involve consecutive adoption of newly created norm by states, in other words, "*norm cascade*". Finnemore and Sikkink argue it happens because states want to maintain their identity of an international community member, thus showing conformity. Ultimately, "*automatic conformance with the norm*" is internalization – an extreme form of the norm cascade.

At the same time, a normative change may become the result of procedural changes that lead to the creation of new policies. Social practices and background knowledge are central notions for understanding. E. Adler and V. Pouliot define practices as

---

[37] OSCE. (2016). Permanent Council Decision No. 1202. OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies. Vienna. Available from: http://www.osce.org/pc/227281 [Accessed 10 February 2017].

[38] Signed by 50 countries. The United States signed and ratified this Convention in 2007. China did not sign the document, nor did Russia because of the problem "article 32(b)". This article 32 (b) of the Convention allows the obtaining, without the consent of the participating countries, access to the computer data stored on its territory, i.e., to conduct cross-border investigations and investigative activities. Russia considers such a provision a violation of sovereign rights of states.

[39] Finnemore, M., Sikkink, K. (1998) International Norm Dynamics and Political Change. *International Organization*, 52, Issue 4.

> "*socially meaningful patterns of action which, in being performed more or less competently, simultaneously embody, act out and possibly reify background knowledge and discourse in and on the material world.*"[40]

This background knowledge is, in fact, procedural rules that condition the emergence of norms for social practices. If we narrow them to diplomatic practices, we will get written and unwritten rules that constitute the specific game of multilateral diplomacy as procedural rules.[41] for states engaged in the negotiation process, it is highly important to have the ability to use such procedural rules in their favor.

Another point for procedural rules focuses on their ability to facilitate negotiations on a sensitive issue. In our case, the agreement on norms of responsible state behavior for the use of ICTs presents a highly contentious cooperation problem. However, the UN Group of governmental experts on information security (UN GGE)[42] was able to achieve tangible results by the third round of negotiations because the participating states did not object to procedural rules of presenting their positions and assessing those of their counterparts. Thus, Russia and the US came to an agreement that International Law can be applied to the use of ICTs (it is worth noting that neither cyberspace nor information space is used in GGE reports for the satisfaction of the countries' positions). The Table below illustrates the results of the GGE work done by 20 countries on compiling the list of existing and emerging threats in the use of ICT.[43] It also illustrates the progress in alignment of countries' positions on the issue.

---

[40] Adler, E., Pouliot, V. (2011). International practices. *International*. Theory, 3, p. 136

[41] Adler-Nissen, R., Pouliot, V. (2014) Power in practice: Negotiating the international intervention in Libya. European Journal of International Relations, 20, Issue 4.

[42] United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UNODA. Russia, China, and the US were country-members for each GGE convocation.

[43] Table is based on: United Nations General Assembly. (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/70/174*. New York. Available from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement [Accessed 6 April 2016].

Threats and contentious issues		ICT use in violation of international law – territorial integrity and sovereignty	Militarization of cyberspace	Political cyber espionage	ICT use in terrorist purposes	Cybercrime (network exploitation, intrusion, e.g. crimes with ICT use)	Dissemination of information harmful for public order and society (including extremism)	Digital gap and IT technology dependence from other country	Information expansion of foreign media in country and distortion of domestic and international news picture	Threats to safe and stable functioning of the global and national critical information infrastructures	Cyber attacks on national critical infrastructure and industrial control systems	Intellectual property theft (industrial cyber espionage)	Threats to Internet freedom and free flow of information	
Common grounds	USA													USA
	China													China
	Russia													Russia
	GGE													GGE

Tab. 3: Finding common grounds within the UN GGE

Nevertheless, the GGE recommendations for norms, rules, and confidence building measures are still non-binding and serve rather as guidelines for voluntary observance than institutionalized norms with clear consequences for incompliance. One of the problems to turn these recommendations into legally binding rules is the complicated nature of cyberspace and a wide circle of stakeholders that includes not only governments but private actors as well. States are trying to solve a puzzle: even if they follow strategic social construction with procedural norms of UN General Assembly First Committee, what will the international regime for cyberspace look like? One way that is advocated by the US and its allies is to apply the existing international norms to cyberspace – those written in the UN Charter, the law of armed conflict and law of responsible state behavior. Partly, the GGE resulted in acknowledging such a way. On the other hand, cyber/information space may require a special multilateral treaty. The main challenge for this option is the definition of the space under consideration, whether it is global commons or a sovereign territory. Uncertainty in this issue blocks any further state cooperation.

K. Erskine and M. Carr define main challenges for developing norms for cyberspace.[44] First, they are new practices displaying the characteristics of cyber-governance of the global domain system, coordination of individual networks, social media usage, protection from cyberattacks,

[44] Erskine, K., Carr, M. (2016) Beyond 'Quasi-Norms': the Challenges and Potential of Engaging with Norms in Cyberspace. In: Anna-Maria Osula and Henry Roigas (Eds.) *International Cyber Norms: Legal, Policy & Industry Perspectives*. Tallinn: NATO CCD COE Publications.

and the like. There is still no clear understanding of what behavior is wrong or right that would be accepted by all stakeholders. Another factor is competing value systems of stakeholders – understanding of the privacy/transparency/anonymity balance that defines the perception of security in cyberspace. As can be seen from Tab. 2, even the three countries differ in their preferences. In addition, a variety of stakeholders also contribute to the values competition. For example, private sector aims at maximizing its profits rather than at concerning with national security issues. Finally, the problem of attribution allows actors to deny any allegations for harmful activities in cyberspace.

In the end, Erskine and Carr stress the idea of quasi-norms for cyberspace. Stakeholders

> "*will seek to impose rules and codes of conduct on practices that further their interests or values*";

but

> "*imposed rules are not norms, they are normative aspirations*",

because norms should first of all be internalized by stakeholders, since norms inform the behavior through the prescriptive and evaluative nature.[45] In this respect, the normative aspiration of the US to import norms from the law of armed conflict to cyberspace may seem useless, as imported norms from another domain "*risk to significantly lose meaning and moral force*".

5. CONCLUSIONS

The international cybersecurity regime is at the initial stages of its construction, a norm-creation stage. However, the contours of this regime are still vague. There are two possible scenarios for further development – adjustment of the existing international law to cyberspace peculiarities (which is likely to be a stalemate), or elaboration of special governance mechanisms. The special governance mechanisms remain mired in uncertainty, raising questions if cybersecurity is subject to top-down multilateral regulation, or more non-state stakeholders should have their say, including the IT industry.

[45] Ibid.

The multilateral approach for cybersecurity would hardly define the new regime. The reasons for such argument are strong: there is still no common agreement on the substance of a treaty or a convention on international cybersecurity. Cyberspace and information space differ substantially in their underlying meaning. The content analysis of the countries' perceived cyber/information threats revealed the fault line between the values promoted by the US, on the one hand, and Russia and China on the other. While the US is concerned with secure computer networks simultaneously providing the open, secure Internet with free flow of information and freedom of expression, it also builds up offensive cyber capabilities to protect the current status quo. Russia and China place high priority on information security and combating against threats that may harm society, the political regime, and the stability of a state. Such threats also include terrorism, extremism, and separatism; moreover, Russia emphasizes information expansion of the foreign media in the country and distortion of the domestic and international news picture.

Cybersecurity is a very complex multi-component issue for a single international regime. Despite divergence in threat perceptions, the three countries have common concerns: ICT use for terrorist purposes, cybercrime, stability and resiliency of the Internet critical infrastructure, network security, and militarization of cyberspace. The UN GGE work made a significant contribution to the consensus between member-states and even broadened the understanding of common challenges. But the group still has a long way to go for achieving tangible results. If to separately regulate each area, agreed to be a high priority for countries, multilateral approach will still be weak despite the assumption that the established procedural rules for norm-formulation make this process easier. That was proven by the example of the impossibility of the arms control treaty for cyberspace: there is still no globally accepted definition of what a cyber weapon is. In addition, technologies of dual-use are predominant in the IT area. Though states have already agreed on a number of international treaties for arms-control and non-proliferation, the pool of procedural rules and behavior patterns is widely used; the cyber arms control treaty is hard to design because of the difficulties in controlling compliance.

Confidence building measures (CBMs) to protect critical infrastructure could be taken through a multilateral approach – and there are already

examples of bilateral agreements, and even UN GGE recommendations contain a substantial list of particular steps for CBMs. In reality, the majority of cases show that CBMs exist only on paper. And here we can see a security dilemma – if one state exhibits more vulnerabilities than another, then the second state would probably use this information with malicious intentions.

The multilateral approach also has another considerable drawback – it neglects non-state actors in the process of norm-making. The case of cyberspace is unique in the sense that the IT industry exerts a great influence on the cyber policy both in creating security solutions and in constructing new cyber threats as collateral consequences of their business.

One of the areas for ensuring stability and resiliency of the Internet critical infrastructure is the Internet governance. It was multistakeholder from the very beginning. States entered "*the game*" after the distributed system of allocation and governance of Internet critical resources had been invented. Any attempts by states (Russian and China in particular) to establish control or intrude into the governance system are firmly pushed back. Undoubtedly, states will have a say in the Internet governance policy, but formulas for respective roles are still to be found.

Multistakeholderism should not be taken as a good solution to problems caused by cyberspace features. It has a lot of limitations, where the distribution of authority between stakeholders is the most strong. One of the problems for a multistakeholder approach to cybersecurity is to ensure a win-win public-private partnership. Firstly, the IT industry is willing to participate in security projects for national critical infrastructure when economic benefits overcome costs. Secondly, the absence of shared principles of cyber or information security that define the privacy/security equilibrium considerably hampers collaboration. Even in democratic countries, the IT industry suffers from the effects of the government policy aimed at protecting national interests and security to the detriment of protecting various human rights, such as privacy and free flow of information. At least, multistakeholderism may hopefully produce principles that would constitute the basis for cybersecurity norms to be accepted by all stakeholders.

LIST OF REFERENCES

[1] Adler, E., Pouliot, V. (2011). International practices. *International. Theory*, 3, p. 136.

[2] Adler-Nissen, R., Pouliot, V. (2014) Power in practice: Negotiating the international Intervention in Libya. *European Journal of International Relations*, 20, Issue 4.

[3] Axelrod, R. Keohane, R. (1986) *Cooperation Under Anarchy*. Princeton: Princeton University Press.

[4] Barlow, J. Electronic Frontier Foundation. (1996) *A Declaration of the ndependence of Cyberspace.* [record] 8 February, Davos. Available from: https://www.eff.org/cyberspace-independence [Accessed 15 March 2015].

[5] Buzan, B. (1991). *Peoples, States and Fear: an Agenda for International Security Studies in the Post-Cold War Era*, 2nd ed. Boulder, CO: Lynne Rienner.

[6] Buzan, B., Waever, O. and De Wilde, J. (1998). *Security: a New Framework for Analysis*. Boulder, CO: Lynne Rienner.

[7] Chang, A. (2014) *Warring State: China's Cybersecurity Strategy*. [online] 3 December, Center for a New American Security. Available from: https://www.cnas.org/publications/reports/warring-state-chinas-cybersecurity-strategy [Accessed 10 February 2017].

[8] Clarke, R., Knake, R. (2010) *Cyber War: the Next Threat to National Security and What to Do about It.* New York: HarperCollins Publishers.

[9] Clausewitz, C; Howard, M., Editor and translator; Paret, P., Editor and translator (1989) [1832]. *On War*. Princeton, NJ: Princeton University Press.

[10] Craig, A., Valeriano, B. (2016) Conceptualising Cyber Arms Races. In: N. Pissanidis, H.Rõigas, M.Veenendaal (Eds.) *8th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications.

[11] Dartnell, M. (2003) Weapons of Mass Instruction: Web Activism and the Transformation of Global Security. *Millennium*, 32, Issue 3, pp. 477-499.

[12] Drake, W. (2011) Multistakeholderism: Internal Limitations and External Limits. In: Wolfgang Kleinwächter (ed.) *Discussion Paper Series No. 1, MIND #2 Internet Policy Making*. Berlin-Nairobi: Internet and Society Co:llaboratory.

[13] Dunn Cavelty, M. (2013) From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review,* 15, Issue 1, March.

[14] Eichensehr, K. (2015) the Cyber-Law of Nations. *Georgetown Law Journal*, 317. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2447683 [Accessed 7 December 2016].

[15] Erskine, K., Carr, M. (2016) Beyond 'Quasi-Norms': the Challenges and Potential of Engaging with Norms in Cyberspace. In: Anna-Maria Osula and Henry Roigas (Eds.) *International Cyber Norms: Legal, Policy & Industry Perspectives.* Tallinn: NATO CCD COE Publications.

[16] Finnemore, M., Sikkink, K. (1998) International Norm Dynamics and Political Change. *International Organization*, 52, Issue 4.

[17] Gartzke, E. (2013) The Myth of Cyber War. Bringing War in Cyberspace Back Down to Earth. *International Security*, Vol. 38, No. 2, pp. 41-73.

[18] Goldsmith, J. (1998) The Internet and the Abiding Significance of Territorial Sovereignty, *Indiana Journal of Global Legal Studies*, 5, Issue 2. Available from: http://www.repositorylaw.indiana.edu/cgi/viewcontent.cgi?article=1130&context=ijgls [Accessed 15 March 2015].

[19] Haggard, S., Simmons, B. (1987) Theories of international regimes. *International Organization*, 41, Issue 3, pp. 491- 517.

[20] Hansen, L., Nissenbaum, H. (2009) Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly,* 53, Issue 4, pp. 1155-1575.

[21] International Telecommunications Union. (2012) *WCIT-12 Final Acts*. Dubai. Available from: www.itu.int/en/wcit-12/documents/final-acts-wcit-12.pdf [Accessed 19 April 2015].

[22] Johnson, D., Post, D. (1996) Law and Borders — The Rise of Law in Cyberspace, *Stanford Law Review*, 48, Available from: https://cyber.harvard.edu/is02/readings/johnson-post.html [Accessed 12 March 2015].

[23] Keohane, R. (1984) *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press.

[24] Krasner, S. (1982) Structural Causes and Regime Consequences: Regimes as Intervening Variables. *International Organization*, 2, Issue 36, Spring, pp. 185-205.

[25] Krasner, S. (1983) International Regimes. Ithaca: Cornell University Press.

[26] Kurbaljia, J. (2014) *Introduction to Internet governance.* 6th ed. Malta: DiploFoundation.

[27] Legro, J. (1997) Which Norms Matter? Revisiting the 'Failure' of Internationalism. *International Organization*, 51, Issue 1.

[28] Martin, L., Simmons, B. (1998) Theories and Empirical Studies of International Institutions. International *Organization*, 52, Issue 4, Autumn, pp. 729-757.

[29] Mearsheimer, J. (1995) The False Promise of International Institutions. *International Security*, 19, Issue 3, Winter, pp. 5-49.

[30] National Research Council, Computer Science and Telecommunications Board. (1999) *Realizing the Potential of C4I: Fundamental Challenges*. Washington, D.C.: National Academy Press.

[31] OSCE. (2016). *Permanent Council Decision No. 1202.* OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies. Vienna. Available from: http://www.osce.org/pc/227281 [Accessed 10 February 2017].

[32] Raymond, M., DeNardis, L. (2015) Multistakeholderism: anatomy of an inchoate global institution. *International Theory*,7, Issue 3, November, pp. 572-616. Available from: https://doi.org/10.1017/S1752971915000081 [Accessed 3 July 2016].

[33] Rid, T. (2013) *Cyber War Will Not Take Place*. New York: Oxford University Press.

[34] Snidal, D. (1985) The limits of hegemonic stability theory. *International Organization*, 39, Issue 4, pp. 579-614.

[35] The Russian Government (2015*) Soglashenie mezhdu Pravitel'stvom Rossijskoj Federacii I Pravitel'stvom Kitajskoj Narodnoj Respubliki o sotrudnichestve v oblasti obespecheni a mezhdunarodnoj informacionnoj bezopasnosti*, Moscow. Available from: http://government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf [Accessed 10 June 2015].

[36] The Russian Government. (2016) *Doktrina Informacionnoi Bezoasnosti*. 5 December, Moscow. Available from: http://kremlin.ru/acts/bank/41460 [Accessed 10 February 2017].

[37] The White House. (2011) *The U.S. International Strategy for Cyberspace*. Washington D.C. Available from: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [Accessed 15 March 2015].

[38] The White House. (2015). *President Obama and President X joint statement on cybersecurity* [press release], 25 September. Available from: https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states [Accessed 25 March 2015].

[39] Trautmann, C. (2011) Multistakeholderism needs fundamental and decisive legitimation. In: Wolfgang Kleinwächter (ed.) *Discussion Paper Series No. 1, MIND #2 Internet Policy Making.* Berlin-Nairobi: Internet and Society Co:llaboratory.

[40] U.S. Department of Homeland Security. (2011) *United States and India Sign Cybersecurity Agreement*. [press release], 19 July. Available from: https://www.hsdl.org/?view&did=682137 [Accessed 25 March 2015].

[41] UK Government. (2015*). UK-China Joint Statement on building a global comprehensive strategic partnership for the 21st Century*. [press release], 22 October. Available from: https://www.gov.uk/government/news/uk-china-joint-statement-2015 [Accessed 25 March 2015].

[42] United Nations General Assembly. (2011) *Letter dated 12 September 2011 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations. A/66/359*. New York. Available from: http://undocs.org/A/66/359 [Accessed 15 March 2015].

[43] United Nations General Assembly. (2015) *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations. A/69/723*. New York. Available from: https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf [Accessed 15 March 2015].

[44] United Nations General Assembly. (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/70/174*. New York. Available from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement [Accessed 6 April 2016].

[45] Waltz, K. (1979) Theory of international politics. Reading, MA: AddisonWesley Pub. Co.

LIST OF DOCUMENTS FOR TAB. 2 AND TAB. 3

[1] SCO. (2009) *Soglashenie mezhdu pravitelstvami gosudarstv – chlenov SHanhajskoj organizacii sotrudnichestva o sotrudnichestve v oblasti obespecheniya mezhdunarodnoj informacionnoj bezopasnosti*. Available from: http://docs.cntd.ru/document/902289626 [Accessed 25 March 2016].

[2] The Russian Council of Federation. (2013) *Koncepciya strategii kiberbezopasnosti*, Available from: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf [Accessed 25 March 2016].

[3] The Russian Ministry of Defense. (2011). *Konceptualnye vzglyady na deyatelnost vooruzhennyh sil Rossijskoj Federacii v informacionnom prostranstve*.

[4] The Russian Ministry of International Affairs. (2011). *Convetion on International Information Security*. Available from: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=en_GB [Accessed 25 March 2016].

[5] The Russian President. (2009) *O Strategii nacionalnoj bezopasnosti Rossijskoj Federacii do 2020 goda*. Available from: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102129631 [Accessed 25 March 2016].

[6] The Russian President. (2014) *Voennaya doktrina Rossijskoj Federacii.* Available from: http://kremlin.ru/events/president/news/47334 [Accessed 25 March 2016].

[7] The Russian President. (2015) *Strategiya nacionalnoj bezopasnosti Rossijskoj Federacii.* Available from: http://kremlin.ru/acts/news/51129 [Accessed 25 March 2016].

[8] The Russian President. (2015) *Voennaya doktrina Rossijskoj Federacii*. Available from: http://kremlin.ru/supplement/461 [Accessed 25 March 2016].

[9] The Russian President. (2016) *Doktrina Informacionnoi Bezopasnosti*. 5 December, Moscow. Available from: http://kremlin.ru/acts/bank/41460 [Accessed 10 February 2017].

[10] United Nations General Assembly. (2015) *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations. A/69/723.* New York. Available from: https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf [Accessed 25 March 2016].

[11] The US Department of Defense (2015). *The DoD Cyber strategy*. Available from: https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf [Accessed 25 March 2016].

[12] The US Department of Homeland Security. (2003) *The national strategy for secure cyberspace*. Available from: https://www.dhs.gov/national-strategy-secure-cyberspace [Accessed 25 March 2016].

[13] The US Department of Homeland Security. (2009) *Cyberspace policy review*. Available from: https://www.dhs.gov/publication/2009-cyberspace-policy-review [Accessed 25 March 2016].

[14] The US Senate. (2014) *Worldwide Threat Assessment of the US Intelligence Community. Testimony of J. Clapper*. 29 January, Washington. Available from: https://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf [Accessed 25 March 2016].

[15] The US Senate. (2015) *Worldwide Threat Assessment of the US Intelligence Community. Testimony of J. Clapper*. 26 February, Washington. Available from: https://www.dni.gov/index.php/newsroom/testimonies/209-congressional-testimonies-2015/1175-dni-clapper-opening-statement-on-the-worldwide-threat-assessment-before-the-senate-armed-services-committee [Accessed 25 March 2016].

[16] The White House (2010) *National Security Strategy*. Available from: http://nssarchive.us/national-security-strategy-2010/ [Accessed 25 March 2016].

[17] The White House. (2011) *The U.S. International Strategy for Cyberspace*. Washington D.C. Available from: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [Accessed 25 March 2016].

[18] China's Central Military Commission (2014). *Opinion on Further Strengthening Military Information Security Work.*

[19] China's National Informatization Leading Group. (2006) *National Informatisation Development Strategy, 2006-2020.*

[20] China's State Informatization Leading Group. (2003) *Opinions for Strengthening Information Security Assurance Work ("Document 27").* Available from: http://www.btpta.gov.cn/publish/portal7/tab550/info92345.htm [Accessed 25 March 2016].

[21] The Information Office of the State Council. (2013) *White Paper: The Diversified Employment of China's Armed Forces*. Available from: http://www.nti.org/media/pdfs/China_Defense_White_Paper_2013.pdf [Accessed 25 March 2016].

[22] The Information Office of the State Council. (2015) *China's Military Strategy*. Available from: http://eng.mod.gov.cn/Press/2015-05/26/content_4586805.htm [Accessed 25 March 2016].

DOI: 10.5817/MUJLT2017-1-8

ICANN: TRANSFORMATION OF APPROACH TOWARDS INTERNET GOVERNANCE

by

VERONIKA ŽOLNERČÍKOVÁ*

Internet Corporation for Assigned Names and Numbers (ICANN) is one of the world's prior organizations governing the Internet. Since its establishement in 1998 it faced criticism concerning the lack of legitimacy and accountability. ICANN was also challenged because of the ongoing tight relationship with the US government, which was not considered to be acceptable by the rest of the world. The article focuses on the development of ICANN and its approach towards the criticism. It elaborates on the sector-specific issues regarding Internet governance. And finally it informs the reader about the process of transformation of ICANN, which severed the link between the US government and ICANN.

KEY WORDS

ICANN, Internet Governance, Self-regulation, Internet, Domain

1. INTRODUCTION

The year 2016 was a year of change when it comes to Internet governance. It is to be remembered as the year when the debate over the prevailing substantial influence of US on the management of the Internet escalated. After numerous debates on the subject in the last two decades, a shift forward to more neutral and independent Internet governance was taken. The final step was executed in September 2016, when the newspaper stated that the former president of the US, Barack Obama, had given away the Internet. That is obviously a rather simplified statement. The Internet is an intangible object, a network incapable of being a tradable property and as such cannot be handed over. What happened from a legal viewpoint

* v.zolnercikova@gmail.com, Veronika Žolnerčíková is a student of Charles University in Prague, Faculty of Law, Czech Republic.

in autumn 2016 is that the contract allowing US to oversee one of the critical functions of the Internet Corporation for Assigned Names Numbers (ICANN), an industry regulator with much power, has expired.

The focus of this article lies in ICANN, what ICANN is and why it is an important entity in the field. This paper will clarify what its day-to-day tasks are and what are the concerns related to its neutrality and accountability since it was established. Lastly, it will offer a summary of recent development of Internet governance regarding ICAN.

1.1 INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS

ICANN is an organization based in United States and created as an industry regulator of the Domain Name System (DNS). DNS is sometimes called the "*Internet address book*"; its core function is to translate IP addresses into more meaningful form from the viewpoint of an Internet user. An IP address consists of string of numbers (IPv4) or numbers and letters (IPv6) designating the access point in a network. The point of origin or termination is a certain device, for example, a computer. An IP address serves as a label for that device and allows other devices its localization and connectivity.[1] There are two IP standards, IPv4, which is widely used at present, and its possible replacement, IPv6. The stock of IPv4 addresses had soon run low, and they had become a rare commodity. The stock was exhausted in 2011.[2] That is a reason for implementation of IPv6. The new Internet protocol offers an inexhaustible number of combinations for the foreseeable future.[3]

However, IP addresses are hard to remember. That is why DNS translates these addresses into what we know as domain names, such as "*google.com*". It is unnecessary for the user to know the precise address and location of the device containing the desirable content. And the provider of the content wants its content accessible as easily as possible. This is why the provider aims to obtaIn an easily memorable

---

[1] Mueller, M. L. (2010) *Networks and states: the global politics of Internet governance*, MIT Press. p. 230; Bygrave, L. A. & Bing, J. (2009) *Internet governance: Infrastructure and institutions*, Oxford University Press, pp. 147–150.

[2] The so-called free pool stock of IPv4 addresses assigned directly by the Internet Assigned Numbers Authority to regional internet registries. Source: 2011. *Free Pool of IPv4 Address Space Depleted*. [online] Available from: https://www.nro.net/ipv4-free-pool-depleted/ [Accessed 10 May 2017].

[3] *What is Ipv6?* [online] Available from: https://www.apnic.net/community/ipv6/ [Accessed 10 May 2017].

domain name. As the full name of ICANN suggests, it plays a key role in the allocation of domain names.

If we look at the mentioned domain name "*google.com*", we can see a top-level domain name (TLD). TLDs can be either generic (.com, .net, .gov, .edu) or country specific (.cz, .uk, .at, .no). The first are designated as gTLDs, the second as ccTLDs.[4] It is within the powers of ICANN to establish what is and what is not a gTLD and grant or not grant a ccTLD.[5] Although it may seem that there cannot be much dispute when it comes to ccTLDs, issues may arise when it comes to countries or parts of countries that seek independence but are not recognized world-wide.[6]

The mappings between domain names, TLDs and IP addresses are contained in a plain text file called the root zone file.

> "*The root zone file is the master definition for the DNS and contains the authoritative list of top-level domains and the information needed to find the authoritative domain name servers for each domain name.*"[7]

Although ICANN is the regulator and coordinates the content of the root zone file, the file is housed by a private non-profit company called VeriSign. In 2000, VeriSign acquired a company called Network Solutions, Inc., a government contractor, who had in a fact a monopoly granted by the US, since it was the only registrar for domain names. By doing so for an initial fee and a yearly fee, the company made a fortune. The contract with the US and all its perks succeeded to VeriSign.[8]

1.2 ICANN AS THE GOVERNOR

ICANN governs multiple key elements of the Internet necessary for its function, either directly or through multiple associated or supporting organizations. Among these some have been formally delegated by ICANN and some can be controlled by ICANN factually. Here is a summary: ICANN a) manages the IP address spaces, b) assigns addresses to regional registries, c) creates and assigns TLDs, d) maintains the root name servers,

---

[4] Bygrave, L. A. & Bing, J. (2009) *Internet governance: Infrastructure and institutions*, Oxford University Press, p. 163.

[5] Ibid., pp. 147-148.

[6] For example, a gTLD (not a ccTLD) .cat was created for the Catalonian community in Spain.

[7] 1987. *Domain names: implementation and specification*. [online] Available from: http://www.ietf.org/rfc/rfc1035.txt [Accessed 14 January 2017].

[8] Koppell, J. G. (2005) Pathologies of accountability: ICANN and the challenge of "multiple accountabilities disorder". *Public Administration Review,* 65**,** 94-108, p. 101.

e) maintains registries of IP identifiers, and f) adopts Internet policies and standards.[9]

That is why ICANN is considered to be one of the world's main organizations governing the Internet. The legitimacy to govern Internet is not bound to one jurisdiction; it is neither derived from any of the established international organizations nor is it granted to one specific entity. Internet governance is a complex concept being executed by multiple bodies with unclear hierarchy and usually unclear legitimacy as well. The model of Internet governance will be discussed in more depth later. Nevertheless, a working definition is needed to clarify what I am referring to when I discuss Internet governance. For these purposes, I will use the definition that can be found in a report from 2005 by the Working Group on Internet Governance,[10] which goes as follows:

> „*Internet Governance is the development and application by governments, the private sector and civil society, in their respective role, decision-making procedures, and programmes that shape the evolution and use of the Internet.*"[11]

1.3 CHALLENGES OF INTERNET GOVERNANCE

Because of the rather special nature of the Internet, a need for more flexible organizations is arising. ICANN is a new type of organization that is tied deeply to the private sector, yet it has the unprecedented power to implement a set of rules, which will then be followed all around the world. National regulation has only a limited effect on discourse nowadays, as the Internet is the first man-made invention that is truly transnational.

The legitimacy of an internationally recognized organization should derive from sovereign nations, which will then be bound by the measures adopted by that organization. But the legitimacy derived only from the US, and the relationship with the US faced criticism from other countries.[12]

---

[9] For detailed description of ICANN's functions, I recommend Chapter 3 of BYGRAVE, L. A. & BING, J. 2009. *Internet governance: Infrastructure and institutions*, Oxford University Press.

[10] Working Group on Internet Governance (WGIG) was initiated by the United Nations after the World Summit on Information Society in 2003 as a response to a debate concerning what Internet governance is and what are the respective roles of governements, international organizations etc. in the Internet field.

[11] 2005. *Report of the Working Group on Internet Governance*. [online] Available from: http://www.wgig.org/docs/WGIGREPORT.pdf [Accessed 12 February 2016].

There is an effort to sever the bond since ICANN's standards became recognized world-wide.

ICANN is an organization that was raised from the bottom up. It was never officially established as a standard setting body; its beginning was merely a group of people dealing with the technicalities of the Internet. And eventually their task became more complex along with their powers.

Therefore, the legitimacy of the establishment of ICANN was contested multiple times.[13] The relationship with the US was one of the core problems since its establishment, but not the only one. Another reoccurring issue is the paucity of legislation defining the scope of ICANN's powers, which the international community would prefer to control ICANN somehow. ICANN is limited only by memorandums and affirmations that are not enforceable. ICANN is constricted by numerous contracts as well, but again, with the US. There are no means of control beyond US borders.

The reason why its limited accountability should make the Internet community nervous, is because ICANN is a policy maker and at the same time maintains exhaustible resources. There is a discussion within United Nations about perceiving Internet access as a fundamental human right,[14] yet the resources essential for it are limited and subject to trade. Therefore, ICANN is an organization that is a public rule-maker and a private company with customer oriented approach at the same time. Those two do not go well together. However, there is not much of a dispute when it comes to efficiency of ICANN.

2. MODEL OF INTERNET GOVERNANCE

ICANN is a non-profit public benefit corporation that was registered in California in 1998. It is a corporation with no public authority, its autonomy gained through numerous contracts.[15] There are (at least) two reasons for the fact that one of the major governors of the Internet is a private corporation set up in one state. The first reason is that the Internet

---

[12] Mueller, M. L. (2010) *Networks and states: the global politics of Internet governance*, Mit Press, p. 64.

[13] See Chapter 4 in Bygrave, L. A. (2015) *Internet Governance by Contract*, Oxford University Press.

[14] 2016. *Draft resolution on the promotion, protection and enjoyment of human rights on the Internet*. [online] Available from: ap.ohchr.org/documents/E/HRC/d_res_dec/A_HRC_32_L20.docx [Accessed 10 May 2017].

[15] Bygrave, L. A. & Bing, J. (2009) *Internet governance: Infrastructure and institutions*, Oxford University Press, p. 112.

was originally a US invention and as such it was managed by US organizations. The second reason is that ICANN and associated bodies were created with the sole goal to manage the technical issues related with the Internet.[16] The unique controlling position of the US made sense at the time, when all of the Internet users were located in the US and perhaps a few other countries, but not since the Internet became a global phenomenon.[17]

ICANN's primary goal is to edit the root zone file: in other words, to manage the DNS. Having an organization with this function is critical for the existence of the Internet. Before ICANN was established, the Internet was viewed as a free, self-governing, politically neutral entity. It was not until later that ICANN took over other tasks as well and became a centralized body controlling the Internet. This transformation was criticized by the public.[18]

2.1 ESTABLISHMENT OF ICANN

ICANN was not built in a day. Its main goal, to control the DNS, was originally managed by the Internet Assigned Numbers Authority (IANA). It was upon IANA to decide which domains would be marked as TLDs (top level domains, such as .com) and how a domain name could be registered. The first public reference acknowledging IANA's existence can be found in a memo considering Internet protocol standards from 1988. The significance of the root file was yet to be discovered, hence there was no public scrutiny concerning IANA's establishment and who was in charge. It was one Jon Postel, a UCLA[19] graduate student, working in the Information Science Institute, who was enlisted as an IANA contact in the memo.

Jon Postel's task was to coordinate the Internet protocol and assign IP numbers and domain names. Therefore, it was solely in his hands, as the head of the department, to decide which TLDs would be created. He was also personally registering domain names.[20]

---

[16] More on establishment of ICANN in Mueller, M. (2002) *Ruling the root: Internet governance and the taming of cyberspace*, MIT Press.

[17] Froomkin, A. M. (2011) Almost Free: an Analysis of ICANN`s 'Affirmation of Commitments'. *Journal of Telecommunications and High Technology Law*, 9, p. 194.

[18] Mueller, M. L. (2010) *Networks and states: the global politics of Internet governance*, MIT Press, p. 64.

[19] The University of California in Los Angeles.

In these days, IANA was working on consensus based procedures, when it came to adoption of Internet standards. This pleased the Internet community, however the situation changed once the US Government gained more control over IANA. Under a series of contracts, control passed to The US Department of Commerce.[21] A wave of criticism followed. An important question was raised. Is any government entitled to legitimize an organization governing a world-wide rare resource, and if so, why is it only one government on its own?[22] The response of the US was to privatize IANA by creating ICANN, a private company, which officially took control over IANA's functions in 1999[23] when the government's contracts expired.

2.2 SELF-REGULATING INDUSTRY

There is not one central body governing the Internet.[24] The task is spread amongst multiple bodies with various backgrounds, and ICANN is just one of them. Whereas the opinions on the efficiency of this system differ, the validity of delegation of power to these bodies is widely deemed questionable; the same goes for their accountability.

On the basis of a closer look into this industry, it can be said that legitimacy issues are a sector specific problem.[25] Most of the governing bodies were raised from the bottom-up, and they were not formed with the purpose to adopt rules. Their focus lies on the technicalities; they were established to deal with the functions of the Internet, not with rule-making. However, in this industry, resolving of technical issues goes hand in hand with setting binding standards. As a user of the Internet, you cannot freely decide not to follow these standards, not because you can be legally punished for it, but because you will be disconnected from the network (except for those parts which follow the same standard as you do). Alternative standards do exist, but only one standard is accepted globally.

---

[20] More on conduct of ICANN during the early days and Jon Postel`s role can be found in Mueller, M. (2002) *Ruling the root: Internet governance and the taming of cyberspace*, MIT Press. Bygrave, L. A. & Bing, J. (2009) *Internet governance: Infrastructure and institutions*, Oxford University Press.

[21] Froomkin, A. M. (2003) Habermas@ discourse. net: Toward a critical theory of cyberspace. *Harvard Law Review*, 116, 749-873., pp. 840 – 841.

[22] Ibid., p. 94.

[23] Bygrave, L. A. & Bing, J. (2009) *Internet governance: Infrastructure and institutions*, Oxford University Press, p. 102.

[24] Ibid., p. 92.

[25] See also Bonnici, J. P. M. (2008) *Self-regulation in cyberspace*, Cambridge University Press.

Another thing that resulted from the rather uncommon nature of these governing bodies is that their roots lie originally in research facilities. Also, these facilities were connected with the US government, since the US is the place where the project unwound. In the beginning, the Internet was just a project; it was not until later that its significance exceeded US borders. Thereafter, the people working on the development of the Internet, engineers and researchers, continued working in those bodies and adopted decisions even after their significance expanded.

That is how this so-called self-regulating industry emerged. One of the characteristics of self-regulation is that the rules are adopted by those who are taking part in the activity. The main advantage of this system of regulation is that it is more flexible.[26] It allows skipping the middle man. If you are a part of that industry, you have the best notion of what is needed. You are the expert and the rule-maker at the same time.

One of the examples of such organization is IETF, the Internet Engineering Task Force. ICANN is considered to be a self-regulatory body as well, but with one exception: there is a state intervening in its affairs.[27] That is generally considered to be a disqualification for a self-regulating organization. But, as stated earlier, ICANN is of a rather special nature and does not fit in any categories.

This system of self-regulation puts above all its ability to implement a wide variety of its member's interests into its policy. It is run by a group of people that are themselves vested in the subject matter and on the basis of their experiences adopt regulation concerning their common interest. This is called a semi-autonomous social field (SASF)[28], and the rules adopted in that field are binding for its members. On the one hand, if members adopt the rules themselves, they are more likely to be satisfied with them. On the other hand, are all of the affected parties truly present or just "*most*" of them? All interests should be represented equally, and if not, the effectively and legitimacy of that system can be doubted.[29]

[26] Ibid., pp. 23-24.
[27] Ibid., pp. 25-26.
[28] Ibid., pp. 25-26.
[29] Ibid., p. 102.

2.3 INTERNET ENGINEERING TASK FORCE AS A ROLE MODEL

IETF is another self-regulating organization operating on the Internet field. IETF deals with standard-setting processes; its first meeting, held in 1986, was attended by 21 US government officials. Since 1991, these meetings became open to non-governmental organizations as well, and later the organization became independent from the US government.[30] That constitutes the biggest difference between IETF and ICANN.

IETF does not have regular members; it is made of volunteers. Meetings of IETF are open to all, and everyone can join its mailing list and help develop Internet standards. Everyone, without discrimination, has a say. When ICANN was formed it sought to enjoy the same source of legitimacy as IETF.[31] ICANN considers IETF to be an exemplary model of what a self-governing multistakeholder organization should look like.[32] What is a stakeholder? A person, group or organization that has vested its interest or stake in organizations like ICANN or IETF because it is capable of affecting the organization or/and being affected by it.[33] Therefore, a multistakeholder organization is such an organization that allows multiple entities to influence its decisions.

Following IETF's model, ICANN also opened the discussion for volunteers, and its meetings are public. However, it is facing critique for making it hard for an ordinary user to be truly heard. Unlike IETF, ICANN does not discuss its matters on the Internet; therefore one must attend meetings of ICANN, which take place all around the world.

Furthermore, IETF is a standard setting body, whereas ICANN is a body governing a rare resource with the potential to affect competition by its actions. It manages a public resource on one hand; on the other, it is a private company capable of generating profit and has a customer driven approach as well.

---

[30] *Internet Engineering Task Force*. [online] Available from: https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force [Accessed 14 December 2016].

[31] Froomkin, A. M. (2003) Habermas@ discourse. net: Toward a critical theory of cyberspace. *Harvard Law Review,* 116**,** 749-873., pp. 842 – 843.

[32] Ibid., pp. 843 – 844.

[33] 2014. *Cross Community Working Group (CCWG) Charter*. [online] Available from: https://www.icann.org/news/announcement-2014-11-05-en [Accessed 14 January 2017], p. 2.

3. ACCOUNTABILITY

Even though ICANN is one of few organizations operating in the field of Internet governance, and we already established that the nature of all of these organizations is uncommon, ICANN faced criticism the most. ICANN chose to apply the multistakeholder model the same as IETF, but it did not treat all of the voices alike. So, unlike IETF, it did not have the public behind all of its actions. It did not have international support either, since the only sovereign capable of controlling ICANN was the US. And the US itself was step by step losing control over ICANN, although for a good reason: to satisfy other countries and to support the idea of truly independent organization.

As a result, ICANN was repetitively accused of being unaccountable.[34] But to whom should be ICANN accountable? And what do we mean, when we talk about „*accountability*"?

3.1 FIVE DIMENSIONS OF ACCOUNTABILITY

In 2005, an article discussing ICANN accountability was written by Jonathan GS Koppell. The mentioned article is called "*Pathologies of Accountability: ICANN and the Challenge of 'Multiple Accountabilities Disorder'*".[35] Accountability in Koppell's perspective reflects one's understanding of the place of bureaucracy in a democratic state.[36] Those who exercise power are bound to exercise it within external means and internal norms. Therefore, they are accountable for performing their actions within these borders. But each individual is accountable by different means, to different entities and with different consequences arising from the breach of these constraints. That is why Koppell states that it is unfortunate to use one word to describe several conditions, which may or may not be found all together.

Koppell then describes five dimensions of accountability that are generally referred to when talking about accountability. The typology is

---

[34] See Chapter 4 in Bygrave, L. A. (2015) *Internet Governance by Contract*, Oxford University Press.

[35] Koppell's article includes case study of ICANN and it shows very well the problem it is dealing with. ICANN accountability is suffering from something that Koppell describes as "*multiple accountabilities disorder*". It will serve to our purpose of defining accountability within ICANN well; nevertheless, keep in mind, that some of the issues with ICANN mentioned in Koppell's article itself are already resolved.

[36] Koppell, J. G. (2005) Pathologies of accountability: ICANN and the challenge of "multiple accountabilities disorder". *Public Administration Review*, 65, 94-108, p. 94.

as follows: an organization is 1) transparent, when it reveals facts about its performance, 2) liable when it faces the consequences of its actions, 3) controllable, if it follows the orders of a principal, 4) responsible, if it follows the rules and 5) responsive, when it is able to fulfil the demands.[37]

Koppell further elaborates on the typology. He stresses that transparency is an important instrument for assessing a company's performance, since transparent organizations explain or account for their actions and therefore admit mistakes and do not avoid scrutiny.[38]

Liability follows transparency. An entity is liable when it faces the consequences of its actions, is punished for unlawful behaviour or is rewarded for success. In the public sector, it relates to elected officials, who can be punished by removal from their office. For example, judges are not liable in this sense. In the private sector, managers are rewarded on the basis of their performance.[39]

Controllability requires the existence of another entity that has the power to induce behaviour on an organization, resulting in accountability of that organization to the controlling entity. The organization is constrained by the commands of the principal.[40]

On the other hand, if the actions of the organization are bound by laws, rules and norms (including professional standards, company policies), not by commands, we talk about responsibility.[41]

Finally, we have responsiveness, which is contrary to controllability and responsibility, a horizontal type of accountability. A company is responsive when its policy has a customer-oriented approach and when its attention focuses on the needs of its constituents.[42]

3.2 ICANN AND MULTIPLE ACCOUNTIBILITIES DISORDER

ICANN is an organization which was first established as a controllable organization, acting on the behalf of the US Government. The US is its superior, which must be satisfied with the actions of ICANN. However, its goal is to satisfy different groups of actors on the Internet field as well (for example, potential owners of TLDs, constituents). That further

[37] Ibid., p. 96.
[38] Ibid., p. 96.
[39] Ibid., p. 96-97.
[40] Ibid., pp. 97-98.
[41] Ibid., p. 98.
[42] Ibid., pp. 98-99.

establishes accountability in the means of responsiveness. ICANN itself desires to be responsive, to act on the basis of the needs of the community, but this notion sometimes clashes with other responsibilities of ICANN. ICANN's biggest struggle is with responsibility, since it failed to follow its own procedural norms repeatedly in the past, even to the extent that its elected officials were publicly criticizing the approach.[43]

When an organization fails to satisfy some of these different notions of accountability, it is simply marked as non-accountable. The different meanings of the term are ignored, as Koppell states in his article. Hence, if one focuses on responsibility, let's say, s/he would label ICANN as non-accountable, even though it would satisfy the criteria for responsiveness. This creates pressure on the organization. Every entity should be by design accountable only in the sense that is necessary for its proper function.

Those organizations, which behave on the basis of incentives from multiple entities, then suffer from something Koppell calls the "*multiple accountabilities disorder*", in other words the "*MAD*" problem. Such organization is expected to be accountable in every sense, and that is a challenge, if not impossible. The organization will sometimes emphasize the directives of principals, while at other times trying to focus on customers. In the long run, everyone is displeased.[44]

4. TRANSFORMATION OF ICANN

ICANN was always aware of the problem with its unclear accountability. The US thought that the creation of ICANN as a private corporation will soothe the critics of the on-going oversight of US Government over the Internet. But even after the transformation of IANA functions to ICANN, contracts with the Department of Commerce were still intact. ICANN dealt with the problem by multiple means, but the biggest changes came in three steps, the first of which was the Affirmation of Commitments from 2009, revisiting the ICANN-US relationship, followed by the creation of Cross Community Working Group in 2014 preparing the final departure of ICANN from the US government and dealing with accountability issues, finalized in 2016 by the IANA transition. As you can see, the major changes

[43] Froomkin, A. M. (2003) Habermas@ discourse. net: Toward a critical theory of cyberspace. *Harvard Law Review,* 116, pp. 749-873.

[44] Koppell, J. G. (2005) Pathologies of accountability: ICANN and the challenge of "multiple accountabilities disorder". *Public Administration Review,* 65, 94-108, p. 99.

have been made just recently, and it is still too early to say if they served their purpose.

4.1 AFFIRMATION OF COMMITMENTS

On September 30, 2009, the US Department of Commerce signed an Affirmation of Commitments with ICANN to review their relationship. The ICANN CEO states that ICANN remains a private non-profit organization, not under control of a single entity and reviewed by public scrutiny.[45] The US relationship with ICANN was maintained through a series of contracts, the most important of which is the Memorandum of Understanding, which later transitioned into the Joint Project Agreement (2008) and the IANA contract.[46]

As the IANA contract was about to expire in 2011, there was a hope for ICANN to gain more independence. However, the Affirmation of Commitments does not cover the future of the IANA contract at all, resulting in doubt that an actual change will happen. Still, the Affirmation grants ICANN more independence, and it is clear that the US Government is willing to address the critique for not letting ICANN be free. This is proven by the commitment of the US not to prolong the Joint Project Agreement, as is stated in the first paragraph of the Affirmation.[47]

The rest of the stipulations not to interfere with ICANN tasks made by the Department of Commerce, even though promising, are not to be taken for granted. There is no enforceability of such statements.

4.2 CROSS-COMMUNITY WORKING GROUP

Enhancing ICANN accountability became the primary goal of the ICANN community. In 2014, an intention to evaluate ICANN accountability was laid down, and for that purpose a Cross-Community Working Group on Enhancing ICANN Accountability (herein after "*CCWG*") was created. All the criticism on ICANN during its short existence made clear that ICANN needs to review its accountability standards to satisfy its constituents.

The promises in the Affirmation of Commitments were held after all, and the US Government let the Joint Project Agreement expire. New

[45] Froomkin, A. M. (2011) Almost Free: an Analysis of ICANN`s 'Affirmation of Commitments'. *Journal of Telecommunications and High Technology Law,* 9, p. 188.

[46] Ibid., p. 192.

[47] Ibid., p. 198.

revision mechanisms were needed to compensate for the loss of the principal.[48] Since the IANA contract was prolonged only for it to expire in 2016 instead of 2011, another important matter was to be discussed.

Unfortunately, the first ICANN proposal to create a revisory body was not met pleasantly by the public. A community driven change was demanded. A CCWG was formed as a result of a meeting convened by the board in Los Angeles.[49] The CCWG was established as a body that was proposed by the multistakeholder community, to be run by the community, and accessible to anyone willing to contribute.[50]

The CCWG has two goals, represented by two separate work streams. One is to propose solutions for enhancing ICANN's accountability within the time frame of IANA transition. The second goal is to focus on addressing accountability topics unrelated to The transition that can be implemented after the transition.[51]

4.3 NEW BYLAWS

The first proposal by the CCWG was drafted in May 2015.[52] It proposes to amend the bylaws of ICANN to specify what ICANN does — not changing it, just clarifying. New revisory mechanisms should be adopted to control that ICANN stays within the limits of the bylaws and the purpose stated therein. This Independent Review Process will be granted powers to reject or approve changes to the bylaws, reject proposals (budget, operating and strategic plans), remove a member of the board or to recall the entire board. The goal of this provision is to be able to resolve a situation when there is an impasse in finding a consensus.[53]

New bylaws were adopted on May 27, 2016 as a result of the CCWG efforts. Article III of the bylaws is dealing with Transparency, and Article IV is designated to Accountability and Review.[54] The bylaws propose to enhance transparency by the pledge to make information on its tasks

[48] *ICANN accountability*. [online] Available from: https://icannwiki.com/ICANN_Accountability [Accessed 5 December 2016].

[49] Ibid.

[50] The working progress can be observed and the effort joined here: https://community.icann.org/display/acctcrosscomm/WS1+-+Enhancing+ICANN+Accountability.

[51] 2014. *Cross Community Working Group (CCWG) Charter*. [online] Available from: https://www.icann.org/news/announcement-2014-11-05-en [Accessed 14 January 2017], p. 2.

[52] *ICANN accountability*. [online] Available from: https://icannwiki.com/ICANN_Accountability [Accessed 5 December 2016].

[53] Ibid.

and meetings publicly available and for that purpose adopt a new Documentary Information Disclosure Policy and Independent Review proceedings.

Revised accountability mechanisms include the following instruments:

- Reconsideration Process, which allows those materially affected by ICANN decisions to request a reconsideration of that action by the Board;
- Independent Review Process, which allows those eligible to request Reconsideration Process to request also a review by a third independent party, if ICANN performs an action that can be deemed to be in collision with the bylaws. The result of such Review is then published on the ICANN webpage.
- Ombudsman, which is an independent entity, who can evaluate the complaints of members of the ICANN community who are deemed to be treated unfairly by a member of ICANN staff, Board or constituent body.[55]

4.4 IANA STEWARDSHIP TRANSITION

In March 2014, the intent to hand over IANA functions to the global multistakeholder community was announced. Since that meant abandoning the historical contractual relationship with the US, the CCWG was also given the task to consider the impact of the transition on ICANN's accountability.

On October 10, 2016, the contract between IANA and the US Department of Commerce expired.[56] Following a long process starting in 2014[57] preparing the transition of IANA to the hands of the Internet global community, the cord between ICANN and the US Government, representing 20 years of development, was cut.

---

[54] *BYLAWS for INTERNET CORPORATION for ASSIGNED NAMES AND NUMBERS*. [online] Available from: https://www.icann.org/resources/pages/bylaws-2016-02-16-en [Accessed 5 December 2016].

[55] *Accountability Mechanisms*. [online] Available from: https://www.icann.org/resources/pages/mechanisms-2014-03-20-en [Accessed 10 December 2016].

[56] *Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends*. [online] Available from: https://www.icann.org/news/announcement-2016-10-01-en [Accessed 14 December 2016].

[57] The process of the transition is available to public scrutiny here: https://www.icann.org/resources/pages/transition-2014-03-23-en

Regardless of how dramatically the "*hand-over of the Internet*" was perceived by media, from the viewpoint of an ordinary user, nothing changes. But those, who are interested in participating, can sign up to a newsletter and watch the progress online.[58]

5. ICANN IN THE PRESENT

As Koppell states, the MAD problem is bestowed upon those organizations that are trying to listen to commands from multiple sources. Therefore, it can be partially fixed by clarifying the goal of the organization and acting accordingly with the sole purpose of achieving that goal. The problem of ICANN was its need to respond to commands from above, as well as from the bottom. Since the cord to the US Government was recently cut, ICANN can now fully focus on satisfying the Internet community.

Nevertheless, keep in mind that the power to control an agency operating in a complex, technical area is always small, since a citizen's ability to make resolved judgment in the field is limited.[59] Such a company will always have broader borders for its behaviour. Now, with the election process established for ICANN, there is at least a way to make the elected officials liable for their unsatisfying actions and to remove them from office. And with the US Government out of the picture, ICANN is now not divided between its principal and its constituents.

From 2014, when the preparation for the transition started, ICANN claims to be willing to hear out everyone who wants to participate, the same as its role model IETF does. The only difference between a member appointed by a chartering organization and an individual participant is that the unappointed participant cannot have a say in a consensus call or a decision.[60]

Even after the transition, ICANN remains dependant on multiple contracts granting it its power. This organisation does not derive from traditional legislative bodies and is not governed by public international law.[61] Criticism may not be the only result of ICANNs specific nature, as there are already judicial disputes over its legitimacy.

---

[58] Sign up to a newsletter is available on https://icannwiki.com/

[59] Koppell, J. G. (2005) Pathologies of accountability: ICANN and the challenge of "multiple accountabilities disorder". *Public Administration Review,* 65**,** 94-108, p. 97.

[60] 2014. *Cross Community Working Group (CCWG) Charter*. [online] Available from: https:// www.icann.org/news/announcement-2014-11-05-en [Accessed 14 January 2017], p. 5.

[61] See Chapter 4 in Bygrave, L. A. (2015) *Internet Governance by Contract,* Oxford University Press.

In 2006, Danish Supreme Court dealt with the question, whereas the Memorandum of Understanding (later transformed in the Joint Project Agreement, as discussed above) signed between ICANN and US Department of Commerce gives ICANN the competence to manage .dk domains. The decision was, that it is indeed possible to constitute legal competence by delegation via contract.[62]

Similar issue concerning ICANN's power over area specific domains was raised in front of California Superior Court. The case revolved around the right to delegate the .africa top level domain, a dispute between ICANN and DotConnectAfrica (DCA) originating in 2013. Both preliminary injunctions by DCA were dismissed so far.[63]

6. CONCLUSION

The transition of ICANN does not fix all its problems. Only a legal framework could amend the shortcomings with the responsibility dimension of accountability. So far, there are no legal requirements for ICANN. ICANN is trying to compensate for the lack of it by setting out its own behavioural norms and policies. Despite that, it can be expected that its unclear responsibility will remain a major issue for ICANN and will be challenged once more in the future.

LIST OF REFERENCES

[1] 1987. *Domain names: implementation and specification*. [online] Available from: http://www.ietf.org/rfc/rfc1035.txt [Accessed 14 January 2017].

[2] 2005. *Report of the Working Group on Internet Governance*. [online] Available from: http://www.wgig.org/docs/WGIGREPORT.pdf [Accessed 12 February 2016].

[3] 2011. *Free Pool of IPv4 Address Space Depleted*. [online] Available from: https://www.nro.net/ipv4-free-pool-depleted/ [Accessed 10 May 2017].

[4] 2014. *Cross Community Working Group (CCWG) Charter*. [online] Available from: https://www.icann.org/news/announcement-2014-11-05-en [Accessed 14 January 2017].

[5] 2016. *Draft resolution on the promotion, protection and enjoyment of human rights on the Internet.* [online] Available from: ap.ohchr.org/documents/E/HRC/d_res_dec/A_HRC_32_L20.docx [Accessed 10 May 2017].

[62] See Chapter 4 in ibid.

[63] *ICANN Free to Proceed with the Delegation of AFRICA Following Court Decision*. [online] Available from: https://www.icann.org/news/announcement-3-2017-02-09-en [Accessed 15 May 2017].

[6] *Accountability Mechanisms*. [online] Available from: https://www.icann.org/resources/pages/mechanisms-2014-03-20-en [Accessed 10 December 2016].

[7] Bonnici, J. P. M. (2008) *Self-regulation in cyberspace*, Cambridge University Press.

[8] Bygrave, L. A. & Bing, J. (2009) *Internet governance: Infrastructure and institutions*, Oxford University Press.

[9] Bygrave, L. A. (2015) *Internet Governance by Contract,* Oxford University Press.

[10] *BYLAWS for INTERNET CORPORATION for ASSIGNED NAMES AND NUMBERS.* [online] Available from: https://www.icann.org/resources/pages/bylaws-2016-02-16-en [Accessed 5 December 2016].

[11] Froomkin, A. M. (2003) Habermas@ discourse. net: Toward a critical theory of cyberspace. *Harvard Law Review,* 116, pp. 749-873.

[12] Froomkin, A. M. (2011) Almost Free: an Analysis of ICANN`s 'Affirmation of Commitments'. *Journal of Telecommunications and High Technology Law,* 9.

[13] *ICANN accountability*. [online] Available from: https://icannwiki.com/ICANN_Accountability [Accessed 5 December 2016].

[14] *ICANN Free to Proceed with the Delegation of .AFRICA Following Court Decision*. [online] Available from: https://www.icann.org/news/announcement-3-2017-02-09-en [Accessed 15 May 2017].

[15] *Internet Engineering Task Force*. [online] Available from: https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force [Accessed 14 December 2016].

[16] Koppell, J. G. (2005) Pathologies of accountability: ICANN and the challenge of "multiple accountabilities disorder". *Public Administration Review,* 65**,** pp. 94-108.

[17] Mueller, M. (2002) *Ruling the root: Internet governance and the taming of cyberspace*, MIT Press.

[18] Mueller, M. L. (2010) *Networks and states: the global politics of Internet governance*, MIT Press.

[19] *Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends*. [online] Available from: https://www.icann.org/news/announcement-2016-10-01-en [Accessed 14 December 2016].

[20] *What is Ipv6?*. [online] Available from: https://www.apnic.net/community/ipv6/ [Accessed 10 May 2017].

<<< ARTICLES

COMMENTARIES >>>

DOI: 10.5817/MUJLT2017-1-9

THE NEW EU RULES ON ELECTRONIC INSOLVENCY REGISTERS

by

MICHAEL BOGDAN*

This paper deals with those provisions of the new EU Regulation No. 2015/848 on Insolvency Proceedings (Recast) that create a system of national insolvency registers and establish a decentralized system for the interconnection of such registers by means of the European e-Justice Portal.

KEY WORDS

E-justice, European Union, Insolvency Proceedings, Insolvency Registers

The EU Regulation No. 2015/848 of the European Parliament and of the Council on Insolvency Proceedings (Recast), published in the Official Journal of the European Union on 5 June 2015,[1] is intended to replace, on 26 June 2017, the present Council Regulation No. 1346/2000 on Insolvency Proceedings.[2] Even though the new Insolvency Regulation (in the following "*the Regulation*") purports to be a mere recast of its predecessor, it contains a number of new features, one of them being the subject of this paper.

The Regulation, like its predecessor, accepts the fact that the rules of substantive insolvency law, such as rules on security interests and preferential rights, vary widely among the Member States of the European Union, making it impossible to introduce truly European

* Michael.Bogdan@jur.lu.se, Professor of Law, University of Lund, Sweden.

1 Regulation (EU) No. 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings (recast). *Official Journal of the European Union* (O.J. 2015 L 141/19) 5 June. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:320 15R0848 [Accessed 31 May 2017].

2 Council regulation (EC) No. 1346/2000 of 29 May 2000 on insolvency proceedings. *Official Journal of the European Communities* (O.J. 2000 L 160/1) 30 June. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000R1346&qid=1496217899248 [Accessed 31 May 2017].

insolvency proceedings, treating the whole EU as a single jurisdiction. No attempt is made to create supra-national insolvency proceedings governed by EU law. The system is based on national proceedings, governed by national law, and the national insolvency laws are neither unified nor harmonized, subject to some minor exceptions. The Regulation limits itself in principle to regulating aspects of private international law, such as jurisdiction, applicable law, recognition and enforcement, and cross-border cooperation. Like other instruments enacted within the framework of judicial cooperation in civil matters, the Regulation does not apply in relation to Denmark.

The basic controversy within international insolvency law is the conflict between the territorially limited powers of each individual State on the one hand and on the other hand, the very purpose of insolvency proceedings (in the following in an oversimplified manner referred to as "*bankruptcy*"), i.e. to achieve control of the totality of the debtor's assets in order to achieve the equal treatment of all creditors. At first glance, it might seem that the principle of universality of the proceedings, meaning that there should always be only one single bankruptcy adjudication comprising all assets regardless of where they are situated, is the optimal solution to this conflict. If applied in its pure form, this principle gives exclusive bankruptcy jurisdiction to the courts of one single country, for instance, the country of the debtor's domicile or seat. The courts in other countries must abstain from initiating rival proceedings, recognize the foreign bankruptcy administrator's right to dispose of the local assets and stop individual creditors who might attempt to attach such assets. All creditors have to lodge their claims in the sole bankruptcy proceedings and satisfy themselves with the dividends they receive in those proceedings. in real life, however, things are not that simple. Reasonable and realistic solutions in this field must be based on compromises between the principle of universality and the opposite principle of territoriality, which, in its pure form, means that a bankruptcy comprises only the assets situated in the country where the bankruptcy was opened and that separate bankruptcy proceedings have to be initiated in each country where the debtor owns assets.

The system created by the EU is consequently also based on a compromise between the two principles. The starting point and the main rule, following from Article 3(1) of the Regulation, is that

the Regulation applies only where the debtor's "*centre of main interests*" is situated within the territory of a Member State, and that the courts of that Member State have exclusive jurisdiction to open "*main insolvency proceedings*" comprising the debtor's assets in the whole EU (whether the proceedings have the ambition to comprise assets outside of the EU is not dealt with by the Regulation and depends thus on the national law of the Member State of the opening of the proceedings). This basically universalist, or at least truly European, approach is partially modified by the same Article 3, which allows each Member State where the debtor owns an establishment to open insolvency proceedings despite the debtor's centre of main interest being in another Member State; the effects of such secondary insolvency proceedings are, however, territorial in the sense that they are restricted to the assets of the debtor situated in the territory of the Member State where they have been opened.

One of the major obstacles standing in the way of the universality or extraterritorial effects of bankruptcies is the risk that persons residing in countries other than the country of the opening of the proceedings do not find out about them, since the usual publicity measures, such as advertising in the official gazette of the country of bankruptcy, have very little effect abroad. This may lead to two types of negative consequences. The first type is that creditors residing in other countries may suffer economic losses due to their failure to participate in the proceedings by lodging their claims or due to lodging their claims too late. The second is that persons abroad who owe debts to the bankrupt, unaware of the opening of the proceedings and of the bankrupt's loss of legal control of his assets, discharge their debts to the bankrupt instead of to the bankruptcy administrator (in the Insolvency Regulation of 2000 ominously called "*liquidator*", but in the new Regulation given the more appealing title "*insolvency practitioner*"). As the Regulation grants "*main insolvency proceedings*" extraterritorial effects within the whole EU, it is compelled to deal with the potential negative consequences of the two kinds just described.

The need to protect persons who, acting in good faith, pay their debts to the bankrupt instead of to the bankruptcy administrator is dealt with by Article 28 of the Regulation, which obliges the insolvency practitioner to request that notice of the judgment opening the proceedings be published in any other Member State where the debtor has an establishment, in accordance with the publication procedures provided

for there. He can request such publication also in other cases, if he deems it necessary. The law of the Member State of an establishment, or where the debtor owns immovable property, can also require that the decision be published in the land register, company register or any other public register (Article 29). Registration according to Article 28 must not be made a precondition for the recognition of the proceedings opened in another Member State (Recital 75), but it can be decisive for the determination of whether a person, who has paid his debt there to the bankrupt[3] instead of to the insolvency practitioner, has acted in good faith and is therefore discharged of the debt (Article 31). Payments made before the publication are presumed, in the absence of proof to the contrary, to have been made in good faith, while later payments are presumed to have been made with knowledge about the opening of the proceedings. These provisions are similar but not identical to Articles 21, 22, and 24 of the Regulation of 2000. For example, while Article 21 of the 2000 Regulation provides that the bankruptcy administrator "*may*" request that notice of the judgment opening the proceedings be published in another Member State, Article 28 of the new Regulation stipulates that such request must ("*shall*") be made in any Member State where the debtor has an establishment. The abovementioned registers can in most European countries nowadays be accessed online, but this depends on the domestic law of the country of the register concerned.

The described publicity measures do not, however, remove the most difficult problem caused by the fact that the foreign creditors of the bankrupt may not be aware of the proceedings and thus fail to lodge their claims in a timely manner. Such creditors may reside in many countries, and their existence and residence may be unknown to the bankruptcy administrator. Advertising every bankruptcy in all other Member States would be expensive and require much administrative work. The idea of advertising all bankruptcies, or at least all bankruptcies with substantial assets, in a special annex to the *Official Journal of the European Communities* was discussed several decades ago and quickly discarded due to the large daily volumes it would require. The advent of the new information technologies has radically changed the situation, making it possible to easily access and process large amounts of information

[3] See the ECJ judgment *Van Buggenhout v. Banque internationale* (2013) Case C-251/12, Court of Justice of the European Union (Third Chamber), 19 September.

in a digital form. The focus of this paper is, therefore, on a completely new feature in the new Regulation's Articles 24-27, namely the system of interconnected national insolvency registers having no counterpart in the Regulation of 2000. This novelty will be of great practical importance, even though pursuant to Article 24(5) the publication of information in this system of registers will not have any legal effect under the Regulation other than that set out in national law and in Article 55(6), the latter requiring creditors to lodge their claims within the period of time stipulated by the law of the Member State of the opening of the proceedings. In respect of creditors from the other Member States, this period must not be less than thirty days following the publication of the opening in the insolvency register of the Member State of the proceedings.

Article 24(1) of the new Regulation obliges the Member States, by 26 June 2018, to establish and maintain in their territory a national register or several national registers called "*insolvency registers*", where information concerning insolvency proceedings is to be published as soon as possible after the proceedings have been opened. The registers will be accessible to the general public, so that the information contained therein will be publicly available. Article 24(2) lists the information that must be made public in this manner (the Regulation speaks of "*mandatory information*"). The list includes, inter alia, the type and date of the opening of the insolvency proceedings, the court and the case number (if any), whether the proceedings are "*main insolvency proceedings*" or not, the debtor's name, registration number (if any) and address, the name and address of the appointed insolvency practitioner, where and how the decision opening the proceedings can be challenged and, most importantly, the time limit for lodging claims or a reference to the criteria for calculating that time limit. If they wish, Member States are free to include in their registers additional information; they may make access to such additional information conditional, for example, upon the existence of a legitimate interest on the part of the person requesting the information. Such conditions cannot, however, be imposed as far as access to the mandatory information is concerned.

In view of Article 24(3), permitting Member States to include additional information in their insolvency registers, and Article 24(5), permitting Member States to give the publication in their insolvency registers additional legal effects set out in national law, it seems that a Member State

can use its new insolvency register to replace the traditional publication in the Official Gazette and thus give the register even the effects under Article 31 regarding the discharge of debtors who have paid their debts to the bankrupt instead to the bankruptcy administrator (see supra).

Article 24 does not explicitly require that the national insolvency registers be accessible in an electronic form, but that requirement, which was probably considered so self-evident that it was not worth mentioning, follows from the rules in Article 25 on the interconnection of the national insolvency registers described above.

In accordance with Article 25(1), the Commission will namely establish a system for the interconnection of the national insolvency registers, composed of the national registers themselves and a central public electronic "*access point*" functioning as entrance to the information contained therein. As this access point will serve the existing European e-Justice Portal, which will provide a search service in all of the EU official languages. Pursuant to Article 25(2)(a), the Commission is required to issue, by 26 June 2019, implementing acts regulating the various technical aspects of the interconnection, such as the technical specifications

> *"defining the methods of communication and information exchange by electronic means on the basis of the established interface specification of the system of interconnection of insolvency registers,"*

the minimum information technology security standards for communication and distribution of information, minimum criteria for the search service provided by the European e-Justice Portal, minimum criteria for the presentation of the results of such searches, and a glossary containing a basic explanation of the national insolvency proceedings of the Member States.

While each Member State will bear the costs of its national insolvency register, the establishment, maintenance and future development of the system of interconnection of insolvency registers will pursuant to Article 26 be financed from the general budget of the EU. The "*mandatory information*" in the registers will be publicly available free of charge, but the Member States can impose a reasonable charge for access to the voluntary additional information contained therein; this applies even

if it is accessed through the system of interconnection of insolvency registers via the European e-Justice Portal.

The creation of the system of national insolvency registers and their interconnection at the European level will require a substantial effort and time. Even though the Regulation as such is to apply to insolvency proceedings opened after 26 June 2017, exception is therefore made for the new register system. According to Article 92, the provisions on establishment of national insolvency registers in Article 24(1) will not apply before 26 June 2018, and Article 25 on the interconnection of insolvency registers will not apply before 26 June 2019. This should give the Member States and the Commission sufficient additional time to construct and test the system.

The functioning of interconnected national insolvency registers involves obviously sharing of potentially sensitive personal information concerning debtors who are natural persons (human beings). Therefore, Article 24(4) gives the Member States the right not to include in their national registers information relating to individuals not exercising an independent business or professional activity, or to exclude such information from the European interconnecting registration system. The publication of "*mandatory information*" in the insolvency register and in the European system can with regard to such persons be replaced by individually informing known "*foreign creditors*" (meaning creditors having their habitual residence, domicile or registered office in the other Member States), but the proceedings in question shall not affect the claims of such creditors who have not received the information.

Equally important is that all processing by the Member States of personal data within the framework of the Regulation will be in principle subject to EU rules on the protection of personal data, namely Regulation No. 2016/679 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,[4] whereas the Commission's European e-Justice Portal must abide by Regulation No. 45/2001 on the Protection of Individuals with regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data.[5] According to Article 79 of the Insolvency Regulation, each Member State must designate a person or body that will exercise the functions of controller in accordance with the EU personal data protection rules and communicate its name to the Commission, which will publish it on the European e-Justice portal. With regard to that Portal, it is the Commission itself that will assume the responsibilities of controller pursuant to Regulation No. 45/2001. Articles 82 and 83 of the Insolvency Regulation make it clear that the Portal will not store any personal data, which will be kept in the national insolvency registers only and remain accessible via the Portal only for as long as they remain accessible in the national registers pursuant to national law.

LIST OF REFERENCES

[1] Regulation (EU) No. 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings (recast). *Official Journal of the European Union* (O.J. 2015 L 141/19) 5 June. Available from: http://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/uri=CELEX:32 015 R0848 [Accessed 31 May 2017].

[4] Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union (*O.J. 2016 L 119/1) 4 May. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX: 32016R0679 [Accessed 31 May 2017]. At the time of writing, this new Regulation is not yet applicable, but it will become applicable as from 25 May 2018, i.e. simultaneously with the beginning of the use of national insolvency registers and one year before the interconnection of national insolvency registers starts functioning on 26 June 2019. Regulation No 2016/679 will on 25 May 2018 replace the current Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, O.J. 1995 L 281 p. 31. The new Insolvency Regulation refers in Article 78 and 79 to Directive 95/46, but these references shall be construed as references to Regulation No 2016/679, see Article 94 thereof.

[5] Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. *Official Journal of the European Communities* (O.J. 2001 L 8/1) 12 January. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001R0045 [Accessed 31 May 2017].

MUJLT Official Partner (Slovakia)

AS Legal s.r.o., Law Office
www.aslegal.sk

MUJLT Official Partner (Czech Republic)

ROWAN LEGAL, advokátní kancelář s.r.o.
www.rowanlegal.com/cz/

Cyberspace 2016 Partner

Wolters Kluwer ČR, a. s.
www.wkcr.cz

Cyberspace 2016 Partner

AION CS
www.aion.cz

Cyberspace 2016 Media Partner

PRÁVNÍ PROSTOR.CZ
www.pravniprostor.cz

Notes for Contributors

Focus and Scope

Masaryk University Journal of Law and Technology (ISSN on-line 1802-5951, ISSN printed 1802-5943) is a peer-reviewed academic journal which publishes original articles in the field of information and communication technology law. All submissions should deal with phenomena related to law in modern technologies (e.g. privacy and data protection, intellectual property, biotechnologies, cyber security and cyber warfare, energy law). We prefer submissions dealing with contemporary issues.

Structure of research articles

Each research article should contain a title, a name of the author, an e-mail, keywords, an abstract (max. 1 500 characters including spaces), a text (max. 45 000 characters including spaces and footnotes) and list of references.

Structure of comments

All comments should contain a title, a name of the author, an e-mail, keywords, a text (max. 18 000 characters) and a list of references.

Structure of book reviews

Each book review should contain a title of the book, a name of the author, an e-mail, a full citation, a text (max. 18 000 characters) and a list of references.

Structure of citations

Citations in accordance with AGPS Style Guide 5th ed. (Harvard standard), examples:

Book, one author: Dahl, R. (2004) *Charlie and the Chocolate Factory*. 6th ed. New York: Knopf.
Book, multiple authors: Daniels, K., Patterson, G. and Dunston, Y. (2014) *The Ultimate Student Teaching Guide.* 2nd ed. Los Angeles: SAGE Publications, pp.145-151.
Article: Battilana, J. and Casciaro, T. (2013) The Network Secrets of Great Change Agents. *Harvard Business Review*, 91(7) pp. 62-68.
Case: *Evans v. Governor of H. M. Prison Brockhill* (1985) [unreported] Court of Appeall (Civil Division), 19 June.
Citation Guide is available from: https://journals.muni.cz/public/journals/36/download/CitationguideMUJLT.pdf

Formatting recommendations

Use of automatic styles, automatic text and bold characters should be omitted.
Use of any special forms of formatting, pictures, graphs, etc. should be consulted.
Only automatic footnotes should be used for notes, citations, etc.
Blank lines should be used only to divide chapters (not paragraphs).
First words of paragraphs should not be indented.
Chapters should be numbered in ordinary way – example: "5.2 Partial Conclusions".

Submissions

Further information available at
https://journals.muni.cz/mujlt/about

Dan Jerker B. Svantesson: Editorial 3

LIST OF ARTICLES

Ioannis Revolidis: Judicial Jurisdiction over Internet Privacy Violations and the GDPR: a Case of "Privacy Tourism"? 7

Pieter Van Cleynenbreugel: The European Commission's Geo-blocking Proposals and the Future of EU E-commerce Regulation 39

Anabela Susana de Sousa Gonçalves: Choice-of-court Agreements in the E-commerce International Contracts 63

Ulf Maunsbach: The CJEU as an Innovator – a New Perspective on the Development of Internet Related Case-law 77

Anna-Maria Osula, Mark Zoetekouw: The Notification Requirement in Transborder Remote Search and Seizure: Domestic and International Law Perspectives 103

Ilona Stadnik: What Is an International Cybersecurity Regime and How We Can Achieve It? 129

Veronika Žolnerčíková: ICANN: Transformation of Approach towards Internet Governance 155

LIST OF COMMENTARIES

Michael Bogdan: The New EU Rules on Electronic Insolvency Registers 175