European University Institute
ROBERT SCHUMAN CENTRE FOR ADVANCED STUDIES

WORKING PAPERS

RSCAS 2019/03
Robert Schuman Centre for Advanced Studies

Off-line Digital Jurisdiction

Mariavittoria Catanzariti

European University Institute
Robert Schuman Centre for Advanced Studies

Off-line Digital Jurisdiction

Mariavittoria Catanzariti

EUI Working Paper **RSCAS** 2019/03

ISSN 1028-3625

Printed in Italy, January 2019
European University Institute
Badia Fiesolana
I – 50014 San Domenico di Fiesole (FI)
Italy
www.eui.eu/RSCAS/Publications/
www.eui.eu
cadmus.eui.eu

Robert Schuman Centre for Advanced Studies

The Robert Schuman Centre for Advanced Studies, created in 1992 and currently directed by Professor Brigid Laffan, aims to develop inter-disciplinary and comparative research on the major issues facing the process of European integration, European societies and Europe's place in 21st century global politics.

The Centre is home to a large post-doctoral programme and hosts major research programmes, projects and data sets, in addition to a range of working groups and *ad hoc* initiatives. The research agenda is organised around a set of core themes and is continuously evolving, reflecting the changing agenda of European integration, the expanding membership of the European Union, developments in Europe's neighbourhood and the wider world.

For more information: http://eui.eu/rscas

Abstract

The paper examines the issue of the jurisdiction over personal data from a particular angle: it aims to investigate the conditions under which European law might be competitive with other legal systems by strengthening the protection of fundamental rights such as data protection and privacy within trans-border relations and, in particular, by widening the scope of European courts' jurisdiction in such cases.

The aim of the paper is to show the clash between the un-physical nature of information as commodity and the physical notion of state borders, upon which the notion of jurisdiction is based. Such endeavor explores the use of extraterritoriality of data protection and privacy in international law, with the purpose of finding broader solutions inspired to functional criteria other than the territorial connection.

Keywords

Data Jurisdiction; State sovereignty; Territory; Data protection; Privacy

1. Introduction[*]

'Off-line digital jurisdiction' is apparently an oxymoron. From the legal standpoint, it links together creaky terms forced to coexist. Nonetheless, the reality goes much beyond what the law can do through regulatory measures. Not all that is in nature is possible in law and not all that is in law is possible in nature. Digitization highlights the shortcomings of a sovereignty model centred on the notion of territory, as the internet is borderless by definition.[1]

In the 'off-line' world the paradigm of territorial jurisdiction has been developed since the Middle Ages[2] as the foundation of state sovereignty. Jurisdiction and sovereignty are conceived as interdependent terms, as any definition of sovereignty is strictly tied to the exercise of jurisdiction by a state over a territory.[3] According to the territoriality principle, a state exerts jurisdiction over activity that occurs within its territorial borders[4]. Territory can thus be both the object of power and the limit to the power of other nation states.[5]

In the words of Neil Walker,

> "Sovereignty has long held a dual significance in legal thought. It has been part of the deep and taken-for-granted conceptual structure through which law is authorized and organized as law and in terms of which we are able to conceive of legal order in general."[6]

This quintessential notion of sovereignty is profoundly rooted in the Western legal tradition as it is based on the category of territory. The notion of state positive law has been accepted as a state's control over a territory. Indeed, the conceptualization of territory levels differences among the population, as the existence of a territory in itself does not require that the people living in that territory have a common characteristic.[7] The definition of sovereignty provided by Grotius, as "absolute power within a community and absolute independence externally and full power as a legal person in international law,"[8] is clear enough to imply that without relying on territory there would be no internal or external limits to sovereign powers.

---

[*] Jean Monnet Fellow at the Robert Schuman Centre of the EUI during the academic year 2017/18.

1 On the idea of the 'tyranny of territoriality,' see D. J. B. Svantesson, *Solving the Internet Jurisdiction Puzzle* (Oxford University Press, 2017), 13; D. J. B. Svantesson, *International Information Sovereignty*, in Polčák, R. and Svantesson, D. J. B., *Information Sovereignty. Data Privacy, Sovereign Powers and the Rule of Law*, (Edward Elgar, 2017), 32, 34.

2 In general, see C. H. McHilwain, *Constitutionalism: Ancient and Modern*, (Cornell University Press, 1947), 115; Pietro Costa, *Jurisdictio. Semantica del potere politico nella pubblicistica medievale (1100-1433)*, (Giuffrè, 2002), 63, 105; for a historical analysis of the territoriality principle, see C. Ryngaert, *Jurisdiction in International Law*, (Oxford University Press, 2008), 45-54.

3 A. Peters, *Membership in the Global Constitutional Community*, in *The Constitutionalization of International Law*, (Oxford University Press, 2009), 181.

4 M. N. Schmitt (ed.), *Tallinn Manual 2.0 on International Law applicable to cyber operations*, (Cambridge University Press, 2017), 52: "Jurisdiction is closely related to the principle of State sovereignty (Rule 1). Since sovereignty is predominantly territorial under international law, the most common basis for the exercise of jurisdiction is territoriality. Under international law, a State enjoys full territorial jurisdiction (prescriptive, enforcement, and judicial) over persons and objects located on its territory, as well as conduct occurring there (Rule 9)"; see D. Ireland-Piper, *Accountability in Extraterritoriality. A Comparative and International Law Perspective*, (Edward Elgar, 2017), 23.

5 According to R. Bernhardt (ed.), *Encyclopaedia of Public International Law*, (Oxford University Press, 2003), 512, "State sovereignty in the sense of contemporary public international law denotes the basic international legal status of a State that is not subject, within its territorial jurisdiction, to the governmental, executive, legislative, or judicial jurisdiction of a foreign State or to foreign law other than public international law."

6 R. Rawlings, P. Leyland and A. L. Young (eds.), *Sovereignty and the Law. Domestic, European and International Perspectives*, (Oxford University Press, 2013), 18.

7 A. Khan, *The extinction of Nation-States*, American University International Law Review, (1992), vol.7 (2):197.

8 H. Grotius, *De Iuri Belli ac Pacis Libri Tres* (The Law of War and Peace in Three Books), Prolegomena §§ 14-15, F. Kelsey transl. 1925, original 1625.

On the contrary, in an 'on-line' world the territoriality principle seems to be inadequate to cater for the non-physical overarching character of the digital reality. Thus, the idea of an 'off-line digital jurisdiction' evokes an inherent tension in contemporary legal systems, as in cyberspace sovereignty is not conceivable.[9] Nonetheless, nation states may exert jurisdiction over all activities that occur in their territory.[10] The clash between digital space and its physical location has been addressed by legal regulatory models using the idea of territorial connection.[11] While nation states cannot assert sovereign powers over cyberspace, they can bypass this obstacle by regulating cyber infrastructure and communication cables through which it is possible to establish a territorial connection.[12]

This could mean that, regardless of the fact that the 'data subject' may be, for instance, a European citizen, her or his data could fall within the jurisdiction of the state where the owners of the infrastructure – namely the fibre optic cables through which the data pass – are established. In this scenario, a reflection on which kind of jurisdiction data may require is extremely important. For example, a model of extraterritoriality can act as a trigger for the export of a system of values such as, for example, human rights, but also as a paper tiger by means of which the strongest jurisdictions exert more power to the detriment of the weakest jurisdictions.[13] By contrast, a model of digital sovereignty aims to overlap digital borders with physical borders, with the consequence that the legal regime of information is strictly dependent on data location[14].

It is no wonder, in fact, that in both the academic debate and on the legislative agenda two opposite positions are equally represented: one stresses the transnational nature of data and emphasizes the need to guarantee their unimpeded flow and processing; the other (emblematically represented by the most recent Chinese legislation[15]) aims to strengthen the paradigm of digital sovereignty and data nationalism by reaffirming through legal and technological measures the state's control over the digital flow of information.[16]

It is important to make it clear that the effects of extraterritoriality should be the opposite to digital sovereignty. The former aims to protect the free flow of data across borders, whereas the latter invokes an omnipresent control exercised through jurisdiction over the digital flow. However, in both alternatives the term of reference seems to always be territory.

---

9 According to *Rule 1* "Sovereignty (general principle)" of the Tallinn Manual "The fact that cyber infrastructure located in a given State's territory is linked to cyberspace cannot be interpreted as a waiver of its sovereignty. Indeed, States have the right, pursuant to the principle of sovereignty, to disconnect from the Internet, in whole or in part, any cyber infrastructure located on their territory, subject to any treaty or customary international law restrictions, notably in the area of international human rights law," M. N. Schmitt (ed.), *Tallinn Manual 2.0 on International Law applicable to cyber operations*, (Cambridge University Press, 2017), 12-13.

10 According to B. J. Koops and M. Goodwin, *Cyberspace, the Cloud and Cross-border criminal investigation. The limits and possibilities of International Law*, (Tilburg University, 2014), 35, "Jurisdiction, or 'the life of the law', remains spatially organised. It has become commonplace to suggest in the context of globalisation that law is being de-territorialised. What is meant is that the claim of exclusive authority or jurisdiction over a defined place that was such a key part of modernity – the territorial state – is being increasingly undermined. In its stead, a given space can host multiple claims to legal authority."

11 On this, see Z. Xinbao and X. Ke, *A Study on Cyberspace Sovereignty*, China Legal Science, (2016), 4: 33-75.

12 K. Kittichaisaree, Jurisdiction and attribution of State Responsibility in Cyberspace, in P. Casanovas and G. Sartor (eds.), Public International Law of Cyberspace, (Springer, 2017), 28.

13 A. El Ouali, *Territorial Integrity in a Globalizing World. International Law and States' Quest for Survival*, (Springer, 2012), p. 169: "extraterritoriality has, over the past decades, developed in two divergent directions, one towards the extension abroad of powerful states' sovereignty to the detriment of weaker states, and the other towards the protection of human rights through universal jurisdiction."

14 On the notion of data sovereignty see A. K. Woods, *Litigating Data Sovereignty*, Yale Law Journal, (2018), 128: 329, 360, 369.

15 A. Coleman and J. N. Maogoto, "*Westphalian" Meets "Eastphalian" Sovereignty: China in a Globalized World*, Asian Journal of International Law, (2013), 3(2): 237. China's Cybersecurity Law came into force on 1 June 2017.

16 For a comparative analysis of legislative reforms on digital sovereignty, see A. Chander and U.P. Lê, *Data Nationalism*, Emory Law Journal, (2015), 64: 677, 708, 714, 718.

The strength of nation states has been measured over time as their ability to produce, gather and control information about individuals. By contrast, the challenge for democratic nation states is also for this ability to rely on the level of protection ensured to its citizens.

This paper examines the issue of jurisdiction over personal data from a particular angle: it aims to investigate the conditions under which European law might be made a competitive legal system by strengthening the extraterritorial protection of data outside EU jurisdiction.

In particular, the first part explores the conceptualization of possible alternatives to the territoriality principle in the field of digital rights (parr. 2-3); the second part describes the main traditional models of extraterritoriality in international law as applied to data jurisdiction (par. 4); the third part examines the potential of the global reach of EU law through EU courts' judicial activism (parr. 5 and 6).

This analysis underpins an underlying tension between the so-called *de facto* and *de iure* 'Brussels effect'.[17] According to the first of these, the export of jurisdictional exclusivity becomes a way to justify forms of cultural imperialism; according to the second, the inclusion of EU-derived norms in third-country law could be a way to foster the development of global law.[18]

The issue of data jurisdiction should lead to a shift from the idea of a state information monopoly to a competing model across countries based on the broadest protection of individual rights arising from the use of data. Nevertheless, far from developing an approach inspired by the idea of 'forum shopping' – which often privileges private intermediaries rather than individuals – this approach requires that data protection standards should be met universally or at least also be universally applied in those jurisdictions which have lower standards.

As Christopher Kuner correctly points out,

> "when an individual in the EU enters data in an internet search engine or uploads data onto an online social network operated from a server outside the EU, this is not generally considered to result in an 'international data transfer.'"[19]

This example shows how 'tangible' the intangibility of data is and how relevant the legal definition of this intangibility is.

The endeavour to disconnect the non-physical nature of information from the notion of state borders should explore all the legal models of extraterritoriality in international law which could potentially offer broader solutions,[20] which would be integrated within the functional context across which data flows run – other than mere jurisdictional enforceability in the digital world.[21]

---

17 A. Bradford, *The Brussels Effect*, Northwestern University Law Review, (2012), 107(1): 1, 12, 22, 48.

18 For a reconstruction of the global rule of law, see J. Waldron, *Are Sovereigns entitled to the Benefit of the International Rule of Law?*, The European Journal of International Law, (2011), 22: 315; G. Palombella, *The rule of law beyond the state: Failures, promises, and theory*, International Journal of Constitutional Law, (2009), 7: 442-467.

19 C. Kuner, Regulation of Transborder Data Flow under Data Protection and Privacy Law, OECD Digital Economy Paper, (2011), 187: 25; see also Y. Poullet, Transborder Data Flows and Extraterritoriality: The European Position, J. Int'l Commerc. L. and Tech. (2007), 2:146; even in 2002 the art. 29 Working Party affirmed that "a high level of protection of individuals can only be ensured if web sites established outside the European Union but using equipment in the EU as explained in this working document respect the guarantees for personal data processing, in particular the collection, and the rights of individuals recognised at European level and applicable anyway to all web sites established in the European Union" (S. Rodotà, Article 29 Working Group, Working Document on Determining the International Applications of EU Data Protection Law to Personal Data Processing on the Internet by Non-E.U. Based Web Sites 15, The Working Party, Working Paper No. 56, 2002).

20 On the applicability of different models of human rights law jurisdiction to EU data protection law, see M. Taylor, *The EU's human rights obligations in relation to its data protection laws with extraterritorial effect*, International Data Privacy Law, (2015), 5(4): 246, 250.

21 See P.J. Slot – E. Grabandt, *Extraterritoriality and Jurisdiction*, Common Market Law Review, (1986), 23: 545.

2. Quasi *extra territorium*

In the case of jurisdiction over data, an enlargement of the territorial scope of EU law and the extraterritorial jurisdiction of the EU essentially entails broadening or limiting the notion of jurisdiction. Data, indeed, does not easily fit into the territorial constraints that ultimately rely on state borders. In fact, the very nature of information curtails one of the bastions of classical state law: the territoriality principle. Indeed, the category of territory is conceived in jurisprudence as the basic foundation of the Western concept of law, as both the condition for and the limit of the law's applicability to a certain set of relations. Even though cross-border relationships characterize many aspects of our contemporary life, legal regulatory schemes are still dependent on classical spatial categories, which are no longer consistent with a pattern of global relationships mostly not tied to the physical location of persons and goods, namely data.

I hesitate to use the term 'extraterritoriality' as efforts devoted to assessing a distinction between the extraterritorial reach of a given jurisdiction and extraterritoriality in the strict sense[22] are highly controversial and disputable. Scholars regard the resulting situations as 'conflicts of jurisdiction.'[23] Nonetheless, what is relevant for the aim of this paper is that extraterritoriality – coined for the first time by Grotius as *quasi extra territorium*[24] – is currently being used as both a term of reference and as the watershed of an inside and an outside to territorial borders.[25] I do not employ categories like global law[26] as in my hypothesis judicial jurisdiction is still a necessary benchmark between entities which adjudicate rights and those which cannot – even though global phenomena are necessarily pushing towards pluralistic and less formalistic models in which stakeholders and decision-makers may negotiate composite solutions.[27]

The digitization of information is challenging the general distribution of power on a geopolitical scale, to an extent that ultimately affects the enforceability of jurisdictional rules. The impacts of this phenomenon are wide-ranging and differ in various ambits of legal regulation. In the field of data protection, for instance, this factor is critical, as the ubiquity of data and their intangible character call into question the scope of judicial jurisdiction, especially with regard to cross-border data transfers.[28]

The examples are many and various: there are cases pending before national and supra-national courts in which states may be held accountable for violations of the information rights of foreigners, such as in the several lawsuits originated by the overarching US-UK mass surveillance scandal,[29] and cases in which law enforcement authorities seek to assert sovereign powers over data related to their citizens which are located outside the territory, as in the well-known *Microsoft* litigation recently brought before the US Supreme Court (and subsequently addressed by the CLOUD Act).[30] There are

---

22 D. J. Svantesson introduced a distinction between 'bite jurisdiction' and 'bark jurisdiction.' See *A Jurisprudential Justification for Extraterritoriality in (Private) International Law*, Santa Clara Journal of International Law, (2015), 13(2): 556.

23 K. W. Dam, *Extraterritoriality and Conflicts of Jurisdiction*, Am. Soc'y Int'l L. Proc., (1983), 77: 370.

24 See T. L. Putnam, Courts Without Borders. Law, Politics, and U.S. Extraterritoriality, (Cambridge University Press, 2016), 17; and C. R. Rossi, Sovereignty and Territorial Temptation. The Grotian Tendency, (Cambridge, 2017*), 277.*

25 *W. S. Dodge, Extraterritoriality* and Conflict-of-Laws Theory: An Argument for Judicial Unilaterlism, Harv. Int'l. L. J., (1998), 39:101, 108.

26 See, for instance, the reconstruction in H. Lindhal, *Law and the Globalisation of Inclusion and Exclusion*, (Cambridge University Press, 2018), 10-45.

27 See M. Koskenniemi, *From Apology to Utopia. The Structure of International Legal Argument*, CUP, Cambridge, 2005, 231: "Ultimately, the very concept of sovereignty loses its normative significance under the legal approach. If a State cannot refer to its sovereignty to justify its action but has to find a rule of law which has given it the right, liberty or competence to act in a certain way, then to speak of 'sovereignty' at all is merely superfluous or, at best, a description of the norms whose normative force is in their being incorporated in some legal act, not in their being inherent in statehood."

28 See Els De Busser, *Adequate Transatlantic Data Exchange in the Shadow of the NSA Affair*, in R. Miller (ed.), *Privacy and Power: a Transatlantic Dialogue in the Shadow of the NSA-Affair*, (Cambridge University Press, 2017), 615.

29 See, for example, the recent judgement ECtHR *Big Brother Watch and Others v. UK* (application nos. 58179/2013, 58170/13, 62322/14, 24960/15), judgment 13 September 2018.

30 829 F.3d 197 (2dCir.2016), *petitionforcert.filed*, (U.S. June 23, 2017 No.17-2)

other cases in which a cross-border violation of citizens' privacy rights perpetrated by third parties has been affirmed with the aim of protecting EU fundamental rights, stigmatized, for instance, by the *Google Spain* case,[31] and cases in which the global reach of an injunction regarding the removal of contents has been justified to prevent unfair competition on a global scale.[32]

In this area, the idea of information sovereignty is highly fragmented, amongst other reasons because of the intrinsic character of data, which are goods of a particular nature. They are – to employ terminology from economics – non-rivalrous in consumption, immaterial and non-territorial.[33] Therefore, because of their not having a physical location, they can be accessed and used by several persons at the same time in different places. Nonetheless, the more data is de-localized, the more states try to erect borders.[34]

The non-territorial character of data should instead deserve a notion of 'non-territorial jurisdiction,' which is not a legal category in customary international law: everything that is not territorial in nature implies either a territorial extension or an extraterritorial jurisdiction, both of which are exclusive and not alternative. Nevertheless, neither of these options deviate from the territoriality principle.[35]

Regarding jurisdiction over data, great emphasis has been put on enlargement of the territorial scope of EU law, a model essentially built on the universal character of human rights.[36] Nonetheless, each form of jurisdiction enlargement which implies going beyond a definite space calls into question the very notion of sovereignty and its challenges. This is extremely debatable in law regarding the internet as 'Internet' – as 'everybody's land' or *res communis omnium* – has not yet been accepted within the state sovereignty perspective.[37]

In this respect, every enlargement of territorial jurisdiction which may assume the form of extraterritoriality, territorial extension or a universal application of rights is proven to be an old answer to the new and so far unsolved problem of the non-territorial character of data.[38] The ubiquity of data requires a new description of meaningful concepts as the location of data is not necessarily connected to the rationale behind a regulatory model for data.[39] Nevertheless, any solution could lead to an ambivalent notion of an extraterritorial reach of a given jurisdiction. This is the case in general, but when applied to data, as Dan Svantesson, one of the most eminent scholars on the topic, argues, the distinction between territorial and extraterritorial jurisdiction in the field of data protection should make room for other criteria such as a substantial connection (a connection between the subject matter of the litigation or the damages suffered and the jurisdiction issuing a judgement or an order). This could be

---

31 See C. Kuner, *Extraterritoriality and regulation of international data transfers in EU data protection law*, International Data Privacy Law, (2015), 5(4): 235.

32 *Google Inc. v. Equustek Solutions Inc*. [2017] 1 S.C.R. 824.

33 J. Daskal, *The Un-territoriality of Data*, Yale Law Journal, (2015), 125(2):328, 365-377... 0, p. :ev.,Law, (2011), 2: 11le of lawty ed. data, 2005,ionsnce. not escapable situation.
jurisdictions whereas those rights

34 *See* A. Chander and U.P. Lê, *Breaking the Web: Data Localization vs. The Global Internet*, UC Davis, Legal Studies Research Paper, (2014), 1: 32.

35 A very meaningful definition of sovereignty was set out in the Island of Palmas in 1928 using the idea of exclusivity: "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the function of a State." On this, see M. N. Schmitt (ed.), *Tallinn Manual 2.0 on International Law applicable to cyber operations*, (Cambridge University Press, 2017), 11.

36 See N. Butha, *The Frontiers of Extraterritoriality. Human Rights Law as Global Law, in The Frontiers of Human Rights. Extraterritoriality and its Challenges*, (Oxford University Press, 2016), 10.

37 D. J. B. Svantesson and D. Kloza, *Transatlantic Data Privacy Relations as a Challenge for Democracy*, (Intersentia, 2017), 545, 557.

38 As C. Ryngaert points out, "Where data are everywhere and become disconnected from physical territory, extraterritoriality may seem the only viable regulatory option." See *Guest Editorial. Symposium issue on extraterritoriality and EU data protection*, *International Data Privacy Law*, (2015), 5(4): 221.

39 For a substantial critique of territoriality, see D. J. B., Svantesson, *Solving the Internet Jurisdiction Puzzle*, (Oxford University Press, 2017), 30, 33, 40.

the case of adjudicatory criteria such as *ratio materiae* rather than *forum loci*, or the "balance between legitimate interests of states."[40]

In order to limit and clarify the scope of my analysis, I essentially make two points: 1) the operability of legal systems through judicial deference has been ultimately challenged;[41] 2) recognition of the extraterritorial reach of jurisdiction over data is determining an enlargement of the territorial scope of EU law, often triggered by the universal claim of protecting human rights.[42]

The implications of cross-border data flows for extraterritoriality are many, as the many different examples of extraterritorial jurisdiction over data require non-unique solutions.[43] Not all extraterritorial models apply to the same extraterritorial cases as no one-size-fits-all solution applies in this field. Sometimes, in other areas of the law, such as environmental law, a territorial connection has been sought depending on the production of a harm. In the case of data transfers and information sharing, it is not always easy to single out spatial or temporal criteria to apply to the moment of the transfer or the data location, or sometimes the harm location is not always meaningful or easy to assess because of the fluctuating nature of data flows. Furthermore, the extraterritorial reach of jurisdiction in the case of sovereign powers exerted in order to gather data from a foreign party is a different case from the extraterritorial reach of fundamental rights according to which a state must comply with the standard of rights protection provided by a foreign state.

Moreover, the global relationship between a large range of actors should be investigated using new paradigms which ensure accountable mechanisms of recognition of judgements and/or judicial enforceability among EU countries and third countries. Indeed, the more the interaction between different actors is subject to changes, the more the traditional category of state sovereignty does not cover composite regulatory regimes in the global geopolitical order.

While we are facing the erosion of state sovereignty as a direct state control mechanism over information – due also to the need of state actors to increasingly turn to the private sector for data-gathering – judicial scrutiny over data entails rethinking the idea of territory and a reconceptualization of the territorial connection.[44]

3. One territory, one jurisdiction

To some extent – it is debatable and controversial – one is tempted to agree with those scholars who have pointed out that from the perspective of sovereignty the internet does not exist.[45] As Kristen E. Eichensehr correctly points out,

---

40 For a broader analysis, see H. L. Buxbaum, *Territory, Territoriality, and the Resolution of Jurisdictional Conflict*, American Journal of Comparative Law, (2009) 57(2): 631, 674, 635.

41 G. P. Callies and P. Zumbansen, Rough Consensus and Running Code. A Theory of Transnational Private Law, (Hart, 2010), 101.

42 See A. Khan, *The Extinction of Nation States*, American University International Law Review, (1992), vol. 7(2): 197, 199.

43 For a proposal for 'jurisdictional interoperability,' see D. J. B. Svantesson, *Solving the Internet Jurisdiction Puzzle*, (Oxford University Press, 2017), 119-121.

44 According to M. Scheinin, jurisdiction can be seen as a metaphor for State obligations. See *Just Another Word? Jurisdiction in the Roadmaps of State Responsibility*, in M. Langford, W. Vandenhole, M. Scheinin and W. van Genugten (eds.), *Global Justice, State Duties: The Extraterritorial Scope of Economic, Social, and Cultural Rights in International Law*, (Cambridge University Press, 2012), 226: "'jurisdiction' is just a word reflecting the existence of a factual link between the State and the person, which will depend on an interpretation of what kind of factual link is required for triggering State obligations in respect of a person."

45 Zeno-Zencovich, V., Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione, in G. Resta and V. Zeno-Zencovich (eds.) La protezione transnazionale dei dati personali. Dai "safe harbor principles" al "privacy shield", (Roma TrE-press, 2016), 7-22.

> "data intangibility poses significant difficulties for determining where data is located. The problem is not that data is located *nowhere*, but that it may be located anywhere, and at least parts of it may be located nearly *everywhere*. And access to data does not depend on physical proximity."[46]

Even though the notion of physical proximity is most relevant in the field of prescriptive jurisdiction, in the field of judicial jurisdiction the difference between the two notions of extraterritorial jurisdiction and territorial extension is much curtailed. I am essentially referring to two definitions provided by the theory of international law: prescriptive jurisdiction (applicable law) and judicial or adjudicatory jurisdiction (competent forum). Jurisdiction is an exclusive concept, as a state's jurisdiction rules out the possibility of another authority exercising jurisdiction at the same time on the same controversy and for the same grounds.[47]

On the other hand, there is a not an evident layer which is political: as extraterritoriality in international law is limited to strict conditions,[48] it is more convenient for nation states to enlarge the territorial scope of their jurisdiction as much as possible rather than to turn to extraterritorial solutions.[49] Indeed, criminal jurisdiction has traditionally been based on six principles: the territoriality or objective territoriality principle; the nationality or subjective territoriality principle; the protective principle, which determines jurisdiction by reference to national interest injured by the offence; the universality principle, which regards the custody of the person committing the offence; the passive personality principle, or nationality of the person injured by the offence; and the effects principle, which justifies jurisdiction by the fact that conduct outside the state has effects within the state.[50]

Nonetheless, even the application of the personality principle – based on the nationality and the residence of the individuals whose data are processed – clashes with the very notion of data, which is by definition cross-border. What is at stake is the mismatch between the mobile and immaterial character of data and the paradigm of sovereignty. The inherent 'non-territoriality' of data is a source of serious challenges to our legal systems and is one of the main factors behind the trend towards the recognition – in particular in Europe – of controversial forms of extra-territorial jurisdiction. These issues have to be seriously considered, because they might have a disruptive effect on the workings of the legal system and on its ability to effectively regulate the gathering and transfer of information in a data-driven economy.

Indeed, the category of 'territory' is hard to escape because of the existence of 'Leviathans,' as it means crossing the line towards indefinite state authority.[51] Law, even through fictitious modalities, will always seek to justify the linkage between a fact or a person and territory. When it does succeed, negotiations replace the fictitious role of the territorial connection. This has been the case of Mutual Legal Assistance Treaties (MLATs), which ensure the extraterritoriality of human rights "in case of disclosures not authorised by Union or Member States law." Without such limitations, cloud service providers could directly provide data to non-EU-based LEAs without an explicit treaty basis or authorisation from a European supervisory authority. Extraterritoriality would then be only a sensor, not

---

46 K. E. Eichensehr, *Data Extraterritoriality*, Texas Law Review, (2017), 95:144.

47 See, for instance, P. Asp, "*Extraterritorial Ambit and Extraterritorial Jurisdiction*." in Antje du Bois-Pedain, Magnus Ulväng and Petter Asp (eds.), *Criminal Law and the Authority of the State*, (Hart, 2017), 33–46.

48 N. Bialostozky, Extraterritoriality and National Security: Protective Jurisdiction as a Circumstance Precluding Wrongfulness, Colum. J. Transnat'l L. (2014), 52: 617, 622.

49 The distinction between territorial and extraterritorial jurisdiction is only apparently a neutral decision. As A. J. Colangelo correctly observes, "The upshot is that accurate implementation and application of international law can transform exercises of extraterritorial jurisdiction into exercises of territorial jurisdiction and, in turn, change the entire nature of due process analyses regarding the United States' ability to assert jurisdiction over serious violations of international law like torture, hostage taking, and airplane bombing anywhere in the world," A. J. Colangelo, *What is Extraterritorial Jurisdiction*, Cornell Law Review, (2014), 99:1333.

50 In general, see D. J. B. Svantesson, *Extraterritoriality in Data Privacy Law*, (Ex Tuto, 2013); *Extraterritoriality in Data Privacy Regulation*, Masaryk University Journal of Law and Technology, (2012), 7(1): 87-96.

51 See E. Benvenisti, *Community Interests in International Adjudication*, in E. Benvenisti and G. Nolte (eds.) *Community Interests across International Law*, (Oxford University Press, 2018), 70.

even necessarily the solution, for regulatory models provided by the law of the internet. As Svantesson clearly points out, "extraterritoriality is the key ingredient in every controversial claim of jurisdiction in relation to the Internet."[52]

Extraterritoriality has the advantage of ensuring the protection of data privacy and data protection – expressly recognized as fundamental rights under arts. 7 and 8 of the Charter of Fundamental Rights of the EU and included in the notion of private life under art. 8 of the ECHR[53] – outside the territory where an individual has been struck by a violation or outside the territory where a violation has been perpetrated and regardless of whether a person is legally or physically present in the EU.[54]

Judicial extraterritoriality can be defined as "any exercise of jurisdiction[…]to resolve disputes involving conduct occurring wholly or partially outside,"[55] but much criticism has been levelled at claims for extraterritoriality as the non-territorial character of data is not a sufficient condition to deny jurisdiction.

4. Mimetic off-line models

Let us assume that in the on-line world jurisdiction and sovereignty lead to divergent solutions. Indeed, in this constellation the problem of non-territorial data is crucial.

The issue of extraterritoriality has been discussed in various fields, first of all international law. The 2017 edition of the Tallinn Manual, which amended the 2013 edition, in two sections distinguishes the subject matters of 'sovereignty' and 'jurisdiction,' which were originally unified in one chapter, and includes a special sub-section on 'extraterritoriality' under the paragraph on 'jurisdiction' and further sub-sections like 'internal sovereignty' and 'external sovereignty' under 'sovereignty.'[56] In particular, this manual, which is considered one of the most comprehensive analyses of how existing international law applies to cyber operations, provides a definition of extraterritorial jurisdiction: when a state "access[es] electronic data that is publicly available, such as that on the Internet" but "hosted on servers located abroad," the state is "exercising territorial, as opposed to extraterritorial, enforcement jurisdiction based on the fact that the data is publicly available in their State." It is evident that the key issue is what the definition of extraterritoriality encompasses. Here, the criterion seems to be free access to information inside the territory.

The Manual's drafters distinguish the case of territorial jurisdiction founded on the public availability of data from cases in which "data is not meant to be made available to individuals in the State," such as data on a private computer abroad that is connected to the internet but not meant to be accessible. Access to that computer would be extraterritorial if it was not meant to be accessible to users from that state. To give an example, the alternative territorial/extraterritorial jurisdiction is very relevant for law enforcement agencies which aim to reach servers located outside their territory.

---

52 D. J. B. Svantesson, A Jurisprudential Justification for Extraterritoriality in (Private) International Law, Santa Clara Journal, (2015), 13(2): 519.

53 The extension of the notion of private life to data is a result of the longstanding ECtHR case-law. See *Airey v. Ireland*, Appl. no. 6289/73, Judgement of 9 October 1979; *Rotaru v. Romania*, Appl. no. 2834/95, judgment 4 May 2000; *S and Marper v. UK*, Appl. nos. 30562/04 and 30566/04, Judgment of 4 December 2008; *P.G. and J.H. v. the United Kingdom*, Appl. no. 44787/98, Judgment of 25 September 2001; *Peck v. the United Kingdom*, no. 44647/98, Judgment of 28 April 2003; *Amann v. Switzerland*, Appl. no. 27798/95, Judgment of 16 February 2000.

54 According to the definition provided in J. Scott, *Extraterritoriality and territorial extension*, The American Journal of Comparative Law, (2014), 62(1): 89-90: "a measure will be regarded as extraterritorial when it imposes obligations on persons who do not enjoy a relevant territorial connection with the regulating state. By contrast, a measure will be regarded as giving rise to territorial extension when its application depends upon the existence of a relevant territorial connection, but where the relevant regulatory determination will be shaped as a matter of law, by conduct or circumstances abroad."

55 T. L. Putnam, Courts Without Borders. Law, Politics, and U.S. Extraterritoriality, (Cambridge University Press, 2016), 32.

56 M. N. Schmitt (ed.), *Tallinn Manual 2.0 on International Law applicable to cyber operations*, (Cambridge University Press, 2017), 11, 51, 55.

The Manual's "meant-to-be-accessible" standard does not sufficiently clarify who can access that data. However, arguing further, let us consider the hypothesis of data hosted by a service provider established within a certain state and eventually accessed by an individual from outside that territory. If the state where the service provider is established issues a warrant, can the data holder refuse to turn over the data related to that individual, arguing that such data is located abroad? How does the notion of 'territory' apply to information?[57]

The Tallinn Manual does not provide any temporal limit to the idea of 'meant to be accessible.' Therefore, it may not be an exhaustive criterion, as the service provider may have decided to store data on the cloud or intends those data to be accessible from somewhere but only for a limited time. It is thus clear that this solution presents shortcomings as it does not cover cases in which information has to be regulated during a transfer and when it is fragmentated.

A second model is the one employed by the EctHR, which has traditionally handled this problem by providing a spatial connection, which basically gives rise to two schemes: a spatial model – effective control over a territory; and an individual model – authority exercised over an individual. Thus, the theoretical problem is to find a model of judicial jurisdiction without reference to territory,[58] due to the fact that data is transferred in huge quantities at high speed across borders.

In a very recent case, *Big Brother Watch and Others v. UK*, the European Court of Human Rights was called on to rule on the applicability of the European Convention on Human Rights (ECHR) in the field of mass surveillance programmes undertaken by the US and UK. However, the Court did not touch on the extraterritorial implications of the ECHR, taking for granted the universality of art. 8 ECHR (right to private life) as regards issues of bulk interception of communications and communications obtained by service providers. By contrast, in the field of intelligence-sharing no violation of art. 8 was found.[59]

The Court did not engage with the issue of the effective control of fibre optic cables, which enables a state to access electronic traffic directed outside its territory, also through transatlantic mass surveillance programmes, and which could justify the extraterritorial applicability of the ECHR.

In the field of extraterritoriality, even though they do not regard data, two models have been applied: 1) according to the *spatial model*, in order to ensure extraterritorial jurisdiction the state's effective control over territory is necessary;[60] 2) according to the *personal model*, the authority and control by a state or other actor over an individual even outside the territory has been deemed sufficient.[61]

These models have been developed to assess the necessary conditions for a contracting state to be held accountable for a violation of the ECHR.[62] They are controversial examples, essentially based on

---

57 C. Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part 1)*, International Journal of Law and Information Technology, (2010), 18(2): 176,178–81.

58 See D. J. B. Svantesson, *The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses*, Stan. J. Int'l L. (2014), 50(1): 53, 71; *Extraterritoriality and targeting in EU data privacy law: The weak spot undermining the regulation*, International Data Privacy Law, (2015), 5(4): 226-234.

59 *Big Brother Watch and Others v. UK*, Appl. nos. 58179/2013 and 58170/2013*; Bureau of Investigative Journalism and Alice Ross v. UK, Appl. no. 62322/2014; Human Rights Organizations and Others v. UK, Appl. no. 24960/2015*, Judgment of 13 September 2018. On this, see M. Milanovic, *ECtHR Judgment in Big Brother Watch v. U.K.*, EJIL Talk, 17 September 2018. Other applications in the field of electronic mass surveillance programmes have been lodged but are still pending (*Tretter and Others v. Austria*, Appl. no. 3599/10*; Breyer v. Germany*, Appl. no. 50001/12*; Association confraternelle de la presse judiciaire v. France and 11 other applications*, Appl. nos. 49526/15, 49615/15, 49616/15, 49617/15, 49618/15, 49619/15, 49620/15, 49621/15, 55058/15, 55061/15, 59602/15 and 59621/15.

60 *Loizidou v. Turkey*, Appl. no. 15318/89, Judgment of 23 March 1995; Bankovic & Others v. Belgium & Others, Appl. no. 52297/99, Judgment of 12 December 2001.

61 ECtHR, *Al Skeini & Others v. UK*, Appl. no. 55721/07, Judgment of 7 July 2011; *Al-Jedda v. UK*, Appl. no. 27021/08, Judgment of 7 July 2011; *Öcalan v. Turkey*, Appl. no. 46221/99, Judgment of 12 May 2005.

62 For an overview of the extraterritoriality of data privacy in the context of mass surveillance, see I. Georgieva, *The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR*, (2015), Utrecht Journal of International and European Law, 31(80): 104.

reference to territory, of how the issue of extraterritorial jurisdiction has been handled through physical categories. In the ECtHR case law, extraterritoriality has been considered an exception to the principle of territoriality and it is subject to very strict interpretation as it has only been invoked in cases of extradition or expulsion, when a consequence of military action implies effective control over an area outside the territory, in consular, diplomatic and flag jurisdiction cases, and where the acts of state authorities produce effects or were performed outside their own territory.[63]

The restrictions of these models led the ECtHR to frame a third model based on positive and negative obligations of the state, which entails either refraining from any conduct that would impinge on a human rights violation or ensuring that a third party does not violate human rights even outside EU territory. According to Milanovic,

> "The third model is the only one that provides easy, clear answers to whether human rights treaties apply to foreign surveillance. If the negative obligation to respect the right to privacy is territorially unlimited, then any interference with this right in any place in the world would implicate the ICCPR or the ECHR."[64]

The Court endorsed this model in the case *Issa v. Turkey* by ruling that "art. 1 of the Convention cannot be interpreted so as to allow a State party to perpetrate violations of the Convention on the territory of another State which it could not perpetrate on its own territory."[65]

According to the ILA Study Group on Due Diligence in International Law,

> "a sovereign state is obligated to ensure that in its jurisdiction (which includes all those spaces where the sovereign exercises formal jurisdiction or effective control) other states' rights and interests (including those with respect to the protection of their citizens and companies) are not violated."

While art. 1 of the ECHR provides that High Contracting Parties are obliged to "secure to everyone within their jurisdiction the rights and freedoms" protected under the Convention,[66] art. 2 of the ICPCR provides a double reference both to the jurisdiction and the territory: "Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant." Although this double reference has been highly debated,[67] the extraterritorial reach of human rights is textually provided for by the Optional Protocol, which clarifies that the reference is not to the place where the violation occurred but rather to the relationship between the individual and the state in relation to a violation of any of the rights set forth in the Covenant, wherever they occurred. Moreover, the drafters of the Covenant did not intend to allow states to escape from their obligations when they exercise jurisdiction outside their national territory.[68] This is also confirmed by the 1948 Universal Declaration of Human Rights, whose art. 2 provides that

---

63 S. Miller, Revisiting Extraterritorial Jurisdiction: *A Territorial Justification of Extraterritorial Jurisdiction under the European Convention*, The European Journal of International Law, (2010), 20: 1223-1246.

64 *Ibidem*, 120.

65 ECtHR, *Issa v. Turkey*, application no. 31821/96, judgment 16 Nov. 2004.

66 C. Ryngaert argues that the final reference to the jurisdiction rather than to the territory implies that "ECHR Contracting States could be obliged to secure ECHR-based rights also outside their territory." See C. Ryngaert, *Clarifying the Extraterritorial Application of the European Convention on Human Rights; Al-Skeini and others v. United Kingdom app. no. 55721/07 (ECtHR, 7 July 2011)*; and Merkourios (2012), 28 (74): 58, whereas the drafting history shows an original reference to persons "residing" within territories. See M. Milanovic, *Extraterritorial Application of Human Rights Treaties*, (Oxford University Press, 2011), 38; M. Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, Harvard International Law Journal, (2015), 56(1): 81; P. Margulies, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, Fordham L. Rev., (2014), 82(5): 2137.

67 On this point, see M. Scheinin, Extraterritorial Effect of the International Covenant on Civil and Political Rights, in Coomans and Kamminga (eds.), Extraterritorial Application of Human Rights Treaties, (Intersentia, 2004), 73–81; I. Kanalan, Extraterritorial State Obligations Beyond the Concept of Jurisdiction, German Law Journal, (2018), 19 (1):44, 47.

68 See *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, ICJ Rep. 2004, par. 109: 179.

> "Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self governing or under any other limitation of sovereignty."

As applied to non-territorial data, the two international sources ensure the extraterritorial application of art. 8 ECHR (respect for private and family life) and art. 17 ICCPR (protection against unlawful interference of the right to privacy).[69]

It is understood that the criterion for whether a state can assert its own territorial or extraterritorial jurisdiction also depends *ex post* on the effects which will stem from this. As Milanovic argues,

> "New technologies can today frequently lead to a disconnect between the location of the individual and the location of the interference with the individual's privacy […] The question is how to determine state jurisdiction in situations in which the interference was done in an area under a state's control, but the individual is not in any such area."[70]

In several fields, this reflection challenges the grounds of the traditional assumption about territorial sovereignty, which is essentially based on four parameters: exclusive state powers; the equality of nations principle; the immunity principle; and the right against interference by any foreign power in domestic affairs.[71]

A model which has attracted particular attention but scarce application in the last decade is the 1935 Harvard Draft Principle (which was designed for law enforcement matters), which essentially provides as follows:

> "In the absence of an obligation under international law to exercise jurisdiction, a State may only exercise jurisdiction where: a) there is a substantial connection between the matter and the State seeking to exercise jurisdiction; b) the State seeking to exercise jurisdiction has a legitimate interest in the matter."

Dan Svantesson suggests amending this draft by adding a third exception to the territoriality principle applicable to data, based on a broader understanding of the protective principle, relying on whether "the balance between the State's legitimate interests and other interests is reasonable."[72] Svantesson's proposal seems to ensure the broadest range of extraterritorial jurisdiction in the digital reality, since it is not necessarily connected with the idea of physical territory. If combined with the positive and negative obligations theory, this idea may better address the protection of individual freedom.[73]

---

69 On this, see F. Bignami and G. Resta, *Human Rights Extraterritoriality*, in E. Benvenisti and G. Nolte (eds.) *Community Interests across International Law*, (Oxford University Press, 2018), 357-380, 377.

70 M. Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, Harvard International Law Journal, (2015), 56(1): 81, 124.

71 D. J. B. Svantesson, *Sovereignty in international law - How the Internet (maybe) changed everything but not for long*, Masaryk University Journal of Law and Technology, (2014), 8(1): 137, 141.

72 D. J. B. Svantesson, *A new jurisprudential framework for jurisdiction: beyond the Harvard Draft*, American Journal of International Law, (2015), 109: 69-74.

73 What Svantesson points out is very relevant to the relationship between information privacy and information sovereignty: "We assume that information privacy and information sovereignty cannot be treated as binary concepts, i.e. one cannot say that some information totally or exclusively is, or is not, under some sovereign rule. Instead, we argue that information may at the same time be subject to a multitude of sovereign rights of various entities. In case of conflicts of these rights, we argue that only a proper assessment of their intensities can lead to legal solutions that are fit to serve the fundamental purposes of law. It is here that the proposed method built on the three core principles, i.e. substantial connection, legitimate interest and interest balancing, becomes important. This method does not represent any definite solution that could be mechanically applied as such, but it gives guidance as to which factors are to be considered in such assessments and how the consideration should be structured," Polčák, R. and Svantesson, D. J. B., *Information Sovereignty. Data Privacy, Sovereign Powers and the Rule of Law*, (Edward Elgar, 2017).

5. ECJ Activism towards legal competition

As stated, the aim of this paper is to examine whether European law might be made competitive with other legal systems by strengthening the protection of fundamental rights for individuals within trans-border relations and in particular by widening the scope of European courts' jurisdiction in such cases. This question is also relevant considering that the EU is not competent to sign human rights treaties and therefore to acquire the status of party to these treaties, which would confer the ability to require compliance by the other parties.[74]

The important electronic mass-surveillance controversy has offered the ECJ the occasion to revisit the traditional doctrine of extraterritoriality in order to answer in a more effective way the social demands arising from a context in which a violation of fundamental rights can be easily carried out – both by private parties and by public authorities – across national borders. The famous ECJ *Google Spain*[75] decision declared that EU data protection law was applicable to a search engine service operated by a corporation based outside the European borders. This is a clear example of such an effort to adjust the scope of traditional legal concepts to the new non-territorial reality of cyberspace[76].

Even the *Digital Rights* case[77] showed very well the tension around the problem of extraterritoriality (prescriptive in this case), as the court, by finding that the Data Retention Directive was an infringement of the European Charter of Fundamental Rights, of Directive 45/96/EC on personal data protection and of Directive 2002/58/EC on the protection of personal data and privacy in the telecommunications sector, held that Europeans' personal data were not sufficiently guaranteed against the U.S. National Security Agency (NSA) and its PRISM program.

The issues at stake are clearly also exemplified by the *Schrems* case[78]. If the ECJ had not taken a proactive stance, Facebook would have continued to deliver data to the NSA, because this practice was valid and mandatory under American Law (§ 702 FISA).[79] In this case, the Court of Justice was proactive in making an indirect use of extraterritoriality, aiming to extend the scope of the protection guaranteed by the Charter to the transfer of data outside EU jurisdiction. This case involved an Irish national who voluntarily signed up for a Facebook account and had to accept a user agreement granting Facebook permission to transfer all or some personal data to the US, where it would undergo "data processing" according to US law. By affirming Max Schrems's fundamental right to privacy for data that was physically located in another country, to which he was only connected by virtue of his Facebook account, the EU demonstrated that the fundamental rights paradigm protected by EU law has extraterritorial reach.

---

74 E. Cannizzaro, *The EU's Human Rights Obligations in Relation to Policies with Extraterritorial Effects: A Reply to Roland Bartels*, The European Journal of International Law, (2014), 25(4): 1093-1099.

75 Case C-131/12, Google Spain SL v Agencia Española de Protección de Datos, Judgment of the Court (Grand Chamber) of 13 May 2014. On this, see G. Sartor and M.Viola de Azevedo Cunha, *Il caso Google e i rapporti regolatori USA/EU*, in G. Resta and V. Zeno-Zencovich (eds.) *Il diritto all'oblio su Internet dopo la Sentenza Google Spain*, (Roma Tr-Epress, 2015), pp. 99-124.

76 B. Alsenoy and M. Koekkoek, *Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted,' Int'l Data Privacy L.*, (2015), 5(2):105, 110 -111. The change of paradigm in Google Spain is very visible as it contrasts with the position of the ECJ in the *Lindqvist* Case, C-101/01: par. 68: "One cannot presume that the Community legislature intended the expression transfer [of data] to a third country to cover the loading, by an individual in Mrs Lindqvist's position, of data onto an internet page, even if those data are thereby made accessible to persons in third countries with the technical means to access them," 69. "If Article 25 of Directive 95/46 were interpreted to mean that there is transfer [of data] to a third country every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet" See D. J. B. Svantesson, *The Google Spain Case: Part of a Harmful Trend of a jurisdictional overreach*, EUI Working Paper RSCAS 2015/45,7, 20.

77 Joined Cases C-203/12 and C-594/12, *Digital Rights Ireland Ltd v. Ireland*, Judgment of the Court (Grand Chamber) 8 April 2014.

78 Case C362/14 *Schrems v. Data Protection Commissioner*, Judgment of the Court (Grand Chamber) of 6 October 2015.

79 Section 702 FISA covers foreign intelligence information, which is defined as "information with respect to a foreign-based political organization or foreign territory that relates to, and if concerning a United States person is necessary to the conduct of the foreign affairs of the United States." See the FISA Amendments Reauthorization Act of 2017.

These operative solutions deserve some brief remarks on the different conceptualization of the right to privacy across the Atlantic, also in order to be aware of the underlying possibility of different conceptions of data jurisdictions. While in Europe the right to privacy is considered a fundamental right linked to the concept of human dignity, in the United States the idea of privacy belongs to the sphere of individual self-determination against interference by public and private actors, which can also be waived by agreement at the contractual level. In the US, for instance, the logic of privacy as control over information has never been accepted. Constitutional privacy is deeply embedded in the logic of American constitutional adjudication, but this basically means intangibility of domicile, liberty and self-determination in fundamental choices that affect the human body. Information privacy is, meanwhile, irrelevant to the American constitutional 'culture.'[80] This is the constitutional idea of privacy under the umbrella of the Fourth Amendment. By contrast, the right to self-determination, which is the conceptual framework within which the continental idea of privacy is inscribed, furthers the project of the free development of personality.[81] In Europe, protection is advanced at the level of data acquisition through the intermediation of independent administrative authorities; in the US, the initial acquisition of data does not mean data processing. Therefore, the protection is shifted to a higher level. This can be explained by the propensity to adversarial legalism in the US, whereas in Europe, administrative negotiations are intended to avoid the intervention of the judiciary. For this reason, American privacy has been defined as *reactive* whereas European privacy has been considered *proactive*.[82]

Even if data extraterritoriality is linked to the broader paradigm of the universality of EU human rights, the problem also regards a possible clash between different conceptualizations of human rights.[83] This is, for example, the case of data privacy, for which the extraterritorial assessment of a violation provided by a court may entail a divergent law being applicable.[84] For instance, by applying the criterion of territorial linkage, a person's entitlement to constitutional rights like the right to privacy depends on whether he or she is territorially bound to the United States as a citizen or permanent resident.[85]

Nonetheless, it is interesting that the ECJ's activism was broadly embraced in the General Regulation on Data Protection no. 679/2016 (GDPR) in at least two provisions: one regarding the increasing territorial scope (art. 3); the other regarding the possibility of prohibiting cross-border data transfers or disclosures not authorised by the Union (art. 48[86]). The first solution adopted in the General Data Regulation is consistent with the non-territorial character of information insofar as it takes into account the case of controllers and processors which are not established within the Union (art. 3) only when the

---

80 J. Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty***,** Yale L.J., (2004), 113: 1151.

81 In general, see S. Rodotà, *Tecnologie e diritti*, (Il Mulino, 1995); *Tra diritti fondamentali ed elasticità della normativa: il nuovo Codice sulla privacy*, Europa Diritto Privato, (2004), 1; S. Simitis, *Einleitung: Geschichte-Ziele-Prinzipien*, in S. Simitis (ed.), *Kommentar zum Bundesdatenschutzgesetz*, (Nomos, 2014), 81-194.

82 On this, see F. Bignami, *European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, in Bost. Coll. L. Rev. (2007), 48(3): 609; A. Busch, *From Safe Harbour to the Rough Sea? Privacy Disputes across the Atlantic*, Script-ed, (2006), 3(4): 318; F. Bignami and G. Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation*, Law and Contemporary Problems, (2015), 78: 231-266.

83 *Data Protection Standard in the AFSJ*, in F. Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*, (Springer, 2012), 24: "The ECtHR's jurisdiction can stipulate overarching principles in fields where the control of European Courts was limited by the treaties. Many EU instruments and national legal orders refer directly or indirectly to the ECHR provisions and their interpretation. The ECHR standard is therefore the broadest and farthest-reaching data protection standard in Europe applicable regardless of (former) EU pillars, national borders or competence obstacles."

84 See, for example, P. Schwartz and K. N. Peifer, *Transatlantic Data Privacy Law*, The Georgetown Law Journal, (2018) 106: 115; L. Moerel, *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?,* Int'l Data Privacy L., (2010), 1(1): 28; J. R. Reindenberg, *E-Commerce and Trans-Atlantic Privacy*, in Hous. L. Rev., (2001-02), 38: 717-728.

85 M. F. Din, *Data without Borders: Resolving Extraterritorial Data Disputes*, J. Transnat'l L. &Pol'y, (2016-2017), 26: 1, 23.

86 Art. 48, *Transfers or disclosures not authorised by Union law: "*Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter."

processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment by the data subject is required, to such data subjects in the Union; or (b) monitoring their behaviour if the behaviour takes place within the Union. The second solution is a result of a compromise, as in the draft Regulation approved by the European Parliament, this clause (the so-called anti-FISA clause) prohibited third countries (such as the United States and other non-EU member states) from accessing EU personal data when required by a non-EU court or administrative authority without prior authorization by an EU data protection authority (supervisory authority). The drawback would have been that the anti-FISA clause, as reported in the final official text of the Regulation, would have been extended to controllers/processors in EU markets. This is one of the reasons why the final version provided for international agreements to be an exception to extraterritorial enforcement of decisions by courts and administrative authorities.

If this provision had been passed, the Cloud Act, for example, would not have had the extraterritorial potential to reach every foreign country signing Cloud Act agreements (or so-called executive agreements). Together with rogatory and mutual legal assistance agreements, executive agreements are new forms of cross-border data sharing between the US and other countries. Whereas MLATs create treaty-based obligations between governments which often conflict with the prohibition by US law to disclose data, executive agreements are faster and directly bind service providers to release the contents of electronic communications to the foreign government with whom the US has signed one via a system of certifications which are not subject to judicial or administrative review.[87] In MLAT and letters rogatory processes, a federal court reviews and approves a foreign government's request for information before issuing a warrant or a court order; under CLOUD Act agreements, foreign governments can submit orders directly to service providers.

As regards EU law, the Cloud Act created a conflict of jurisdiction with Art. 48 GDPR.[88] In fact, the final text of this article (which is only a surrogate of the so-called anti-FISA clause) provides that any judgment of a court or tribunal and any decision by an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a member state. This means that any extraterritorial exercise of judicial jurisdiction over Europe can be regulated by executive agreements which fall under US jurisdiction. In this case, it does not matter whether jurisdiction on data transfers is territorial or extraterritorial. Indeed, the GDPR is conceived as an enlargement of the territorial scope of EU law against data nationalism, as it even applies to controllers and processors not established in the EU but offering good and services on the EU market, irrespective of whether a payment by the data subject is required.

This led to a paradoxical opposite effect, as providers of internet data storage services have located their data centres in the EU to escape restrictions on international data transfers, as the EU may block recognition of third-country legal measures.[89] In contrast, Directive no. 680/2016 on data processing for purposes of law enforcement and policing does not include any provision similar to art. 48 GDPR. This is an example of how contractual clauses go faster than law enforcement regimes, which are more reluctant to allow data sharing, which ultimately leads to the most relevant conflicts of jurisdiction.[90]

---

87 S. P. Mullinghan, *Cross Border Data Sharing Under the Cloud Act*, Congressional Research Service, 2018, 17, available at www.grs.gov.

88 C. Kuner, *The Internet and the Global reach of EU law*, Working Paper, LSE, 2017, 4: 26.

89 *Ibidem*, 25.

90 C. Kuner, *Regulation of Transborder Data Flow under Data Protection and Privacy Law*, OECD Digital Economy Paper, (2011), 187: 26: "geography will continue to play a role in the regulation of transborder data flows, since 'human beings tend to cluster geographically, based on shared cultures, languages, tastes, wealth, and values' […]. Geography will also remain important with regard to law enforcement access to data, since more and more governments are likely to demand that entities offering communications in their countries also maintain communications equipment there, in order to facilitate such access."

6. Conclusions

In the field of personal data transfers, the adjudication of rights suggests viewing borders as non-physical entities.[91] This challenge needs to take into account the applicability of criteria other than physical parameters. This is also due to the fact that online intermediaries – in the context of internet governance – are actors towards whom jurisdictional claims may be directed in a mediated way,[92] but not necessarily on the basis of a territorial connection. As long as extraterritoriality is interpreted as an exception to the territoriality principle rather than as an alternative way to contrast the shortcomings of territorial constraints, it can only be used as a trigger to enhance sovereign powers outside physical frontiers. In this sense, extraterritoriality seems to be not a symptom of the erosion of sovereignty but instead a reaffirmation of the sovereign powers of nation states no longer within their own territory but outside their borders.

Endeavouring to not stick to forms of territorial connection in all cases regarding cross-border data flows could be a valuable option. Reflection on the global reach of EU law on cross-border data governance has been facilitated by the constitutional status of fundamental rights (arts. 7 and 8 of the CFR). This understanding is likely to converge with the attempt to frame the issue of extraterritoriality of privacy and data protection within the theory of states' positive and negative obligations and also seems coherent with a wide interpretation of the protective principle. In my view, this theory could be oriented towards a balance between the legitimate interests of states based on a substantial connection between the jurisdictional claim and the object of the controversy. In this sense, extraterritoriality may be used as a way to extend a better protection of fundamental rights within jurisdictions which do not ensure the same standard of protection. The solution of extraterritorial jurisdiction may curb downward competition among legal systems by exporting legal models based on a higher level of protection of rights. Nevertheless, while this is commonly acceptable in the field of fundamental rights, it becomes problematic in other areas of legal regulation which tackle personal data but are not triggered by a violation of fundamental rights or when the potential violation of fundamental rights has been balanced with other competing interests, such as national security, intellectual property, fair competition or public information.

Taking these examples seriously requires an effort to test substantial connection as a functional criterion useful to tackle 'bare data' disentangled from the concept of territorial connection and more connected to the factual situations involved, for instance whether the matter refers to data upon which there is an exclusive right or for which an issue of public order can be raised.

Alternative criteria to the territorial one might be based on the effective possibility of accessing data for end users or on the volume of profit gained by companies handing data over to third parties. This comprehensive approach could contribute to establishing a broader and integrated legal status of information.

This paper has ultimately been an attempt to reflect on data jurisdiction and carefully examine the issue of extraterritoriality, for at least two reasons: physical extraterritoriality is diverging from non-physical territoriality, as only the former can use territory as a term of reference; and extraterritorial applications of law and extraterritorial powers of a nation state differ case by case, making it hard to set up a systematic use of them.

Nonetheless, one of the limits to refraining from the use of the territoriality principle as regards data jurisdiction is a mismatch between the applicable law (prescriptive jurisdiction) and the natural *forum* (judicial jurisdiction), which has to be addressed through coherent solutions.

---

91 For a complete reflection on this, see Myra F. Din, *Data without Borders: Resolving Extraterritorial Data Disputes*, J. Transnat'l L. & Pol'y (2016-2017), 26: 23.

92 H. Bloch-Wehba, Global Platform Governance: Private Power in the Shadow of the State, SMU Law Review (forthcoming 2019).

In the global constellation of data transfers, the use of extraterritoriality made by the EU seems to respond to a horizontal model of jurisdiction that a renowned scholar has termed 'us/them' jurisdiction, as opposed to the vertical US 'in/out' model based on the relationship between the power of courts and defendants.[93] Europe is taking on the role of 'gentle civilizer of nations' as regards the required standard protection of fundamental rights even outside EU territory. In this process, the distinction assigned to boundaries in terms of *allocation* rather than of *delimitation* is also relevant to thinking of a new idea of territory.[94]

In the absence of an adequate approach to extraterritoriality which disregards reference to territory, the EU enlargement of standard protection of fundamental rights looks like an effort to rethink territory (and the territorial connection) as an opportunity to adjudicate a better protection of rights. This is, of course, not the best option but at least the result of an awareness, as a matter of fact, that any technical distinction between territorial extension or extraterritorial reach risks becoming meaningless when applied to data. Extraterritoriality may turn out to be a valuable option only as far as it envisages functional criteria not depending on a reference to territory. In the meantime, an 'enlightened' interpretation of the territoriality principle implies not justifying sovereign powers over non-located data regarding third countries and imposing a minimum standard of protection of rights to web giants who somehow profit from EU relations. Global balances are constantly and rapidly changing and political choices in the field of data jurisdiction are urgent but should not necessarily be taken in a direct way, as their outcomes affect the very notion of the geopolitical order. These issues are becoming increasingly connected to the data-jurisdiction puzzle. One recent example is the reference for a preliminary ruling from the High Court (Ireland) made on 9 May 2018 in the so-called *'Schrems II*' case on the compatibility of the Privacy Shield with EU law.[95] One of the questions referred is whether the level of protection afforded by the US respects the essence of an individual's right to a judicial remedy for breach of his or her privacy rights guaranteed by Article 47 of the Charter, and if so whether the limitations imposed by US law on an individual's right to a judicial remedy in the context of US national security are proportionate within the meaning of Article 52 of the Charter and do not exceed what is necessary in a democratic society for national security purposes. Thinking in terms of judicial remedies may be useful to apply the notion of data jurisdiction in a less formalistic way.

Finally, there is a current debate on data storage in space regarding the possibility of storing data in space within data centres beyond the reach of Earthly laws. Such data is then transferred from space to third parties in order to circumvent any legal obligations. Such a phenomenon seems a somewhat radical alternative to the territoriality principle. Nonetheless, it confirms that the law on the Earth is the law of territory and for non-territorial data there is no space other than space.

93 R. Michaels, *Two Paradigms of Jurisdiction*, Michigan Journal of International Law, (2006), 27 (4)H: 1004, 1027, 1038.
94 *Ibidem*, 1058.
95 Reference for a preliminary ruling from the High Court (Ireland) made on 9 May 2018 in *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (Case C-311/18).

Author contacts:

Mariavittoria Catanzariti
Centre for Judicial Cooperation
Robert Schuman Centre for Advanced Studies
European University Institute
Via Boccaccio 121
I-50133 Firenze

Email: Mariavittoria.Catanzariti@eui.eu