The GDPR's Extra-Territorial Scope

Data Protection in the Context of International Law and Human Rights Law

*Stephan Kolo*ß*a*[*]

Abstract

Jurisdiction is currently one of the most debated topics in international law. It has various forms and is used differently in general international law and in human rights law. Global internet platforms massively challenge the existing frameworks of jurisdiction. The existing international legal order is based on the Westphalian notion of state-centrism and state sovereignty. The most important link is usually a state's territory. Yet, activities conduct-

[*] The author is Ph.D. candidate at the Ruhr University Bochum and the Institute for International Law of Peace and Armed Conflict (IFHV) and member of the transdisciplinary research group "SecHuman – Security for People in Cyberspace".

ZaöRV 80 (2020), 791-818

ed online frequently ignore a state's territorial borders. In the area of human rights law, the notion of jurisdiction has equally moved away from the territorial towards a generally extraterritorial application. This, however, leads to a conflict of jurisdictions. In the field of data and privacy protection, the European Union's General Data Protection Regulation (GDPR) prominently standardises the domestic-market principle in Article 3(2) GDPR. According to this provision that is titled "territorial scope", data controllers and processors may fall within the range obligations stipulated in the regulation even if they are located outside of the European Union (EU) and have their main business abroad. Given the potential of creating a global privacy and data protection system, this brings up the important questions: What is the territorial scope of application of the GDPR? Which is the current role of "territory" in issues on jurisdiction? How to deal with overlapping jurisdictions? The current article examines the GDPR's territorial scope under Article 3(2) GDPR in the light of the recent judgments delivered by the European Court of Justice (ECJ) and gives a brief analysis of the GDPR's standard-setting potential in protecting privacy and data protection online. The article will show that the current jurisprudence of the ECJ recognises the need for an extensive protection of privacy and data protection online but fails to set out clear guidelines or criteria that may help solve potential clashes with other, more closely linked jurisdictions.

I. Introduction

The topic of jurisdiction has been a contentious issue for decades. Global internet platforms are yet posing various legal problems to national as well as international law with regard to the scope of jurisdiction. In international law that is based on the Westphalian notion of state-centrism and exclusive state sovereignty, the most important link is usually a state's territory. Jurisdiction has nevertheless begun to more and more extend extraterritorially, e.g. in the areas of human rights law and antitrust law. While such extensive application of domestic law has started off as a rare exception, it is nowadays common practice. Where jurisdiction moves away from the limits of territorial borders, it poses a problem on its application in cyberspace. In the field of data and privacy protection, the European Union's General Data Protection Regulation (GDPR)[1] prominently standardises the domestic-

[1] Regulation (EU) 2016/679.

market principle in Article 3(2) GDPR. According to this provision that is titled "territorial scope", data controllers and processors are potentially under the obligations stipulated in the regulation even if they are located outside of the EU and have their main business abroad. Given the potential of creating a global privacy and data protection system, this brings up the important aspects on the territorial scope of application of the GDPR, the current role of "territory" in issues on jurisdiction, reconciling overlapping jurisdictions. The current article examines the scope and limits of Article 3(2) GDPR in order to interpret the "territorial scope" of the GDPR in line with international legal standards, most importantly in a way that respects the principle of state sovereignty. The paper will analyse current developments regarding the jurisdiction to prescribe particularly in the light of the recent judgments delivered by the European Court of Justice (ECJ) and gives a brief analysis of the GDPR's standard-setting potential in protecting privacy and data protection online.

II. The GDPR Beyond EU's Borders

Public international law is traditionally state-centric. The internet on the other hand constitutes a global network of mostly private entities and institutions and moreover creates part of what is often referred to as cyberspace. The concepts are not interchangeable but highly interrelated. The question of jurisdiction in cyberspace has been given new attention as to the continuously emerging importance for conducting business as well as exercising fundamental rights and the state's role in this regard. Websites are often available regardless of the geographical position of the user. Goods or services are available online on a global scale. Ideas and opinions, may they be political or simply display personal character, are potentially shared freely, without restraints, and open to be analysed.

During the early times of the internet as we know it today, cyberspace has often been regarded as a separate, de-territorialised space. Most prominently *John Perry Barlow* has called for the cyberspace to be independent and in particular from state interference.[2] Today it has become evident that even though cyberspace is largely run by private entities, states do play important roles in the way it functions. Governments are able to block data traffic and to have the technical capacity to largely intercept individual

[2] *J. P. Barlow*, A Declaration of the Independence of Cyberspace, <https://www.eff.org> (last access 17.1.2020).

communications. Provided that some physical infrastructure of cyberspace is built upon a state's territory, cyberspace cannot be immune from national jurisdictions. Therefore, there has been seen the need to categorise cyberspace in a way that is meaningful and protects its particularity while restricting states' manoeuvres. Accordingly, cyberspace has been categorised, e.g. as *global commons* such as outer space and the high seas. Unfortunately, that has proven difficult and inadequate as cyberspace is man-made, fully intangible, and highly volatile. The exploitation of data does not lead to its destruction. Hence, cyberspace has a *sui generis* character. This characterisation is important for the regulation of the cyberspace. Cyberspace is not a separate space in the meaning of geographical location. Instead, it rather pushes the importance of territorial borders into the background while not rendering them redundant.

States have first tried to simply apply existing laws as they stand to the situations in cyberspace.[3] Lately, however, more and more legislation has been enacted that appears specifically tailored to the situations online.[4] Against the backdrop of the potential opportunities and threats, the role of human rights protection comes into play. The GDPR has deemed to be ground-breaking in the field of data protection and the protection of privacy world-wide in that regard.[5] Although the GDPR does not provide a complete set of detailed rules, nor a full harmonisation package in all the affected legal sub-branches already due to the more than 70 opening clauses, it cannot be denied that overall the GDPR sets important standards and benchmarks: It constitutes foundational rules for the processing of personal data, including but by far not exclusively, by relying on a person's consent and thereby aiming at supporting informational self-determination.[6] It stipulates standards such as data protection by design and data protection by default.[7]

Moreover, it also strives for a broad scope of application in order to aim for comprehensive privacy and data protection. The GDPR in its Article 3

[3] *U. Kohl*, Jurisdiction and the Internet, 2007, 256.

[4] On the international level, the Convention on Cybercrime (or Budapest Convention) is the most prominent example.

[5] See *R. J. Kokshoorn*, EU GDPR – New Rules, Wider Reach – the Biggest Change to Data Protection Laws in 20 Years, <https://www.citco.com>, 2017, (last access 17.1.2020); *A. Santario*, G.D.P.R., A New Privacy Law, Makes Europe World's Leading Tech Watchdog, <https://www.nytimes.com>, 2018, (last access 17.1.2020).

[6] See Article 6 Regulation (EU) 2016/679.

[7] Article 25 Regulation (EU) 2016/679.

codifies an extensive type of "territorial scope".[8] The latter aims at a protection of persons in the EU that is as complete as possible and – against the backdrop of the global networked digital era – attempts to protect the digital privacy of persons regardless of the geographical location of a data controller or data processor. Under the title "territorial scope", Article 3 GDPR prescribes:

> "1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
> 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
> the offering of goods or services […] to such data subjects in the Union; or
> the monitoring of their behaviour as far as their behaviour takes place within the Union."

The GDPR binds data controllers as well as processors to the EU rules of the GDPR regardless of their actual geographical location or statutory seat under the requirements of Article 3(1) and (2) GDPR. The aspect of jurisdiction in this regard may *prima facie* deemed an issue of private international law because the aspect of overlapping jurisdictions would have to be solved by the conflict of laws.[9] However, the matter at hand is in fact a core concern of public international law. The protection of privacy with its foundation in human dignity and human and fundamental rights protection reaches out to the core of statehood and to the essence of governmental regulation. (Supra-)National laws cannot be exclusive to decide upon the proximity to a national jurisdiction of the case at hand. Instead international human rights law plays an important role as well as public international law principles, such as state sovereignty as well as the principle of non-intervention.[10] Overall, the aspect of international jurisdiction can be seen as a crucial part of finding a way to reduce conflicts between states.[11] As states have conferred parts of their sovereignty and powers onto the EU, this article will regard the EU an entity that equally exercises jurisdiction in the area of privacy protection and the protection of personal data.

---

[8] Article 3 Regulation (EU) 2016/679.

[9] *M. Taylor*, Permissions and Prohibitions in Data Protection Jurisdiction, Brussels Privacy Hub, Working Paper Vol. 2 No. 6, 2016, 3.

[10] *M. Taylor* (note 9); *J. A. Cannataci/P. M. Mifsud-Bonnici*, Weaving the Mesh: Finding Remedies in Cyberspace, 2007, 74.

[11] *C. Ryngaert*, Jurisdiction in International law, 2nd ed. 2015, 29.

From a perspective of international law, this potentially extremely far-reaching scope of the GDPR is remarkable, and exceeds the prior rule set out by the Data Protection Directive (DPD).[12] Yet, it is no surprise either. From a position of the EU in the attempt to protect people in the EU as comprehensively as possible, e.g. from data processors outsourcing their tasks or foreign entities that process personal data of individuals residing in the EU, it is only a logical consequence.[13] However, the problem stems from a (potential) clash of jurisdictions. Even the GDPR itself has foreseen a conflict.[14] Those problems may result in legal uncertainties and may ultimately threaten the protection of personal data and privacy. Therefore, it is necessary to scrutinise the extraterritorial scope of the GDPR.

III. Practical Relevance of the GDPR's Territorial Scope

The question of the GDPR's (potentially) global scope of application is not only a matter of academic interest or political rhetoric. Indeed, the GDPR has become the trendsetter in the area of data protection law and privacy law worldwide. Not only has the GDPR been deemed a landmark regulation, but also has it been used as a role model for other emerging laws in this area such as the latest data protection law of Brazil[15] and also the Californian Consumer Privacy Act[16]. Whereas the global relevance of the GDPR cannot be denied, the actual question of the EU's data protection law's very own legal scope has also been up to the European Court of Justice to decide.

[12] See Article 4c) Directive (EC) 95/46/EC.

[13] See Article 29 Working Group, Working Paper on the Question of the International Applicability of the EU Data Protection Law on the Processing of Personal Data by non-EU Websites, WP 56, 2002.

[14] See Recital 115 Regulation (EU) 2016/679.

[15] Brazilian General Data Protection Law (LGPD), Federal Law No. 13,709/2018 of 15.8.2018.

[16] California Consumer Privacy Act (CCPA), Assembly Bill No. 375 of 29.7.2018.

1. *Google v. Costeja Gonzáles*

The first important case in that regard has been the case of *Google Spain & Google Inc. against the Spanish data protection agency AEPD and Mr. Mario Costeja Gonzáles* (*Google Spain* case) from 2014.[17] In this case, the ECJ had to determine the global reach of the so-called right to be forgotten. In 1998, the Spanish newspaper *La Vanguardia* published announcements in connection to a forced sale of properties that resulted from massive social security debts. One of the properties belonged to Mr. *Mario Costeja González*. His name was published in the newspaper and thereby mentioned in connection with financial problems. The publications finally were included in the Google search engine. Every time that someone searched for Mr. *González* on Google, the first search results showed him linked to his prior financial issues. Justifying his claim with the irrelevance of this information from his past, he requested Google to dereference the search results. Legally based not on the GDPR but on its predecessor, the Data Protection Directive, the ECJ had to decide i.a. upon the global scope of the DPD and more precisely, whether Google was under the obligation to de-index Mr. *Gonzales* only on the level of Google Spain, Google's EU-wide search engines, and lastly and most crucially, on a global, world-wide scale.

2. *Google v. CNIL*

Another, more recent case directly concerned the scope of the GDPR.[18] Five years after the *Google Spain* case has preoccupied the ECJ, the "territorial scope" of the EU's jurisdiction regarding data protection law is still an open question. The case at hand emerged from a dispute between Google and the French data protection authority CNIL. CNIL requested Google to delist search results on a global scale as this was the only effective way to protect the affected persons' right to privacy. Google denied the request arguing that the EU Court would not have the competence to ask Google for such global removal of search results because such wide-ranging decision could in fact be abused by authoritarian regimes. Google instead suggested a geo-blocking technique. Such technological feature restricts the access to certain websites depending of the geographical location of the person surf-

[17] *Google Spain & Google Inc. against the Spanish data protection agency AEPD and Mr. Mario Costeja Gonzáles*, ECJ Case C-131/12 2014, ECLI:EU:C:2014:317.

[18] *Google v. CNIL*, ECJ Case C-507/17 2019, ECLI:EU:C:2019:772.

ing the website. The ECJ therefore had to consider the actual scope of the GDPR under its Article 3.

3. *Glawischnig-Piesczek v. Facebook Ireland*

Another case that is of importance for the question on the territorial scope of EU law is the one where the former Austrian politician *Eva Glawischnig-Piesczek* requested the deletion of hate speech against her.[19] During her time as active politician and leader of the Austrian green party, she published a post regarding the treatment of refugees. As reactions to the post, people called her a "lousy traitor", "corrupt oaf", and engaged in further hate speech. While Facebook blocked the access on an EU level, Mrs. *Glawischnig-Piesczek* requested the world-wide removal of hate speech against her. While the matter in this case does not directly imply the GDPR but the eCommerce Directive,[20] the case nevertheless sheds light on the global dimension of EU legislation in connection with cyber-related disputes.

IV. The GDPR in the Context of International (Human Rights) Law

Before analysing the above-mentioned court cases and scrutinising the ECJ's line of reasoning in order to establish the limits to Article 3 GDPR, it is first necessary to consider the underlying legal problems that involve aspects of jurisdiction and state sovereignty as well as effective human rights protection. Whereas the rules on jurisdiction describe the potential of a state's legislative action, human rights law claims the utilisation of this potential for the benefit of human rights protection. In the context of the GDPR it means that the EU exercises a certain discretion but at the same time fulfils – and must fulfil – its duty as of a positive obligation under the human rights to data protection and privacy.[21]

---

[19] *Glawischnig-Piesczek v. Facebook Ireland,* ECJ Case C-18/18 2019, ECLI:EU:C:2019:821.

[20] Directive (EC) 2000/31/EC.

[21] *C. Ryngaert/M. Taylor*, The GDPR as Global Data Protection Regulation?, AJIL 114 (2020), 5.

1. Jurisdiction (to Prescribe)

The principles of jurisdiction in public international law as well as international relations are of fundamental importance: They concern the allocation between states and other entities, such as the EU, of the competence to regulate daily life.[22] It includes the competence of a state to manage its own population and secure the differences that make each state a distinct society.[23] As *Milanovic* points out correctly, these notions of jurisdiction must not be confused with those in the area of human rights law because they are independent from each other.[24] Jurisdiction in the context of data protection law should be evaluated by the rules of public international law.[25]

Jurisdiction in international law is a highly controversial topic and includes various meanings and nuances.[26] In other words, jurisdiction forms part of a state's sovereignty,[27] its right to regulate its own public order. Equally, the state may define its coercive powers. Jurisdiction is closely linked to the territorial sovereignty of states.[28] Limitations on it particular in extraterritorial situations stem from the equal sovereignty of other states. The question of jurisdiction in cyberspace that highly ignored territorial state borders is therefore particularly challenging existing international law.

Despite the lack of a clear consensus of an international concept of jurisdiction, one may generally categorise three types of jurisdiction, whereas the most crucial aspect is the so-called jurisdiction to prescribe or *compétence normative*.[29] It classically describes the state's prerogative to establish rules for people on its own territory.[30] A United States (US) national physically visiting German territory is bound by German rules. Yet, states also prescribe rules that reach beyond the conduct within a state's town territory. Prominent examples are the areas of antitrust law, criminal law as well as

22 *B. H. Oxman*, Jurisdiction of States, in: R. Wolfrum (ed.), MPEPIL, 2007, A.

23 *U. Kohl*, Territoriality and Globalization, in: S. Allen/D. Costelloe, M. Fitzmaurice/P. Gragl/E. Guntripal (eds.), The Oxford Handbook of Jurisdiction in International Law, 2019, 300 et seq.

24 *M. Milanovic*, Extraterritorial Application of Human Rights Treaties, 2011, 26.

25 Article 29 Working Group (note 13), 2.

26 See in general *C. Staker*, Jurisdiction, in: M. Evans (ed.), International Law, 5th ed. 2018, 289; *M. N. Shaw*, International Law, 8th ed. 2018, 588 et seq.; *C. Ryngaert* (note 11), 5 et seq.

27 See only *M. N. Shaw* (note 26), 481.

28 See Art. 2(1) Charter of the United Nations; *M. Schmitt*, Tallinn Manual 2.0, 2018, Rule 1.

29 See *C. Staker* (note 26); *M. Milanovic* (note 24), 23.

30 *I. Brownlie*, Brownlie's Principles of Public International Law, 9th ed. 2019, 297.

human rights law.[31] These extraterritorial rules are often set out without the other states' consent.[32] Important exceptions to the territorial basis of jurisdiction concern the location of where an act is initiated or consummated (subjective and objective territoriality), the nationality of affected persons, and the ramifications of an act felt within a state (effects doctrine).[33]

Generally, extending the State's competence to set up rules beyond its own territorial borders is a contested undertaking. E.g. according to the passive personality principle the state may prohibit certain conduct that directly harms its nationals, even if the perpetrator does not possess its nationality and the conduct takes place outside its territory. Exercising jurisdiction based on the passive personality principle has by now been established in international law. It has been applied in singular circumstances such as against a US citizen by Mexico already in 1885 who was based in the US and alleged of libelling a Mexican national in a US newspaper.[34] Simply because the victim was Mexican, Mexico assumed jurisdiction over the perpetrator. The US denied any jurisdiction for Mexico. However recently, there might have been a trend in international law in favour of accepting the type of passive personality jurisdiction. One of the Separate Opinions in the *Arrest Warrant* case[35] noted that at least for some kind of criminal offenses the passive personality principle seems to meet little opposition nowadays. On the other side, one should be careful to simply derive a general acceptance from several instances of criminal law cases. Therefore, one may doubt that the principle equally applies on a general level.

a) "Territory" as a Type of Jurisdictional Nexus

When applying the dichotomic distinction between territorial and extraterritorial jurisdiction, the cyberspace places particular challenges, as the mere territorial geographic location does not matter much. In order to find a suitable concept for cyberspace and the internet, it is necessary to analyse the actual relationship between the classic categories and scrutinise the underlying idea.

---

31 See *K. Meessen*, Extraterritorial Jurisdiction in Theory and Practice, 1996, ix.
32 See only *M. Milanovic* (note 24), 24.
33 *M. Taylor* (note 9).
34 See *J. B. Moore*, A Digest of International Law, Vol. 2, 1906, 431 et seq.
35 *Case Concerning the Arrest Warrant of 11 April 2000* (*Democratic Republic of the Congo v. Belgium*), ICJ Reports 2002, 2.

Approaching the roots of (extra-)territorial jurisdiction from a purely public international law perspective one rapidly stumbles upon landmark decisions. One is the case of Island of Palmas, in which it has been pointed out that a state has exclusive power and competence regarding its own territory because it enjoys sovereignty over it.[36] A general aversion against interfering into another state's jurisdiction may also be inferred from the International Court of Justice's (ICJ) decision in the *Barcelona Traction* case, where it was expressed that state sovereignty and the principle of non-interference limits the state extraterritorial jurisdiction.[37] The mostly cited case in this context, however, is the *Lotus* decision, a landmark case decided in 1935 by the Permanent Court of International Justice (PCIJ). As to the facts, the PCIJ had to decide upon the criminal jurisdiction of Turkish courts upon a French officer from the S.S. Lotus. Two ships, the French *Lotus* and the Turkish *Boz-Kourt*, have collided on the high sea. The incident resulted in the death of eight Turkish seamen. The responsible French officer of the *Lotus* was afterwards tried in front of Turkish courts that in the end found him guilty of involuntary manslaughter. France did not agree with the Turkish courts exercising jurisdiction over the French seaman and the consequences over an incident that happened on the High Seas and deemed French courts to be more appropriate because the captain was a French national and has to be held responsible in front of French courts. Whether Turkey indeed had the legal capacity to prescribe rules for behaviour beyond its territory, adjudicate the case in front of Turkish courts and enforce the verdict was up to decide for the PCIJ. It held in its famous *Lotus* decision:

> "the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule of the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention."[38]

Therefore, the default rule in international law is that a state cannot exercise jurisdiction within the territory of another state unless there is a per-

[36] *Island of Palmas Case* (*United States v. Netherlands*), Award 1928, ICGJ 392, 4.4.1928, 838.

[37] *Case concerning Barcelona Traction, Light and Power Company Ltd.* (*Belgium v. Spain*), Separate Opinion of *Judge Sr Gerald Fitzmaurice*, 1970, ICJ Reports 65, para. 70.

[38] *The Case of the S.S. Lotus* (*France v. Turkey*), (1927) P.C.I.J., Ser. A, No. 10, 18 et seq.

missive rule to the contrary. It did allow, however, the application of extra-territorial jurisdiction in the following manner by pointing out that:

> "It does not, however, follow that international law prohibits a State from exercising jurisdiction in its own territory, in respect of any case which relates to acts which have taken place abroad, and in which it cannot rely on some permissive rule of international law."[39]

Especially with regard to the GDPR's Article 3 in the context of a cyber-related issue one may be tempted to simply rely on these core aspects of the *Lotus* decision.[40] However, it is more revealing to isolate the underlying task of the court and the purpose of the balancing act the court conducted. Although objections against the reference to the *Lotus* decision raised i.a. by *Svantesson*[41] and *Mills*,[42] one may carefully benefit from the gist of the decision. Back then, the PCIJ had to interpret Article 15 of the 1923 Convention of Lausanne which reads:

> "Subject to the provisions of Article 16, all questions of jurisdiction shall, as between Turkey and the other contracting Powers, be decided in accordance with the principles of international law."

This means, the starting point for finding the legal solution to the dispute in front of the court concerned an international peace treaty about the conditions of residence and business and jurisdiction between the contracting parties (Ottoman Empire, French Republic, British Empire, Kingdom of Italy, Empire of Japan, Kingdom of Greece, and Kingdom of Romania). The balance between the sovereign interests at stake was carried out against the backdrop of peace and security. Therefore, a state must not carry out coercive or forceful measures outside its territory without a permissive rule. At the same time, a situation taking place abroad may well be subject to domestic legislation if there is a sufficient nexus that justifies such action. Territory has served well as prominent example for a nexus,[43] as it has traditionally been the strongest one. The nexus-based approach finds support in

39 *The Case of the S.S. Lotus* (note 38), 19.

40 Just to mention one example of an explicit reference to the Lotus principle in cyber-related matters apart from the GDPR: Report of the Council of Europe's Transborder Group adopted by the T-CY on 6.12.2012.

41 *D. J. Svantesson*, Solving the Internet Jurisdiction Puzzle, 2017, 22 et seq.

42 *A. Mills*, Rethinking Jurisdiction in International Law, BYIL 84 (2014), 191.

43 International Law Commission, Report on the Work of Its Fifty-Eighth Session (1 May – 9 June and 3 July – 11 August) UN Doc. A/61/10, Annex E, para. 42; *C. Ryngaert*, Cosmopolitan Jurisdiction and the National Interest, in: S. Allen/D. Costelloe, M. Fitzmaurice/P. Gragl/E. Guntripal (note 23), 209 et seq.

other branches of international law that are closely linked to data protection law, such as economic law.

b) Extraterritorial Application in Other Scenarios

Data protection law is not exclusively anchored in fundamental rights law but the idea of a free flow of information is connected with essential economic interests. One area of law that forms a prominent part of economic law and that knows an extraterritorial scope is antitrust law. In economy-related matters, the EU has managed to seize its market power and more importantly its market access as a tool to influence players abroad.[44] This is what has been prominently coined the "*Brussels effect*".[45] Earlier, the EU itself contested the exercise of extraterritorial jurisdiction in antitrust-related matters by states such as the US. In the meantime, the EU has largely adopted extraterritorial legislation itself. Nevertheless, the adoption of a GDPR-like regulation by other states is not a unilateral decision by the EU unlike the wide interpretation of the GDPR's scope.

Antitrust law is equally in need of a justification when it applies a scope that reaches beyond the classic territorial borderline. Interestingly the justification is usually accepted by establishing a certain nexus. A frequent example of such nexus is the reliance on specific effects. The EU merger control regime on the basis of EC Regulation No. 139/2004 i.a. includes an effect-nexus.[46] Antitrust law and in particular the merger control law aims at protecting market competition. Foreign companies may have the power to severely affect the domestic market. However, to justify a (potential) intrusion into another state's jurisdictional sovereignty it is insufficient to rely on all kinds of economic effects. Interesting insights come from a look to the US as another major economic and political player on the international level. The US nowadays applies the Sherman Anti-Trust Act[47] in an extraterritorial manner. The extraterritorial effect was not clearly set out in the Sherman Act itself and the Courts at first denied such wide application. Stressing one important aspect, in the *American Banana* case, *Justice Holmes* explained that interpreting the Sherman Act as applicable outside the US

[44] See *J. Resnik*, Law's Migration: American Exceptionalism, Silent Dialogues, and Federalism's Multiple Ports of Entry, Yale L. J. 115 (2006), 1564.
[45] *A. Bradford*, The Brussels Effect, Nw. U. L. Rev. 107 (2013).
[46] See Council Regulation (EC) No. 139/2004.
[47] US Department of Justice, Sherman Antitrust Act 1890.

would be an "interference with the authority of another sovereign" and therefore "contrary to the comity of nations".[48] Later, the jurisprudence by the US Courts turned to favouring an application extraterritorially.[49] E.g. in *Sabre Shipping Corp. v. American President Lines Ltd.*, the US Court stated:

> "The antitrust laws of this country extend to any activity (unless plainly and clearly exempted by statute), whether carried on by a foreigner or a citizen, which affects the trade and the commerce of the United States; and this is so irrespective of the citizenship of the actor and the place where the activity took place (*United States v. Alcoa*)."[50]

The reaction to this expansion of a US law was strong, not only by other states but also by members of parliament. From the United Kingdom (UK) side, a member of the House of Lords expressed his disagreement by emphasising the principle of reciprocity. He asked how the US would react if other states did the same and bind US companies to their laws in a comparable manner.[51] The UK rejected the extraterritorial application of US laws by enacting a Protection of Trade Interests Act.[52] The example followed Australia, Canada, France, Italy, The Netherlands, South Africa, and West Germany.[53] One member of the US parliament noted that

> "Once a court system gets an ideology into its mind to such a degree of fanaticism as one can find in the United States it is no surprise, however deplorable it may be, that it becomes a matter for imperialism overseas."[54]

However, the US Supreme Court has later on rejected the comity arguments.[55]

> "[T]he fact that conduct is lawful in the state in which it took place will not, of itself, bar application of the United States antitrust laws, even where the foreign state has a strong policy to permit or encourage such conduct."[56]

---

48 *American Banana Co. v. United Fruit Co.*, 213 U.S. 347 (1909), 356.

49 *D. E. Knebel*, Extraterritorial application of U.S. antitrust laws: principles and responses, Jindal Global Law Review 8 (2017), 181, 189.

50 *Sabre Shipping Corp. v. American President Lines Ltd.*, 285 F. Supp. 949 (S.D.N.Y. 1968), 953.

51 *D. L. Hacking*, The Increasing Extraterritorial Impact of U.S. Laws: A Cause for Concern Amongst Friends of America, Nw. J. Int'l L. & Bus. 1 (1979).

52 United Kingdom Protection of Trading Interests Act 1980, Chapter 11.

53 *D. E. Knebel* (note 49), 193.

54 *A. K. Huntley*, The Protection of Trading Interests Act 1980: Some Jurisdictional Aspects of Enforcement of Antitrust Laws, ICLQ 30 (1981), 213, 224.

55 *Hartford Fire Ins. Co. v. California*, 509 U.S. 764 (1993), 799.

The extraterritorial application is permitted, if there is a direct, substantial, and reasonably foreseeable effect.[57] Accordingly decided the EU in the field of antitrust law. At first, one could find a big opposition towards such wide scope of domestic laws. The General Court of the EU hence declared that first, the effect-based jurisdiction is a matter of public international law and second, it is justified if it is foreseeable that a proposed concentration will have an immediate and substantial effect within the EU.[58] Such qualified effect under US as well as EU law aims at balancing the interests at stake while taking into account the economic context as well as the object and purpose of both, the foreign sovereignty and the domestic legitimate economic interests. It demonstrates that the extraterritorial application is nowadays well established but may generally depend, nevertheless, on a limiting interpretation.

2. The Fundamental Rights to Data Protection and Privacy

The GDPR as a type of EU secondary legislation,[59] is directly applicable throughout the EU member states' territory.[60] In contrast to other examples of such kind of legislation such as the eCommerce Directive, the GDPR is not merely a regulation serving economic freedoms, but it directly realises the fundamental right to data protection. Against such backdrop, the possibly global application of the GDPR does not come without problems. The difficulties begin with the fact that the right to data protection is not yet recognised as an independent human right on the international plane. While the International Covenant on Civil and Political Rights (ICCPR) or the European Charter on Human Rights (ECHR) only know the right to privacy in this regard, the EU Charter on Fundamental Rights (EU Charter) stipulates the right to privacy in its Article 7 as well as the right to data protection in its Article 8 as two distinct fundamental rights. This does not mean that the protection of personal data is unfamiliar to international hu-

56 The American Law Institute, The Foreign Relations Law of the United States, 1965, 415.

57 See, e.g. *R. Beckler/M. Kirtland*, Extraterritorial Application of U.S. Antitrust Law: What is a "Direct, Substantial, and Reasonably Foreseeable Effect" Under the Foreign Trade Antitrust Improvements Act?, Tex. Int'l L. J. 38 (2003).

58 EC Case T-102/96 ECR II-753 1999, para. 90.

59 Secondary legislation in the EU context means the law enacted below the level of the foundational treaties of the EU.

60 See Article 288(2) Regulation (EU) 2016/679.

man rights law. However, it is usually regarded as a part of the right to privacy.[61] As an independent human right apart from the right to privacy, data protection is exclusively prescribed in the EU Charter.

In order to ensure a comprehensive protection of the newly established right, the question necessarily arises as to its actual potential when it comes to the globally interconnected, virtual, and borderless cyberspace which in the end most likely include third states' affairs.

3. The State's Duty to Protect

The general limited concept of the extraterritorial scope has to be pushed to the edge of these limits in the context of human rights law. As the fundamental rights of data protection and privacy are at stake, the EU does not only have the obligation to refrain from any infringement of the rights but also bears the obligation to protect people from third party activities that curtail the people's fundamental rights.[62] The ECHR in its Article 1 requires the member states to "secure to everyone within their jurisdiction the rights and freedoms defined in Section I of the Convention". Article 8(1) ECHR provides for everyone to have the right to respect for his or her private life. Particularly from the term "respect", the ECtHR has derived from an early stage on that a state not merely has the duty to refrain from intervening in a person's private life but is also under positive obligations.[63] It includes "the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves".[64] This duty persists with regard to cyberspace and the aspect of data protection.[65] Furthermore, the positive dimension also extends to what in human rights law is known as extraterritorial situations. While the ECHR typically deals with situations of an extraterritorial nature, where a state has effective control over either a (part of a) territory or a person or entity, it also applies to the cases without such degree of control.

---

[61] See only *Rotaru v. Romania*, 4.5.2000, ECtHR, App. No. 28341/95.

[62] See only *M. Klatt*, Positive Obligations under the European Convention on Human Rights, HJIL 71 (2011), 691.

[63] *Marckx v. Belgium*, 13.6.1979, Series A No. 31; *Von Hannover v. Germany*, 24.6.2004, Reports of Judgments and Decisions ECtHR 2004-VI, § 57; *Stubbings and Others v. the United Kingdom*, 22.10.1996, Reports of Judgments and Decisions ECtHR 1996-IV, § 61-62.

[64] *Von Hannover v. Germany* (note 63).

[65] *Mosley v. the United Kingdom*, 10.5.2011, ECtHR, App. No. 48009/08; *Roche v. the United Kingdom* 23.5.2002, ECtHR, App. No. 32555/96.

> "Even in the absence of effective control of a territory outside its borders, the State still has a positive obligation under Article 1 of the Convention to take the diplomatic, economic, judicial or other measures that it is in its power to take and are in accordance with international law to secure to applicants the rights guaranteed by the Convention."[66]

In this light, an extensive interpretation of Article 3 GDPR lies well within the positive dimension of human rights obligations. Whenever there is a substantial threat to a person's fundamental right to privacy and data protection in the online sphere, a state must take the appropriate measures even if it involves a private actor beyond the state's borders. Yet, as the court emphasised, the human rights obligation is not without restraint but in fact limited by rules of international law, most importantly the sovereignty of a third state and jurisdictional competences. This is equally enshrined in Article 21 Treaty on the European Union (TEU). Therefore, it is necessary to balance the aspects of third states' sovereignty and jurisdiction with a maximum of fundamental rights protection.

V. Territorial Scope of the GDPR

As introduced above, international law is not unfamiliar with extraterritorial jurisdiction. Yet, it is not accepted without a sufficient nexus and limitations in place. It is interesting that the GDPR in the name of protecting the right to data protection boldly establishes the domestic-market principle and thereby relying on certain effects *vis-à-vis* EU citizens regardless of the location or nationality of the data controller or processor. It is necessary to be careful when determining the current international legal status of such rule. A clash of jurisdictions is otherwise becoming hard to avoid. As the *Google Spain* decision has shown, an EU decision on a global de-referencing would – at least *prima facie* – massively clash, e.g. with the US right to information. Albeit several GDPR comparable data protection laws have been adopted world-wide, a harmonisation is not easy to achieve. As long as the level of data protection is the same everywhere, potential jurisdictional conflicts between data protection laws will most likely remain resolvable in practice. However, disputes will arise in situations when the ma-

66 *Treska and Treska v. Albania and Italy*, 29.6.2006, ECtHR, App. No. 26937/04.

terial laws differ from one another. So far, states seem to claim as much jurisdictional space as they can get.[67]

As a consequence, the tendencies of jurisdiction do not necessarily favour aspects of territoriality as core basis. Of crucial importance remains a specific nexus and the circumstances of the situation that requires a careful balance between the different sovereign interests at stake. As a further analysis of the latest jurisprudence of the ECJ will show, prescriptive jurisdiction is not absolute but flexible and varies according to the situation at hand. This is particularly important as the internet has become a prominent example of space that is rooted in physical territory but goes beyond mere physicalness. *Svantesson* i.a. asks for a massive reduction of the role of territory in jurisdictional matters involving the internet.[68] The ECJ seems to follow the same approach as evidenced by the recent case-law on the EU level.

1. Restrictive Interpretation of the Wording of Article 3 GDPR

Article 3(1) GDPR stipulates that the regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. This rather straight forward wording comprises cases such as *Google Spain*, where the question arises as to whether the scope includes Google Inc. on the global scale (incl. google.com) and justifies a right to be forgotten in such dimension. The wording of Article 3(2) GDPR enumerates two main case scenarios, one in which an entity abroad offers goods or services to a person in the EU and one where the person in the EU is only involved insofar as their behaviour is monitored. Its wording now applies to every entity meeting its requirements regardless of an establishment in the EU. At the heart of the provision is the criterion of targeting individuals in the EU.[69]

As the wording of Article 3(2) GDPR is potentially wide, it is not surprising that introducing the provision has undergone substantial critique at first. During the discussions, different member states uttered their discon-

[67] For a general overview, see: *D. J. Svantesson*, Internet & Jurisdiction Global Status Report 2019.

[68] *D. J. Svantesson*, Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation, International Data Privacy Law 5 (2015), 226 et seq.

[69] European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR, Version 2.1, 12.11.2019, 13.

tent.[70] According to such critical remarks, the wide scope only pretends to grant safety for data subjects without an actual effective remedy. Without an EU-based representative according to Article 25 GDPR, the global application of the GDPR is meaningless as the EU legislation does not offer a relevant enforcement mechanism. It was even suggested to eliminate Article 3(2) GDPR as it stands right now and substitute it with a provision of the previous EU Data Protection Directive, namely Article 4(1)(c) which reads:

> "(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."

In the end, the states reached an agreement on the current wording. It should however be interpreted according to international law and on a case-by-case basis.[71]

a) "Offering of Goods and Services"

As to the first variant, the meaning of "offering of goods or services" is crucial. Over the Internet it has become fairly simple to access foreign companies' websites that are not specifically directed towards the global population regardless of any state's territorial borders. That, however, potentially includes customers everywhere in the world. Compared to an example from the analogous world, a physical store usually offers goods to the biggest group of potential customers. Displaying a product in the showcase does usually not imply the will only to sell the product to fellow nationals. Instead, an *invitatio ad offerendum* is construed as an open invitation to everyone interested without recourse to the geographical background of the customer. It is not necessary that there is any payment required or expected. There is *prima facie* no reason why the ordinary meaning should change in an online situation.

The offering of services is a very crucial requirement. It has been defined in EU law and EU case-law. It includes the offering of information society services as laid down in Article 1(1)(b) EU Directive 2015/1535, i.e.

---

70 See EU Council Document 9897/2/12 of 18.7.2012.
71 European Data Protection Board, (note 69), 12.

> "any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".

As to the context, the GDPR itself offers some guidance on the interpretation of the term "offer" in its recitals. The GDPR legislator has already envisaged that the widest scope needs restrictions. Therefore, it explained that the mere accessibility of a website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain the intention to offer goods or services.[72] Factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.[73] Personal data processing that is related to the activity falling within the scope of Article 3(2) GDPR is covered by the scope of the GDPR as well. According to the European Data Protection Board, however, there must be a connection between the processing activity and the offering of goods or services.[74]

The above-mentioned aspects that have been introduced into Recital 23 GDPR share a close relationship with EU Regulation 1215/2012 on jurisdiction and enforcement of judgements in civil and commercial matters. Article 17(1)(c) of such regulation uses the requirement of directing activities to EU Member States. The ECJ has elaborated on the meaning of the wording stipulating that the trader must manifest his or her intention to establish commercial relations with the customers in question.[75] In other words, the trader's will of doing business with the customer in question must be evident.[76] Such evidence can only be derived from more than the mere accessibility of a website, such as the existence of a local patent right, the use of a specific top level domain or even the nature of the product itself such as

---

72 Recital 23 Regulation (EU) 2016/679.

73 Recital 23 Regulation (EU) 2016/679.

74 European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 15.

75 *Peter Pammer v. Reederei Karl Schlüter GmbH & Co. KG* and *Hotel Alpenhof GesmbH v. Oliver Heller*, ECJ Joint Cases C-585/08 and C-144/09 2010, ECLI:EU:C:2010:740, paras. 64 et seq.

76 *Peter Pammer v. Reederei Karl Schlüter GmbH & Co. KG* and *Hotel Alpenhof GesmbH v Oliver Heller* (note 75), para. 76.

tourist trips.[77] On the basis of the given prevailing case-law, the European Data Protection Board developed further criteria such as the designation by name of the EU or a Member State, the use of an internet referencing service for search engines in order to facilitate access from within the EU, or travel advice from the EU.

b) "Monitoring" of Data Subjects' Behaviour

The monitoring of EU data subjects' behaviour is the second ground triggering the extraterritorial scope of the GDPR under Article 3(2) GDPR. As Recital 24 highlights,

> "in order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes."

Recital 24 mentions explicitly the aspect of "tracking". The European Data Protection Board goes further and suggests the extension of this notion to other forms of behavioural monitoring.[78]

In contrast to the act of offering of goods and services, behavioural monitoring does not require a certain level of intent. Nevertheless, the term "monitoring" already implies that the data controller or processor follows a specific purpose and that the controller or processor envisages the monitoring. Not every type of data collection suffices in this regard. Instead it must be taken into account the object and purpose of the monitoring and in particular the subsequent use of such data.[79] In order to further restrict the still wide scope of the behavioural monitoring variant of Article 3(2) GDPR, two cumulative criteria must be fulfilled. First the monitored behaviour must relate to a data subject in the EU. Second, the monitored behaviour must take place in the EU. A variety of monitoring activities may trigger the scope of Article 3(2)(b) GDPR, namely online tracking through cookies, market survey based on individual profiles and many more.[80] Still, such

[77] *Peter Pammer v. Reederei Karl Schlüter GmbH & Co. KG* and *Hotel Alpenhof GesmbH v. Oliver Heller* (note 75), paras. 81 et seq.
[78] European Data Protection Board (note 69), 17 et seq.
[79] European Data Protection Board (note 69), 18.
[80] European Data Protection Board (note 69), 18.

considerations have not played a large role in the most recent case-law of the ECJ because platforms such as Google or Facebook supersede the classical online business.

2. EU Legal Nexus Basis

The interpretation of the requirements of Article 3(2) GDPR has shown so far that some legal nexus is necessary to either EU territory or people in the EU. The question is now how to place such interpretation into the international legal framework.

In the pre-GDPR era, the EU Data Protection Directive spoke about the applicable national law in this context. The GDPR instead speaks about the protection of individual in the Union which does not necessarily have a (geographical or spatial) territorial connotation albeit the title of Article 3 is admittedly named "territorial scope".[81] While the main field in which the EU core competence has been deployed has been its territory, it may be interpreted differently according to the factual circumstances of cyberspace. Indeed, the Advocate General in the *Salemink* case explained that

> "for EU purposes, the 'territory' of the Member States is the area (not necessarily territorial, in the spatial or geographical sense) of exercise of the competences of the Union".[82]

Therefore, the territory seems to be regarded more as a field of competence rather than understood in a geographical sense. EU law in economic matters knows this wide scope of its jurisdiction yet in other regulations and directives. E.g. the EU Distance Selling Directive was applicable not only to persons within the EU, but to non-EU-based entities that sell goods to EU citizens over the Internet.[83] In this context, scholars have called for an abolishment of the general dichotomy of territoriality and extra-territoriality.[84] Despite the favourable nexus oriented approach, it cannot be denied that territory in international law has lost all substance. This is also not about to change regardless the borderless nature of the internet. Moreover, the distinction is indeed useful for the further requirements that must

[81] See *M. Taylor* (note 9), 10.

[82] *A. Salemink v. Raad van bestuur van het Uitvoeringsinstituut werknemersverzekeringen*, ECJ Case C-347/10 2011, ECLI:EU:C:2011:562, para. 56.

[83] Article 29 Working Group (note 13), 3 et seq.

[84] *D. J. Svantesson* (note 68), 226.

be met in order to comply with international legal standards. The ECJ seems to take up on a modern approach to territory in the era of digitisation. Unfortunately, it does not offer much guidance in terms of a meaningful restriction of a potentially vast jurisdiction.

Furthermore, scholars have argued that the GDPR's scope in fact is not extraterritorial in the international legal sense but forms a separate category that relies on a territorial extension.[85] Such extension as a concept describes the remainder of a territorial nexus that is required for the application of the GDPR while acknowledging that conduct or situations in third states have a significant influence on the manner in which the GDPR applies to these situations.[86] This category, however, does not achieve much legal clarity. The concept is rooted in the above-mentioned nexus that has to reveal sufficiently strong ties with the situation in question. Moreover, the idea of a territorial extension can also be seen as one example of the effect-based jurisdiction.

Taking into consideration the criteria for Article 3(2) GDPR as set out above, there always is at least some reference to the territory. It is not surprising that the mentioned criteria are exclusively based on economic considerations. But both variants, offering of goods and services as well as behavioural monitoring are connected to persons in the EU meaning being physically present in the EU. The general application of the GDPR in such broad terms is therefore not without legal foundation. Yet, another question refers to the actual concrete obligations of data controllers or processors abroad that stem from the GDPR such as the obligation to erase certain kind of personal data.

3. Guidance Through EU Jurisprudence

In general, it is possible to derive important considerations for the EU's jurisdiction from the case of *Google v. CNIL* of 2019. When Google was asked to de-index the relevant search result globally, it countered the argument stressing the EU's lack of enforcement jurisdiction in such a dimension. While the actual global jurisdiction to enforce digital rights is not at

[85] *J. Scott*, The New EU "Extraterritoriality", CML Rev 51 (2014), 1343, 1350; *J. Scott*, Extraterritoriality and Territorial Extension in EU Law, Am. J. Comp. L. 62 (2014), 87; equally *M. Taylor*, The EU's Human Rights Obligations in Relation to Its Data Protection Laws with Extraterritorial Effect, International Data Privacy Law 5 (2015), 247 et seq.

[86] *J. Scott*, Extraterritoriality and Territorial … (note 85), 90; *M. Taylor* (note 85), 247.

stake here, the ECJ interpreted the territorial scope (of the GDPR's predecessor) carefully against the background of a global internet and a comprehensive protection of the right to privacy and personal data on the one, and the competing sovereign interests of the international community on the other. First, the court regarded the global Google conglomerate as one whole that carries out one single act of data processing which is *per se* subject to the EU data protection laws. More specifically, it stipulates a relative approach to jurisdiction (while admittedly the different types of jurisdiction are vastly intermingled in the text of the decision).

> "57. In a globalised world, internet users' access — including those outside the Union – to the referencing of a link referring to information regarding a person whose centre of interests is situated in the Union is thus likely to have immediate and substantial effects on that person within the Union itself.
>
> 58. Such considerations are such as to justify the existence of a competence on the part of the EU legislature to lay down the obligation, for a search engine operator, to carry out, when granting a request for de-referencing made by such a person, a de-referencing on all the versions of its search engine.
>
> 59. That being said, it should be emphasised that numerous third States do not recognise the right to de-referencing or have a different approach to that right.
>
> 60. Moreover, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality […]. Furthermore, the balance between the right to privacy and the protection of personal data, on the one hand, and the freedom of information of internet users, on the other, is likely to vary significantly around the world.
>
> 61. While the EU legislature has, in Article 17(3)(a) of Regulation 2016/679, struck a balance between that right and that freedom so far as the Union is concerned (see, to that effect, today's judgment, GC and Others (De-referencing of sensitive data), C‑136/17, paragraph 59), it must be found that, by contrast, it has not, to date, struck such a balance as regards the scope of a de-referencing outside the Union."[87]

It further notes:

> "Lastly, it should be emphasised that, while […] EU law does not currently require that the de-referencing granted concern all versions of the search engine in question, it also does not prohibit such a practice. Accordingly, a supervisory or judicial authority of a Member State remains competent to weigh up, in the light of national standards of protection of fundamental rights […], a data sub-

[87] *Google v. CNIL* (note 18), paras. 57-61.

ject's right to privacy and the protection of personal data concerning him or her, on the one hand, and the right to freedom of information, on the other, and, after weighing those rights against each other, to order, where appropriate, the operator of that search engine to carry out a de-referencing concerning all versions of that search engine."[88]

The ECJ thereby confirms that the EU does potentially have jurisdiction without close recourse to its territory. While emphasising that the EU legislator did not consider all of the various interests at stake stemming from another state's competence to govern its society and the people living in it, it becomes apparent that it is possible to do so. Even more, it explicitly states that national laws may have a global jurisdictional capacity provided the various interests are appropriately balanced.

This has also been confirmed by the Advocate General in the case of *Glawischnig-Piesczek v. Facebook Ireland*[89] concerning the request of the Austrian politician requesting the deletion of the defamations of her. The ECJ in its final decision did not decide upon the jurisdiction of privacy and data protection laws but on the interpretation of Article 15(1) Directive 2000/31, the so-called e-commerce directive. However, the Advocate General specifically draws inferences to the case of Google and explains:

"The situation at issue in the main proceedings is, prima facie, different from that which constituted the starting point of my analysis concerning the territorial scope of a de-referencing of the results of a search engine in Google (Territorial scope of de-referencing), (32) cited by Facebook Ireland and the Latvian Government. That case concerns Directive 95/46/EC, (33) which harmonises, at Union level, certain material rules on data protection. It was, notably, the fact that the applicable material rules are harmonised that led me to conclude that a service provider had to be required to delete the results displayed following a search carried out not only from a single Member State but from a place within the European Union. (34) However, in my Opinion in that case I did not exclude the possibility that there might be situations in which the interest of the Union requires the application of the provisions of that directive beyond the territory of the European Union."[90]

Continuously moving away from the territorial basis, one may find that the will to regulate cyberspace increases. In general, this makes sense because provided the state's territory has served as space for the evolution of a

88 *Google v. CNIL* (note 18), para. 72.
89 *Glawischnig-Piesczek v. Facebook Ireland* (note 19).
90 *Glawischnig-Piesczek v. Facebook Ireland* (note 19), para. 79.

particular and distinct society, such proclamation cannot not be upheld anymore in a globalised networked world.[91] One can evidently see, that the court has been fully aware of the full scope of the issue. But unfortunately, the current cases decided by the ECJ have been only informative as to whether or not the court sees the necessity to limit jurisdiction. It has not been overwhelmingly enlightening as to the exact limitation process and precise aspects that must be taken into account. It rather contributes to the trend of an increase of jurisdictional claims online.[92] It actually missed the chance to clearly stipulate mechanisms that may opt for improvement. This is even more crucial as it has famously explained the general dominance of data protection law over other interests in *Schrems*[93] and *Canada-EU Passenger Name Record*[94].

4. Result: Two-Step Effect-Based Balancing

In sum, the GDPR is built on an effect-based jurisdictional nexus.[95] As demonstrated, such basis is contested in international law, yet not unprecedented. Therefore, the EU does not set out for new shores. Moreover, effect-based legislation is nothing worrisome if handled with the necessary care.[96] In order to respect and balance all interests at stake, it is important to apply a two-step approach: The first (rather low) threshold concerns whether the GDPR overall is applicable; the second one focuses on the concrete obligation in question.

As a first step, one may rely on a rather broad effect of the online behaviour in question. While in the context of the *effective control test* for state behaviour under human rights law, *Peters* convincingly speaks of virtual control when it comes to the digital space.[97] While the control tests are usu-

91 See i.a. *U. Kohl* (note 23).

92 For an overview over the trend, see *D. J. Svantesson* (note 67), 57 et seq.

93 *Maximillian Schrems v. Data Protection Commissioner*, ECJ Case C-362/14 2015, ECLI:EU:C:2015:650.

94 ECJ, Opinion 1-15 on Draft EU-Canada PNR Agreement (2017), ECLI:EU:C:2017:592.

95 See only *D. J. Svantesson* (note 67).

96 See *C. Kuner*, Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law, International Data Privacy Law 5 (2015), 235 et seq.

97 *A. Peters*, Privacy, Rechtsstaatlichkeit, and the Legal Limits on Extraterritorial Surveillance, in: Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair, R. A. Miller (ed.), 2017, 156; *A. Peters*, Surveillance Without Borders: The Unlawfulness of the NSA Panopticon, EJIL:Talk 2013, <https://www.ejiltalk.org>, (last access: 17.1.2020).

ally applied to state action, it may also be invoked on a broader level by private entities in order to trigger positive human rights obligations by the relevant state. Regardless of whether it is a case of Article 3(1) GDPR or Article 3(2) GDPR, the threat to the rights to data protection as well as privacy are imminent. Hence, it is justified from a protective point of view to leave aside the aspects of territorial boundaries. The overall application does not *per se* violate another state's sovereignty. It simply creates the opportunity to enter into the phase of balancing the concrete legal rights and obligations of the affected entities under public international law. Provided that the nation state has developed as essentially territorial while the internet has emerged as substantially a-territorial and global, this step recognises the necessity to protect fundamental rights online and the obligation to respect state sovereignty. The existing criteria for triggering Article 3(2) GDPR are in line with international standards. Moreover, the number of national data protection laws for internet-related situations have drastically emerged in recent years. Often the GDPR has set an example that other states follow. In order to enable and intensify interoperability of those laws, a generally wide scope of application is helpful as it allows a detailed balancing of the relevant interests on the second step on a more concrete basis.

Consequently, the second step refers to the actual obligation in question and whether the wide scope of application can be justified to render entities abroad to comply with such claim. In concrete terms, for the right to be forgotten (as of Article 17 GDPR), this concrete right must be balanced with conflicting rights that stem from the sovereign rights of the foreign state. When requesting the erasure of personal data from a US-based corporation, e.g. the data subject's right to be forgotten must be weighed against the US right to information and also the absence of a right to erasure on the federal US level. In cases where the data subject is domiciled in the EU and has its life focus inside the EU, the US interest in keeping certain information indexed may be dominated by that individual's privacy. Each case deserves a final proportionality test.[98] Unfortunately, it is hardly possible to generalise the scenarios without the decisive details of the case in question. The existing potential of global de-referencing is addressed in the ECJ's decision of *Google v. CNIL*, and even fully exercised in a Canadian Supreme Court case.[99] In the latter, the Canadian Supreme Court confirmed a global de-referencing injunction based on intellectual property right infringements. Google's comity argument that such decision could not have been

[98] See *D. J. Svantesson* (note 68), 227.
[99] *Google Inc. v. Equustek Solutions Inc.*, [2017] 1 S.C.R. 824 (Can.).

obtained in the US did not convince the Canadian Court. Overall, the development is indeed a challenge for international law and legal certainty. Yet, the EU's practice can be well interpreted in line with public international legal rules. Finally, and most importantly, a continuation of jurisprudence for the purpose of exemplification will fill the gap of legal uncertainty. Further socio-techno legal research will support this endeavour.

VI. Outlook and Conclusion

The current developments especially in the light of the recent judgments of the ECJ demonstrate the focus of most effective protection of individuals while taking the notion of territory merely as a starting point. That does not mean, however, that by engaging in cyber-related matters a state automatically is entitled to exercise global jurisdiction. Such capacity continues to hinge on a certain nexus. With regard to the EU level and the GDPR it can be best categorised as rooted essentially in the application of the effects-doctrine. This is not surprising as the provisions aim at protecting the EU persons and their data online as comprehensively as possible. Yet, it may be difficult to find a generally well-funded and stable basis for such as broad jurisdiction online at least without necessary limitations. This may be only possible so far for specific provisions, not for the GDPR as a whole. Article 3 GDPR is currently best interpreted together with the relevant right or provision in question such as the right to de-index. Behind that lies the reason that it is not simply the question of finding the best entity competent to regulate but to effectively protect a person and their data while finding a fair balance between different interests at stake such as security or transnational business. Provided the plurality of values in the international community, it is extremely difficult to find a fair balance. The latest decision by the ECJ has shown that the jurisdiction is most likely to be interpreted in a tendency towards a wide application of jurisdiction, although the court denied the global dimension of the obligation to de-index in the case at hand. It made, however, clear that the discussion of the jurisdiction in data protection and privacy matters is not over but remains an imminent and fascinating topic for further research.