STUDIA IURIS

Jogtudományi Tanulmányok / Journal of Legal Studies

2024. I. évfolyam 4. szám

Károli Gáspár Református Egyetem
Állam- és Jogtudományi Doktori Iskola

A folyóirat a Károli Gáspár Református Egyetem Állam- és Jogtudományi Doktori Iskolájának a közleménye. A szerkesztőség célja, hogy fiatal kutatók számára színvonalas tanulmányaik megjelentetése céljából méltó fórumot biztosítson.
A folyóirat közlésre befogad tanulmányokat hazai és külföldi szerzőktől – magyar, angol és német nyelven. A tudományos tanulmányok mellett kritikus, önálló véleményeket is tartalmazó könyvismertetések és beszámolók is helyet kapnak a lapban.
A beérkezett tanulmányokat két bíráló lektorálja szakmailag. Az idegen nyelvű tanulmányokat anyanyelvi lektor is javítja, nyelvtani és stilisztikai szempontból.
A folyóirat online verziója szabadon letölthető (open access).

Kiadó: Károli Gáspár Református Egyetem Állam- és Jogtudományi Doktori Iskola
Székhely: 1042 Budapest, Viola utca 2-4
Felelős Kiadó: Tóth J. Zoltán

A tipográfia és a nyomdai előkészítés Csernák Krisztina (L'Harmattan) munkája
A nyomdai munkákat a Robinco Kft. végezte, felelős vezető Gembela Zsolt

Honlap: https://ajk.kre.hu/index.php/jdi-kezdolap.html
E-mail: doktori.ajk@kre.hu
ISSN 3057-9058 (Print)
ISSN 3057-9392 (Online)
URL: KRE ÁJK - Studia Iuris
https://ajk.kre.hu/index.php/kiadvanyok/studia-iuris.html

THE EXTRATERRITORIAL EFFECTS OF DATA PROTECTION LAWS

Ali Sanar Shareef[1]

ABSZTRAKT ■ A joghatóság kérdésében, különösen az adatvédelemre tekintettel nincsenek egységes nemzetközi szabályok. A Lotus-ügyet számos állam precedensnek tekinti arra vonatkozóan, hogy a törvények alkalmazását a határain túlra is kiterjesztik. Mivel a digitális kor példátlan kihívásokat állít a fizikai határok elé, az államok között uralkodó tendencia, hogy elfogadják az ilyen törvények határokon átnyúló alkalmazását. Releváns nemzetközi jogszabályok hiányában azonban egyes államok extraterritoriális hatályt előíró adatvédelmi törvényeket fogadtak el, és nem korlátozták azok alkalmazási körét például a minimális kapcsolódásra vagy a fórumok alanyainak célzott szándékára. Ez ezen jogszabályok ütközéséhez, valamint a vállalatok és a weboldalak számára bizonytalansághoz vezethet. E tanulmány megvizsgálja, hogy az egységes nemzetközi jog hiánya miként vezetett az államok által elfogadott különböző megközelítésekhez, és az adatvédelmi törvények hatályának a határaikon kívülre történő kiterjesztéséhez, valamint elemzi ezen szabályozás lehetséges jogi következményeit. A tanulmány végül ajánlásokat fogalmaz meg a probléma kezelésére szolgáló mechanizmusokra, beleértve az egységes univerzális szabályok létrehozását.

ABSTRACT ■ data protection. The Lotus case is considered a precedent by many countries to extend the application of their laws beyond their borders. With the digital age presenting unprecedented challenges to physical borders, there is a prevailing trend among states to accept the cross-border application of such laws. However, in the absence of relevant international law rules, some states have enacted data laws with extraterritorial effects and without limitations on their scope, such as minimum connection or the intention to target forums' subject. This can lead to conflict of these laws and uncertainty for companies and websites. This study will examine how the absence of unified international law led to different approaches adopted by states in extending the reach of their data laws outside their borders, and the possibility of legal implications of these regulations. Finally, recommendations will be made for mechanisms to address the issue, including the establishment of unified universal rules.

Keywords: data protection, jurisdiction, extraterritorial effect, sovereignty

[1] PhD Student, Doctoral School of Law and Political Sciences, Károli Gáspár University of the Reformed Church in Hungary.

1. Introduction

Nothing has complicated legal jurisdiction more than the internet, marking the first time that jurisdiction has had to deal with individuals committing violations in the forum of other states, without being physically present. As the internet develops, so does online international business and vice versa[2]. Consequently, the increase in international transactions via internet poses greater challenges to the international legal system and states sovereignty. Due to its nature, internet contents cross borders and trigger multiple jurisdictions, and it becomes clear that mere domestic solutions are inadequate in addressing these challenges. Therefore, the development of international solutions for jurisdiction becomes inevitable[3].

The issue of jurisdiction in data protection presents a significant challenge due to the absence of a unified international legal framework governing jurisdiction. Consequently, it paved the way to governments to seek greater power internationally, aiming at extending their jurisdiction to cover as many cases as possible. While the protection of data is undeniably crucial, being both a human right and part of state security, it should not come at the expense of violating other international law principles, such as sovereignty, which is guaranteed by the UN Charter. The questions of jurisdiction are often intertwined with issues of state's sovereignty, territorial integrity, and non-intervention policies. Jurisdiction in the context of data protection law ought to be evaluated through the lens of public international law[4]. However, this rule is not absolute, there is an understanding among states to have at least a certain degree of extraterritoriality, but this is not open without limitations, rather there should be certain limitations. So having these laws now in itself is not a problem as the nature of internet and data compels that, but the problem lies in having these laws without any limitations on their scope, which can lead to, inter alia, conflict of law. The inherent nature of data in the digital era necessitates the existence of laws with cross-border reach, this

[2] In Hanson v. Denckla, the Supreme Court of U.S noted that *"[a]s technological progress has increased the flow of commerce between States, the need for jurisdiction has undergone a similar increase."* Twenty seven years later, the Court observed that jurisdiction could not be avoided *"merely because the defendant did not physically enter the forum state"*. The Court observed that: *"[I]t is an inescapable fact of modern commercial life that a substantial amount of commercial business is transacted solely by mail and wire communications across state lines, thus obviating the need for physical presence within a State in which business is conducted"*. Burger King, 471 U.S. at 476, 105 S. Ct. at 2184 https://law.justia.com/cases/federal/district-courts/FSupp/952/1119/1432344/ Accessed by 5/2/2024.

[3] R. Vaishnavi: Internet and Jurisdiction. Global Status. *Indian Journal of Law and Legal Research*, 5/2023, 1–9. 1.

[4] Stephan Kolossa: The GDPR's Extra-Territorial Scope. *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht*, 4/2020, 791–818. 779.

in itself is not the problem. However, the problem arises when these laws are without clear limitations on their scope.

The complexities and sensitivities surrounding the matter are not adequately addressed or accommodated in the status quo[5]. Currently, many states have enacted data protection laws with extraterritorial effects. This situation has resulted in a proliferation of multi regulatory approaches, conflicts of law, and uncertainty for companies. The questions that arise here are: what is the concept of jurisdiction, especially when it comes to data protection? How does international law deal with jurisdiction in data protection? What is the international law perspective on laws with extraterritorial effects? How do different legislators tackle jurisdictional matters in data protection?

The study aims to explain how states extend their jurisdiction to reach entities located in other jurisdictions, focusing on the nuances of this extension's absoluteness and the lack of limitations on their scope, and recommending possible solutions.

The study is of great significance as it touches upon a universal issue bereft of universal rules, highlighting how the absence of international legal framework has led to the proliferation of laws with extraterritorial effects. It underscores the paramount challenges to data protection, especially in trans-border scenarios where multiple courts may claim jurisdiction in a single case.

For this purpose, we divided the study into five parts. The first part addresses the concept of jurisdiction. The second discusses the international legal framework for jurisdiction in data protection. The third delves into several examples of laws from different countries that exhibit extraterritorial effects. The final part analyses the Disparity in Degrees of Extraterritoriality in Data Protection Laws. Lastly, we will outline the recommendations and necessary steps that should be taken.

2. The concept of Jurisdiction

Jurisdiction is essentially the legitimate authority a state possesses to act in each matter[6]. This power, granted or confirmed by international law, enables it to conduct business, making decisions solving disputes[7]. The ability a state has to affect its legal concern is widely accepted as a foundational principle,

5 Vaishnavi 2023, 3.

6 Vaishnavi 2023, 2.

7 Joanna Kulesza: Transboundary Challenges to Privacy Protection in Cloud Computing. *Ukrainian Journal of International Law*, 2/2017, 117–128. 123.

which is commonly encapsulated in the term "jurisdiction"[8]. Unfortunately, the concept of jurisdiction is complex and not straightforward. We can say that it is a state's power to rule sovereignly by creating and exercising laws. In this sense, jurisdiction encompasses the commanding acts of all the three authorities of the state: legislative, executive, and judicial. In other words, jurisdiction reflects a state's sovereignty in relation to its three authorities[9].

Traditionally, jurisdiction consists of three types[10]: firstly, legislative (prescriptive, substantive), it is the state's power to implement its laws to cases that involve foreign elements. Secondly, judicial or adjudicative, which means the authority of the state's court to try cases include foreign component. Finally, executive one, which refers to the power of the state to perform actions in another state's territory[11].

The issue of jurisdiction, and whether national law applies to situations with links to several countries is not specific to data protection, or to the Internet. It is a general question of international law, which arises in on-line and off-line situations where one or more elements are present that concern more than one country. A decision is required on what national law is to be applied before a solution on substance can be developed.[12]

The problems of choice of jurisdiction, choice of applicable law and recognition of foreign judgements have proved to be complex in the context of trans border data flows. The question arose, however, whether and to what extent should it be attempted at this stage to put forward solutions in Guidelines of a non-binding nature[13].

The conventional approach to jurisdiction extends based on pecuniary, subject matter and territorial jurisdiction. However, in so far as the internet is concerned, there exist no physical, territorial boundaries, thus making the application of

[8] Kai Burmeister: Jurisdiction, Choice of Law, Copyright, and the Internet. Protection against Framing in an International Setting. *Fordham Intellectual Property, Media & Entertainment Law Journal*, 2/1999, 625–723. 637.

[9] Krzystof Zalucki: Extraterritorial Jurisdiction in International Law. *International Community Law Review*, 4-5/2015, 403–412. 407.

[10] Amnesty International, Universal Jurisdiction. 4. https://www.amnesty.org/en/wp-content/uploads/2021/06/ior530032001en.pdf (accessed October 12, 2023).

[11] Christopher Kuner: Data protection law and international jurisdiction on the Internet (part 1). *International Journal of Law and Information Technology*, 2 /2010, 176–193. 184.

[12] Article 29 Data Protection Working Party, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites. Brussels, 2/2002. 2.

[13] OECD, Recommendation of the Council on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy. https://www.oecd.org/digital/privacy/ : https://www.oecd.org/digital/privacy/, 46.

law extremely difficult. This becomes further challenging when a certain issue is legal in a country, but not in another country where the issue extends.[14]

2.1. Basis for jurisdiction

Public international law recognizes; when establishing a state's jurisdiction over persons, events, or goods; five basic principles, namely territoriality, effectiveness, personality, protection, and universality[15]. Domestic courts cite one or more of these principles to establish extraterritorial jurisdiction over crimes under national law of international concern as well as offences of international concern[16].

Territoriality: for a state to claim jurisdiction over a particular case, it must show evidence that the offense has taken place, in part or in whole, within its borders. This formulation was echoed in the lotus case and adopted by criminal codes of numerous countries.[17] Traditionally, jurisdiction over a person depends on their physical presence in the forum. However, the evolution of business life, especially the advancement of modem means of transportation and communication technologies, as well as commercial transactions involving parties in the entire country, challenged the traditional standards and requirements of the physical forum presence. As a result, courts began to exercise jurisdiction over persons who were not physically present in the court's forum, leading to the development of the minimum contact principle[18].

One of the state's main functions ensuring order within its territory[19], to this end the territoriality doctrine allows a state to govern the acts and behaviors of persons located within its boundaries. This doctrine plays a crucial role in the realm of data protection law. For example, article 4 (1)(c) of the EU data protection directive seems to reflect the principle of objective territoriality, as it is based on the occurrence of an act, or in other words the utilization of equipment within the EU[20].

Effects doctrine: the American law institute's restatement (second) of conflict of laws 37 (1971) defines the effect doctrine as the authority possessed by the state to assert judicial jurisdiction over a person for actions conducted elsewhere,

14 Vaishnavi 2023, 2.
15 Kulesza 2017, 123.
16 Amnesty International 2023, 9, 2.
17 Michael Akehurst: Jurisdiction in International Law. *British Year Book of International Law,* 46/1972-1973, 146–257. 152.
18 Burmeister 1999, 640.
19 Akehurst 1972, 152.
20 Kuner 2010, 188.

have consequences within it, provided these consequences give rise to a cause of action. Unless the nature of the effects and of the individual's connection to the state do not render the exercise of such power unreasonable[21].

Often, jurisdiction based on objective territorial principles, invoked via the effects doctrine, addresses acts that have caused or are aimed at causing harmful outcomes within a country's border. It is submitted that adopting 'primary effects' approach is more effective than 'constituent elements' in terms of maintaining state's jurisdiction within reasonable bounds[22].

Personality**:** there are three types of personality jurisdictions: the active one which relies on the nationality of the suspect, by contrast the passive one which considers the nationality of victim, the final one is protective, invoked when national interests are at risk[23]. The APEC Privacy Framework ensures the protection of personal data within APEC member states by emphasizing 'accountability'. According to this principle, the original data collector remains responsible for upholding privacy standards, even when data is transferred universally. This indicates that the privacy laws of the country from whom the data was collected continue to apply, regardless of the data's destination, that is to guarantee a continual protection[24].

Universality: this principle allows a court in any country to prosecute persons for crimes committed in another country, even if there is no link to the forum country through the nationality of the suspect or victim, or any harm to its own national interests[25].

Universal jurisdiction is still a developing concept within international law, lacking well-defined and established standards. The principle most closely allied to universal jurisdiction is *aut dedere aut judicare*. It obligates countries to either extradite or prosecute offenders found within their bounds. This term has often been used interchangeably with universal jurisdiction by scholars. Many international treaties and conventions included this principle in its provisions[26].

Some scholars and courts have posited that there is another form of extraterritoriality jurisdiction: the representational principle (which is based on the jurisdiction conferred upon a state by another state). However, when there

21 Betsy Rosenblatt: Principles of Jurisdiction. *Berkman Klein Center for Internet & Society at Harvard University*. https://cyber.harvard.edu/property99/domain/Betsy.html.

22 Akehurst 1972, 155.

23 Amnesty International 2023, Ibid.

24 Kuner 2010, 189.

25 Amnesty International 2023, Ibid.

26 Meghna Rajadhyaksha: Universal Jurisdiction in International Law. *Law Review, Government Law College* 2/2002-2003, 1–34. 2.

is no link to the exercising jurisdiction, this principle is simply an extension of universal jurisdiction[27].

2.2. Jurisdiction and internet

The question of state jurisdiction over personal data and individual privacy interests is demanding, the borderline of public and private law, making the, in itself ambiguous, distinction fairly irrelevant[28].

While enforcing national privacy and security laws falls within a state's jurisdiction and upholds its fundamental rights,[29] this authority isn't limitless. International law dictates that while states can legislate based on their interests, they must respect the legitimate interests of other nations.[30] As the Article 29 Working Party[31] acknowledges, data protection law jurisdiction is assessed through international law, due to the internet's global nature,[32] the general principles of international jurisdiction, present in international public law may be addressed to assert jurisdiction over personal data or protection of individual privacy[33]. Therefore, states aren't entirely free to establish unilateral rules. Instead, "reasonableness" governs their reach. As stated in section 421 of the Restatement (Third) of Foreign Relations, a state can exert court jurisdiction over a person or entity only if its connection justifies such an action. This implies balancing national interests with international legal principles and respecting other states' sovereignty[34].

3. International legal framework for Jurisdiction in data protection

The international framework governing jurisdictional issues in data protection is deemed insufficient, and there is no unified, legally binding international

27 Amnesty International 2023, Ibid.
28 Kulesza 2017, 123.
29 Ibid.
30 Burmeister 1999, 637.
31 The Article 29 Working Party (Art. 29 WP), established by Directive 95/46/EC, addressed privacy and personal data protection matters until May 25, 2018, when the General Data Protection Regulation (GDPR) came into effect, and its responsibilities were taken over by the European Data Protection Board (EDPB).
32 Kuner 2010, 184.
33 Kulesza 2017, 123.
34 Burmeister 1999, 639.

framework determining which state has jurisdiction over a specific case. All that we have are either non-binding guidelines or regional rules with limited application. There is no instrument under public international law of universal application containing jurisdictional rules for data protection law[35].

Back in 1999, the Hague Conference on Private International Law examined jurisdiction and applicable law in data protection during 'Geneva Round Table on Electronic Commerce and Private International Law'. However, this discussion didn't give any solution, except by issuing a statement that further investigation is needed[36].

Despite the recent attempts, the "Hague Conference" failed to make progress on a draft convention regarding the applicable law in contracts due to disagreements on the decisive criterion. This impasse indicates the heart of the problem: striking a fair balance between the diverse legal interests of involved parties.[37]

In 1999, the Hague conference on private international law jointly with Geneva university held The Geneva Round Table to explore the challenges facing private international law in the context of electronic commerce and the internet. The event spanned three days and convened in Geneva, Switzerland[38].

Back in 2005, the APEC Privacy Framework set guidelines for data privacy. Accordingly, each APEC economy should establish a legal framework that follows these principles. The framework ensures transferred data within the APEC region remains protected through the accountability principles.[39] But it contains no rule regarding jurisdiction in data protection.

In preparation for submitting it to the United Nations and under the chairmanship of the Spanish Data Protection Authority, a group of data protection authorities worldwide initiated the drafting of a universal legal instrument on data protection in 2009. Initial drafts included the following provisions that determined Jurisdiction over personal data processing based on the location of the responsible entity's operations or its targeted activities, with "establishment" broadly defined encompassing any stable operational presence. However, this provision was dropped in the final version[40].

35 Kuner 2010, 186.

36 Geneva Round Table on the Questions of Private International Law raised by Electronic Commerce and the Internet, organised jointly by the University of Geneva and the Hague Conference on Private International Law. Geneva, 2-4 September 1999.

37 Article 29 Data Protection Working Party, 5.

38 Stephen Kobrin: Safe Harbours Are Hard to Find. The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance. *Review of International Studies*, 1/2004, 111–131. 113. http://www.jstor.org/stable/20097901.

39 Ibid. 114.

40 Kuner 2010, 187.

Regulation (EU) No 1215/2012, enacted on 12 December 2012, set out rules governing jurisdiction and the recognition/enforcement of court decisions in civil and commercial matters across the European Union. Article 16 is designed to prevent individuals from facing unexpected lawsuits in foreign courts regarding privacy breaches or defamation, guaranteeing legal actions are predictable and just[41].

The Internet and Jurisdiction Global Status Report (2019) examines challenges posed by the cross-border nature of the internet, especially regarding jurisdiction issues and the rise in online crimes, heightened by the shift to online activities due to COVID-19. The report emphasizes the limitations of domestic approaches and the necessity for global frameworks due to conflicting legal priorities among countries. It stresses the need for a collaborative approach to address jurisdiction complexities, legal ambiguities, and potential negative impacts on global governance arising from inconsistent policies.

Given the above-mentioned issues, the report underscores the need to adopt a multistakeholder-based approach that is to begin at the earliest. It is crucial to investigate the seriousness of the issue domestically and adequately address the problems stemming from fragmented frameworks[42].

The Explanatory Memoranda of the OECD Privacy Guidelines highlights the problems of determining jurisdiction, applicable law and recognition of foreign judgements in the context of trans-border data flows. It raises the question of whether and to what extent it is appropriate at this stage to put forward solutions in Guidelines that are advisory and not mandatory[43].

The issues revolving around the internet and jurisdiction are still evolving in nature[44]. Political concepts of jurisdiction and community are not naturally defined, but socially constructed. In a world where spill-over and inter-jurisdictional conflict are becoming the norm and political space as a bounded geographic construct is losing meaning, establishing effective governance structures, which retain some sense of democratic legitimacy, may require reconceptualising both jurisdiction and political community[45].

41 Regulation (EU) No. 1215/2012 of the European Parliament and of the Council, of 12 December 2012, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

42 The Internet and Jurisdiction Policy Network released their first-ever Global Status Report in Berlin on 27 November 2019.

43 OECD, Digital Economy Papers. No. 360, "Explanatory Memoranda of the OECD Privacy Guidelines". 2023. 22.

44 Vaishnavi 2023, 4.

45 Kobrin 2004, 113.

Sitting aside the complexity of jurisdiction, which is a complicated problem across all fields of law, data protection itself lacks worldwide rules governing its principles. The privacy rules that exist in human rights conventions are not sufficient to tackle data protection challenges, especially with the rapid increase of trans border commercial transactions. This is because the internet has made data protection issues more universal. Moreover, data protection issues extend beyond commercial concerns; they are surrounded by security dimensions on one side and political dimensions on the other. The security dimension relates to the transfer of subjects' data outside the country, which may pose threats to the national security of a state. States may try to expand their jurisdiction to have access to specific data, even abroad. On the other hand, governments attempt to enact domestic laws to access people's data within their country under the pretext of protecting national security. Sometimes political regimes use these laws for wiretapping opposition and activist calls. Therefore, predicting a breakthrough in the near future regarding the agreement on unified international rules is not feasible.

4. States' practice

When examining states' practice, it is clear that states frequently use a variety of standards to broadly define the boundaries of their domestic legal systems, to control conduct occurring outside of their boundaries, particularly concerning online activity[46].

The goal of providing broad protection to industry and national consumers is what motivates this strategy. As a result, circumstances involving cross-border components usually result in the application of several national laws[47].

Because so many governments are passing rules that apply to overseas businesses, the question of whether data laws have an extraterritorial reach has received a lot of attention. US officials contend that the effects of European data privacy regulations extend across national borders.[48] Article 29, on the other hand, asserts that in nations such as the United States, international websites are governed by national laws and municipal regulations because of domestic court decisions. The aforementioned conversation highlights the complex and interconnected terrain of global data governance, wherein nations wrestle with and establish control over data-related issues that transcend national

[46] Kuner 2010, 176.
[47] Article 29 Data Protection Working Party, 5.
[48] Kuner 2010, 176.

boundaries.[49] This debate has not emerged from nowhere, many states have laws with extraterritorial effects, leading to Legal complexity, uncertainty, and jurisdictional challenges. As demonstrated by examples such as Microsoft v. USA[50].

"Extraterritorial laws are laws in a given territory that can produce effects and be applicable within a sovereign foreign territory. A major consequence of such laws is that they create a 'denial of territoriality' i.e. the attempt to exercise control over persons, situations or areas outside the controller's territory"[51]. Traditionally, these laws are acceptable in exceptional circumstances only[52].

There are not clear sufficient rules in international law govern jurisdictional rules, and all what we have are headlines without enough details, such as sovereignty principle which considered a limitation on the exercise of jurisdiction outside borders. Even international law cases haven't provided clear details about extraterritoriality.

According to international law, the sovereignty principle underscores the exclusive right to exercise certain power within its bounds. This principle is mostly rooted in customary international law, such as 1648 Westphalia treaties and is also referenced in certain international frameworks like the 1945 United Nations charter[53]. Due to the limited body of international case law, the 'Lotus case' is still considered as foundational source base for deriving general principles governing jurisdiction. Three important principles established by the case. The first principle is the issue of extraterritorial jurisdiction is a matter of international law, and states don't have the freedom to extend their jurisdiction unilaterally. Second, International law, generally, prohibits enforcement jurisdiction, unless it is specifically permitted. The last principle is related to extraterritorial prescriptive and adjudicative jurisdiction, which is only permitted if there is sufficient connection between the forum and the event. However, regarding the third point, Kamminga believes that state practice has taken a different

[49] Article 29 Data Protection Working Party, 4.

[50] Microsoft Corp. v. United States, 586 U.S. (2018).

[51] Wissame En-Naoui – Laurence Bégou: How Extraterritorial Laws Impact Your Organization's Sovereignty. *Atos*, accessed February 19, 2024. https://atos.net/en/lp/digital-sovereignty-cybersecurity-magazine/how-extraterritorial-laws-impact-your-organizations-sovereignty#_ftn3.

[52] Menno Kamminga: Extraterritoriality. In: Rüdiger Wolfrum (ed.): *The Max Planck Encyclopedia of Public International Law.* Oxford University Press, 2020. 3. https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1040.

[53] William Julie – Sophie Menegon – Alice Murgier: United States extraterritoriality. European Union sovereignty at stake. Accessed February 19, 2024. https://www.ibanet.org/article/CF85E59E-6564-4AA3-9408-3F47C6449C9D.

approach and denies any such jurisdiction unless there is a rule in international law allows that[54]. But reality shows otherwise, there may have been a recent trend in international law to accept this kind of jurisdiction with passive personality[55]. In the Democratic Republic of the Congo v. Belgium Arrest Warrant Case, Judges Higgins, Kooijmans and Buergenthal noted in their combined individual judgment that "the movement is towards bases of jurisdiction other than territoriality"[56]. Based on the two aforementioned cases, the extraterritorial prescriptive and adjudicative jurisdiction are acceptable at least in certain circumstances and the territoriality is no longer the only principle for asserting jurisdiction. However, the new era of the internet has exacerbated the uncertainty of jurisdiction even more and the inherent nature of the internet necessitates more cross-borders legislations. Nowadays, technology laws have extraterritorial effects, and it is understandable that this is unavoidable. Therefore, the question is not whether it's allowed to have these laws or not, rather the question concerns the extent of extraterritoriality, to what extent these laws contain limitations on their scope and what is the level of states' respect to the sufficient connection principle. Additionally, the issue of enforcement and whether states have entered into mutual agreements for judgment enforcement is crucial, as it is clear that in the absence of international rules, the lack of mutual enforcement agreements makes the enforcement of courts' judgments impossible.

In the following paragraphs, we will explore examples of laws and case laws from various countries that have extraterritorial reach, highlighting the disparities between them, in terms of their scope of cross-border application.

Certain EU countries' court cases have applied their laws with extraterritorial effect. For instance, the Paris County Court ruled in a landmark decision that Yahoo! Inc., a US-based company, was subject to French jurisdiction regarding its online auction site, Yahoo Auctions, which featured artifacts associated to the Nazi movement[57]. The court's ruling illustrated the digital age's extraterritorial application of national laws, showing that nations may impose their legal obligations on internet corporations even if they are based abroad.

Google, a US-based corporation, was found to be liable for its search engine results in Spain under the Spanish Data Protection Act (LOPD) by the Court

54 Kamminga 2020, 7-9.
55 Kolossa 2016, 800.
56 Kamminga 2020, 7-9.
57 League Against Racism & Antisemitism v. Yahoo! Inc. & Yahoo France, Paris County Court, Order dated May 22, 2000.

of Justice of the European Union (CJEU). The court's ruling demonstrated the territorial scope of the European Union's (EU) data protection law's[58].

The standards set forth by the EU General Data Protection Regulation (GDPR) go beyond traditional characteristics of natural persons, such as citizenship or place of habitual abode[59].

The Data Security Law of the People's Republic of China[60], PRC Personal Information Protection Law and the 2017 Draft for Public Comments on the Safety Assessment Guide for Data Transferred Outside of China have extraterritorial effects. The guide applies to foreign data controllers or processors who sell goods or services to people in China even though they are not registered in China[61].

The Data Security Law permits its rules to be applied internationally. Legal responsibility must be prosecuted in accordance with the law when data handling operations jeopardize national security, the public interest, or the legitimate rights and interests of PRC residents or organizations. Terms used by the law like national security and public interests are not defined and can be interpreted widely.

Order of the Cyberspace Administration of China No. 4 Article 3 provides for the application of the order to the collection, storage, use, disclosure and exchange of children's personal information via network activities inside the borders of the People's Republic of China[62].

The legal position in the United States is significantly more advanced than that of other nations. The legal position with respect to internet jurisdiction in the country has evolved through multiple levels in courts through several tests[63]. Businesses operating in several jurisdictions may be subject to both federal and state data protection laws about their operations that impact citizens of the United States. These rules apply in situations where the company gathers, saves, sends, handles, or distributes personal data about people living in the United States.[64]

58 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Court of Justice of the European Union (CJEU), Case C-131/12, Judgment of 13 May 2014.

59 Jie Jeanne Huang: Applicable law to transnational personal data. Trends and dynamics. *German Law Journal*, 6/2020, 1283–1308. 1297.

60 Data Security Law of the People's Republic of China, adopted on June 10, 2021, and promulgated on September 1, 2021.

61 Huang 2020, 1297.

62 Order of the Cyberspace Administration of China No. 4, Provisions on the Cyber Protection of Children's Personal Information (Aug. 22, 2019, effective Oct. 1, 2019).

63 Vaishnavi 2023, 4.

64 https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa.

The CLOUD Act[65], enacted as result of the Microsoft case, expanded the US government's ability to access data abroad and allowed the government to enter into executive agreements with other governments for cooperation in criminal investigations. The act raised concerns about data violation alongside jurisdictional challenges. Simply by having a subsidiary in the USA, a foreign company can be subject to US jurisdiction. Its operational ties to the U.S. through an office bring it within the ambit of U.S. law under the CLOUD Act. The purview of this Act includes companies that operate in or with the United States in addition to those with their headquarters there. Moreover, the CLOUD Act may extend its extraterritorial reach to any entity that makes use of services having a direct or indirect corporate link to the United States. Therefore, the United States has jurisdiction over a foreign business's U.S.-based operations or links, rather than the foreign firm itself[66]. As for the crimes the cloud covers, the cloud mentions (serious crimes) and without any further explanation[67].

The Children's Online Privacy Protection Act of 1998 (COPPA) in the United States is not limited to U.S. companies but extends its jurisdiction to foreign websites that collect personal information from children on U.S. soil. COPPA applies to companies "located on the Internet", meaning the physical location of the website is irrelevant if it conducts business within the U.S.[68]

According to the California Consumer Privacy Act, companies that gather personal data from Californians and satisfy one of three requirements – namely, having an obvious relationship to the state – come under its purview.

A. Businesses whose total yearly gross revenue as of January 1st of the previous calendar year was more than twenty-five million dollars ($25,000,000).

B. Organizations that purchase, sell, or exchange personal data from 100,000 or more customers or households each year, either singly or jointly.

C. Companies whose sales or sharing of customer personal information generate at least 50% of their yearly income.[69]

65 Cloud Act (Clarifying Lawful Overseas Use of Data Act) was enacted in the United States. Public Law No. 115-141, 132 Stat. 1213 (2018) https://www.eurojust.europa.eu/publication/cloud-act#:~:text=The%20Clarifying%20Lawful%20Overseas%20Use,the%20context%20of%20criminal%20investigations. Accessed by February 2, 2024.

66 European Union Agency for Criminal Justice Cooperation. "The CLOUD Act". Last modified December 22, 2022. https://www.eurojust.europa.eu/publication/cloud-act. Accessed February 25, 2024.

67 Ibid.

68 Article 29 Data Protection Working Party, 4.

69 California Legislature (2018). California Consumer Privacy Act of 2018, § 1798.105. Cal. Civ. Code. [2/1/2024, Codes Display Text (ca.gov)].

India is not exempt from extraterritorial effect laws. Clause 75 of the Information Technology Act, subject to certain restrictions, extends its application to any person, regardless of nationality, for offenses or violations committed outside the borders of India. The act is applicable if the behavior or acts that constitute the violation include a computer, computer system, or computer network located inside the borders of India[70], it is based on effects test.

The Delhi High Court used the effects test and determined whether the website was interactive in the cases of India TV Independent News Service Pvt. Ltd v. India Broadcast Live Lic, and Banyan Tree Holding Pvt Ltd v. A Murali Krishna Reddy.[71]

Greek law used to extend the Data Protection Authority over data controllers outside of Greece who processed data on Greek residents by requiring them to appoint a representative in Greece who would be liable for such data processing. The Greek provision was changed in 2006 following objections by the European Commission.[72]

Other law examples that have extraterritorial effect are: Hessisches Datenschutzgesetz of 30 September 1970 (Data Protection Act of the German federal state of Hessen); Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (French Act N. 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties); Swedish Data Protection Act of 11 May 1973[73].

In the absence of universally binding regulations, the existence of these laws becomes inevitable, particularly in the realm of online transactions. The practices of various states indicate a degree of recognition of this trend, potentially elevating it to the status of international customary law. This issue is no longer about questioning the legitimacy of such laws; instead, it revolves around establishing clear boundaries for their scope.

5. Disparity in degrees of extraterritoriality

While these laws have extraterritorial effects, they are not all to the same degree. There is variation between them, some of which include conditions that may restrict their scope and making them more acceptable than others.

[70] The Information Technology Act, 2000 (No. 21 OF 2000).
[71] Vaishnavi 2023, 5.
[72] Kuner 2010, 188-189.
[73] Ibid. 176.

In China, both of the Data Security Law of the People's Republic of China[74] and the PCR's Personal Information Protection Law[75] have provisions with extraterritorial effect similar to GDPR, however with certain differences.

Guidance on understanding the notion of offering goods or services can be found in Recital 23 of GDPR. It highlights that merely having contact information or a website accessible within the Union is not enough to ascertain such intent. Nonetheless, a controller's purpose to provide goods or services to data subjects in the Union may be indicated by actions like utilizing currencies or languages that are frequently associated with Member States, allowing orders in those languages, or mentioning users or customers within the Union.

A similar requirement can be found in Article 15 of Regulation 44/2001, known as the Brussels Regulation[76], in that context, a joint declaration by the EU Council and the Commission states that *"the mere fact that an Internet site is accessible is not sufficient of Article 15 to be applicable"*.[77] Thus, the mere availability or accessibility of a particular business online, does not qualify it to be considered as sufficient under the regulation and comes into conflict with article 3(2) of GDPR.[78]

In contrast to GDPR, Samuel Yang believes that the wording of PIPL Article 3(2)(I)[79] implies that regardless of whether they originally intended to target Chinese consumers with their offers, any foreign data controller or processor that sells goods or services to individuals in China and processes that individuals' personal information may be subject to the PIPL.[80]

And while Recital 24 of the GDPR describes data subject monitoring as following someone online, which may result in decision-making and profiling based on personal information, Samuel Yang believes that article 3(2)(b) of the

74 Data Security Law of the People's Republic of China, adopted on June 10, 2021, and promulgated on September 1, 2021.

75 PRC Personal Information Protection Law (Final), adopted on August 20, 2021, and effective from November 1, 2021.

76 Council Regulation (EC) No. 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. Official Journal L 12, 16 January 2001, 1-23.

77 The GDPR's Reach, Material and Territorial Scope Under Articles 2 and 3, WR LLP, 2017. https://www.wileyrein.com/newsroom-newsletters-item-May_2017_PIF- The_GDPRs_ReachMaterial_andTerritorialScopeUnderArticles_2_and_3.html.

78 Amogh Mittal: Territorial Jurisdiction of GDPR and Its Application in India. *International Journal of Law Management & Humanities*, 2/2019, 124–127. 126.

79 PRC Personal Information Protection Law (Final), 2021.

80 Samuel Yang: A Look at the Extraterritorial Applicability of China's Newly Issued PIPL. A Comparison to the EU's GDPR. *International Association of Privacy Professionals, 2020.* Accessed February 8, 2024. https://iapp.org/news/a/a-look-at-the-extraterritorial-applicability-of-chinas-newly-issued-pipl-a-comparison-to-the-gdpr/.

draft PIPL, broadens the definition to cover foreign processing operations that assess and analyze people's conduct in China. This broader terminology may include any type of analysis, evaluation, or study of people's conduct in China in addition to the monitoring activities specified in the GDPR[81].

PIPL extends its application even more to reach "other circumstance as provided by any law or administrative regulation". This is indicating an open-ended list of possible cases for extraterritorial application.

The formation of jurisdictional rules in the United States has been profoundly affected by prior court decisions. The minimum contact standard was established by the seminal decision of International Shoe Co. v. Washington. It requires a certain degree of interaction with the jurisdiction for a court to assert its jurisdiction without having to be a resident. After that, Hanson v. Denckla established the condition for purposeful availment, which states that a party must have intentionally got engaged with the state; limited contact is not adequate. These ideas were then further developed in Zippo Manufacturing Co. v. Zippo.com, which distinguished between passive and interactive internet activity for the purpose of establishing jurisdiction. These three principles limit the extraterritorial reach of laws and present a positive solution in this regard.

However, other laws adopted a broad approach and extended the scope and reach of their application. For example, the CLOUD Act allows the United States to compel companies under its jurisdiction to disclose any data, regardless of its origin. The law extends its application to third parties, which include both the controller and processor on one hand, and data subjects on the other. If a citizen's data in the EU has been collected by an entity in the EU and later stored its data with a cloud company in the USA, this connection can trigger the application of the USA's CLOUD act on that EU entity and its stored data, which means the law is applied to what I term as (passive parties). Regarding crimes covered by the act, it applies to serious crimes, without any definition to it. Similarly, certain terms used by the Chinese Data Security Law without providing clear definition, such as national security and public interests, so they can be interpreted widely.

Undoubtedly, the challenges posed by the rapid development in cyberspace have made it difficult to confine the applications of domestic laws within a state's borders, and the increasing rate of laws with extraterritorial effects has become unavoidable. The problem now is extraterritoriality without any limitations, when laws assert jurisdiction over any website displayed on computers inside the country without any specifications or limitations. These laws can be generally accepted when demonstrating a state's connection with the persons or

[81] Ibid.

circumstances it intends to regulate[82]. In other words, these laws are somehow tolerated when states show connections to cases reached by their laws. According to section 421 of the restatement (third) of foreign relations, a state may assert jurisdiction when the connection warrants such action. This implies weighing domestic interests against international legal principles such as respecting the sovereignty of other states.

Principles used in cases in the USA can limit the extraterritorial reach of jurisdiction to a reasonable degree. Other more nuanced approaches have a positive effect, such as those outlined in Recitals 23 and 24 of the GDPR, which focus on a controller's intention to offer goods or services to data subjects and use criteria like currencies or languages associated with specific member states. Additionally, the Brussels Regulation used the same language, it asserts that merely having an online presence is not enough to subject a business to a specific jurisdiction.

China's Personal Information Protection Law applies to anyone providing services to its citizens, regardless of the purpose or active/passive nature of their online presence. This absoluteness can lead to the extension of the law's reach.

Indeed, the mere existence of laws with cross-border effects is sometimes problematic, as not all states have mutual agreements. For example, China is not recognized by the EU Commission for providing adequate protection. Additionally, there is a lack of mutual judicial assistance between the EU and China. In most cases, China doesn't recognize the jurisdiction of EU data protection authorities and courts. Moreover, the reluctance of Chinese to acknowledge and enforce court decisions could continue in the Chinese judicial system for a considerable time[83]. Therefore, the EU's inability to enforce its laws in China raises doubts about the efficacy of its data protection legislation.

To sum up, when it comes to data protection jurisdiction, two interests are at stake: privacy and human rights on one hand, and state sovereignty on the other. Jurisdiction forms part of a state's sovereignty, its right to regulate its own public order.[84] Since the issue relates to sovereignty, public international law must govern the matter, especially given that human rights and jurisdiction are both components of public international law. Therefore, jurisdiction in the context of data protection law should be evaluated by the rules of public international law, as it was argued by 'Lotus case' and has been asserted by Article 29 Working Party.

[82] Julie – Menegon – Murgier, Ibid.

[83] Chicago 17th ed. Bo Zhao – Weiquan Chen: Data Protection as a Fundamental Right. The European General Data Protection Regulation and Its Exterritorial Application in China. *US-China Law Review*, 3/2019, 97–113. 109.

[84] Kolossa 2016, 779.

There are fine lines between different interests of states, and the issue of balance is sometimes problematic. Restricting states' ability to extend their jurisdiction beyond their borders could undermine data protection rights and sovereignty. Conversely, granting states the right to extend the effects of their laws outside its borders may violate other states' sovereignty and access peoples' data outside their jurisdiction. For this end it is crucial to find a precise and fair balance between these two opposite interests. Additionally, data collection is not only a human rights concern but also a security concern, as other states could potentially use this data in ways that harm others.

6. Conclusion and recommendations

Data protection is recognized as a human right, and it is a multifaceted issue. Governments, while claiming to expand their jurisdiction for the protection of their citizens' privacy, often violate it for their own interests and may persecute internal opponents. Therefore, maintaining a balance between conflicting interests remains delicate and challenging. The issue becomes more complex when it collides with sovereignty, and other interests overlap, such as protecting national security, leading to more complexity of the issue and ultimately making it difficult to achieve a balance. Anyway, the study focused more on jurisdiction and sovereignty concerns, in addition to the possibility of conflicting laws. Jurisdiction, which is essentially the legitimate power a state possesses to act in a given matter, is a cornerstone of sovereignty, should be governed by public international law, as highlighted by the Lotus case and article 25 of the working party. However, there is almost a lack of unified rules in international law regarding jurisdiction, especially in data protection. Presently, international law cases offer only specific guidelines, notably from cases like Lotus. According to this case, states can extend their jurisdiction beyond their borders in the absence of prohibitive rules, provided there is a connection between the forum and the case.

Moreover, the widely repeated states practice enacting laws with extraterritorial effect, suggesting a tolerant attitude towards such legislations. However, with the rise of internet technology, physical borders have become less relevant, promoting states to safeguard their citizens' data and national security with more vigilance. While these laws are generally tolerated, the concern lies in the absolute nature of some of them, and lacking limitations on their scope, such as requiring minimum contact or the explicit targeting of individuals' data. Now the problem is with the extent to which states extend their jurisdiction and to what extent they put limitations on the extraterritorial reach of their data laws.

The absence of comprehensive international law rules leads to states extending the power of their laws according to their interests, often without considering the consequences. Consequently, companies and websites may find themselves subject to multiple jurisdictions simultaneously, creating potential conflicts of laws and legal uncertainty for websites.

Recommendations

- Establishing a unified international legal framework to govern jurisdiction in cyberspace generally and data protection specifically.
- While achieving binding rules is challenging, promoting soft law – nonbinding declarations – is crucial.
- Any international rules should strike a balance between the legitimate concerns of nations regarding their national security and peoples' data on one hand, and the respect of the sovereignty of other states from the other.
- Laws with extraterritorial effects should include specific limitations, such as sufficient connection to the forum and the specific intent to target individuals within their jurisdiction.
- To avoid their misinterpretation, vague terms such as 'national security' should not be left without clear boundaries.
- The application of extraterritorial laws should be confined only to third parties with minimal connection, and not to people with a passive connection, or what I term 'passive parties', as seen in the US CLOUD act.

Bibliography

Court cases

Hanson v. Denckla, Supreme Court of U.S., https://law.justia.com/cases/federal/district-courts/FSupp/952/1119/1432344/ Accessed by 5/2/2024.

Microsoft Corp. v. United States, 586 U.S. (2018).

Legal documents and regulations

Stephan Kolossa: The GDPR's Extra-Territorial Scope. *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht*, 4/2020, 791–818.

Regulation (EU) No. 1215/2012 of the European Parliament and of the Council, of 12 December 2012, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

Geneva Round Table on the Questions of Private International Law raised by Electronic Commerce and the Internet, organised jointly by the University of Geneva and the Hague Conference on Private International Law, Geneva, 2-4 September 1999.

The Internet and Jurisdiction Policy Network released their first-ever Global Status Report in Berlin on 27 November 2019.

Order of the Cyberspace Administration of China No. 4, Provisions on the Cyber Protection of Children's Personal Information (Aug. 22, 2019, effective Oct. 1, 2019).

European Union Agency for Criminal Justice Cooperation. "The CLOUD Act". Last modified December 22, 2022. https://www.eurojust.europa.eu/publication/cloud-act. Accessed February 25, 2024.

California Legislature (2018). California Consumer Privacy Act of 2018, § 1798.105. Cal. Civ. Code. [2/1/2024, Codes Display Text (ca.gov)].

Data Security Law of the People's Republic of China, adopted on June 10, 2021, and promulgated on September 1, 2021.

PRC Personal Information Protection Law (Final), adopted on August 20, 2021, and effective from November 1, 2021.

Council Regulation (EC) No. 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. Official Journal L 12, 16 January 2001.

Journal articles

R. Vaishnavi: Internet and Jurisdiction. Global Status. *Indian Journal of Law and Legal Research*, 5/2023, 1–9.

Joanna Kulesza: Transboundary Challenges to Privacy Protection in Cloud Computing. *Ukrainian Journal of International Law*, 2/2017, 117–128.

Kai Burmeister: Jurisdiction, Choice of Law, Copyright, and the Internet. Protection against Framing in an International Setting. *Fordham Intellectual Property, Media & Entertainment Law Journal*, 2/1999, 625–723.

Krzystof Zalucki: Extraterritorial Jurisdiction in International Law. *International Community Law Review*, 4-5/2015, 403–412.

Christopher Kuner: Data protection law and international jurisdiction on the Internet (part 1). *International Journal of Law and Information Technology*, 2 /2010, 176–193.

Stephen Kobrin: Safe Harbours Are Hard to Find. The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance. *Review of International Studies*, 1/2004, 111–131. http://www.jstor.org/stable/20097901.

Recommendations and guidelines

OECD, Recommendation of the Council on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy. OECD/LEGAL/0352 Retrieved from https://www.oecd.org/digital/privacy/ : https://www.oecd.org/digital/privacy/.

OECD, Digital Economy Papers. No. 360, "Explanatory Memoranda of the OECD Privacy Guidelines". 2023.

Reports and working documents

Amnesty International, Universal Jurisdiction. 4. https://www.amnesty.org/en/wp-content/uploads/2021/06/ior530032001en.pdf (accessed October 12, 2023).

Article 29 Working Party: Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites' Brussels - Belgium 2/2002.

The Internet and Jurisdiction Policy Network released their first-ever Global Status Report in Berlin on 27 November 2019.

Websites and other sources

Betsy Rosenblatt: Principles of Jurisdiction. *Berkman Klein Center for Internet & Society at Harvard University*. https://cyber.harvard.edu/property99/domain/Betsy.html.

Wissame En-Naoui – Laurence Bégou: How Extraterritorial Laws Impact Your Organization's Sovereignty. *Atos*, accessed February 19, 2024. https://atos.net/en/lp/digital-sovereignty-cybersecurity-magazine/how-extraterritorial-laws-impact-your-organizations-sovereignty#_ftn3.

Menno Kamminga: Extraterritoriality. In: Rüdiger Wolfrum (ed.): *The Max Planck Encyclopedia of Public International Law.* Oxford University Press, 2020. 3. https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1040.