Untangling the Jurisdictional Web in Cyberspace

Yassin Abdalla ABDELKARIM ✉ ✉
The Egyptian Ministry of Justice, Egypt

Abstract

The ambiguous theme of cyberspace and its broad widespread inflict a major effect on the legal procedures of litigations. Since litigation might include several nationalities, because of the cosmopolitan nature of cyberspace, determining the competent court is not as direct as traditional litigations. Cyber litigations complicate this procedural threshold as the traditional application of jurisdiction determinants might not suit cyber disputes. Furthermore, jurisdiction conflicts in cyberspace frustrate settling the dispute as courts avoid giving their judgments due to invalidity.

Therefore, these conflicts introduce a modern issue to private international law theorists. It is indisputable that drafting obvious jurisdictional rules enhances the rule of law in cyberspace. Thus, the research analyses this issue and establishes a comparison to determine the state of the art regarding it. The article reviews the relevant academic contributions and legislation to point out how they crystallize the aspects of the research question. Besides, it studies relevant case laws from the UK and US judiciaries to conclude the legal principle they adopt to settle these conflicts and to enhance the validity of their judgments. Eventually, it introduces a comprehensive theory on settling jurisdiction conflicts regarding cyber litigation, which enhances the rule of law in cyberspace.

Keywords: cyberspace; jurisdiction conflicts; private international law; comparative study; case laws; legal theory.

JEL Classification: K24; K33; K41.

Introduction

The borderless nature of cyberspace stands as an obstacle before determining the competent judiciary over cyber incidents since several states might be involved in a single cyber dispute. Consequently, it provides cybercriminals with the best camouflage to move under to achieve their illegal purposes.

Moreover, settling jurisdiction conflicts on transnational cyber is required. This jurisdiction, when determined, is competent to settle the dispute. It is a chief procedural threshold of the judgment validity. Therefore, it facilitates handling cyber disputes by initiating the appropriate legal process. Moreover, determining cyber jurisdiction legitimizes the entire judicial proceedings. National laws are effective in settling judicial disputes regardless of the substance of those disputes, commercial, civil, criminal, and so on. Nevertheless, the scope of these laws is limited by the boundaries of the state and, hence, cannot work beyond them. Put differently, no state can impose its laws within other states’ borders. Yet, cyber disputes may include more than one legal system, for instance, imagine a dispute between a Common Law state and a Latin Law state. This case reflects a conflict of jurisdiction in cyberspace; a dire situation that jeopardizes the stability of legal relations in cyberspace. Thus, the article introduces a comparative study to conclude the approaches that the identified judiciaries adopt to settle jurisdiction conflicts in cyberspace.
1. Research Background

It is essential, in the first phase, to shed light on the relevant scholarships and contributions by legal theorists to put a grasp on their attitudes towards settling jurisdiction conflicts in cyberspace. They underscore the prominence of solving these conflicts to stabilize legal prepositions in cyber disputes.

The nature of the Internet complicates the question of national jurisdiction for several reasons:

- Its borderless nature limits the state’s power to impose its laws (Khalifa, 2020).
- The effect of illegal cyber activity goes beyond the limits of the *lex loci delicti*, Place of the tort factor, doctrine as there is no prerequisite correlation between the place where the illegal activity occurred and the place that suffers its harmful consequences. This is a result of the high speed of information exchange through the Internet (Raut, 2004).
- The lack of legislation on the Internet facilitated the violation of the state’s existing laws. This is caused by the novelty of cybercrime litigations that created a serious legal vacuum as most of the laws are yet to be completely enforced.
- The anonymity of Internet users granted the illegal activists a major advantage before the prosecution authorities in cyberspace (Appazov, 2014).
- It is easy for a single disguised individual in cyberspace to launch a harmful massive attack targeting a state’s interests and security (Appazov, 2014).

Therefore, the need to formulate judicial norms determining the competent jurisdiction in cyberspace to avoid conflicts of cyber jurisdiction is urgent.

The doctrine has three main schools: The first, which is led by Barlow, insists on the principle of cyberspace independence. It thus refuses any state legal jurisdiction over it; it should have its norms and rules (Barlow, 1996). Barlow in his declaration was influenced by the sphere of political freedom that prevailed in Europe after the collapse of Communist regimes that had taken this attitude far away from the context of legal surveillance.

Johnson and Post (1996, p.258), representing the second school, decided that a set of laws is necessary for cyberspace. This school states that cyberspace should be handled as an independent sphere where its distinctive unique set of laws applies. Adams and Albakajai, (2016, p.258) criticize the existing legal systems when dealing with cyber disputes as their regulations cannot deal with the fast-advanced cyber legal issues. They believe that legal cyber disputes should be allocated specific rules to be settled under and not the traditional legal rules that settle real-world legal disputes.

The third school, led by Lawrence Lessing, tries to fill the gap between the previous ones. He states that the architecture of cyberspace imposes regulations and rules upon its users. He concludes that cyberspace is not far from being regulated. Indeed, cyberspace cannot be free of rules, but those rules which govern cyberspace should be seen from the viewpoint of technology. Put differently, let technology regulate cyberspace as an area of technology (Lessing, 2006). He resorts to a hybrid solution. Also, since technology is dynamically developed, the regulation of cyberspace may create outdated rules quickly and their amendments would cause delays. Moreover, if those amendments were made on time there is still the possibility that some legal systems may have no idea about them. The result is the conflict about jurisdiction may be exacerbated over a single cyber dispute.

In a conference held in Fort Mead, USA, Koh (2012) claimed that cyberspace cannot be a “law-free” zone, but international law rules should organize it under the supervision of the international concerned bodies, such as the World Trade Organization and commercial arbitration chambers. He highlighted the need to keep up with the accelerating technological developments in cyberspace.
Moreover, Willie's (2023) study explores the correlation between organizational culture and cybersecurity practices, underscoring the significance of cultivating a culture prioritizing security within organizational settings. In the contemporary digital era, organizations have leveraged unparalleled connectivity and technological progress, resulting in heightened efficiency and productivity.

Reidenberg argues that the inevitability of state jurisdiction over cyber disputes is supported by public policy requirements and favours the rule of law. He argues that these factors come in advance to the technological advancements needs. Moreover, even if multiple states disputed the jurisdiction over a cyber dispute this would encourage creativity more than the traditional technical approaches (Reidenberg 2005, p.1974). His vision concurs with governments' vision of matters where they prioritize their interests and policies when legislating on a matter of concern that affects the state's interests. This does not exclude cyberspace issues.

Brenner and Koops (2004) believe that international law should allow informal entities, such as civil society organizations, to play a part in regulating cyberspace. This approach, they argue, might support resolving the growing cyber disputes apart from the bureaucratic process of enforcing legal rules since it manifests a flexible approach. The practice shows that this approach weakens the state sovereignty in cyberspace required for maintaining flexibility with cyber disputes.

Despite the differences between physical crimes and cybercrimes, traditional jurisdiction factors applicable to the former are still applicable to the latter; the practice shows that many states apply the fact of location, either of the act or the effect, whether of the offender or the victim, regarding demanding their jurisdiction upon a cyber dispute (Brenner and Koops, 2004). This created a group of contradictory international interpretations of the location concept. Hence, exerting more harmonization efforts by the dispute states is a need. Furthermore, Nowikowska (2022, p229) indicated that the Polish CSIRT MON extends its jurisdiction over cyber incidents that inflict damage on national critical infrastructure on the basis of *ratione personae*. Consequently, when critical infrastructure is been inflicted by a cyber-attack, the CSIRT MON intervenes to prosecute the attackers.

An international ad hoc tribunal might be the best authority to have jurisdiction over international cyber offences. Besides, any state might claim this jurisdiction regarding cybercrimes. Alexandra Perloff Giles bases her opinion on that cybercrime should be considered “an enemy of mankind” (Perloff-Giles, 2018). She adopts the universal jurisdiction over cyberspace attitude. She justifies that by the common features between cybercrimes and piracy crimes since they both threaten international trade interests. International law concerning the latter adopts the universal jurisdiction doctrine according to the UNCLOS (UNCLOS 1994, art. 101 c). She also argues that domestic courts should take precedence over practising this jurisdiction according to the principle of complementarity, otherwise, this jurisdiction should belong to the International Criminal Court.

Nonetheless, her study is limited to cybercriminal offences that she compared with naval piracy. In the meanwhile, she does not mention the jurisdiction over non-criminal cyber disputes. Moreover, her study does not include a mechanism to transfer the jurisdiction from the domestic courts to the ICC when the principle of complementarity is applicable.

Notably, Schmitt (2017) mentions that the states can practice their subject and personal jurisdiction under international law. Besides, he argues that the nationality factor applies to cyber incidents even overseas. Remarkably, the Manual presents a combination of several international and regional conventions that grant it prominence as a guide to determine the jurisdiction in cyberspace.

Remarkably, Bu (2018, p.398) claims that the US judiciary tends to limit its jurisdiction over cyber disputes that include a foreign body provided that the litigated conduct occurred within the US territory restraining, therefore, its jurisdiction from covering conducts done by American entities outside the US. He establishes this view on the approach of the US courts in certain cases. This limited approach created hardships before US courts when trying
to obtain evidence located outside the US territory. His view highlights the importance of the global jurisdiction doctrine over cyber disputes. Concerning the US legislation, Vinokurov noted that American IT Giants exploited the personal jurisdiction rule against their clients in non-American whereabouts. Their attitude was a consequence of the judicial interpretation of personal jurisdiction in the Asahi Case because the US Supreme Court permitted the defendant to determine the jurisdiction where it operates. Thus, he argued that the judicial interpretation of personal jurisdiction in cyber litigations should be at an international level due to the universal sphere of cyberspace (Vinokurov, 2022, p.277).

Khalifa (2020, p.54-66) suggests determining the jurisdiction according to certain factors which are: the interests of the litigation parties and their states. Also, he considers the harmed state's interest to ensure the remedy rights. Moreover, to guarantee the legality of this determination, he refers to considering the most relevant jurisdiction regarding criminal proceedings. Although, he has not drafted a path to settle jurisdiction conflicts. He describes the required factors concerning settling these conflicts.

Notably, the Directive (EU) 2019/713, European Parliament and the Council of the European Union 2019, art 12) imposes conditions on Member States to practice their jurisdiction in cyberspace. These conditions are:

- The exclusive application on the offences that the Directive included.
- The effective application that ensures the best practice of the national judiciaries in cyberspace.
- The national jurisdictions include the crimes committed within each State’s borders or by their nationals or that had damage within the State’s territory.

Moreover, the Directive establishes a rule to settle jurisdiction conflicts. It refers to State Members conducting direct consultation supervised by Eurojust. Nonetheless, this Directive is narrow in its scope; it organizes the jurisdiction over certain cybercrimes which goes against the continuous evolution of cybercrimes. Furthermore, the jurisdiction conflict solution it includes is not effective; it depends on consultations between the concerned states with the capability of resorting to Eurojust assistance. Thus, it leaves the slot empty of legal alternatives if the consultations fail.

The UK Legislator extends its jurisdiction over crimes like child abuse, sexual offences, fraud, and terrorism. This extraterritorial jurisdiction enhances the UK nationals’ protection against these acts in cyberspace; the Crown Prosecution Service can prosecute the perpetrators outside the UK and try them before the British courts.

Likewise, the Combating Information Technology Crimes Law extended, in Art 3, the Egyptian jurisdiction largely over cybercrimes to cover, besides the traditional jurisdiction factors noted in the Penal Code, all offences committed by non-nationals provided that:

- The crime was committed on board any naval aerial or land transportation registered in Egypt or raising its flag.
- The victim is Egyptian.
- The crime was planned surveyed or funded in Egypt.
- The criminal is an organized group working in several countries among them Egypt.
- The crime might harm any of Egypt’s interests or security or any citizen’s or residents’ interests or security.
- The criminal was found in Egypt after committing the crime and was not yet extradited.

This ample approach by the Egyptian Legislator is a result of the legal vacuum that the Egyptian judges suffered regarding cyber disputes. Moreover, it secured moving through cyberspace for both Egyptians and foreign residents under Egyptian legal protection.
2. Research Methodology

A qualitative research method is adopted to achieve the objective of establishing a firm structure of the cyber judicial principles regarding settling cyber jurisdiction conflicts. These principles should be applicable and integrated within several judicial systems. The core of this study is an integration of the doctrinal with aspects of the comparative approach.

The doctrinal approach depends on analysing the legal prepositions found in case laws or legislations via logical reasoning. This approach is important for the fulfilment of the research purpose since it analyses the norms that the judgments included. The research investigates legal records and law libraries to study the relevant case laws. Then, it analyses the norms entailed in their judgments to constitute a comprehensive theory of the judicial approaches concerning its question.

The comparative approach is the second building block of the research methodology. It is relevant to a project involving several legal systems to determine their agreements and differences. In this research, the primary element of the comparison is to study the relevant cases in UK and US jurisdiction and extract the differences and commonalities between them.

Indeed, studying cases from the USA and the UK would provide modern and stable judicial norms concerning cyber disputes. These norms were born within the judicial system of the developed nations in the field of cybersecurity which guarantees their validity to the article's purpose. This approach shall be achieved qualitatively as this research tries to determine the judicial principles that the case laws deployed through conceptual analysis, regardless of their numerical data.

3. The Court’s Contributions to Settle Cyber Jurisdiction Conflicts

According to the aforementioned methodology, the article studies case laws from the courts of the UK and the US. Their judgments include the required legal norms to constitute the theory that settles the research question.

The US courts adopted the following norms to determine their jurisdiction over cyber disputes, in *Palantir Techs. Inc. v. Abramowitz*, the court pointed out that federal courts’ jurisdiction is limited and the plaintiff’s prayer for relief cannot establish a federal jurisdiction question if the district court lacks the subject matter jurisdiction. Hence, it refined the concept of federal jurisdiction by referring to its limited nature since they exercise powers included in the US Constitution exclusively. Like the instructions of the Tallinn Manual 2.0 (Schmitt, 2017), the US courts imposed their jurisdiction on a subject-matter basis. In *Patel v. Facebook. Inc*, the Ninth Circuit of the US Court of Appeals defended its jurisdiction to review the district court’s interlocutory decisions under Section 1292 regardless of the plaintiff’s standings.

In *Heretick v. Exactis, LLC*, the court imposed its original jurisdiction under the Class Action Fairness Act (CAFA) as one of the parties is American and the litigation sum exceeds the included limit. Furthermore, the court in *Microsoft Corp. v. Doe* assured its personal jurisdiction as the illegal cyber activity occurred within its local jurisdiction.

Alternatively, the US courts managed to peel off this jurisdiction under certain conditions. In *Thorium Cyber Sec., LLC v. Nurmi*, the court decided that it should not impose its supplemental jurisdiction over a non-compulsory counterclaim if it lacked the subject matter jurisdiction. In addition, the court in *Democratic Nat'l Comm. v. Russian Fed'n decided* that it lacked subject matter jurisdiction because the entire tort occurred outside the US lands. They agree with Bu (2018) in this limitation to prevent the nullity of their judgments.
Furthermore, the court in *Hatheway v. Sirochman* refused to impose personal jurisdiction as she considered that passive advertisement, accessible in every state, could not establish the court’s personal jurisdiction. The court asserted that personal jurisdiction requires that the advertisement is purposefully directed to the plaintiff which does not apply to online advertising. Thus, the court lacks personal jurisdiction over the dispute.

In addition, in *Sawa v. RDG-GCS Joint Ventures III*, the court, concerning an illegal cyberstalking activity, declined to exercise supplemental jurisdiction over state law claims once it has dismissed all claims over which it has original jurisdiction under Section 1367 of the 28th US Codes.

The UK courts adhered to the national jurisdiction depending on the British nationality of the parties. In *AA v Persons Unknown & Ors, Re Bitcoin*, the court exercised its jurisdiction as the plaintiff was an English entity that suffered a loss within the court’s jurisdiction.

Besides, they applied the jurisdiction factors included in the outstanding legislation. In *Fish v Barker*, the court established its jurisdiction over interim injunction applications on the basis included in section 37(1) of the Senior Courts Act 1981 “Powers of High Court concerning injunctions and receivers”. Also, the UK courts, in *Hanger Holdings v Perlake Corp SA* and *Ras Al Khaimah Investment Authority v Azima*, established their jurisdiction on the provision included in the investment agreement between the litigation parties because of the binding force of that agreement’s clauses.

**Conclusion**

To conclude, the research shows that the national courts adopted several attitudes to determine jurisdiction in cyberspace. They ensured the exercise of their jurisdiction over cyber disputes that would threaten the state’s sovereignty or security by applying the same jurisdiction factors applicable to the traditional litigations. It is a prerequisite for the national court to determine its jurisdiction boundaries over a dispute to deliver its judgment. Otherwise, it would be annulled.

The US judiciary refined the concept of cyber jurisdiction to ensure that the judgments are given by the competent jurisdiction. They imposed their jurisdiction according to traditional factors, like subject-matter and personal. However, they limited their jurisdiction in certain cases. Thus, the US courts enhanced the authority of the judgments in cyberspace by assuring that the judgment is delivered by the competent judge and developed the concept of jurisdiction over cyber disputes.

The UK judiciary widened the range of the national jurisdiction to ensure effective protection of the state’s interests in cyberspace. The British courts enforced their jurisdiction over cyber disputes, including a British citizen or entity. Besides, they applied the CPS interpretation of the jurisdiction factors which extends it globally over certain offences\(^1\), regardless of their location or the defendant’s nationality. Thus, they extended the UK jurisdiction offering global protection to the state’s interest. Also, the UK courts admitted the litigation parties’ agreements as a jurisdiction factor. That flexibility promoted the trustworthiness of the UK judiciary in cyberspace which eliminates the legal vacuum that prevailed therein.

Notably, the Anglo-Saxon judiciaries do not mention the question of the universal jurisdiction of these disputes. Unlike Alexandra Perloff Giles\(^2\), they do not admit the global nature of cybercrimes, but they consider them a direct threat to state security. Consequently, they consider the national court to be the competent body to determine jurisdiction in cyberspace.

---

\(^1\) The Crown Prosecution Service (2021), ibid.
\(^2\) Alexandra Perloff-Giles (2018), ibid.
Despite the clear approach of the Egyptian Legislator regarding jurisdiction in cyberspace, the Egyptian judiciary did not deliver similar judgments. The judgments in Egypt do not refer to the court jurisdiction since it is a prerequisite to initiate the hearing procedures. Put differently, the court once has jurisdiction under the law, it initiates the litigation procedures without mentioning that in its judgment. That approach created a vacuum within jurisprudence regarding jurisdiction determiners. Thus, it becomes important to redraft the Egyptian judgments to include the principles that the court adopts about jurisdiction. Then, jurisprudence could study them to conclude the relevant norms.

Credit Authorship Contribution Statement

The author performed all tasks involved in manuscript preparation, research, and writing.

Conflict of Interest Statement

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References


---

3 Law No 175/2018, ibid pt 1 art 3.
Untangling the Jurisdictional Web in Cyberspace

Y. A. Abdelkarim


Cite this article:

Article’s history:
Received: 1st of October, 2023; Revised: 17th of November, 2023; Accepted for publication: 14th of December, 2023; Available online: 18th of December, 2023.
Published: 30th of December, 2023 as article in Volume II, Issue 2(4).

© The Author(s) 2023. Published by RITHA Publishing. This article is distributed under the terms of the license CC-BY 4.0, which permits any further distribution in any medium, provided the original work is properly cited maintaining attribution to the author(s) and the title of the work, journal citation and URL DOI.
Table of Legislations

Table of Cases
[2019] EWHC 3556 (Comm), UK.
[2021] EWHC 604 (QB), UK.
[2021] EWHC 81 (Ch), UK.
[2021] EWCA Civ 349, UK.
3:18-cv-822-J-39PDB, US.
392 F. Supp. 3d 410 (S.D.N.Y. 2019), US.
The Asahi Case, Asahi Metal Industry Co. v. Superior Court, 480 U.S. 102 (1987), US.
Case No. 16-cv-5857-PJH, US.
CIVIL ACTION NO. 15-6585, US.
F.3d 1264 (9th Cir. 2019), US.
No. 3:19-cv-07669-WHO (N.D. Cal. Dec. 10, 2020), US.