Microsoft Corp. v. United States and the 'Hot Pursuit': A Case Study Against the Application of the Law of the Sea into the Cyberspace

Patricia A. Vargas-León*
The Fletcher School at Tufts University, Medford, United States of America
patriciaavl@gmail.com

Abstract 755
Keywords 756
Introduction: The Cyberspace as a Challenge for the Traditional International Order 757
I. Application of International Law and Law of the Sea 759
1. Hot Pursuit: A Policy Beyond Territorial Sovereignty 761
2. Selection of the Hot Pursuit Principle 764
II. Case Study: *Microsoft Corp. v. United States* 765
1. Facts 766
2. Arguments of the Parties 768
a) The US Government 769
b) Microsoft 770
III. Application of the Hot Pursuit: Negative Repercussions 772
1. A Call for Nation-States: Bits under Nation-States' Sovereignty 773
2. Direct Access v. MLATs: Private Actors Using Arguments of International Law 774
3. A 'Virtual Fragmentation' with 'Practical Consequences': A Call for the Nation-States Westphalian Model 776
4. More Centralised Government Control and Less of a Governance Model 778

Abstract

In today's world, no treaty regulates the cyberspace or the Internet. To some extent, the multi-stakeholder model has successfully kept the Internet free of a unique point of control, yet some nation-states advocate for a government-based-model. Amid the Internet Corporation for Assigned Names and Numbers (ICANN) transition debate, some governments favoured a cyberspace regulation in the hands of an inter-governmental organi-

* Postdoctoral Scholar, The Fletcher School, Tufts University; Visiting Fellow Information Society Project, Yale Law School, PhD (Syracuse University), Law Degree (Pontifical Catholica University from Peru).

The work described in the paper was partially supported by NSF grant CNS 1923528, grant Hewlett 2018-7277 and grant Hewlett 2020-1484.

DOI 10.17104/0044-2348-2021-3-755 ZaöRV 81 (2021), 755-779

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

sation. Additionally, western democracies have advocated to declare the cyberspace a fifth domain.

Reasons for these different perceptions are related to the different conceptions nation-states have what should be the governance model for a resource beyond their traditional borders. Considering this dichotomy, this paper analyses the negative implications of applying the law of the sea into cyberspace. For this purpose, this paper will explore the concept of the '*right of hot pursuit*', one of the provisions of the United Nations Convention on the Law of the Sea (UNCLOS).

The research methodology includes as a case-study *Microsoft Corp. v. United States*, also known as the '*Microsoft Ireland*' case. This case was selected because it exemplified how government administrations attempt to use the principles of international law to protect their sovereignty over the Internet infrastructure located in their territory, even when the access to that infrastructure is 'virtual' and there is no need to access such infrastructure physically.

Facing this scenario, where governments try to exercise their sovereignty beyond their territorial borders, this paper will:

1. Provide an overview of the International Court of Justice (ICJ) and the International Tribunal for the Law of the Sea (ITLOS) interpretations of the hot pursuit to determine the international legal conception over this principle.
2. Analyse the arguments of the parties involved in the *Microsoft Ireland* case about why one nation-state's sovereignty should be applied or not beyond the borders of its territory.
3. Analyse the negative repercussions of including the hot pursuit and the fictional fragmentation of the ocean into the cyberspace.

Findings expect to enrich the discussion within the Internet governance debate and understand the consequences of (1) applying the international law over the Internet infrastructure and (2) clarify the traditional legal approach that spaces without nation-states' sovereignty should not exist.

Keywords

Hot Pursuit – Cyberspace – UNCLOS – *Microsoft Corp. v. United States*

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

Introduction: The Cyberspace as a Challenge for the Traditional International Order

The cyberspace is defined as a global space, the virtual world, for interactions among Internet users, where nation-states' territorial borders are irrelevant. The concept has been considered a sort of 'third force', different from governments and businesses. The cyberspace also has a 'global connotation' because it is considered a worldwide domain consisting of an interdependent network of information technology infrastructures, including the Internet, telecommunications networks, and computer systems.[1]

Unlike the traditional territorial borders, the cyberspace is 'aterritorial',[2] invisible, unidentifiable, cannot be felt, or identified in any way and does not have natural or physical characteristics. It is also characterised by anonymity and ubiquity.[3] For some academics, the law cannot control the cyberspace, it only can control the use that human beings put to it.[4]

The current international landscape witnesses a growing state power over the Internet infrastructure, which has created a definition of cyberspace as a military domain or fifth domain. As consequence, nation-states see fit that the traditional 'Westphalian model' should be the role for the cyberspace as well. Therefore, if nation-states are the sovereign authority within their territories, they also should be the supreme sovereign authority within the cyberspace and the Internet infrastructure located in their territories.[5]

Claims of sovereignty come from all types of regimes and in different circumstances.

The North Atlantic Treaty Organization (NATO) declared the cyber as the fifth domain, alongside water, fire, land, and space.[6] During the ICANN transition debate, some governments (Russia, India, Iran, and Saudi Arabia) argued in favour of a cyberspace regulation in the hands of an inter-govern-

1 Milton Mueller, *Ruling the Root Internet Governance and the Taming of Cyberspace* (Cambridge, Mass.: MIT Press 2002); Shabtai Rosenne and The Hague Academy of International Law, *The Perplexities of Modern International Law* (Leiden: Martinus Nijhoff 2004).

2 'Aterritoriality' refers to the lack of applicability of the territorial criteria that exists in nation-states.

3 Stephen C. Jacques, 'Comment Reno v. ACLU: Insulating the Internet, the First Amendment, and the Market Place of Ideas', The American University Law Review 46 (1998), 1945-1992; Joanna Kulesza, *International Internet Law* (London: Routledge 2012); Rosenne and Hague Academy of International Law (n. 1).

4 Kulesza (n. 3).

5 Robert Jackson, 'Sovereignty in World Politics: A Glance at the Conceptual and Historical Landscape', Pol. Stud. 47 (1999), 431-456; Milton Mueller, 'Against Sovereignty in Cyberspace', International Studies Review 22 (2020), 779-801.

6 Steve Ranger, 'Cyberwarfare Comes of Age: The Internet Is now Officially a Battlefield' (2016), <https://www.zdnet.com/>.

DOI 10.17104/0044-2348-2021-3-755 ZaöRV 81 (2021)

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

mental organisation.[7] Additionally, in 2011, former President Obama pointed out that the creation of rules and norms for state behaviour in cyberspace does not require re-inventing customary international law or rendering existing international norms. For the United States' (US) government, long-standing international norms guiding state behaviour (in times of peace and conflict) also apply in cyberspace.[8]

In view of the constant sovereignty claims over the cyberspace, a group of academics[9] and non-academics[10] have called to apply similar policies to the ones contained in the Convention on the Law of the Sea to this domain. In the US, the military called to move from 'sea power' to 'cyber power' and, in June 2016, NATO announced that the 28-member alliance agreed to declare cyber an operational domain, like sea, air, and land.[11] Furthermore, the Tallinn Manual 2.0 contains clear provisions of UNCLOS that should be included in case of a cyberwarfare.

In the real world, this conception framed according to the views of the national sovereignty refers to an international order based on mutually recognised territorial borders and in the absence of overlapping jurisdictions.[12] Nevertheless, no nation-state in the world may claim sovereignty over the cyberspace. In the same way, although no nation-state can control the cyberspace, nation-states understand the conception of the cyberspace as a 'whole thing', which explains the comparison with the oceans and the outer space, instead of continental land.[13]

For those who claim that the rules of UNCLOS should be applied into the cyberspace, the comparison between the cyberspace and the sea is adequate because, in the past, the sea was considered a space for communications, economic production, transportation, and war, many of the characteristics

7 Edward Moyer, US Hands Internet Control to ICANN (2016), <https://www.cnet.com/>.

8 White House, 'International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World', White House (2011), <https://obamawhitehouse.archives.gov>.

9 Julija Kalpokienė and Ignas Kalpokas, 'Hostes Humani Generis: Cyberspace, the Sea, and Sovereign Control', Baltic Journal of Law & Politics 5 (2012), 132-163; Michael Sechrist, 'Cyberspace in Deep Water: Protecting Undersea Communications Cables by Creating an International Public-Private Partnership', Harvard – Belfer Center for Science and International Affairs (2010), <http://belfercenter.ksg.harvard.edu>.

10 Kris E. Barcomb, 'From Sea Power to Cyber Power: Learning from the Past to Craft a Strategy for the Future', National Defense Unit, <https://ndupress.ndu.edu>; Steven M. Barney, 'Innocent Packets? Applying Navigational Regimes from the Law of the Sea Convention by Analogy to the Realm of Cyberspace', Nav. L. Rev. 48 (2001), 56-83.

11 Barcomb (n. 10); Colin Clark, 'NATO Declares Cyber A Domain' Breaking Defense, (2016), <http://breakingdefense.com/>.

12 Robert Jackson, 'Sovereignty in World Politics: A Glance at the Conceptual and Historical Landscape', Pol. Stud. 47 (1999), 431-456; Mueller (n. 5).

13 Mueller (n. 5).

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

attributed to cyber-space today.[14] The ocean has been a subject of a global governance regime,[15] in many ways similar to what nation-states attempt to do with the cyberspace today.

For others, the comparison between the sea and cyberspace is linked to the concepts of war and state-practice. This though can be summarised in two points: (1) wars are traditionally fought over territory, but the concept of territory has evolved to incorporate cyberspace,[16] and (2) the existence of UNCLOS (and similar treaties) proofs the existence of a state practice of claiming any space beyond nation-states' territorial borders.[17]

This contribution discusses the consequences of applying the provisions of UNCLOS into the cyberspace and the Internet infrastructure as nation-states claim. For this purpose, this paper has selected one of the principles of UNCLOS to be subject to analysis, the 'hot pursuit'. As it will be explained in this paper, this principle has been selected because it represents the unrestricted respect to a nation-state's sovereignty even when another nation-state has a legitimate legal claim to pursue beyond its own zones of national sovereignty.

A first part will define the role of international law in the attempts to create a legal framework for the cyberspace, legal conceptualisation of the hot pursuit according to UNCLOS and the rulings of international courts. The second part will analyse the hot pursuit principle, from a theoretical and practical point of view, as this is one of the core elements for analysis. The following parts will explain the reasons why this principle was selected and the arguments of the selected case study. Finally, this paper will address the augments against the creation of an international legal regime based on UNCLOS for the cyberspace.

I. Application of International Law and Law of the Sea

It is quite complicated to apply old principles of international law, linked to human history from its beginning, to new circumstances and technologies that do not recognise the basic principles on which the current international order was built.

The cyberspace and the Internet represent a new opportunity for mutual interactions among individuals and entities subject to different sovereignties.

14 Philip E. Steinberg, *The Social Construction of the Ocean* (Cambridge: Cambridge University Press 2001); Barney (n. 10).

15 Dire Tladi, 'Ocean Governance: A Fragmented Regulatory Framework', A Planet for Life (2011), <http://regardssurlaterre.com/>.

16 Andrew Sheng, 'The Coming CLASS War', Project Syndicate (2014), <https://www.project-syndicate.org/>.

17 Wolff Heintschel von Heinegg, 'Legal Implications of Territorial Sovereignty in Cyberspace' in: Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds), *4th* International Conference on Cyber Conflict (Tallin: NATO CCD COE Publications 2012), 7-19.

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

In this regard, lawmakers of each territory involved in a particular interaction claim the right to regulate a specific behaviour or to sanction a harmful conduct. Therefore, nation-states have taken action to exercise their coercive capacity over online activities. This situation directly affects Internet users as they may not be sure, and therefore they may not take informed decisions about what the legislation is applicable to their activities.[18]

For some international law scholars, such as Shabtai Rossene[19] and Ian Brownlie,[20] the law of the sea is an inherent part of the theory of international law, therefore, they should not be considered as separated disciplines. In any case, it cannot be denied that there are similarities between the cyberspace (as a whole), which is shared by all the networks that formed the Internet, and the ocean, a space that is shared by the humankind.

This could lead to conclude that any regulation over the cyberspace should be an international one, based on the rules of international law. The achievement of international regulation is also essential for those who desire the achievement of concrete standards especially when human rights are involved, such as data privacy and freedom of expression.[21]

Nevertheless, the particular characteristics of the cyberspace, which do not make it possible for a nation-state to control it, but make it difficult to achieve rules based on international law to regulate it. Moreover, nation-states behind every potential attempt to regulate the cyberspace, have completely different visions about the regime that should set the rules of interaction within the cyberspace. For this particular characteristic, many legal scholars consider the cyberspace a 'perplexity' for the classic theory of international law.[22]

One of the clearest attempts to concretise this tendency to apply the rules of international law into the cyberspace and cyber operations was the Tallinn Manual from 2013,[23] a comprehensive intellectual attempt to include the concept of sovereignty into the cyberspace. Elaborated under the sponsorship of the NATO Cooperative Cyber Defence Centre of Excellence, the Tallinn Manual created considering State practice and statements on the applicability of international law to cyber operations.

18 Kulesza (n. 3).

19 Rosenne and Hague Academy of International Law (n. 1).

20 James R. Crawford, *Brownlie's Principles of Public International Law* (8th edn, Oxford: Oxford University Press 2012).

21 Molly Land, 'Toward an International Law of the Internet', Harv. Int'l L.J. 54 (2013), 393-458.

22 Rosenne and Hague Academy of International Law (n. 1).

23 Michael Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare, prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, (Cambridge: Cambridge University Press 2013). CCDCOE, 'The Tallinn Manual', (2021) <https://ccdcoe.org/>.

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

According to the Tallinn Manual from 2013 a government can exercise control over the national cyberinfrastructure and any activity within the borders of the nation-state territory.[24] A subsequent project, the Tallinn Manual 2.0 from 2017[25] focuses on the physical capacity around Internet access. This perspective is crucial because, although the cyberspace may be aterritorial, every piece of the Internet infrastructure that exists in a geographic location is owned, operated, and maintained by a specific entity subject to the local legislation.[26] Following this logic, local governments have created national statutes that have created international controversies, as it will be explained in the next paragraphs.

1. Hot Pursuit: A Policy Beyond Territorial Sovereignty

UNCLOS is a multilateral treaty that covers multiple aspects of the regulation of the spaces and activities in the ocean and sets out the framework for legal governance within which all activities in the oceans must be conducted and the institutions that must oversee those activities.[27] However, UNCLOS's main and most controversial characteristic is the creation of fictional spaces or legal areas where coastal nation-states sovereignty decreases with increasing distance of the coast. UNCLOS defines nation-states' rights and obligations from coast to coast and from the surface to the deep sea in these zones. This policy is known as 'maritime jurisdiction'[28] or a 'fragmented governance'[29] model. This paper will use the term a 'virtual fragmentation' of the ocean.

The hot pursuit is a classic principle of the doctrine of international law, the law of the sea, and is part of modern nation-states' practices. The doctrine related to the hot pursuit evolved through history and developed as customary international law. In 1982, the principle obtained international legal recognition by being included in UNCLOS.[30]

---

24 Schmitt (n. 23).

25 Michael Schmitt and NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn manual 2.0 on the international law applicable to cyber operations*, (2nd edn, Cambridge: Cambridge University Press 2017).

26 Kris Barcomb, Dennis Krill, Robert Mills and Michael Saville, 'Establishing Cyberspace Sovereignty', International Journal of Cyber Warfare and Terrorism 2 (2012), 26-38.

27 World Ocean Review, 'A Constitution for the Seas' (2010), <https://worldoceanreview.com/>.

28 Alfonso Arias-Schreiber Pezet, *El Derecho del Mar [Law of the Sea]*, (Lima: Academia Diplomática del Perú 1984).

29 Tladi (n. 15), para. 4; Julia A. Ekstrom, Oran R. Young, Steve D. Gaines, Maria Gordon and Bonnie J. McCay, 'A Tool to Navigate Overlaps in Fragmented Ocean Governance', Marine Policy 33 (2009), 532-535.

30 Vasilios Tasikas, 'Unmanned Aerial Vehicles and the Doctrine of Hot Pursuit: A New Era of Coast Guard Maritime Law Enforcement Operations', Tul. Mar. L. J. 29 (2004), 59-80.

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

UNCLOS defines the hot pursuit principle as the right of a nation-state to pursue and seize a non-national vessel suspected of having committed a crime within the nation-state's internal waters and territorial sea (where the nation-state has sovereign rights) and arrest it. Such a right remains, even if the vessel moves onto the high sea (where the coastal nation-state has no sovereign rights).[31]

The territorial sea is the extension of seawaters adjacent to coastal states until the distance of 12 miles. According to UNCLOS provisions, nation-states are sovereign in the territorial sea and the internal waters, as if they were in their territory.[32]

The hot pursuit principle of a foreign ship may be undertaken when there are reasons for the coastal nation-state's competent authorities to believe that a foreign ship violated its laws and regulations. The main characteristics of the pursuit are:[33]

1. The pursuit must start when the foreign ship or one of its boats is within the internal waters, the territorial sea or the contiguous zone of the pursuing nation-state.
2. The pursuit must be continuous and only can continue outside the territorial sea if there were no interruptions and there was a warning, visual or auditory signal for the crew of the prosecuted ship.
3. The pursuit must end as soon as the chased ship enters into the territorial sea of its nation-state or a third nation-state's territorial sea (entering into other nation's state territorial sea is the equivalent to enter into that nation-state's territory).

According to the rules of UNCLOS, the hot pursuit purpose is 'to bring escaping wrongdoers before the jurisdiction of the injured State'.[34] The hot

31 Eugene Kontorovich, 'Law of the Sea – Visit and Seizure of Vessels at Sea – Definition of Piracy – Right of Hot Pursuit – Enforcement Jurisdiction at Sea – Compliance with Provisional Measures', AJIL 110 (2016), 96-102.

32 United Nations Convention on the Law of the Sea of 1982

Part II. – Territorial Sea and Contiguous Zone

Article 2: Legal status of the territorial sea, of the air space over the territorial sea and of its bed and subsoil

1. The sovereignty of a coastal State extends, beyond its land territory and internal waters and, in the case of an archipelagic State, its archipelagic waters, to an adjacent belt of sea, described as the territorial sea.

2. This sovereignty extends to the air space over the territorial sea as well as to its bed and subsoil.

3. The sovereignty over the territorial sea is exercised subject to this Convention and to other rules of international law.

Jose Luis Messeguer Sanchez, 'Los Espacios Maritimos en el Nuevo Derecho del Mar [Sea Spaces in the New Law of the Sea]' (Madrid: Marcial Pons 1999).

33 Robin Rolf Churchill and Alan Vaughan Lowe, *The Law of the Sea* (Manchester: Manchester University Press 1999).

34 Nicholas M. Poúlantzas, *The Right of Hot Pursuit in International Law*, (Leiden: Martinus Nijhoff Publishers, 2002), 2.

 DOI 10.17104/0044-2348-2021-3-755

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

pursuit is an exception to the principle and freedom of the high seas and to the exclusive jurisdiction of the flag-state that rules the vessels in the high seas.[35]

As established by ITLOS[36] in the case of the merchant vessel *M/V Saiga*,[37] conditions to exercise the hot pursuit are set out in Article 111 of UNCLOS.[38] Such conditions must be accumulative; each one must be satis-

35 Poúlantzas (n. 34), 239.

36 The International Tribunal for the Law of the Sea (ITLOS) is an independent judicial body created by UNCLOS to solve disputes related to the interpretation and application of the Convention. The Tribunal is composed of 21 independent members and, according the article 21 of its statute, ITLOS has jurisdiction over any dispute concerning the interpretation or application of the Convention, and over all matters specifically provided for in any other agreement which confers jurisdiction on the Tribunal. In practical terms, ITLOS is a parallel jurisdiction to the ICJ, and the final venue to solve a controversy is a matter of decision for the involved parties.

37 ITLOS, *The M/V 'SAIGA' Case No. 2* (Saint and Vincent The Grenadines v. Guinea), judgment of 1 July 1999, para. 146.

38 United Nations Convention on the Law of the Sea of 1982

Part VII. – High Seas

Article 111: Right of Hot Pursuit

1. The hot pursuit of a foreign ship may be undertaken when the competent authorities of the coastal State have good reason to believe that the ship has violated the laws and regulations of that State. Such pursuit must be commenced when the foreign ship or one of its boats is within the internal waters, the archipelagic waters, the territorial sea or the contiguous zone of the pursuing State, and may only be continued outside the territorial sea or the contiguous zone if the pursuit has not been interrupted. It is not necessary that, at the time when the foreign ship within the territorial sea or the contiguous zone receives the order to stop, the ship giving the order should likewise be within the territorial sea or the contiguous zone. If the foreign ship is within a contiguous zone, as defined in article 33, the pursuit may only be undertaken if there has been a violation of the rights for the protection of which the zone was established.

2. The right of hot pursuit shall apply mutatis mutandis to violations in the exclusive economic zone or on the continental shelf, including safety zones around continental shelf installations, of the laws and regulations of the coastal State applicable in accordance with this Convention to the exclusive economic zone or the continental shelf, including such safety zones.

3. The right of hot pursuit ceases as soon as the ship pursued enters the territorial sea of its own State or of a third State.

4. Hot pursuit is not deemed to have begun unless the pursuing ship has satisfied itself by such practicable means as may be available that the ship pursued or one of its boats or other craft working as a team and using the ship pursued as a mother ship is within the limits of the territorial sea, or, as the case may be, within the contiguous zone or the exclusive economic zone or above the continental shelf. The pursuit may only be commenced after a visual or auditory signal to stop has been given at a distance, which enables it to be seen or heard by the foreign ship.

5. The right of hot pursuit may be exercised only by warships or military aircraft, or other ships or aircraft clearly marked and identifiable as being on government service and authorised to that effect. […]

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

fied to claim the principle.[39] In the *Corfu Channel* case,[40] the ICJ recognised that the use of force is allowed when the pursued vessel subject to arrest refuses to stop. The idea of using necessary force is authorised even though that it is a severe infringement on freedom in the high seas.[41]

In 2013, in the case of the *Arctic Sunrise*[42] ITLOS stablished new clarifications surrounding the claim of the hot pursuit principle. As established by ITLOS, signals of the coastal nation-state ship for the vessel suspected of having committed a crime must be clear and ratified that boarding must be urgent. Additionally, in 2015 and about the same case, the Permanent Court of Arbitration (PCA Tribunal)[43] also stablished that boarding must be immediate; the coastal nation-state boat must not be shadowing the vessel suspected of committing a crime. If those requirements are not met, the chance to claim the hot pursuit may disappear.

2. Selection of the Hot Pursuit Principle

The principle of hot pursuit can be exercised to act in circumstances of necessity or criminal activity. Main critiques against the hot pursuit claim that it is a principle that allows a nation-state to enforce its domestic laws extraterritorially against non-national ships that flee onto the high seas where nation-states lack jurisdiction.[44] Defenders of the principle claim that, if the hot pursuit empowers a coastal nation-state to pursue a vessel that has violated its laws onto the high seas, this occurs in order to deny to the offending vessel the opportunity of escape punishment by claiming the free navigation designed to protect innocent vessels.[45]

This critique resembles the one related to the cyberspace, where governments (acting on behalf of their nation-states) have acted in two different ways: a) by attempting to expand their sovereignty accessing data stored

39 Saiful Karim, 'Conflicts over Protection of Marine Living Resources: The "Volga Case" Revisited' GoJIL 3 (2011), 101-127.

40 ICJ, *Corfu Channel* Case (UK v. Albania), merits, ICJ Reports 1949, 4 (1949).

41 Craig H. Allen, 'Doctrine of Hot Pursuit: A Functional Interpretation Adaptable to Emerging Maritime Law Enforcement Technologies and Practices', ODILA 20 (1989), 309-341 (20).

42 ITLOS, *Arctic Sunrise* (Kingdom of the Netherlands v. Russian Federation), Provisional Measures, ITLOS Case No. 22, Order of 22 November 2013.

43 In *re Arctic Sunrise* (Netherlands v. Russian Federation), PCA Case No. 2014-02, Merits, PCA Case No. 2014-02, UNCLOS Annex VII Arb. Trib. 14 August 2014.

44 Robert C. Reuland, 'The Customary Right of Hot Pursuit onto the High Seas: Annotations to Article 111 of the Law of the Sea Convention', Va. J. Int'l L. 33 (1993), 557-589; Tasikas (n. 30).

45 Allen (n. 41).

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

beyond the borders of their territory[46] and b) by attempting to keep data within the borders of its territory.[47]

In this regard, a nation-state's territory consists of all the land within its frontiers, together with a belt of sea adjacent to its coast known as the territorial sea, and the airspace above its land territory and territorial sea. National sovereignty is framed by a nation-state's territorial borders and does not extend to the outer space.[48] The hot pursuit is one of the few exceptions that allow governments to go beyond the spaces where they can exercise jurisdiction and yet, the pursuit must stop the moment a space of national sovereignty of a third nation-state gets involved.

Following the nation-states' logic of applying UNCLOS into the cyberspace, the sovereignty claim of one nation-state must stop when another nation-state sovereignty claim starts. The hot pursuit is the best principle to concretise this premise because the hot pursuit is the outcome of the unrestricted respect to the recognition of the fictional borders international law has created in the ocean.

Nevertheless, because the cyberspace lacks traditional territorial borders, nation-states demand respect to the Internet infrastructure located in their own territories, under the assumption that the Internet is the main component of the cyberspace. Following this claim, any access to the physical Internet infrastructure located in a nation-state cannot be accessed from another nation-state. The same logic is the one with the hot pursuit principle, as any international legal persecution must stop as soon as the borders (and anything inside of them) of a third nation-state are affected.

II. Case Study: *Microsoft Corp. v. United States*

The case *Microsoft Corp. v. United States*, or *United States v. Microsoft Corp.*, was a case involving the extraterritoriality of law enforcement seeking electronic data under the 1986 Stored Communications Act, which involved Internet data centres and cloud storage.

This case was selected for the following reasons:

1. It exemplifies the claims to respect sovereignty over anything included within a nation-state territory, including an Internet server.
2. From the facts of the case, it is known that the retrieval of the data did not require physical access to the server. It could be done virtually from US territory, this is through the networks of the cyberspace.

46 David Goldman, 'Microsoft Is Fighting the DOJ Too' 2016, <http://money.cnn.com/>.

47 The Economist, 'Should Governments Be Able to Look at Your Data When It Is Abroad?', 2011, <https://obamawhitehouse.archives.gov>.

48 Rosenne and Hague Academy of International Law (n. 1).

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

3. This case is an example of the potential application of the extraterritoriality of law enforcement seeking electronic data in an attempt to solve a criminal investigation of illegal activities occurred within US territory.
4. The case also clarifies how private corporations are willing to use or support principles of international law when it sues to their business model.

The purpose of this section is describing the facts of the case and the arguments of the involved parties, which included: (1) the authority in charge of the criminal investigation, (2) the interpretation of the law, (3) conflict of jurisdictions, (4) extraterritoriality, and (5) economic argumentation. This paper will focus on the controversy related to the extraterritorial application of the US legislation into Irish territory. Although this became the central issue of discussion, it is also a fact that in order to access the data, Microsoft Corp. did not have to send anyone physically to Ireland to collect it, since the data was under its control to be collected from US territory.

1. Facts

In December 2013, a New York District Court judge issued a warrant requesting Microsoft Corp. to produce emails and private information associated with particular accounts hosted by the company. The data was stored on a Hotmail server located in Dublin, Ireland, and was related to a drug trafficking investigation.[49] [50] To get the data, the U.S. government applied for a warrant according to section 2703(a)[51] of the Stored Communications

[49] 'In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp.', Harv. L. Rev. 128 (2015), 1019-1026.

[50] Mark Scott, 'Ireland Lends Support to Microsoft in Email Privacy Case', The New York Times <http://bits.blogs.nytimes.com/>.

[51] Stored Communications Act

18 U.S. C.

Title 18 – Crimes and Criminal Procedure

Part I. – Crimes

Chapter 121 – Stored Wire and Electronic Communications and Transactional Records Access

§ 2703. Required disclosure of customer communications or records

(a) Contents of Wire or Electronic Communications in Electronic Storage.

A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

Act (SCA), enacted as part of the 1986 Electronic Communications Privacy Act (ECPA).[52] According to the U.S. Department of Justice (DoJ), the government has the right to demand the emails of anyone in the world as long as the electronic email (e-mail) provider has headquarters within borders.[53]

Microsoft sued the US government and refused to deliver the names and accounts contained in the server stored in Ireland, arguing that a US Court has no jurisdiction over information stored out of US territory. Microsoft also argued that the US government should pursue traditional bilateral law enforcement and diplomatic channels in order to work with the Irish government to get the data they required. Such channels are referred as the 'Mutual Legal Assistant Treaties' (MLATs), general agreements signed between two or more nation-states to gather and exchange information to enforce public and criminal laws.[54] Similarly, the Irish government supported Microsoft's opinion and claimed that US Courts do not have the sovereignty to issue search warrants to be executed abroad. The US District Court for the Southern District of New York denied Microsoft's motion, and the company appealed.[55]

Microsoft refused to turn over the e-mails and tried to quash the US government's warrant under the argument that the US government's warrant authority cannot extend extraterritorially and, therefore, the warrant was invalid.

The US government, along with the magistrate judge and district court, disagreed. They concluded that the relevant reference point for warrant jurisdiction purposes was the location of the provider (in this case Microsoft), not the location of the data. In practical terms, the data located in Ireland can be accessed and retrieved by Microsoft employees within US territory.[56]

On 7 July 2016, the 2nd US Circuit Court of Appeals in Manhattan resolved that the US government is not entitled to force Microsoft to turn over customer e-mails stored on servers outside of US territory. According to the appealing Court, US service providers that own servers outside the US are beyond the reach of domestic US laws, and therefore, search warrants

52 Alex Ely, 'Second Circuit Oral Argument in the Microsoft-Ireland Case: An Overview', Lawfare 2015, <https://www.lawfareblog.com/>.

53 Sam Thielman, 'Microsoft Case: DoJ Says It Can Demand Every Email from any US-based Provider', The Guardian 2015, <http://www.theguardian.com/>.

54 United States Department of State, 'Treaties and Agreements' 2016, <http://www.state.gov>.

55 Goldman (n. 46).

56 Jennifer Daskal, 'Case To Watch: Microsoft v. US on the Extraterritorial Reach of the Electronic Communications Privacy Act | Just Security', Just Security 2016, <https://www.justsecurity.org/>.

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

issued under SCA are not applicable.[57] The 2nd US Circuit Court concluded that the US Congress legislation is meant to be applied only within US territory. The court did not mention anything about the extraterritorial application of the SCA.[58]

In October 2016, the US government filed a petition for an 'en banc session' rehearing by the Second Circuit. In January 2017, the Court voted 4 to 4 to rehear the case. The judgment in favour of Microsoft remains in place. Differently from this case, in February 2017, the District Court within the Third Circuit ruled that Google must comply with a warrant of the US government to retrieve data from foreign servers. According to the Third Circuit, the scope of privacy invasion for the case was entirely within US territory, not where the electronic transfer occurs.[59]

2. Arguments of the Parties

The context of the *Microsoft Ireland* case refers to the rise of an electronic medium that cannot be governed by any current territorially based sovereign. In this regard, this case puts on the table an 'international' problem: current national statutes were written before the concept of the cyberspace was created and before the Internet was privatised and open to the public. In this way, US Courts have to guess or interpret what Congress would have written into legislation if the Internet had been available at the time. In this scenario, law enforcement agencies find themselves trying to access data stored abroad, and sometimes facing multiple jurisdictions.

It is a fact that it must be remembered that Microsoft and other companies invested billions in building data centres abroad, especially in Europe. If US authorities and intelligence agencies can access that data, European firms may be reluctant to trust US companies. On the other hand, depending upon the result, this case may encourage other governments to request Microsoft or other companies to hand data stored abroad. This situation could generate a forever conflict of jurisdictions.[60] In any case, the actions of the US government will have significant implications in terms of international law. Just to set an example, in the middle of the *Microsoft* case, the former European

57 Jonathan Stempel, 'Microsoft Wins Landmark Appeal Over Seizure of Foreign Emails', Reuters 2016, <http://www.reuters.com/>.

58 'Cooperation or Resistance? The Role of Tech Companies in Government Surveillance', Harv. L. Rev. 131 (2018), 1722-1741.

59 Cooperation or Resistance? (n. 58).

60 The Economist, 'Should Governments Be Able to Look at Your Data When It Is Aroad?', 2015, <http://www.economist.com/>.

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

Union Justice Commissioner warned that the US warrant's final execution might constitute a breach of international law.[61] This was a clear call to respect the sovereignty of a member of the union.

Here there is a quick note to make. The words of the former European Union Justice Commissioner referring to a breach of the rules of international law, could be read, among lines, as the figure of the 'non-intervention principle', so many times featured by the international law and the United Nations. However, the term must be correctly understood and not confused with political rhetoric. First, there must be an 'intervention' by one state in the affairs of another and second, the intervention must be about issues in which each nation-state has a right to decide freely according to the rules of international law.[62]

The discussion surrounds when nation-states face an issue of their sovereignty. In order to better understand the legal controversy, the next section will describe the main arguments outlined by both parties, Microsoft and the US government, during the trial.[63]

a) The US Government

For the US government, the Federal Bureau of Intelligence (FBI) and US Courts are the authorities in charge of the criminal investigation. Upon their request, private companies (like Microsoft) must disclose customer information or records following the Stored Communications Act (SCA). The exercise of authority is not an issue of international law, but one of the domestic laws that establish a citizen's duty concerning its government request. While the Congress's legislation (unless the contrary intention appears) seems to be applicable only within US territory, the question of its application requires a debate, at least until there is a legislative change. According to the US government, nationality, as a principle, supports the legal requirement that an

61 Viviane Reding, 'Viviane Reding Letter European Commission', European Commission 2015, <http://www.nu.nl>.

62 Mazier Jamnejad and Michael Wood, The Principle of Non-Intervention, LJIL 22 (2009), 345-381.

63 AT&T, 'District Court Amicus Brief in Support of Microsoft', Electronic Frontier Foundation 2014 <https://www.eff.org/>; Preet Bharara, 'Government's Brief in Support of Magistrate's Decision', Electronic Frontier Foundation 2014, <https://www.eff.org/>; 'EFF District Court Amicus Brief in Support of Microsoft', Electronic Frontier Foundation 2014, <https://www.eff.org/>; 'Judge Francis. Magistrate's Opinion Denying Microsoft's Motion to Quash', Electronic Frontier Foundation, 2014, <https://www.eff.org/>; Microsoft, 'Microsoft's Objection to the Magistrate's Opinion', 2014, <https://www.eff.org/>; U.S. District Court, 'Microsoft's District Court Reply Brief', Electronic Frontier Foundation 2014, <https://www.eff.org/>; Verizon, 'Verizon District Court Amicus Brief in Support of Microsoft', Electronic Frontier Foundation, 2014, <https://www.eff.org/>.

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

entity subject to jurisdiction within US territory (like Microsoft) is required to get evidence stored abroad.

According to the SCA provisions, the government can request information through a subpoena, court order, or warrant. On this matter, the SCA was enacted in recognition that the fourth amendment protections that apply in the physical world might not apply to information communicated through the cyberspace. This is why SCA authorises the Court with jurisdiction over the investigation of a criminal act to issue a warrant directly, despite the intervention of its counterpart in the district where the Internet service provider is located.

Additionally, according to the US government, the warrant required in section 2703 of SCA demands the government to show probable cause, but it does not change the duty an entity has to produce information regardless of where the data is located. In this case, the US Congress anticipated that an ISP located within US territory would be obligated to respond to a warrant issued according to section 2703(a) by producing information within its control. Therefore, the warrant triggers a US company's statutory obligation to disclose records within its possession and control to law enforcement within US territory. The purposes of the warrant are: (1) to require Microsoft to disclose the content of any electronic communication under Section 2703, and (2) to authorise a review of that data by law enforcement agents within US territory after the data has been disclosed. Moreover, for purposes to deliver the requested data, Microsoft was not in need of sending anyone physically to Irish soil to retrieve it. The company had the capacity of accessing the data electronically from US territory.

On the other hand, Microsoft argues that it is not required to produce the records demanded by the warrant because those records were stored abroad. According to the US government, that argument finds no support under SCA's rules because any 'court of competent jurisdiction' is authorised to issue a warrant. Those courts include those that have jurisdiction over (1) the offence under investigation, (2) the physical location of the service provider, or (3) the storage site of the relevant records.

b) Microsoft

In 1986, the US Congress enacted ECPA, a statute intended to protect individuals' privacy expectations in electronic communications. To protect these privacy interests, ECPA requires federal, state, and local officers to use forms of process within their own powers and limitations. In terms of privacy, the Sixth Circuit's leading decision ruled that the Fourth Amendment requires the US Government to obtain a warrant to access the contents of e-mail communications. ECPA never meant to allow the government to

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

obtain e-mails without a warrant at all. This practice would be unconstitutional under US law.

However, the extraterritorial application of warrants issued under ECPA represents a violation of international law and reduces privacy expectations at a global level. No provision in the statute ever suggests that this was the intention of the US Congress. If the Congress intended to give the warrant provision from ECPA extraterritorial effects, then the Congress should have been clear indications about it. The legislative history of ECPA confirms that warrants executed according to section 2703 (a) are limited to the US territory.

About the competent jurisdiction, Microsoft also acknowledges that a court of competent jurisdiction is the only one who can issue a warrant, but for the company, this principle is vital. According to section 18, 2703(a) of ECPA, a state or federal entity may compel a provider of electronic communications services to disclose the content of a wire or electronic communication, but only when a warrant is issued by a Court of competent jurisdiction. According to a related SCA provision contained in section 2703(b)[64] compels

64 Stored Communications Act
18 U. S. C.
Title 18 – Crimes and Criminal Procedure
Part I – Crimes
Chapter 121 – Stored Wire and Electronic Communications and Transactional Records Access
§ 2703. Required disclosure of customer communications or records
(b) Contents of Wire or Electronic Communications in a Remote Computing Service.
(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection
(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or
(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity
(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or
(ii) obtains a court order for such disclosure under subsection (d) of this section;
except that delayed notice may be given pursuant to section 2705 of this title.
(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service
(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and
(B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

the disclosure of content information maintained by a remote computing service provider as long as the government obtains a warrant issued by an appropriate state or federal court. To this end, and according to Irish law, in order to obtain the content of electronic mails from an electronic service provider, it is required authorisation from an Irish District Court Judge.

The use of 'cloud' computing services makes it easier for US companies to store data abroad. On this matter, each nation-state may have its data protection law to protect data and impose more strict protection standards than the US law. Regarding the interpretation of the extension of the US legislation's application, courts of justice are not free to re-write national statutes to achieve what they believe the Congress intended to say.

Microsoft does not refuse to provide the information requested by the US Court; however, the company argues that the US authorities should request it through the regular MLAT procedures. MLATs convert a foreign law request for information into a request that conforms to the domestic law requirements. In this particular case, the US government ratified a MLAT applicable to Ireland, the nation-state where the requested information is stored.

Finally, Microsoft mentions an economic argument because the company has encountered concerns in consumers abroad about the US Government extraterritorial pretensions to access their information. Potential customers have decided to hire the services of a provider based out of US territory and therefore, out of US jurisdiction.

III. Application of the Hot Pursuit: Negative Repercussions

Although no nation-state in the world can exercise sovereignty over the cyberspace, some academics argue that the principle of territorial sovereignty protects the Internet infrastructure (which is at the same time, part of the cyber infrastructure) located within a nation-state's territory. Therefore, following the rules of international law, nation-states are prohibited to interfere with the cyber infrastructure located in the territory of another State. States have a right to exercise their territorial jurisdiction over cyber activities within their territories, but not beyond.[65]

The hot pursuit principle clearly serves this principle. Although the Internet infrastructure is part of the cyberspace, a space that everyone shares, the Internet infrastructure is local and can be regulated. Accordingly, nation-states are entitled to enforce their domestic law. The pursue of any legal claim

65 von Heinegg (n. 17), 7-19.

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

cannot access the Internet infrastructure in another nation-state, without its consent. This is also the maximum of the hot pursuit.

Regarding the case, the main legal issues can be summarised as (1) what legislation is applicable, (2) what jurisdiction is the competent one, (3) what nation-state's sovereignty prevails when there is a controversy about the cyberspace. As mentioned before, there is no international treaty or international agreement that solves the problem of the 'right jurisdiction' when a data-access-issue occurs. So, how do the rules of UNCLOS work in this case, more concretely, how do the rules of the hot pursuit work in this case? From the arguments previously exposed, and as it will be explained in the following items, the application of the hot pursuit and the rules of UNCLOS calls to recognise what is known as the Internet fragmentation.

1. A Call for Nation-States: Bits under Nation-States' Sovereignty

A bit (b, short for 'binary digit') is the smallest storage unit used to quantify computer data. Bits are stored in a computer or similar device. A bit has a value, or code, of either 0 or 1, which is used to store data and implement instructions in groups of bytes.[66] In consequence: if bits are stored in a server and such server is located in a specific place in the world, are those bits subject to the sovereignty of the nation-state where the server is located? This is the main argument discussed in the *Microsoft Ireland* case.

Whether subject to applicable customary or conventional rules of international law, governments are entitled to exercise jurisdiction by subjecting objects and persons within its territory. That is their prerogative as the administrative entity of the nation-states. However, the ICJ established that this principle has a two-side-application: territorial sovereignty protects a nation-state against any form of interference by other nation-states, but the principle also imposes obligations. Nation-states are obligated to protect the rights of other nation-states within their own territories too. This includes the right to integrity and inviolability, alongside with the rights each nation-state may claim for itself and its nationals in the foreign territory.[67]

66 TechTerms, 'Bit Definition', TechTerms 2013, <http://techterms.com/>.

67 ICJ, *Corfu Channel* (n. 40), para. 43; As cited by von Heinegg (n. 17), in his Separate Opinion Judge Alvarez stated: 'By sovereignty, we understand the whole body of rights and attributes which a State possesses in its territory, to the exclusion of all other States, and also in its relations with other States. Sovereignty confers rights upon States and imposes obligations upon them.'

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

Regarding the hot pursuit principle, the first condition for its application is the suspicion of criminal activity committed within the territory under a nation-state's sovereignty. In the *Microsoft Ireland* case, the alleged criminal is located in US territory; the required data to solve the investigation is not. To access the data, nobody has to travel (physically) to Ireland for that purpose because the data is under the control of Microsoft and the company can retrieve it at will. Nevertheless, applying the rules of international law refrained the US of compelling Microsoft to retrieve the data; in application of the hot pursuit the US government pursuit stops at the very moment another nation-state territory is involved.

Nevertheless, according to section 2703(b) of SCA the disclosure of content information maintained by a remote provider is legal as long as the warrant is issued by an 'appropriate' state or federal judge. Here lays a procedural point of conflict: (1) For the US government, that judge is one based on US soil. (2) For the Irish law, it must be an Irish judge because to obtain the content of electronic mails it is required authorisation from an Irish District Court Judge.

According to the theory of the hot pursuit principle, no matter what type of criminal activity is under investigation, once the sovereignty of a different nation-state (other than the one where authorities are conducting the investigation) is involved, the pursuit must stop. The absolute end to any extraterritorial activity is the territory of another nation-state. Independently of the case, the pursuit must end as soon as the chased ship enters into the territorial sea of its nation-state or a third nation-state's territorial sea (entering into other nation's state territorial sea is the equivalent to enter into that nation-state's territory). The end of the pursuit means absolute respect to another nation-state's national sovereignty.

The *Microsoft* case was not conducted in an international court, and yet it is an example of an international controversy created by the collision of sovereignties and jurisdictions.

2. Direct Access v. MLATs: Private Actors Using Arguments of International Law

Under the application of both principles, the classic rule of international law (that requires one nation-state to protect other nation-state interests within its territory) and the hot pursuit, the US government (or any other government) can request data storage beyond its territorial borders but cannot access it directly. In this regard, the rule is clear, it is not possible to

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

access the server in another territory, even if there is no need of physical interaction with the server.

The fact that Microsoft (upon request of the US government) does not need to send people physically to retrieve the data does not change the fact that there are actions conducted within Irish territory. Such potential actions generated the Irish government protest.

To retrieve the data, the government that makes the request must follow the traditional mechanisms of communication from government to government, the traditional MLATs. The recognition of sovereignty among nation-states should be honoured by the other nation-state involved. Following the rules of UNCLOS and the hot pursuit, the US cannot access the data stored in foreign territories under the application of its national statute. As Professor Schmitt established, in terms of international law, when sovereignty is involved, 'stopping is a matter of law'.[68]

This is a constant reminder in the Microsoft argumentation, and the Second Circuit Court of Appeals backed it up. According to the Court, SCA does not authorise US Courts to issue and enforce warrants against US-based service providers to get customer e-mail content stored exclusively on foreign servers.[69]

Ironically this conclusion is aligned with those who defend the territorial sovereignty over the cyberspace to benefit their governments. For these academics and non-academics, there is an absolute principle of territorial sovereignty when the cyberspace is involved. Therefore, its infrastructure and activities are under the sovereignty of the government where that infrastructure is located. For these defenders of territorial sovereignty, nation-states are forbidden to interfere with the cyber-infrastructure located within another nation-state's territory.[70] According to this perspective, it is interesting to ask the question changing the role of the participants in the Microsoft Ireland case: Had Ireland been the nation-state interested in retrieving data stored abroad, would the US government have accepted direct access by the company that owns the server where the data is stored? Or, would the US government require Ireland to go to the long and bureaucratic MLAT process?

68 Michael Schmidt, 'International Law and Cyber Operations – Launch of the Tallinn Manual 2.0', Atlantic Council 2017, <https://www.youtube.com/watch?v=riP4kStBBJs>.

69 Stempel (n. 57).

70 von Heinegg (n. 17); Shabtai Rosenne, Essays on International Law and Practice (Leiden: Martinus Nijhoff/Brill, 2007); White House, 'International Strategy for Cyberspace', 2011, <https://www.whitehouse.gov/>.

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

3. A 'Virtual Fragmentation' with 'Practical Consequences': A Call for the Nation-States Westphalian Model

UNCLOS policy of creating fictional spaces in the sea with specific sovereign rights in favour of coastal nation-states in each space is no other thing than 'fragmenting' the ocean until all of it gets 'full' of 'juridical meaning,' an old practice of international law.[71] In this case, the juridical meaning is the allocation of sovereign rights in favour of nation-states in each space created by UNCLOS. Even international spaces ('High Seas' and 'The Zone'), where at least theoretically no nation-state has sovereign rights, have regulations that all nation-states are required to follow.

According to UNCLOS rules, there are no absolute rights in favour of nation-states. The latter remain the main actors in the international realm. In this situation, they are continually trying to use their sovereignty rights over others. Conflicts such as the South Sea in China, the Arctic, and constant claims of sea boundary delimitation are a clear example of this government practice.[72]

Different from the sea, the cyberspace is aterritorial and invisible. However, the Internet infrastructure, one of the most vital elements of the cyberspace, is not. As defined, the Internet is a global collection of networks that connect in different ways to form the single entity known as 'the Internet'.[73] At the same time, the networks that compose the Internet share a similar architecture and protocols that allow communication within and among different constituent networks. The data that travels through the Internet is broken into small pieces, called 'packets', which are transmitted to their destination by routers and servers, using the 'TCP/IP protocol' (Transmission Control Protocol/Internet Protocol).[74]

In this context, most Internet users assumed that universal connectivity would be a primary benefit. However, nation-states may decide to apply specific policies over the Internet infrastructure within their territories. When the policy decision of acting over the Internet infrastructure is political and is

71 Raul Ferrero Rebagliati, *Derecho Internacional Publico [Public International Law]* (Peru: Pontificia Universidad Católica del Perú, Facultad de Derecho y Ciencias Políticas 1962).

72 BBC, 'Why Is the South China Sea Contentious?' 2016, <http://www.bbc.com/>; Atle Staalesen, 'Conflict Over Arctic Shelf Unlikely', Barents Observer 2015, <http://barentsobserver.com/>.

73 Jeff Tyson, 'How Internet Infrastructure Works', HowStuffWorks 2017, <http://computer.howstuffworks.com/>.

74 David Clark, Thomas Berson, Herbert Lin and the National Research Council (US) (eds), *At the Nexus of Cybersecurity and Public Policy* (Washington D. C.: The National Academies Press 2014).

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

strictly in governments' hands, academics created the term 'Internet fragmentation'.[75] Fragmentation is a concept related to governments' policies and actions in the exercise of their sovereignty within their territorial borders. According to UNCLOS rules, there are no absolute rights in favour of nation-states. The latter remain the main actors in the international realm.[76] Fragmentation becomes the outcome of the collision point sovereignty and cyberspace.

It is possible to talk about Internet fragmentation when the conditions of the Internet infrastructure and government policies constrain or prevent specific uses of the Internet and do not allow interoperating and exchanging the Internet data packets consistently at all end points.[77] Governments worldwide are continually trying to exercise sovereignty rights and apply specific policies over the Internet infrastructure. These policies vary from censorship, filtering, data protection, and more drastic policies, such as the 'Internet kill switch'. These policies not only affect the Internet traffic; they are also significantly costly for the nation-states themselves.[78] Nevertheless, the fragmentation results from the basic principle of international law that governments (acting on behalf of the nation-state) exercise jurisdiction (as the application of the law) over the people and infrastructure located within the borders of their territory.

Following the tradition of governments' practices, the application of the hot pursuit into the cyberspace carries the possibility of fragmenting the Internet infrastructure alongside the territorial boundaries of national jurisdictions. Those are the basis of the hot pursuit, no matter how urgent the chase of a ship is, no matter how important it is, the chase must stop when another nation-state's sovereignty gets involved. Similar to other principles of international law, the hot pursuit and the rules of UNCLOS are built based on the strict respect of nation-states' sovereignty rights.

To some extent, the ICANN transition attempted to increase the resilience of the Internet because governments were not supposed to have control over the critical Internet resources. However, nation-states constantly try to construct borders around the Internet infrastructure to reaffirm their sovereignty one more time. When one government's actions affect another nation-state's

75 Vint Cerf, 'The Fragmentation of the Internet', *IEEE Internet Computing 20* (2016), 88-93.

76 Milton Mueller, *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace* (Hoboken: Wiley 2017).

77 William Drake, Vint Cerf and Wolfgang Kleinwachter, '*Internet Fragmentation: An Overview, EFF District Court Amicus Brief in Support of Microsoft*', World Economic Forum 2016, <https://www.weforum.org/>.

78 Darrell M. West, 'Internet Shutdowns Cost Countries $2.4 billion Last Year', Brookings Institution 2016, <https://www.brookings.edu>.

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

territory, a 'collision' of sovereignties is a possibility. The situation becomes more dangerous if nation-states decide to enforce national jurisdiction over global Internet services that happen to be incorporated in their national territories.[79] As it was mentioned before, when sovereignty and jurisdictions are involved, stopping becomes an obligation, a matter of law. In this case, consequences cannot be foreseen.

The application of UNCLOS's policy model and the hot pursuit into the cyberspace have similar negative consequences. Despite the existence of different stakeholders that do not exist in the sea, UNCLOS's policy is no other than a virtual fragmentation of the oceans. Therefore, the application of the hot pursuit carries the risk of falling into the traditional nation-states' Westphalian model, where the territorial sovereignty of nation-states is the rule and only source of law and practice.

4. More Centralised Government Control and Less of a Governance Model

Nation-states' persistent claims to apply policies over spaces beyond national jurisdictions reflect the Westphalian model that dominated the international realm until the twentieth century. Although questioned during the time of 'globalisation', now seems to be back.

The application of UNCLOS rules, the hot pursuit included, brings the possibility of a higher level of government control to the detriment of the multi-stakeholder governance model, the model that so far has kept the Internet free from a single point of control.

The multi-stakeholder model aims to bring together businesses, civil society, governments, research institutions, and non-government organisations to achieve joint decisions over the Internet infrastructure and create negotiated policies.[80]

The multi-stakeholder model was also the conceptual framework behind the negotiated ICANN transition in 2016. Today the model is under questioning after the 'renaissance' of the nation-state sovereign model and the 'failure' of the globalisation process. In any case, there is interest in the international community, represented by ICANN, that the cyberspace re-

79 Paul Fehlinger, 'Cyberspace Fragmentation: An Internet Governance Debate Beyond Infrastructure', Internet Policy Review 2014, <http://policyreview.info/>.

80 Milton Mueller, John Mathiason and Lee McKnight, 'Making Sense of Internet Governance: Defining Principles and Norms', Internet Governance Project Syracuse University – The Convergence Center 2004, <https://www.wgig.org/>.

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - CC BY-SA

mains aterritorial and free of local legislation's execution. At the same time, it could be observed that the same international community has an interest in participating in any decision about how to regulate the cyberspace.

Whether in agreement with a model based on nation-states' sovereignty or the multi-stakeholder model, it has been the latter the one who has kept the Internet free from a single point of control. To some extent, the multi-stakeholder model is one of the 'palliatives' against the Internet fragmentation and centralised government control over the Internet infrastructure. As mentioned before, this fact is important because the Internet remains the primary physical element of the cyberspace that can remain under government control, and with its limitations, the multi-stakeholder model is the one that has allowed us to keep a free Internet as we have become to know.

https://doi.org/10.17104/0044-2348-2021-3-755 https://www.inlibra.com/de/page/agb - Open Access - CC BY-SA