media LAWS
Law and Policy of the Media in a Comparative Perspective

Law and Media Working Paper Series

no. 4/2021

JACOPO BRATTA

Jurisdictional issues in cybercrimes

SUMMARY: 1. Introduction. – 2. Cybercrime's structure. – 3. General jurisdictional theories. – 4. The use of new theories. – 5. Issues and solutions. – 6. Suggestions for the development of new solutions. – 7. The Australian Scenario. – 8. Conclusion.

1. *Introduction.*

The purpose of this research paper is analysing which are the main theories that threaten the jurisdiction over cybercrime activities which take part in different countries. In particular, I believe that it is important to start the work focusing on what are the main aspects which differ cybercrimes from other criminal activities. On this point, one critical aspect related to this topic is that online crimes happen without boundaries, attacks can come from outside the borders of one State, thus scattering crime scenes through two or more countries, sometimes in more than one continent.

2. *Cybercrime's structure.*

Cybercrime has a complicated structure, which involves features specific for this field. First of all, as already reported, cybercrime is inclined to occur in several territory. For instance, the perpetrator could commit an attack settling in Italy, whereas his victims can be in France, UK or

Law and Media Working Paper Series

Codice ISSN: 2531-484X

EDITORE: Oreste Pollicino - COORDINATORE EDITORIALE: Marco Bassini

SEDE: Via Roentgen, 1 – 20136 Milano e-mail: submissions@medialaws.eu

Spain.[1] In this way, we have more than one country which is involved in the cybercrime. As it can be understood, there are few problems related to the application of the general principle of jurisdiction which are used in the resolution of "*real-world*" crimes. As first step, we must distinguish two categories of cybercrime: local cybercrime and transnational ones.[2] For the first one, there are no specific problems seeing as how the cybercrime takes place within the area of a single sovereign, that is, both the perpetrator and the victim are physically in the sovereign's territory. For this reason, there are no features which differ from a traditional crime since there is a well-defined area whereby the harm is committed. On the other hand, as regards the transnational cybercrime's field, we can have a situation where the perpetrator has the chance to commit a crime remotely. Indeed, if in a real-word crime the physical space is considered as an essential characteristic, in the cyberspace is totally irrelevant. Notwithstanding, it is useful to cite the five jurisdiction theories, which are based on the principles asserted in the general international law, in order to understand if they can be still used as tool for figure out who have jurisdiction over a cybercrime.

3. *General jurisditcional theories.*

The first theory which might be applied is the "*territoriality theory*", whereby the jurisdiction is established by taking into account the place where the offence is perpetrated. By means of this theory, the State has sovereignty within its territory, having jurisdiction upon misconducts which threaten its space.

Secondly, we have the "*nationality theory*" (also known as "*active personality theory*") which afford to establish the jurisdiction by considering the nationality of the offender. In this way, the offender's country has the possibility to exercise jurisdiction even if the individual is in a different country, taking into account his/her nationality.

The third theory, the "passive personality theory", gives the jurisdiction over a case in relation to the nationality of the victim. This principle is globally stated in several national code, such as in Article 10 of the Italian *Codice Penale*, article 113-7 of the French *Code Pénal*, Section 7 of the German *Strafgesetzbuch* and article 5 of the Portuguese *Código Penal*.

On the other hand, the "*protective theory*" (either called "*security principle*" or "*injured forum theory*") can be used when the State sees its interest in jeopardy because of an offensive action.

In the end, the last "general" theory is the "universality principle", which focus its attention on the "international character of the offence", giving the opportunity to each State to claim jurisdiction for specific offences even if those offences have no direct effect on the asserting State. Nonetheless, this theory requires two elements for assuming the jurisdiction over a specific case: 1) the State which affirms its jurisdiction over the case must have the defendant in custody and 2) the crime must be considered as offensive towards the international community (examples of offences under the international community are genocide, slave traffic, piracy as well as hijacking and torture).

After this initial presentation, it is possible to consider which are the major issues related to the jurisdiction of computer cybercrime. Indeed, as already asserted at the beginning of this work, owing to virtual and transnational characteristics, the basic principles of the traditional space found themselves in front of the peculiarities which involves computer cybercrime. First of all, the main aspects which differ traditional crimes are the lack of virtuality and unlimited expansibility, whereby these features are considered as essential aspects in computer cybercrimes. In addition, if

[1] Susan Brenner, "Cybercrime jurisdiction" (2006) *Crime Law Soc Change* 46, 189-206.
[2] Ibid.

we consider the features of the network, we find out how it is possible for offenders to perpetuate crimes through virtual spaces which can bring to negative effects in an unlimited number of countries without close contact. For instance, in the 2000 a virus was launched from the Philippines, which infected a number of countries near to twenty. As likewise reported by Brenner:

"Cyberspace and computer technology make geography irrelevant". For this reason, several consequences arose from this quotation: jurisdiction may be completely lacking, jurisdiction might exist but be impossible to assert, jurisdiction may be asserted simultaneously by more than one country. Notwithstanding, the territory is actually considered the essential factor in "determining whether a sovereign can exercise jurisdiction to prescribe law, to adjudicate claims that has been violated and to impose sanctions for violations".[3]

4. *The use of new theories*

Actually, several new theories about the criminal jurisdiction have been proposed to be applied within the cybercrime's field.[4]
For instance, we can cite the "*theory of new sovereignty*".
Called in several ways (such as "radical independent jurisdiction theory"), the main concept asserted by this theory is the forecast of a global civil society with its own form of organization which is independent from the government and have the right to self-government. The purpose of this theory is to establish an ad hoc legal system which must operate in the cyberspace sector.
Secondly, there is the "*theory of jurisdictional relativity*", developed by Professor Darrel Menthe of Stanford University.
Professor Menthe supposes the creation of a new jurisdiction for cybercrimes with specific rules which give speciality from the traditional jurisdiction. In this way: "if a citizen illegally enters the computer cyberspace and commits a crime in space, any country may exercise jurisdiction upon the perpetrator according to the laws of its own country".

Successively, among these new theories we can find the "theory of website jurisdiction". In this case, two conditions are necessary: 1) the website must be constant from both the space and the time as well, 2) it must be a link between the website space and the specific jurisdiction. Nevertheless, we should consider two different scenarios: a) if the website's owner conducts the activity within his country as well as there are not function to upload or download information, the criminal jurisdiction is entrusted to its own country; b) if we have a website where the owner sends messages with information to people who are in other countries and outside the website's country, this situation develops a relationship between the site and the jurisdiction. In this scenario, a jurisdictional conflict could arise among the countries involved because the owner might be subject to several jurisdictions.

It is important to cite the "*principle of limited jurisdiction*" as well, whereby the main word which can be used to describe this theory is "*connection*". Certainly, the point is this: if an effect or damages which are the result of a computer cybercrime are connected with citizens, only in this case the country involved has the right to have jurisdiction over the case, in accordance with its own laws.
Eventually, the last new principle developed by scholars is "*the principle of minimum contact*". The principle was stated by the United States Supreme Court, which asserted that it is requested a minimal contact between the country and the accused "*in order to meet the requirements of due process*

[3] Ibid.
[4] Xiaobing Li et al. Procedia Computer Science 131 (2018) 793-799.

provisions and fairness". The yardstick which stand behind this concept is that if, for instance, the offender is trying to be shielded by the laws of another states, the court could affirm its jurisdiction against these illegal activities. On the other hand, if there was not the interaction between the perpetrator and the correspondent because the previous one only upload information unilaterally on the website, the justice is forbidden to take action against him. Nonetheless, in a different scenario, where the accused, further than providing information and advertising, offers also services and transactions which are strictly related to the previous actions, the court could exercise jurisdiction.

In addition, taking into account an enquiry lead by Oraegbunam, we could consider other new theories which can be applied in order to find a solution for the jurisdiction problem.[5] Among these, it is remarkable to take into account the "theory of the Uploader and the Downloader", where the uploader puts material into the cyberspace whereas downloader obtains the data. From the civil and criminal point of view, the majority of actions taken by the aforementioned categories does not have any specific jurisdictional problem since a state could ban a particular website in its territory if it could be hazardous for the peace of the territory.

5. *Issues and solutions.*

As already claimed, cybercrime is more likely to transcend national borders, entailing to the commission of crimes in more than one country. If we consider the hypothesis in which more countries want to prosecute the same perpetrator who committed a cybercrime, this situation can produce a positive jurisdictional conflict, that is a "*situation in which more than one country claims jurisdiction over a perpetrator based on the same general course of conduct*".[6]

That is why it is necessary to understand which state owes priority to exercise jurisdiction over the offender. Furthermore, certainly the main problem is how to prioritize a state instead of another one, as well as on which basis assert this decision. Brenner considered that factors which should be taken into account in prioritizing claims are: place of commission of the crime, custody of the perpetrator, harm, perpetrator nationality, victim nationality, strength of the case against the perpetrator, punishment, fairness and convenience. [7]

Now, after this discussion about the main principles which underpin the regulation of the cybercrime jurisdiction, it should be important to consider what is stated in probably the most important document which consider this issue, which is the "*Convention on computer cybercrime*" stipulated by the European Council in 2001, in particular Article 22.

Article 22 says that:

1) Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:
a) in its territory; or
b) on board a ship flying the flag of that Party; or
c) on board an aircraft registered under the laws of that Party; or

---

[5] Ikenga Oraegbunam , "Towards Containing the Jurisdictional Problems in Prosecuting Cybercrimes: Case Reviews and Responses" (2016) 7 *Nnamdi Azikiwe University Journal of International Law and Jurisprudence* 28.
[6] Susan Brenner, "Cybercrime jurisdiction" (2006) Crime Law Soc Change 46, 189-206.
[7] Ibid.

d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2) Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3) Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4) This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5) When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

As it is well-explained throughout the article, the Convention considers only the territoriality and nationality theories as the principles useful to assert jurisdiction over a cybercrime.[8] From my perspective, it is interesting to consider what is stated in Paragraph 2 of article 22, which establish that States have freedom to apply, or not, the jurisdiction grounds, as it is specifically stated in letter b) to d). Nevertheless, they have the duty of action if the offence is committed under their territorial jurisdiction, as reported in letter a). In addition, paragraph 5 of article 22 concerned the positive jurisdiction conflicts (already asserted above).

For these situations, paragraph 5 establishes that parties involved in the conflict for the jurisdiction should work together for the purpose of settle the venue of prosecution. Nevertheless, there is the absence of an obligation to consult (in fact in the text is written "where appropriate"), which reduce the strength of the principle.

In this context, it is also interesting to consider that jurisdictional statutes have been released in order to regulate cybercrime. For instance, in USA several states have followed this suggestion. Thus, the Arkansas' statute establishes that a person is subject to prosecution in this state... if the transmission that constitutes the offense either originates in this state or is received in this state". In a more specific way, the Ohio's statute upon criminal jurisdiction consider that the state's jurisdiction arose when a person "*by means of a computer, computer system, computer network... causes or knowingly permits any writing, data, image, or other telecommunication to be disseminated or transmitted into this state in violation of the law of this state*".[9]

In order to understand deeply the challenges of this topic, we can mention a well- known example, the Yahoo case, which is the best case to show what are the main issues related to the jurisdiction in the cybercrime.[10] The complaint was that in the France's territory was forbidden selling or holding in public racist objects ("Nazi memorabilia") and for this reason with an order enacted by the France government, *Yahoo! Inc* and *Yahoo France* was forced to forbid to French

---

[8] Armando A. Cottim, "Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention on Cybercrime" (2010) *2 3 European Journal of Legal Studies*.

[9] Susan Brenner, "Cybercrime jurisdiction" (2006) Crime Law Soc Change 46, 189-206.

[10] Armando A. Cottim, "Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention on Cybercrime" (2010) *2 3 European Journal of Legal Studies*.

people to buying Nazi memorabilia as well as to demolish the files in their server about these products. Yahoo decided to start an action in front of the U.S District Court in San Francisco, for the purpose of being recognized that the judgement stated in France was not applicable to Yahoo in USA because in contrast with the First Amendment of US Constitution. On the other hand, the two French anti-racism associations, which acted against Yahoo were in contrast with the decision. In conclusion, the case was solved by conferring the jurisdiction over the US District Court. Probably, with the application of the principles settled in the Convention, finding a solution would have been much easier.

In addition, it is also important to underline the relevance of international cooperation in the cybercrime field.

On this point, Article 23 of the Convention on computer cybercrime entitled "*General principles relating to international co-operation*" asserts that:

"*The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence*"

Aside from the Convention on computer cybercrime, other attempts were made to develop international legal mechanism.

Among these, there is the idea of an International Criminal Tribunal for Cyberspace (ICTC), as suggested by Judge Stein Schjølberg, whereby the Tribunal "*should have jurisdiction over cybercrimes that breach international treaties and threaten critical global infrastructure*".[11] In the same way, another attempt was the Global Cyberspace Jurisdiction Project, developed by the American Bar Association, in order to "address the existing jurisdictional barriers international prosecutors face and to foster a universal harmonized effort to combat cybercrimes".[12]

In line with what already written, it is interesting to take into account two well- known case: the "*Love Bug*" virus and *United States v Gorshkov*.

The first case is a demonstration of the necessity of dual criminality as concerns cybercrimes. In fact, In the "*Love Bug*" case, the perpetrator Onel de Guzman, a computer science student, released from Philippines onto the Internet a virus which in particular affected several systems related to the United States. The issue was that owing to the act of hacking and distributing virus were not considered as a crime under the Philippines' laws, de Guzman could not be judged by the US which recognise this behave as unlawful since in the case of extradition is required that both states recognise the action as a crime.

On the other hand, as concerns *United States v Gorshkov* case, we can notice how in the cybercrime's field there is a need of international cooperation in order to apply the rules. In this case Gorshkov, a Russian citizen, was sentenced for several crimes and among these for computer crimes. The problem was that there was the lack of an extradition treaty between Russia and USA and for this reason, through a stratagem, the USA managed to entice Gorshkov in the US' territory, in particular through hacking into Russia's databases to find out information about him.

---

[11] Schjølberg, An International Criminal Tribunal for Cyberspace (ICTC) (2012).

[12] Stewart, Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdictional Issues Created by the Internet (2000)

6. *Suggestions for the development of new solutions.*

In light of these issues and others, it can be said that the Convention on Cybercrime is a good step through creating a framework for States in order to act together against cybercrime, even if it has not found a solution against the issues of international jurisdiction yet. For instance, Armando A. Cottim suggests the implementation of the Convention:

1) by taking over the sentence "where appropriate" with something that fix an obligation ("*Should the Convention create an obligation to consult – instead of merely allowing for this consultation, as it does with the current wording – this obligation would have the advantage of permitting the determination of the most appropriate venue for persecution, together with an economy of means that would help the international community in not leaving any crime unpunished*") and

2) by creating an internal mechanism which permit to the Parties' police to conduct their activities even in another Party without formal requests ("*The formal request to the other Party's authorities can be useful when dealing with apprehending people or computers. Nevertheless, in cybercrime, sometimes the investigator has to follow the path of the perpetrator of the offence and may find himself messing with a computer that is physically in a place where he does not have jurisdiction. A formal request would probably result in losing the evidence. However, an informal communication would allow the investigator to pursue the investigation in time*").

Besides, citing Cristos Velasco, it is not easy to forecast the future of cybercrime jurisdiction, but surely an important impact can be reached by improving the knowledge of the judiciary power, the development in the coordination among authorities involved in investigations, both nationally and internationally, and the possibility for national court to act against perpetrators despite of their place.[13] Actually, the objective of Velasco's work is intended to find out new ways for judicial authorities in order to create a new space where the different jurisdiction can work more freely and dynamically. For this reason, it is suggested an implementation in using other principles, instead of the principle of territoriality, as well as an improvement in the synchronisation of investigations for the purpose of create a central criminal jurisdiction which can afford to elude conflicts of jurisdictions.

Moreover, even if applying the principle of universal jurisdiction could be hazardous to national or international safety, it is actually the best way to kick out cybercrimes. In particular, by using this theory, can be deal with cases overtaking other theories, such as the boundaries of either the territorial or national jurisdiction as well as agreement among states. In addition, one suggestion may be to assert the universal jurisdiction on cybercrimes, seeing as how any unfavourable conduct in the web field could lead to shocking effects.

States should invest their energies in the diplomatic area to build a mutual assistance in criminal surveys which involve more countries. Even though the legal jurisdiction is an obstacle for cross-border criminal prosecution, everything can be easier if a nation is willing to co-operate. In this way, it might be possible to reduce the jurisdictional obstacles among states. Indeed, the realisation of an extradition process it is fundamental to build mutual assistance and confidence. As suggested by Hackett, when either the option of extradition or a diplomatic endeavour did not

[13] Cristos Velasco, "Cybercrime jurisdiction: past, present and future" in *ERA Forum Journal of the Academy of European Law*, Springer, October 2015, Volume 16, Issue 3, pp. 331-347.

bring to the resolution of the case, an option can be establishing sanctions against states which broke international rules. In this context, sanctions might be a good remedy against nations which shield cybercriminals.[14]

Another suggestion is that countries with a well-established cybersecurity system should help developing nations to reach an optimal level in their framework on

Internet security. One way might be developing the idea of an Internet safe system and provide assistance in order to be ready to help in the case of an international cybercrime prosecution. Nevertheless, the following issue must be considered: even if a group understand that part of their personal information has been stolen, it is not easy to find the proper law enforcement authority to describe the event. Therefore, it is suggested to establish a standard cyber incident-reporting tool, so that it should be an easy procedure both for consumers and businessmen. Moreover, through the use of a cybercrime-reporting tool, experts in the field of cybersecurity could earn much more information such as the technical details and the frequency of the occurrence of an incident. In addition, by these implementations could be reached important objectives in the field of computer forensic processes as well as, by the goals reached in the previous legal cases, the national governments can consider legal precedents to develop the knowledge of international cybersecurity.

Seeing as how the uncertainty that highlight the cyberspace, there are several opportunities that unlawful acts can be committed in places with limitless offenses. In fact, an aspect related to cybercrime is that criminals can fulfil assaults from one state to another and shield their anonymity as well.

Nevertheless, despite of the efforts of experts in cybersecurity, certainly the main problematic aspect is related to the barriers of jurisdiction. Scholars and policymakers have recommended to reconsider the subject of legal jurisdiction as well as the instruments to permit international cooperation. As suggested by several surveys, where there is the lack of cybercrime legislation, there is much less chance for a state to receive support against international criminal investigations.

In addition, these territories which does not want to help for the purpose of fight cybercrime, might be the perfect places for cybercriminals (as in the abovementioned "*Love Bug*" case) Therefore, the development of sanctions and encouragements are the main weapons to help the underdeveloped countries to build a cybersecurity system. By this way, either other countries can obtain advantages. By spreading this awareness the more countries that adopt the concept of cybersecurity, the greater the international cooperation to fight cybercrimes, and the harder it is for cybercriminals to hide.

7. *The Australian scenario*

Moreover, I believe that it is important to have a look to the landscape in the territory of Australia. First of all, we must consider that Australia is part of the Cybercrime Convention, which started to work in Australia on 1 March 2013 by several amendments to the Criminal Code Act 1995 (Cth). Moreover, the Australian Government created a specific plan in order to defeat cybercrime.

As reported in an explanatory memorandum regardless of the amendments to the Criminal Code Act, the Australian Government congratulates to the Convention for the efforts in

[14] Hackett, "Sanctions: America's Best New Weapon Against Cyber Crime" (2015).

introducing an international agreement to erase cybercrime. In the explanatory memorandum is established that:

"The Convention is the first international treaty on crimes committed either against or via computer networks, dealing particularly with online fraud, offences related to child pornography and unauthorised access, use or modification of data stored on computers. The Convention's main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation".[15]

On the other hand, about the jurisdictional problem, we must consider s 15.1 of the Criminal Code Act which asserts that "the Act applies if the conduct constituting the alleged offence occurs wholly outside Australia so long as the result of that conduct occurs wholly or partly in Australia or the offender is an Australian citizen". One massive problem related to international law is enforcement since up to States understand the worth of international law, its application will be restricted. As affirmed by Soukieh:

"Jurisdictional issues will continue to frustrate cybercrime investigations and prosecutions at every level, until all core stake holders begin to see international treaties, not as devaluing of sovereignty, but as pre-requisite to international trade and security".[16]

After this huge analysis through several aspects about the cybercrime issues, it might be possible to deduce some thoughts. First of all, we cannot forget to mention the distinctiveness of the cybercrime, which differ from other crimes for is multijurisdictional and multi-victim capacity. In fact, it is particularly problematic to prosecute this kind of transnational crime but the situation could be harder in the future because of the increasing in complexity. In addition, several problems also arise from the Cybercrime Convention. Indeed, key countries (such as Russia) did not ratify the Convention, obtaining the epithet of "cybercrime havens" for criminals of this field. There are several factors behind the abstention of these countries. For instance, the effort of taking part to the Convention (we can cite what it is stated in Article 37 of the Cybercrime Convention) and the fear of ratifying a tool when the States did not actively contribute in either its improvement or negotiation.

8. *Conclusion*

After all the aspects that I have analysed throughout this paper, it is time to find a conclusion for this work. As I have tried to explain, the main problem which is related to the cybercrime field is how to establish which state has jurisdiction over a criminal offence. At the beginning, some scholars thought that one way to find a solution for this issue was applying the same principles which operate in the traditional issues, such as nationality as well as territorial principle. Nevertheless, as proved in several cases (for instance, in the *Love Bug* case and in *United States v Gorshkov* case), the traditional theories seem to be inconsistent with the actual issues of jurisdiction. Indeed, several implications, such as the dual criminality of the action, cannot afford to the above-mentioned principles to operate properly. In this scenario, it is important to consider the massive work of legal scholars in order to develop new mechanisms for establishing jurisdiction over a

[15] Parliament of Australia, Explanatory Memorandum to the Cybercrime Legislation Amendment Bill 2011.
[16] Kim Soukieh, "Cybercrime – The Shifting Doctrine of Jurisdiction (2011) 10 Can LR 221-226.

complicated case. Indeed, we cannot non-mention the significant results got by some Chinese scholars who gave birth to new principles (such as the downloader and upholder principle) which are much more linked to the specific issues that affect the cybercrime field. Despite of these important steps forward, the jurisdictional issue is always a source of troubles among states for the purpose of establishing who has jurisdiction over a case.

In this context, it is significant to take into account what had been done to strengthen the cooperation among states. The main instrument at the moment is the Convention on Cybercrime, more specifically Article 22, which settled the system to find out who is the state which is nearer to have jurisdiction over the case. Nevertheless, despite of the essential impact of the Convention, even in this situation several problems arise. Among these, the main issue is: how can we solve the jurisdiction problem when one of the states involved in the case is not part of the Convention on Cybercrime?

In conclusion, the problem which is related to this topic is that everyone is aware of the problematic in cybercrime, but too little we are doing to establish concrete solutions. The cybercrime is a space in constant evolution, and we must be ready to face against new challenges. In this context, I believe that can be interesting consider the idea developed by Judge Stein Schjølberg, who deem useful to build cybercrime tribunal. The idea is trusting the power to regulate all the implications related to this problem to only one authority, in order to have a uniform judgment in the resolution of the cases.

As it is emerged from the several sources, too little has been done as well as much more should be done. The speed with which the cybercrime develops new ways to attack does not afford to be stuck in precedent solutions. Certainly, the best way to increase the solutions is raise awareness about these problems as well as the implications related to these ones. The path towards a universal solution is not as easy as it could be. In addition, we must consider the thought of States which refrain from giving power to other institutions in order to enact rules in subjects which can affect their territories.

In the end, solutions in this context has been found by States throughout the years, but this does not mean that everything has been done. New challenges always arise in relation to new ways to attack, and for this reason new solutions must be found for the purpose of being always ready against these phenomena.

***

JACOPO BRATTA – Legal Intern at The Walt Disney Company Italia and LL.M. Candidate in Law of Internet Technology at Bocconi University – jacopobratta@gmail.com

DATE OF PUBLICATION: 20 MAY 2021

ABSTRACT: *Nowadays, in an increasingly interconnected world thanks to the most important developments of the century, one question arises: who has jurisdiction in a cybercrime and/or cyber-attack? Throughout this paper, I have tried to outline the current state of the art regarding the theories that are adopted to settle disputes on the subject of jurisdiction.*
In addition, I have tried to analyse the solutions proposed by academics by outlining their actual applicability. In conclusion, a brief mention of the Australian experience and what it can teach on a continental level.

KEYWORDS: Cybersecurity – Cybercrime – Cyberterrorism – Jurisdiction – Theories