The judgment MacDermid, Inc. v. Deiter. Some remarks on personal jurisdiction on the Internet

Gabriel Ernesto Melian Pérez*

Abstract

The competent authority for settling disputes arising on the Internet, as well as the question of the applicable law, are a constant motive of uncertainty due to the cross-border nature of the Internet (Scotti, 2012). In these cases, it becomes complex for network´s users to determine which law should be obeyed or which jurisdiction responds ("contextual legal environment") (Ramírez Plascencia, 2007).

To have caused any harm within the territory is a relatively common rule on which there is a relative consensus. But the criteria for claiming jurisdiction may be broader depending on the location. In this brief analysis, I will focus on one statute from Connecticut, which states that the court where the server is located has jurisdiction to hear the case. In *MacDermid, Inc. v. Deiter*[1], this issue was contentious.

In this case, Ms. Dieter had sent confidential and unauthorized data files from her corporate email account to her personal email account. All of the events took place in Canada (from a computer in Canada to another computer in Canada). Therefore, let's see what the courts' reflections on jurisdiction were and let's analyze them briefly.

Resumen

La autoridad competente para resolver los litigios que surgen en Internet, así como la cuestión de la ley aplicable, son un motivo constante de incertidumbre debido al carácter transfronterizo de Internet (Scotti, 2012). En estos casos, resulta complejo para los usuarios de la red determinar qué

* Predoctoral fellow in the Civil Law department of the Universitat Pompeu Fabra, Barcelona. He holds a LLM in IP & IT Law from Gottingen University and a Law degree from the University of Havana. His research interests include IP & IT Law, Internet governance, and content moderation.

[1] No. 11-5388-cv (2nd Cir., Dec. 26, 2012), rev'g No. 3:11-CV-0855-WWE (D. Conn., Dec. 1, 2011).

ley debe ser obedecida o qué jurisdicción responde ("entorno jurídico contextual") (Ramírez Plascencia, 2007).

Haber causado algún daño dentro del territorio es una norma relativamente común sobre la que existe un relativo consenso. Pero los criterios para reclamar la jurisdicción pueden ser más amplios dependiendo del lugar. En este breve análisis, me centraré en un estatuto de Connecticut, que establece que el tribunal donde se encuentra el servidor es competente para conocer del caso. En el caso MacDermid, Inc. v. Deiter , esta cuestión fue controvertida.

En este caso, la Sra. Dieter había enviado archivos de datos confidenciales y no autorizados desde su cuenta de correo electrónico corporativa a su cuenta de correo electrónico personal. Todos los hechos tuvieron lugar en Canadá (desde un ordenador en Canadá a otro ordenador en Canadá). Por lo tanto, veamos cuáles fueron las reflexiones de los tribunales sobre la jurisdicción y analicémoslas brevemente.

Descriptive part.

MacDermid, Inc. is a specialty chemical company with its principal place of business in Waterbury, Connecticut. Defendant Jackie Deiter lives near Toronto in Fort Erie, Ontario, Canada, and she was employed in Canada by MacDermid's Canadian subsidiary, MacDermid Chemicals, Inc., as an account manager from May 2008 until her termination in April 2011.

The facts (not disputed) show that MacDermid stores proprietary and confidential electronic data on computer servers that it maintains in Waterbury and that employees of MacDermid Chemicals can access that information only by accessing the Waterbury servers. The record reflects that employees of MacDermid and its subsidiaries are, as a condition of employment, made aware of the housing of the companies' email system and their confidential and proprietary information in Waterbury. Deiter agreed in writing to safeguard and to properly use MacDermid's confidential information and that she was not authorized to transfer such information to a personal email account.

For reasons not relevant here, MacDermid Chemicals decided to terminate Deiter effective April 7, 2011. Deiter became aware of her impending termination and, just prior to it, forwarded from her MacDermid email account to her personal email account allegedly confidential and proprietary MacDermid data files. Deiter had to access MacDermid's Waterbury computer servers both to obtain and to email the files.

MacDermid then sued Deiter in United States District Court for the District of Connecticut, alleging unauthorized access and misuse of a computer system and misappropriation of trade secrets in violation of Conn. Gen. Stat. §§ 53a-251 and 35-51 et seq. Jurisdiction was based on diversity of citizenship and the Connecticut long-arm statute. Deiter moved pursuant to Rule 12(b)(2) to dismiss the complaint for lack of personal jurisdiction. The district court concluded that the long-arm statute did not reach Deiter's conduct and dismissed the complaint. MacDermid appealed. The appellate court reversed the judgment of the district court.

Critical part

Although the procedural rules are not the same in all jurisdictions, *a priori*, we can state that in order for a court to hear and decide on a particular case it "… *must have both subject-matter jurisdiction (jurisdiction over the type of dispute concerned*[2]*) and personal jurisdiction*" (Svantesson, 2018). The concept of personal jurisdiction refers to the power that a court has to exercise its authority over the parties in a dispute. With increasing globalization and the emergence of Internet, jurisdictional issues are facing new challenges: how to adapt these notions, usually based on well-defined geographical boundaries, to a cross-border phenomenon like the Internet.

Historically, the criteria of sovereignty and attribution of jurisdiction have been based on territorial elements. Legal systems have been created within the classic Westphalian model, under the assumption that activities are geographically located and hence territory is the ideal criterion for determining jurisdiction (Pedroza & Jiménez, 2014). The common practice has been that the location of the incident, the parties, the properties, the contracts, the torts, etc. determine the jurisdiction (Svantesson, 2018). These theories rotate around the physical concept of territory, so it is logical that complications arise when trying to apply such theories to events that occur on the Internet.

[2] This refers to the subject matter in which the court (criminal, administrative, civil, etc.), the instance (first instance, second instance, supreme court) or territory (municipal, provincial court) specializes. Subject-matter jurisdiction refers to more formal aspects, not related to the parties, but to the type of process.

With the emergence and expansion of international trade, globalization and the WWW, concepts based on eminently territorial notions are beginning to become obsolete (Svantesson, 2015). Unfortunately, even in the aforementioned reality, States continue to defend the idea that territory is the idyllic criterion for delimiting competencies and claiming jurisdiction (Ryngaert, 2015). We will examine what happened in our analysis case.

In *MacDermid, Inc. v. Deiter*, the Connecticut District Court dismissed the complaint on the grounds that Dieter had not used a computer in Connecticut and that she was not subject to jurisdiction there, however the Court of Appeal overturned the earlier decision and held that: "*While it is true that Deiter physically interacted only with computers in Canada, ... It is not material that [the defendant] was outside of Connecticut when she accessed the Waterbury servers. The statute requires only that the computer ..., not the user, be located in Connecticut… Deiter used the Connecticut servers and because the servers are computers under the long-arm statute, we conclude that Deiter used a computer in Connecticut and that the Connecticut district court had long-arm jurisdiction*". A really interesting case, because both courts applied the long-arm statute[3], in the first instance to deny jurisdiction and on appeal, to assume it (Almy, 2013). However, at this point, I will anticipate that I agree with the decision made by the judges in the Second District, for the reasons I will briefly explain.

The court of appeals applied Connecticut's personal jurisdiction rules. According to this: CONN. GEN. STAT. § 52–59b(a)(5), *"**Jurisdiction of courts over nonresident individuals:** (a) A court may exercise personal jurisdiction over any nonresident individual ... who in person or through an agent: (5) **uses a computer**, as defined in subdivision (1) of subsection (a) of section 53-451, or a computer network, as defined in subdivision (3) of subsection (a) of said section, located within the state."* In other words, in principle, anyone who uses a computer in the state of Connecticut will be subject to its jurisdiction. At this point I think anyone can imagine the important consequences of having a rule of this kind and the very broad powers it gives the court to hear and decide a case. However, later on

[3] A long-arm statute is a statute that allows for a court to obtain personal jurisdiction over an out-of-state defendant on the basis of certain acts committed by an out-of-state defendant, provided that the defendant has a sufficient connection with the state. (https://www.law.cornell.edu/wex/long-arm_statute)

we will analyze why this allegedly very broad jurisdictional rule is not so broad when the American judicial machinery starts to operate.

Let's start by saying that the concept of “computer” referred to in the rule § 52–59b(a)(5)[4], comes from the State Computer Crime Statute[5]. From the reading of the mentioned “computer” concept, I can appreciate that its formulation is quite wide, whose aim is not to include only desktop computers, but all kind of storage devices, including servers. In this respect, Ms. Dieter actually “used” the server to send the information, because the transmitted data was stored inside the server in Connecticut. And here, around the concept of "computer use", lies the difference between the decisions of the District Court and the Second Circuit. The first instance decided that it had no personal jurisdiction because the aforementioned § 52-59b(a)(5) rule had not been met, since Ms. Dieter “had not used” the server[6]. The second circuit court considered the opposite. At this point, what would it be “to use a server”? The second circuit court determined that Ms. Dieter had “used” a computer in Connecticut, even though such use was “remote”[7].

The Second Circuit Court's interpretation in this case seems to me to be correct. We should consider that the broad definition of "computer" in the rules § 53-451(a)(1) and § 52-59b(a)(5) used by the court are intended to combat acts of cybercrime committed outside the territory of the State. A

[4] “*An electronic .... device ... that, pursuant to ... human instruction ... can automatically perform computer operations with ... computer data and can communicate the results to another computer or to a person [or is a] connected or directly related device ... that enables the computer to store, retrieve or communicate ... computer data ... to or from a person, another computer or another device.*”

[5] CONN. GEN. STAT. § 53-451(a)(1) (2012)

[6] *“That the information was originally obtained over the internet from a network of computers in Connecticut does not mean that the defendant used a computer network located within the state, as defined in [the computer crimes statute] ....”*

[7] *“It is not material that Deiter was outside of Connecticut when she accessed the Waterbury servers. The statute requires only that the computer or network, not the user, be located in Connecticut. The statute reaches persons outside the state who remotely access computers within the state... Extending the statute to reach a nonresident who committed any of the above activities while present in Connecticut would not have been necessary because that person would already have been subject to jurisdiction under § 52-59b(a)(2). Further, it cannot be said that Deiter’s conduct is covered by § 52-59b(a)(3) because she is not alleged to have regularly conducted business in Connecticut, or to have derived revenue from her conduct.”* I must add my personal opinion that this rule § 52-59b(a)(3) is too closely linked to commercial requirements, and that the harmful acts caused in a jurisdiction do not necessarily have to be for commercial or monetary purposes. Had this article been drafted differently, it might have been possible to use it in this case. My disagreement is with the formulation of the rule, but the court's reasoning seems to me to be correct.

reasoning such as that of the District Court in the first instance would leave unpunished acts that take place outside the territory of that jurisdiction.

However, would anyone using a Connecticut server be subject to this jurisdiction? Wouldn't this be an excessive claim of jurisdiction? If we look at § 52-59b(a)(5) in isolation, I would say it is excessive. It is already difficult to know under which jurisdiction the acts that people perform on the Internet fall, since such acts can impact on multiple territories. Now, to this, we should add that the person must take into account *also* in which server such information is being stored or which servers are being used to perform the act on the Internet. Nevertheless, jurisdiction in the United States is not exercised in this way and even if the requirements of § 52-59b(a)(5) are met, the court must still conduct extra reasoning and this case is a perfect example to illustrate that process.

Having established that the exercise of jurisdiction was legitimate as explained before, the Second District Court moved on to the second criterion for analyzing personal jurisdiction: whether there was "minimal contact" with the state of Connecticut to justify due process, using the historical judgment *International shoe vs Washington*[8]. Additionally, the court used the Calder test[9], which requires a certain degree of intentionality and knowledge of the scope of its acts on the part of the defendant, and found that Ms. Dieter had at least directed allegedly tortious conduct toward a Connecticut corporation. In this case, Ms. Deiter knew that the information was on the Connecticut server because it was mentioned in her contract. She could not claim ignorance, as someone else would in a similar case. The third step was the court's consideration of whether the use of personal jurisdiction for this case would be fair and reasonable. The court determined that MacDermid, Inc. and the State of Connecticut both had an interest in having the dispute settled there. I understand McDermid's interest, being the injured party, however the State's interest is not very clear to me, which would be in my opinion the only weakness of this Second Circuit judgment.

I would like to emphasize at this point the importance of the sentence analyzed and mainly the use of all these jurisprudential criteria such as the "minimum contacts" and Calder's test to limit as much

[8] *"[D]ue process requires only that in order to subject a defendant to a judgment in personam, if he be not present within the territory of the forum, he have certain* ***minimum contacts*** *with it such that the maintenance of the suit does not offend "traditional notions of fair play and substantial justice*." 326 U.S. 310 (1945)

[9] It has its origin in *Calder v. Jones* judgment 465 U.S. 783 (1984). Calder's model, also called the "effects test", is based on the effects caused intentionally within the place where the court exercises jurisdiction, by the defendant's behavior outside that territory.

as possible the excessive claims of jurisdiction on the Internet. This decision shows how a procedural rule that establishes the rules of personal jurisdiction can clearly be excessive, but there is a set of judicial principles that are used to adapt its application to fairer and more reasonable standards. Based on these principles, not everyone within § 52-59b(a)(5) will be subject to Connecticut's jurisdiction. The court will always have to consider other requirements such as that person's required minimum contacts with the forum and the degree of intentionality of their action. This would eliminate the possibility of claims to jurisdiction without reasonable cause or a sufficiently close connection between the parties and the territory in question.

Almy, R. (2013). Personal Jurisdiction in the Data Age: MacDermid v. Deiter's Adaptation of International Shoe Amidst Supreme Court Uncertainty. *Me. L. Rev., 66*, 327.

Pedroza, I. S., & Jiménez, W. G. (2014). ¿ Cómo establecer la jurisdicción y competencia en casos de internet? *Diálogos de saberes*(41), 15-32.

Ramírez Plascencia, D. (2007). Conflicto de leyes y censura en internet: el caso Yahoo! *Comunicación y sociedad*(8), 155-178.

Ryngaert, C. (2015). The concept of jurisdiction in international law. In *Research Handbook on Jurisdiction and Immunities in International Law*: Edward Elgar Publishing.

Scotti, L. (2012). Internet y derecho internacional privado: retos y desafíos en la era posmoderna. In ALBREMÁTICA (Ed.), Derechos del consumidor y comercio electrónico en el ámbito internacional (pp. 12 – 35). Buenos Aires: Biblioteca jurídica on line Eldial.

Svantesson, D. (2015). A new jurisprudential framework for jurisdiction: Beyond the Harvard draft. *American Journal of International Law Unbound, 109*, 69-74.

Svantesson, D. (2018). Jurisdictional issues and the internet–a brief overview 2.0. *Computer Law & Security Review, 34*(4), 715-722.