ERA Forum (2015) 16:331–347
DOI 10.1007/s12027-015-0379-y

ARTICLE

Cybercrime jurisdiction: past, present and future

Cristos Velasco[1]

Published online: 24 June 2015

Abstract This article describes activities and policies which have been put into place to date in order to deal with aspects related to cross-border access to computer data and cybercrime jurisdiction. It includes an analysis of the European instruments that address the issue of cybercrime jurisdiction; a perspective on the role of Internet Service Providers in facilitating cooperation to law enforcement for the adjudication of jurisdiction to prosecute cases in national courts. The article addresses some of the current international discussions and possible future scenarios and ends with a personal view and assessment of alternative approaches for asserting jurisdiction for the prosecution of internet-related crime.

Keywords Cybercrime · Jurisdiction · Cross-Border Access · International Cooperation · Extraterritoriality · Mutual Legal Assistance

1 Introduction

When the widespread use of computers and internet began in the mid-nineties, one of the major constraints among government, industry and academic circles was the difficulty of applying laws and regulatory frameworks to illegal activity committed

✉ Dr. C. Velasco, Founder and Director
cristosuofa@yahoo.com

[1] Ciberdelincuencia.org, Arndtstr. 21, 68259, Mannheim, Germany

through cyberspace which had real effects and repercussions on individuals who were physically located in the same or different countries.[1]

The jurisdictional aspects of the internet have evolved more rapidly in countries with common law systems, where the national courts have relied on the doctrine of *stare decisis* and legal precedent and the application of traditional tests and standards for exercising and asserting personal jurisdiction based on the doctrine of minimum contacts and real and substantial connection with the forum[2]; on the effects or harm test doctrine[3] or simply based on how *passively*[4] or *actively*[5] a website perform when targeting specific individuals in a certain state or territory.

Internet jurisdiction is at the intersection of different areas of law including criminal law and some courts around the world have issued landmark rulings involving the use of internet in which they have tried to resolve conflicts of jurisdiction when the offender was located in its territory or based in the location where the act was perpetrated or in the location of the computer system or of the servers or when one of its nationals has committed the offence when residing in another country or simply where the damage or effect was produced.[6] For instance, in the United Sates, the case *US v. Aleksey Vladimirovic Ivanov*,[7] *Yahoo Inc. v, LICRA*,[8] in Australia, *Gutnick vs.*

[1] For a broad discussion and for views on internet law and jurisdiction, see: *Goldsmith* [4].

[2] See *International Shoe Co. v. Washington*, 326 U.S. 310, 66 S. Ct. 154, 90 L. Ed. 95 [1945], a landmark decision of the United States Supreme Court which had relevant consequences for corporations involved in intrastate commerce and that resolved that a corporation might be subject to the jurisdiction of a state court if it has "minimum contacts" with the State.

[3] See *Calder v. Jones*, 465 U.S. 783, 790 [1984]. Under this case, the United States Supreme Court resolved that a defendant must: (i) commit an intentional act that is (ii) expressly aimed at the forum state that (iii) causes harm that the defendant knows is likely to suffered in the forum state.

[4] See *Zippo Mfg. Co. v. Zippo Dot Com, Inc*., 952 F. Supp. 1119 [W.D. Pa. 1997]. The court resolved that a passive website was insufficient to establish personal jurisdiction but an interactive site through which a defendant conducts business with the forum residents such as Zippo Dot Com's was sufficient to establish personal jurisdiction.

[5] See *Cybersell Inc v. Cybersell Inc*. 130 F.3d 414 [9th Cir. 1997] was a trademark infringement case dealing with the use of a internet service mark in a website. The United States Court of Appeals for the Ninth Circuit found that the use of a website name was passive and did not constitute commercial activity within the state and that the company had not purposefully availed itself such that it could expect to be subject to the state court's jurisdiction.

[6] For an overview on approaches to cybercrime jurisdiction and the principles and factors determining positive and negative claims on jurisdiction in different countries, see: *Brenner* [2], available in the Social Science Research Network at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=786507.

[7] This case of December 2011 dealt primarily with illicit access to computer systems, email accounts and stolen access credentials and credit card numbers subsequently used by Russian hackers to commit fraud and extortion against Pay-Pal and e-Bay users. Ivanov was finally indicted for charges of computer fraud, conspiracy and extortion and possession of illegal access devices and was sentenced to 48 months in prison followed by 3 months of supervised release. Ivanov was prosecuted and convicted in five District Courts in the United States—more than any other case listed on the United States Department of Justice listing of computer crimes. See United States Department of Justice press release of July 25, 2003 at: http://www.justice.gov/criminal/cybercrime/press-releases/2003/ivanovSent.htm.

[8] *Yahoo! Inc. v. La Ligue Contre Le Racisme et l'antisemitisme* (*LICRA*) 433 F.3d 1199 [9th Cir. 2006]. This is perhaps the most well known case since it involves aspects of content liability of Internet Service Providers, freedom of expression as well as the legality of the execution of foreign judgments in the United Sates and France. In this case dating from 2000, two civil organisations decided to sue Yahoo in France, for having found Nazi propaganda, memorabilia and objects available for purchase in the Yahoo French

Down Jones & Co. Inc[9]; in Philippines the *I Love You* prosecution[10]; and in Germany the *Frederick Töben* conviction[11] are just a few examples of cases with a transnational dimension which involved criminal conduct and cross-border internet jurisdiction.

Despite multiple efforts among law enforcement authorities in different countries, jurisdictional issues and the enforcement of laws against cybercrime continue to present the greatest of challenges particularly when the countries involved have no substantive or procedural laws against cybercrime, insufficient technical expertise in the investigation or lack the required infrastructure and financial capacity to conduct and follow-up an investigation of such complexity with the country or countries involved.

website. The Court of First Instance (Tribunal Grande Instance) decided to investigate these matters and asserted jurisdiction over Yahoo since it found there were sufficient links and connections with the French territory and mainly because the memorabilia and objects were available to residents located in France in contravention of the French Criminal Code. The French Tribunal ordered Yahoo to restrict access to such content and resolved to impose a monetary fine. Yahoo challenged the award of the French court in the District Court of the State of California arguing that the prohibition and restrictions imposed by the French Tribunal infringed the right of freedom of expression under the First Amendment of the Constitution of the United States and resolved in favour of Yahoo United States leaving without legal effect the French award, which was subsequently appealed by the French organisations in the United States Court of Appeals of the Ninth Circuit in 2006. The United States Supreme Court of Justice declined to hear and attract this case. For an academic perspective on this case, see: *Reidenberg* [7], available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=267148.

[9] A case of defamation on the internet brought by an Australian entrepreneur Joseph Gutnick against the American media company Dow Jones & Co. for having published an article in its Barrons Online Magazine that purportedly attributed to him fraud, tax evasion and involvement in money laundering activities in Australia. Gutnick sued Dow Jones in his place of residence in Victoria, alleging that the article published damaged his reputation in that territory and also due to the fact that Australian residents had access to the publication in Victoria even though the company was based in New Jersey. The case was finally settled on 15 November 2004. The full text of the judgment and the case history is available at: http://en.wikipedia.org/wiki/Dow_Jones_%26_Co._Inc._v_Gutnick. For an analysis of the case decision, see: *Garnett* [3], available at: http://www.law.unimelb.edu.au/files/dmfile/downloade52f1.pdf.

[10] The *I Love You* letter was a computer virus which was spread through an email attachment and which affected millions of personal computers and systems around the world in May 2000. The virus was created and disseminated by two computer programmers from the Philippines who were traced by the authorities and counterparts in that country. Since the Philippines did not have a law to punish crimes against the creation and dissemination of viruses at that time, the authorities in that country dropped all the charges against the offenders and they were not criminally prosecuted. This case took a relevant dimension when the United States Department of Justice got involved in the investigation and tried to cooperate in the prosecution and extradition of the offenders to the United States, however such efforts were meaningless precisely because of the principle and requirement of dual criminality, which requires that extradition may be allowed only when the legislation of both countries provides for a specific sanction and punishment, which was not the case in the Philippines. For further information and a synthesis of the judgment of this case, see: *Sy* [10].

[11] This was one of the first cases in Germany that widely touched criminal jurisdictional aspects and internet racism and xenophobia speech in Germany and Australia. In 1999, Frederick Töben, a German citizen with Australian nationality and former director of the Adelaide Institute created and disseminated content and materials in its website vilifying Jewish people and denying the Nazi holocaust occurred during the Second World War. As a result of this conduct, he served two sentences, one in Germany for defaming the dead and breaching Germany's holocaust law and the other in Australia for breaching a court order that ordered him to refrain from publishing materials on his website vilifying the Jewish community, see *Velasco* [12], pp. 248–250.

Another major problem is that law enforcement authorities and the judiciary in some countries do not have the required knowledge of the subject or receive continuous training in the field of preservation and use of digital evidence, technologies and forensic tools in order to track down criminal conduct, situations which make it even more difficult to launch an investigation and prosecute offenders on a coordinated basis.

Another major problem is that some countries may have priorities regarding the types of cybercrime they can investigate and prosecute, so that, for instance, many countries would probably decide to prosecute serious crimes or attacks seeking to damage critical national infrastructure, attacks against national security and child pornography, while some other countries might not necessarily have priorities to investigate crimes directed against the general population like financial and credit card fraud committed through phishing or identity theft techniques, extortion or attack against personal computers and devices.

The purpose of this article is first, to offer an overview of the issues involved in the past, particularly by European institutions to address cross-border jurisdictional concerns regarding cybercrime. Secondly, it is intended to examine and assess whether the current European legal instruments for investigating and prosecuting computer- and internet-related crime continue to be effective considering the evolution and sophistication of cybercrime, the volatility of electronic evidence and the current storage and preservation media, taking into account other factors that play an important role for a court in deciding whether to assert jurisdiction, such as the cooperation of internet and access service providers with investigative authorities. Thirdly, it is intended to offer a perspective on the future discussions and topics surrounding cybercrime jurisdiction. I end this article by offering a personal perspective regarding possible alternatives for approaching cybercrime jurisdictional issues on a more proactive basis.

2 The past

The fast development of information technologies and the growth of the use of computer, networks and the internet particularly in European countries during the decade of the nineties, led the European Committee on Crime Problems to set up a committee of experts in November 1996 specifically to deal with cybercrime. This Committee was subsequently named the Committee of Experts on Crime in Cyber-space (PC-CY) by a decision of the Committee of Ministers. The PC-CY was the original group that undertook the negotiations to draft the Council of Europe Convention against Cybercrime (hereinafter *"Budapest Convention"*) until its adoption and opening for signature in June 2001.[12]

Among the main tasks and issues analysed by the PC-CY were the question of jurisdictional approaches to offences committed through computer systems and information technologies, studying and considering aspects of conflicts of laws (both

[12] See *Explanatory Report of the Convention on Cybercrime*, paragraphs 7–11.

positive and negative), and international principles on jurisdiction during the drafting of the Budapest Convention.[13]

Even before the adoption of the Budapest Convention, a large number of European countries have incorporated international principles on jurisdiction in their constitutions and some others even have procedural legislation on criminal matters offering guidance on how to approach the issue of jurisdiction when two or more countries are involved.[14] In practice, the approaches on asserting jurisdiction differ significantly between countries since it is up to the judiciary and national courts to decide on the precise circumstances of each case presented for a corresponding prosecution (on the basis of territory, nationality or damage to the victims); whether the court should or not prosecute the offender in its territory or to negotiate and consult with other countries the adjudication of jurisdiction and possible scenarios on extradition.

2.1 Cross-border access to computer data

Another task that was the subject of lengthy discussions by the PC-CY was whether a country should be allowed unilaterally to access computer data in another country without the consent and mutual legal assistance of another country. The drafters of the Budapest Convention determined that it was not possible to prepare a comprehensive, legally binding regime regulating cross-border access to data mainly due to the lack of concrete examples and experience with such situations at that time, and the group agreed not to regulate other situations until further experience and practice had been gathered and obtained by a number of countries.[15]

It should be noted that during the period of work of the former European Committee on Crime Problems and the work of the PC-CY, a number of international convention were simultaneously being drafted by the United Nations, such as for instance the Convention against Transnational Organised Crime which contains specific provisions on jurisdiction,[16] which together with international general principles on jurisdiction served as the basis for drafting the scope of Article 22 of the Budapest Convention.[17]

However, with regard to issues of cross-border access to computer data dealt with in Article 32 of the Budapest Convention,[18] there was no international legal source of reference and practice. This was the main reason for the PC-CY's decision not to

[13] See *Explanatory Report of the Convention on Cybercrime*, paragraph 11 v.

[14] See for instance Sections 3 to 9 of the *German Criminal Code*; Articles 6, 7, 9 and 10 of the *Italian Criminal Code*; Articles 4 to 7 of the *Portuguese Criminal Code* and Article 27 of *Portugal's Cybercrime Law nr. 109/2009* and Article 23 of *Spain's Organic Law for the Judicial Power*.

[15] See *Explanatory Report of the Convention on Cybercrime*, paragraphs 293–294.

[16] See Articles 11 and 15.

[17] For an explanation of the scope of Article 22 of the Budapest Convention see: *Velasco* [10].

[18] Article 32 of the Budapest Convention reads as follows: "Article 32—Trans-border access to stored computer data with consent or where publicly available". A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

formulate general rules and regulate situations other than where unilateral access to data was permissible.

In the course of 1999, the former G-8 High-Tech Subgroup of Senior Experts on Transnational Organised Crime discussed the question of unilateral access by law enforcement authorities in one state to data stored in a computer system in a foreign state without the need for mutual legal assistance, and this subgroup approved a document containing principles and guidelines to accessing data in a foreign state during a Ministerial Conference on Combating Transnational Organised Crime in Moscow in November 1999.[19]

The first section of the G-8 principles, which deals with preservation of data stored in computer systems, allows LEAs to secure the preservation of data stored in computer systems and ensures that such preservation is possible through the cooperation of internet service providers and through state requests for the preservation of data contained in the computer systems of another state on an expedited basis and pursuant to national law. The second section of the G-8 principles deals with expedited mutual legal assistance to preserve data through traditional legal procedures, judicial and legal authorisations and through other methods of assistance provided by the law of the requested state. This principle includes the rule that each state should respond to the request on an expedited basis and using communications such as voice, fax or e mail. The third section specifically deals with cross-border access to stored data not requiring legal assistance, which stipulates that a state may not need authorisation from another state when accessing publicly available data regardless of its geographical location; or when accessing, searching, copying or seizing data stored in a computer systems located in other state when the voluntary consent of a person who has lawful authority to disclose the data has been given. The last section provides for the consideration of the searching state to notify the searched state when data reveals a violation of criminal law or when it appears to be in the interest of the state in which the search is carried out.[20]

3 The present

Currently, there are a number of international and regional instruments that address the question of jurisdiction in respect of crimes committed through the use of computers and internet. Most of these instruments are Council of Europe conventions,

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system."

[19]The former G-8 agreed that the principles should be implemented through treaties, national laws and policies and should apply when law enforcement agencies investigate criminal matters and require cross-border access to, copying of, or search and seizure of electronic data. The relevant document is available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/24%208%20Principles%20on%20Transborder%20Access%20to%20Stored%20Computer%20Data_en.pdf.

[20]For a perspective of the G-8 principles on Cross-Border Access, see *Putnam* [6].

council framework decisions and directives containing specific provisions and guidelines on dealing and approaching jurisdictional issues when more than two countries are involved in criminal investigations.

Among some of the instruments of the Council of Europe providing guidance on the question on jurisdiction on crimes committed through the use of computers and internet are: (i) the Budapest Convention;[21] (ii) the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (better known as the Lanzarote Convention);[22] the Council of Europe Convention on Action against Trafficking in Human Beings;[23] and the Council of Europe Convention on the Prevention of Terrorism.[24] These instruments contain *inter alia* provisions on jurisdiction allowing national courts of Member States to assert jurisdiction over criminal offences committed: (i) on that Member State's territory; (ii) on board ships and aircrafts registered under the laws of a state; (iii) by one of a state's nationals when the offence is committed outside the territorial jurisdiction of any state; as well as (iv) provisions to prosecute in the case of denial of extradition and (v) consultations mechanisms to determine and coordinate actions for prosecution and the avoidance of parallel proceedings.

In addition to the Council of Europe instruments, there are three Council Framework Decisions, the purpose of which is to unify national legal frameworks and strengthen judicial cooperative measures across the European Union. These also contain provisions on the adjudication of jurisdiction. Said Council Framework Decisions are the following:

I. *Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings;*[25]
II. *Council Framework Decision 2008/913/JAA of 28 November 2008 on combating certain forms of racism and xenophobia by means of criminal law*;[26] and

[21] See Article 22.

[22] See Article 25.

[23] See Article 31.

[24] See Article 14.

[25] Articles 2 and 10 set out the conditions for establishing consultations between competent authorities conducting parallel criminal proceedings in the European Union in order to avoid positive conflicts of jurisdiction. Article 12 stipulates that when States are not able to reach consensus, the matter shall be referred to *Eurojust* by any competent authority of the Member States involved.

[26] Article 9 contains a provision on the assertion of jurisdiction in relation to offences concerning racism and xenophobia, instigation, aiding and abetting where the conduct has been committed: (i) in whole or in part within its territory; (ii) by one of its nationals; (iii) for the benefit of a legal person that has its head office in the territory of a Member State. When a Member State establishes jurisdiction based on territory, each Member Sate shall take the necessary measures in order to ensure that its jurisdiction extends to conduct committed through an information system and (a) the offender commits the conduct when physically present in its territory, whether or not the conduct involves material hosted on an information system in its territory; and (b) the conduct involves material hosted on an information system in its territory, whether or not the offender commits the conduct when physically present in its territory. Section 3 of this provision offers Member States the possibility of applying or not applying the jurisdiction rule when committed by one of its nationals or for the benefit of an entity with a head office in the territory of a Member State.

III. *Council Framework Decision 2002/475/JAI of 13 June 2002 on combating terrorism.*[27]

One relevant aspect of Council Framework Decision *2002/475/JAI of 13 June 2002 on combating terrorism* is that it seeks to centralise criminal proceedings in a single state, an objective which is highly important in order to avoid multiple investigations and positive jurisdictional conflicts among Member States.

In addition to the Council Framework Decisions, there are two European Union Directives that have recently replaced the Council Framework Decision on attacks against information systems as well as the Council Framework Decision on combating sexual abuse and child pornography. These instruments are:

I. *Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/*JHA. This instrument contains a provision[28] on the assertion of jurisdiction in relation to offences concerning illegal access to information systems, system interference, data interference, illegal interception, tools used for committing offences, incitement, aiding and abetting and attempt when: (i) the offence is committed in whole or in part of their territory; (ii) by one of their nationals. Section 2 provides that when a state decides to assert jurisdiction based on territory, that state shall ensure that (a) the offender committed the offence physically present on its territory whether or not the offence is against an information system on its territory; or (b) the offence is against an information system on its territory whether or not the offender commits the offence while physically present in its territory. Section 3 of Article 12 sets out the obligation on a Member State to inform the Commission when it decides to establish jurisdiction over an offence committed outside its territory including the fact that (a) the offender has his habitual residence in its territory; (b) the offence is committed for the benefit of a legal person establish in its territory.

II. *Directive 2011/92/of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA*. This instrument contains a provision[29] on the assertion by a Member State of jurisdiction and on the coordination of prosecution in relation

[27] Article 9 contains a provision on jurisdiction and prosecution in relation to offences concerning terrorist activities (including inciting, aiding, abetting and attempting such offences) when: (i) the offence is committed in its territory; (ii) if the offence is committed on a ship or aircraft registered or waving a national flag; (iii) if the offender is one of its national or residents; (iv) if the offence is committed for the benefit of a legal person established in its territory; (v) if the offence is committed against institutions or people of a Member State or of the European Union. Section 2 of this article establishes that when the offence falls within the jurisdiction of more than one Member State, they shall cooperate in order to decide the prosecution of offenders with the aim of centralising proceedings in a single Member State and facilitate cooperation between their judicial authorities and coordination of their action and taking into considerations the following factors: (a) the territory where the acts were committed; (b) the nationality or residence of the perpetrator; (c) the origin of the victims; (d) the territory where the perpetrator was found. Section 3 sets for the measure to establish jurisdiction in case of a refusal to hand over or extradite a suspected or convicted individual to another Member State or to a third country. Section 4 allows Member Sates to establish jurisdiction in its territory regardless of the location of the terrorist group or where they conduct its criminal activities. Section 4 stipulates the non-exclusion of the exercise of jurisdiction in criminal matters in accordance with its national legislation.

[28] See Article 12. The transposition deadline for European Union Member States is September 4, 2015.

[29] See Article 17. The transposition deadline for European Union Member States was December 18, 2013.

to offences concerning sexual abuse, sexual exploitation, child pornography, solicitation of children for sexual purposes, incitement, aiding and abetting and attempt when: (i) the offence is committed in that Member State's territory; and (ii) the offender is one of its nationals. A Member State is obliged to inform the Commission when it decides to establish jurisdiction over an offence committed outside of its territory where: (a) the offence is committed against one of its nationals or against a person who is an habitual resident in its territory; (b) the offence is committed for the benefit of a legal person established in its territory; or (c) the offender is an habitual resident in its territory. Section 3 of Article 17 allows a Member State to assert jurisdiction when the offence is committed by means of information and communication technology accessed from its territory whether or not the offence occurred on its territory.

Section 4 provides that for the prosecution of offences committed outside the territory of a Member State and when the offender is one of its nationals, each Member State shall take the necessary measures so that its jurisdiction is not subordinated and conditioned to criminal offence acts committed at the place where they were executed. Likewise, Section 5 provides that for the prosecution of offences committed outside the territory of a Member State and when the offender is one of its nationals, each Member State shall take necessary measures so that its jurisdiction is not subordinated and conditioned so that the prosecution can only be initiated following a report made by the victim or a denunciation from the state of the place where the offence was committed.

One common feature of these Directives is that they establish specific rules for the assertion of jurisdiction for extraterritorial crimes committed outside European Union Member States when the offender is one of the relevant Member State's nationals. However, Directive 2011/92/ of 13 December 2011 goes a step further and expressly includes, as a requirement for the subordination of jurisdiction and the prosecution of offenders, a denunciation report made by the victim or a denunciation from the Sate of the place where the offence was committed, situations that are a necessary preconditions for the prosecution of offenders across the European Union.

The legal framework in Europe concerning the assertion of jurisdiction in respect of crimes committed against computer systems and attacks using the internet is perhaps one of the most comprehensive. Although it seeks to unify the national approaches on the assertion of jurisdiction for the prosecution of cybercrime in this region of the world, the reality is that there is not yet complete uniformity among the approaches adopted by each of the European Union Member States. National courts of European Union Member States continue to apply discretionary powers under national procedural criminal laws in order to prosecute crimes according to their own methodologies and legal traditions for cases dealing with internet crime or crimes committed using the support of information technologies.

3.1 Cooperation of communication and internet service providers with law enforcement

Another important factor for the assertion of jurisdiction over criminal proceedings is the preliminary identification and location of the offender or perpetrator of a crime

through the cooperation of internet and access service providers with law enforcement authorities with or without mutual legal assistance instruments.[30] The information and evidence facilitated by internet service providers plays a crucial role in the subsequent determination of a national court to assert jurisdiction and prosecute cybercriminals.

It should be borne in mind that a large part of the evidence needed in criminal proceedings is hosted and preserved in different servers located or hosted in the cloud by Internet companies like Yahoo, Google, Microsoft and Skype and social network companies like Facebook and Twitter, which have established their own methodologies, criteria and cooperation procedures in order to disclose information and data to law enforcement authorities for the identification of possible suspects.[31]

Unfortunately, there are only very few public documented cases where internet and access service providers have facilitated cooperation with law enforcement authorities for the purposes of the subsequent assertion of jurisdiction in cases brought to the attention of national courts and for the purposes of dealing with investigations related to cybercrime.[32] One example of a European country seeking clarification on the cooperation approach taken by internet service providers with law enforcement authorities for the identification of suspects and legal assistance on criminal investigations dealing with the use of internet is Belgium.

3.1.1 Belgium v. Yahoo, Inc.

In November 2007, the Public Prosecutor of Dendermonde in Belgium brought a direct order—without mutual legal assistance—against Yahoo, Inc. in accordance with Art. 46bis of the Code of Criminal Procedure[33] in order to obtain information linked to seven Yahoo e-mail accounts which had been used to commit and execute computer fraud and internet forgery affecting residents established in Belgium as described in Articles 496, 504 quater and 210 bis of the Criminal Code of Belgium.

The Public Prosecutor argued in his claim that the e-mail accounts in question were used within the Belgian national territory and that although Yahoo is a company legally established in the state of California, Yahoo should also be considered to have a presence within the Belgian national territory, both as a commercial company and as an electronic communication service operator through the internet. Among the data

[30] For a perspective on the use of international mutual legal assistance procedures and mechanisms in criminal investigations, see: *Velasco* [11], pp. 283–287 and United Nations Office on Drugs and Crimes (UNODC), *"Comprehensive Study on Cybercrime"*, United Nations, pp. 185–187 (February 2013).

[31] For a comparative analysis and perspective on the current procedures, guidelines, policies and terms to request legal assistance in criminal proceedings between law enforcement authorities and internet service providers, see: *O'Reily* [5].

[32] Currently, there is no official source of information or initiative in the European Union offering a compilation of cases or at least a synthesis of judgments and investigation dealing with cybercrime.

[33] Article 46 §2 of the *Belgian Code of Criminal Procedure* establishes that any operator of a telecommunications network and any provider of a telecommunications service within the Belgian national territory that may be ordered to communicate the above requested data, is to provide the data that were requested to the Public Prosecutor or the officer of the criminal investigation department. A refusal to communicate the data may be sanctioned with a pecuniary penalty from 143.00 EUR up to 55,000.00 EUR.

that the Public Prosecutor was requesting from Yahoo were (i) the full identification/registration data of the person who created and registered the account, including the IP address, date and time (+time zone) of the registration, (ii) the email address that was linked to the profile, and (iii) any other personal data or information that might lead to identification of the account users.

Yahoo refused to collaborate and facilitate the information linked to the e-mail accounts in question with the Belgian Public Prosecutor based on the provisions contained in the Electronic Communications Privacy Act (ECPA),[34] which among other conditions, set forth that the request should be made through the United States Department of Justice and arguing that the company was neither an operator of an electronic communications network nor a provider of an electronic communications service established in Belgium for the purposes of the interpretation and scope of Article 46 bis of the Code of Criminal Procedure.

The Belgian Public Prosecutor further argued in his initial claim that Yahoo should have been obliged to cooperate with criminal authorities in Belgium and that regulations like ECPA should not undermine the sovereign authority of the Belgian criminal codes and criminal proceedings. The Public Prosecutor resolved to impose a pecuniary fine amounting to 55,000 euros and a penalty payment of 10,000 euros for each day of delay in communicating the requested data to the Public Prosecutor.

In the final judgment of the Court of Appeals of Antwerp of November 20, 2013, the justices confirmed the opinion of the Court of First Instance of Dendermonde and found: (i) that Yahoo had a territorial presence in Belgium, (ii) that Yahoo is and should be considered a provider of electronic communications services within the meaning of Article 46 bis of the Code of Criminal Procedure, and therefore, (iii) that Yahoo should collaborate with investigative authorities in the facilitation of the information requested and (iv) levied a penalty of 44,000 euros against the company.[35]

3.1.2 Microsoft Corporation v. Unites States of America

On December 4, 2013, a Magistrate of the Southern District Court of New York issued a search and seizure warrant to Microsoft Corporation requesting to produce and disclose content information (the message and subject line) and non-content information (sender address, recipient address and date and time of transmission) of an e-mail account belonging to a customer of Microsoft associated with its datacenter located in Dublin, Ireland under the Stored Communications Act (SCA) a legislation passed as part of the Electronic Communications Privacy Act of 1986 (ECPA)[36] and codified under Title 18 U.S.C. §§ 2701–2712. Microsoft produced the non-content data stored in the United States, but objected to disclose the content information of the email account supposedly stored in its datacenter located in Ireland.

[34] For a synthesis of the scope of *ECPA*, see the website of the United States Department of Justice, Office of Justice Programs, available at: https://it.ojp.gov/default.aspx?area=privacy&page=1285.

[35] As of the time of the publication of this article, the final judgment of the Court of Appeals of Antwerp is not final and it is still pending to be enforced against Yahoo in Belgium.

[36] See *supra* note 34.

The warrant was issued under Title 18 U.S.C. §2703(a), which requires the government to use the warrant procedures described in Rule 41 of the United States Federal Rules of Criminal Procedure.

Microsoft moved to quash the warrant for the content of data stored in Ireland on December 18, 2013. Among Microsoft's main arguments are:

(i) that the warrant issued by the Magistrate Judge would require an extraterritorial search and seizure of data stored in its datacenter located in Ireland.
(ii) that a search of digital data occurs where the data is stored and not at the point from which the data is remotely accessed.

Microsoft also argued that since there is no authorisation for extraterritorial application in Rule 41 of the United States Federal Rules of Criminal Procedure, the United States government cannot execute a search and seizure in Ireland, and cannot achieve this end indirectly by forcing Microsoft Corporation to produce the data stored in its datacenter in Ireland since Federal courts do not have the legal authority to issue warrants for the search and seizure of property outside the territorial limits of the United States.[37]

Further, Microsoft argues that the Magistrate Judge conclusion contravene the Fourth Amendment of the United States Constitution[38] and that his judgment could possibly lead to violation of international law and treaties, the territorial integrity of sovereign nations and circumvent the commitments made by the United States under current Mutual Legal Assistance Agreements designed to facilitate cross-border criminal investigations.[39]

The Magistrate Judge rejected Microsoft's motion to vacate the search and seizure order. Among the Magistrate Judge's main arguments are:

(i) that Microsoft analysis is ambiguous and inconsistent with the statutory language and the general structure of the SCA and its legislative history.
(ii) that warrants issued under the SCA are "hybrids", part warrant and part subpoena, and therefore, said legislation does not implicate or involve principles of extraterritoriality.
(iii) a search warrant does not occur until the data is reviewed by law enforcement in the United States, so based on this presumption there are no extraterritoriality issues involved in the matter.[40]

[37]See Memorandum and Order of the US Magistrate Judge James C. Francis IV of the United District Court Southern District of New York in the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation, April 25, 2014, pp. 5–8, available at: http://www.documentcloud.org/documents/1149373-in-re-matter-of-warrant.html.

[38]The Fourth Amendment of the Constitution of the United States prohibits unreasonable search and seizures and arbitrary arrests and is the basis of laws dealing with search warrants, safety inspections, wiretaps and other forms of surveillance including privacy law.

[39]Center for Democracy and Technology CDT, *supra* note 40.

[40]See: Center for Democracy and Technology CDT, *"Microsoft Ireland Case: Can a US Warrant Compel a US Provider to Disclose Data Stored Abroad?"* Security and Surveillance, 30 July 2014, available at: http://cdt.org/insight/microsoft-ireland-case-can-a-us-warrant-compel-a-us-provider-to-disclose-data-stored-abroad/.

This case gained a high level of political attention in the United States and Europe and it was followed by a large number of amicus briefs (friends of the court briefs) mostly supporting Microsoft's views and perspectives. The amicus briefs were filed by well known technology companies, internet service providers, public interest organizations, the Irish government, a member of the European Parliament, computer scientist and experts on international law.[41]

Microsoft appealed the judgment of the Magistrate Judge of the United States District Court for the Southern District of New York on December 18, 2014 and the matter is yet pending to be decided in the United States Court of Appeals for the Second Circuit.[42]

The Microsoft case raises relevant issues of extraterritoriality, jurisdiction, cross-border access to data and conflicts of data protection laws between the United States and Europe. And in particular, the main question that it seeks to clarify is whether law enforcement authorities in the United States have the required statutory powers in order to compel communication and internet service providers to disclose content and personal information of digital communications stored in servers and data centers located abroad.[43]

3.2 Cross-border access to data

Paradoxically, since the NSA revelations by Edward Snowden,[44] there is more general scrutiny on how law enforcement authorities access and monitor internet, but on the other hand, there is also strong pressing needs from LEAs to gain further access and preserve computer data for purpose of investigations related to cybercrime.[45]

A number of countries, mostly signatories of the Budapest Convention, are currently evaluating whether a unilateral search of data located in a computer system or server located in another territory for purposes of a criminal investigation and to secure evidence should be permitted without the consent of the country of which data is being accessed and without the need of a search warrant.[46]

[41] For a short overview of the amicus briefs filed in this case, see *supra* note 40.

[42] See: Brief for Appellant in the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation on Appeal from the United States District Court for the Southern District of New York (14-2985-cv December 18, 2014), available at: http://digitalconstitution.com/wp-content/uploads/2014/12/Microsoft-Opening-Brief-120820141.pdf.

[43] For an academic perspective on the extraterritorial implications of this case, see: *Svantesson* [9].

[44] BBC News, *"Edward Snowden: Leaks that exposed US spy programme"* (17 January, 2014), available at: http://www.bbc.com/news/world-us-canada-23123964.

[45] Reuters, *"Europe's police need data law changes to fight cybercrime-Europol"* (29 September, 2014), available at: http://www.reuters.com/article/2014/09/29/cybersecurity-crime-eu-idUSL6N0RU35M20140929.

[46] This scenario has become a relevant discussion and is currently being analyzed by a working group of the *Cybercrime Convention Committee* (*TC-Y*) of the Council of Europe. According to this working group, current practices in some European countries go beyond the scenarios foreseen in Article 32b—which deals with cross-border access to data with consent—and many countries have not established the necessary safeguards for protecting fundamental human rights during criminal investigations. See: Council of Europe *"Transborder access and jurisdiction: What are the options?"*. Report of the Ad-hoc Subgroup on Jurisdiction and Transborder Access to Data of the Cybercrime Convention Committee (T-CY) of 6 December 2012, 1–69 (TC-Y 2012).

There are different opinions and views on whether cross-border searches of data in computer systems located in foreign countries should be permissible.[47] Notwithstanding the discussion on the legality and permissibility of cross-border searches and access to data, some countries around the world have recently enacted laws and reform criminal procedural frameworks in order to allow LEAs access to data for the purposes of criminal investigations but with the limitation that the service provider be located in its territory.[48]

Current practice shows that there are different approaches in some countries regarding how law enforcement access data unilaterally and without a formal mutual legal assistance request in order to obtain evidence located in computer or mobile systems in foreign countries.[49] In our view, such scenarios will possibly not change in the coming years unless further legal guidance and limits on such proceedings get the necessary general acceptance of countries worldwide.

One of the lessons learned from the Yahoo case in Belgium is that public prosecutors and judicial authorities currently face the challenge in obtaining data and information directly from a foreign service provider without the need to go through formal mutual legal assistance channels, a situation that could possibly hinder or delay the investigation of cybercrime and prosecution of cybercriminals in national courts.

Another lesson learned from the Microsoft vs. United States case is that search warrants or orders to compel internet service providers to disclose content information of customers can have meaningful ramifications and implication for Internet based companies and could potentially lead to conflicts of laws in the field of data protection.

4 The future

Predicting the future of cybercrime jurisdiction is not an easy task, but the success of criminal investigations will largely depend not only on ensuring the correct enforcement of existing jurisdictional principles and laws against cybercriminals, but particularly on the degree of technical formation and training of the judiciary, the facilitation of assistance of internet service providers with law enforcement authorities, the coordination of investigations both nationally and internationally and the aptitude and disposition of national courts to prosecute perpetrators regardless of their geographical location. These are, in our view, minimum requirements which countries should meet and have in place in order to be able to prosecute cybercriminals.

[47] See for instance, *Seitz* [8]. The author is of the general opinion that cross-border searches of computer data located in foreign jurisdiction should not be permissible.

[48] See for instance Articles 189 and 190 of Mexico's new *Federal Law on Telecommunications and Broadcasting*, which impose obligations on telecommunication concessionaires and content service providers to collaborate with security, law enforcement and justice administration authorities in the geographical location in real-time of mobile communication equipment and the retention of data when there is reason to believe that a crime has been committed using mobile telecommunications equipment.

[49] For a comparative analysis of the practice of cross-border access to data by law enforcement in different regions of the world, see *UNOCD Cybercrime Study, supra* note 30, pp. 219–223 and for a comparative perspective on the legal practice in some European countries, see *supra* note 46, pp. 32 to 42.

Discussions on cybercrime jurisdiction, currently show that there are major constrains with respect to the application of the principle of territoriality in virtual cyberspace due to the constant and dynamic movement of data across different servers located in multiple jurisdictions, a situation that has led international organisations to call for a *'paradigm shift'* in order to allow the application of other jurisdictional principles so as to investigate and prosecute criminal conduct committed in cyberspace.[50] In this writer's view, this so-called change of paradigm requires judicial authorities to explore new ideas, paths, and mechanisms to enforce substantial and procedural criminal legislation and to make the existent mutual assistance legal mechanisms to work on a more dynamic and flexible basis. The same discussion will continue to be raised in international fora, but its success will largely depend on a shift in the administration of the criminal justice system at national level.

While cloud services to storage data continue to grow and given that a great deal of information and digital evidence is stored in servers somewhere in the cloud, it is very likely that a number of scenarios will continue to be revisited in order to find balanced approaches for the application of existing international legal principles for asserting jurisdiction over cybercrime investigations.

One of these scenarios is the actual *"loss of location"*[51]—whether in order to determine the exact location of data, the location of the storage media or even the country of residence of the cloud service provider—as a relevant factor to be considered for the purposes of obtaining evidence for criminal investigations.[52]

Another scenario or proposed alternative for determining the jurisdiction to enforce a search or seizure of electronic evidence is *"the power of disposal*,[53] in order for law enforcement investigators to have access to data once the data is not longer used and needed by the data subject, an approach which in our view, however, will likely conflict with safeguards and data protection laws and regulations in the European Union[54] and other jurisdictions around the world.

Cybercrime is evolving and changing rapidly and the technical layers of the net are less noticeable in search engines since a great deal of illegal activity is moving to the

[50]See *supra* note 46, paragraph 134, p. 27 and the document containing the key messages of the *Council of Europe Octopus 2012 Conference on Cooperation against Cybercrime*, Strasbourg, p. 8 (5 July 2012), available at: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Octopus2012/2571_Octo_key_messages_V7c_long.pdf.

[51]For a perspective on other legal connecting factors to prioritise jurisdictional claims in cybercrime investigations, see: Council of Europe, "*Cloud Computing and cybercrime investigations: Territoriality vs the power of disposal?"* Discussion paper prepared for the Project on Cybercrime of the Council of Europe, pp. 8–10 (31 August 2010).

[52]For a perspective on computer data stored in the cloud for purposes of evidence in cybercrime investigations, see: *UNOCD Cybercrime Study, supra* note 30, pp. 216–218.

[53]The power of disposal refers to "the power of a person to alter, delete, suppress or to render data unusable as well as the right to exclude others from access and any usage whatsoever". See *supra* note 46 paragraphs 263–265, p. 50 and *supra* note 50, pp. 10–11.

[54]See for instance Article 15 on Conditions and Safeguards of the Budapest Convention and Regulation No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

so-called *deep web*,[55] which has seen considerable growth in recent years. There is therefore an urgent need for more proactive law enforcement authorities and judges, magistrates and prosecutors who can think outside the box and find practical and innovative solutions to investigate and prosecute criminal activities affecting companies, institutions and individuals as a result of conduct committed in cyberspace, and to facilitate international cooperation on a more dynamic basis within the limits of international law.

5 Conclusion

Illegal activities conducted through internet involve real individuals located in one or different countries and cause real damage to people, infrastructures and the economy as whole. Therefore states through their respective judicial legal systems shall procure to find links and connections to prosecute cybercriminals within their national legal frameworks. These may include the assertion of jurisdiction based: (i) on the location of the activity or where the conduct was committed (territoriality); or (ii) on the nationality of the perpetrator (active nationality principle); or (iii) where the effects and damage to the victims took place (passive nationality principle); or (iv) where the computer systems, storage servers or data centers may be located.

In our view, the principle of territoriality shall not continue to prevail in jurisdictional claims; the application of other principles should also be extended to assert jurisdictional claims.

Coordination of investigations and mechanisms for the centralisation of proceedings on criminal jurisdiction, as described and contained in some of the Council of Europe instruments and Council framework decisions, will play a key role in avoiding possible conflicts of jurisdictions and parallel proceedings in the prosecution of cybercriminals. Countries should prioritise their use.

The permissibility of cross-border access to data for criminal investigations will continue to raise concerns among states, and current practice shows not only a diversity of procedures conducted by law enforcement in each country to get access to evidence located in foreign servers but in particular a lack of uniformity among European Union Members regarding accessing computer data in other countries despite the applicable provisions of the Budapest Convention. This writer strongly believes that cross-border searches for the purposes of accessing data should be allowed as long as law enforcement authorities have established sufficient security safeguards in criminal investigations in order to protect the information and data of third parties, and as long as it has been proved that there are sufficient links to prosecute criminal conduct affecting national state infrastructures or victims of the state seeking to have access to such computer data.

[55]The *deep web* is a term usually referred to the information and content that is not indexed and found by standard search engines where a large number of references and information with illicit content such as drugs, trafficking, terrorism and child pornography is available. For further info on the deep web, see: *Bergman* [1], available at: http://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.0007.104.

Last, mutual legal assistance mechanisms and channels play an important role for the adjudication of criminal jurisdiction by national criminal courts and shall continue to serve as a cooperation vehicle between law enforcement and the private sector for requesting evidence for cross-border criminal investigations. However, we believe that internet companies making use of said mutual legal assistance channels should make them work on a more flexible basis in order to expedite legal proceedings for the purpose of securing and preserving evidence that will lead to the possible identification of perpetrators, and for the purpose of adjudication on jurisdiction by national courts.

References

1. Bergman, K.M.: The deep web: surfacing hidden value. Journal of Electronic Publishing **7**(1) (2001)
2. Brenner, W., Koops, S.u.B.-J.: Approaches to cybercrime jurisdiction. Journal of High Technology Law **IV**(1), 1–46 (2004)
3. Garnett, R., Down, J., Company Inc vs. Gutnick: An adequate response to transnational internet defamation? Melbourne Journal of International Law **4**, 1–21 (2003)
4. Goldsmith, J., Wu, T.: Who Controls the Internet? Illusions of a Borderless World. Oxford University Press, Oxford (2006)
5. Reily D, O.: International criminal justice cooperation with multi-national ISP's. Discussion paper prepared under the Cybercrime@IPA Project from the European Union and the Council of Europe, 1–40 (May 28, 2013)
6. Putnam, T.L., Elliot, D.: International Responses to Cybercrime. In: Sofaer, A.D., Goodman, S.E. (eds.) Transnational Dimension of Cybercrime and Terrorism, vol. 490. Hoover Institution Press, Stanford (2001)
7. Reidenberg, J.: The Yahoo Case and the International Democratization of the Internet, Fordham University School of Law. Research Paper No. 11, pp. 1–19 (2001)
8. Seitz, N., Search, T.: A new perspective in law enforcement? International Journal of Communications Law & Policy/Yale Journal of Law and Technology **9**, 1–18 (2004). Special Issue on Cybercrime
9. Svantesson, D.: After Microsoft v. U.S.—Law Enforcement in the Cloud. First Part published on December 31, 2014 at https://www.linkedin.com/pulse/after-microsoft-v-us-law-enforcement-cloud-1-2-svantesson and Second Part published on January 5, 2015 at https://www.linkedin.com/pulse/after-microsoft-v-us-law-enforcement-cloud-2-dan-jerker-b-svantesson
10. Sy, G.: E-Commerce Act. Republic Act no. 8792 Implementing Rules and Regulations Legislative Highlights "I Love You Virus Case" (2001)
11. The Journal of Electronic Publishing http://www.journalofelectronicpublishing.org/
12. Velasco, C.: La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e Internet, Tirant lo blanch, Valencia (2012)