

Internet Jurisdiction and Applicable Law in Latin America. Towards the Need for Regional Harmonization in the Field of Cybercrime

By

Cristos Velasco San Martín

Paper originally submitted to the 3rd GigaNET Annual Symposium in Hyderabad, India.
Updated by the author for the Octopus Interface 2009 Conference on Cooperation against
Cybercrime, Strasbourg, March 10-11, 2009

Abstract

Jurisdiction and applicable law on the Internet has been the subject of a wide debate among the legal academic community, not only due to the borderless nature of the Internet, and the different levels of technology development among countries, but particularly because of the different regulatory approaches on jurisdiction and applicable law between the common law and civil systems.

The main purpose of this paper is to identify and analyze (on a comparative perspective) the legal and procedural framework governing jurisdiction and legal competence of national authorities and local courts as applied to Internet related activities in Latin America, particularly focusing in the field of cybercrime. Further, this paper seeks to assess the impact of relevant provisions and approaches to Internet jurisdiction contained in international instruments, such as the *Council of Europe's Convention on Cybercrime*, will evaluate whether the application of such international convention provide a reliable uniform framework for Latin-American countries in order to solve issues of competence on cross-border activities on the Internet affecting national individuals, and considers whether a regional legal approach is needed in order to provide harmonization in the enforcement of criminal laws in the region.

"The unique nature of the Internet highlights the likelihood that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulation by states that the actor never intended to reach and possibly was unaware were being accessed. Typically, states' jurisdictional limits are related to geography; geography however, is a virtually meaningless construct on the Internet."

American Library Ass'n v. Pataki, 969 F.Supp. 160, 169 (S.D.N.Y. 1997).

"Civil law countries-where the legal system is much more "bastard" than in common law countries and where statutes of jurisdiction is quite thoroughly written out in letters-makes the jurisdictional system quite inflexible and hinder the innovation of many of the thoughts American legal scholars have suggested, because courts outside US do not have the right to steer into new directions that many scholars holds Cyberspace implement."

Henrik Spang-Hanssen. Cyberspace and International Law on Jurisdiction (2004).

I. Introduction

Since the inception and development of the Internet for commercial purposes¹, the topics of jurisdiction and applicable law in cyberspace have been extensively debated among the legal academic circles, particularly in countries with a common law system like the United States², Canada³, Australia⁴ and England⁵ where the case law has been widely developed under the doctrine of ‘*Stare decisis*’.⁶

Cyberspace jurisdiction has been addressed and contested in different fields of Internet law, including, privacy⁷, domain names and trademark infringement⁸, copyright infringement⁹, spam¹⁰, hate speech¹¹ and liability and defamation.¹²

As a general principle of law, the laws and regulations of a particular jurisdiction normally have effects within the limits or boundaries of that jurisdiction. The application of this

¹ For a legal definition of the ‘Internet’, see *American Civil Liberties Union V. Reno*, 929 F. Supp. 824, 830-831 (E.D. Pa. 1996), *aff’d*, *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

² See e.g. *Yahoo, Inc. v. La Ligue Contre le Racisme et L’Antisemitisme et.al* No. 01-17424 (9th Cir. February 10, 2005) a case where Yahoo asked the Ninth Circuit for legal protection for US Internet portal and servers whose content is protected under the First Amendment of the Constitution of the United States.

³ See e.g. *Bangoura v. The Washington Post et.al.*, [2004] O.J No. 284 Ontario Superior Court of Justice, *rev’d*, 2005 CanLII 32906 (Ont. C.A.); a libel action filed by a former UN official by then a Canadian citizen, against the Washington Post Company concerning a defamatory article the Washington Post published in 1997 while Bangoura was living in Kenya and working for the UN.

⁴ See e.g. *Down Jones & Co. V. Gutnick*, [2002] HCA 56 (Dec. 10, 2002) a case involving an allegedly libelous article about an Australian mining magnate residing in Victoria, Australia and Barrons, an online edition of the Wall Street Journal, an American publication pertaining to Down Jones & Co.

⁵ See e.g. *Harrods Ltd. v. Down Jones & Co.* [2003] EWHC 1162 (QB) a case involving a libelous article that described Harrods as “the Enron of Britain” and that warned that if the company ever went public, investors should “question its very disclosure”.

⁶ *Stare decisis* is a common law doctrine under which judges are obliged to follow the precedents established in prior decisions. The doctrine is divided into two categories: (i) *Vertical Stare decisis* where the lower courts are bound to follow the precedents established by the appellate courts for their jurisdiction and all supreme court precedent; (ii) *Horizontal Stare decisis* refers to the idea that a judge is bound by decisions of earlier judges of similar or coordinated level. To find out more about the doctrine of *Stare decisis* see Wikipedia at: http://en.wikipedia.org/wiki/Stare_decisis (Last visited: February 28, 2009).

⁷ See *Lawson v. Accusearch Inc. (F.C.)*, 2007 FC 125 (CanLII), a decision involving the investigative powers of the Privacy Commissioner of Canada to investigate an American company that collected, used, and disclosed information of a Canadian citizen on the Internet contrary to Canada’s privacy legislation (PIPEDA Act).

⁸ See *Zippo Mfr. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997) a dispute involving the use of a registered trademark and the rights to use domain names similar to the registered trademark of a company.

⁹ See *Metro-Goldwyn-Mayer Studios et.al v. Grokster*, 243 F. Supp. 2 (C.D. Cal. 2003), *aff’d*, 380 F.3d 1154 (9th Cir. 2004), *vacat remanded by* 545 U.S. 913 (2005) a copyright infringement action against distributors of software that allowed users to engage in peer to peer file sharing where the defendant tried to dismiss the case for lack of personal jurisdiction based on the fact that the company’s presence in California was only through its Internet portal. The court concluded that the exercise of jurisdiction was appropriate.

¹⁰ See *e360 Insight v. The Spamhaus Project [Docket Nos. 063779 & 06-4169]* a decision involving the validity of a default judgment without the District Court in California first conducting and affirmative inquiry into whether it had personal jurisdiction over *Spamhaus*, a non-profit company organized under UK laws; and whether service of process was effected in compliance with applicable rules.

¹¹ *Id.* at 2.

¹² See *Polanski v. Conde Nast Publications Ltd.*, [2005] UKHL 10 (Feb. 10, 2005) a libel action brought in an English Court by film director Roman Polanski against *Conde Nast* based on a defamatory story published about him in the magazine *Vanity Fair*.

principle to offline activities is usually approached on a territorial basis taking into account the geographical location of the parties at the specific time of a dispute.¹³

However, cross border activities on the Internet do not respect geographical limits, and as result of illegal conduct or transactions, particularly in the field of Internet commerce, the parties are subject in many cases to a wide array of laws & regulations, and often contradictory claims with regards to the interpretation of the laws and jurisprudence where the parties reside and where the transaction took place. The solutions to resolve conflict of laws issues and determine aspects of applicable law and jurisdiction for cross-border transactions among private parties are usually achieved through the application of private international law.¹⁴

In countries with civil law system, jurisdictional aspects targeting the field of cyberspace has not specifically been addressed due to the judicial system's tradition to strictly follow and interpret legislation contained in written codes and regulations, as well as its inflexibility to follow and adapt foreign rules and precedents on jurisdiction on cyberspace. Furthermore, the academic doctrine and literature in this particular field of law has just started to be developed.¹⁵

As a result of such existing academic gap, we decided to draft this paper, the main purpose of which is to identify and analyze the legal and procedural frameworks governing jurisdiction and legal competence of national authorities and local courts as applied to Internet related activities in three countries of Latin America, particularly focusing in the field of cybercrime.

This paper also reviews the governing provision on jurisdiction an applicable law contained in the *Council of Europe's Cybercrime Convention [hereinafter COECC]*. Aspects of bilateral and multilateral cooperation in international and regional organizations, with regards to the assertion of jurisdiction and competence on Internet based crime, as well as policy recommendations in the area will also be a subject of our analysis.

Our paper will seek to provide an answer to the following research questions: (i) whether the traditional rules on jurisdiction contained in the legislation of Latin American countries provide a solid framework in order to claim territorial jurisdiction on crime and offenses committed on the Internet; (ii) whether Latin American countries should adapt their laws to assert jurisdiction on Internet related conduct or simply continue to rely on traditional

¹³ Chris Reed, *Internet Law. Text and Materials*, p. 217, (Cambridge University Press 2004).

¹⁴ See for instance, the Rome Convention on the Law Applicable to Contractual Obligations, art. 3; Hague Convention on the Law Applicable to Contracts for the International Sale of Goods, art. 7; Council Regulation 44/2001/ EC on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L12 p1, 16 January 2001 (Brussels Regulation), art 23.

¹⁵ Cristos Velasco, *"A Propósito de la Jurisdicción y el Derecho Aplicable en Internet"*, Entérate en Línea, Dirección General de Servicios de Cómputo Académico de la Universidad Nacional Autónoma de México (DGSCA-UNAM, November, 2005), available at: <http://nacpec.org/docs/CristosVelascoJurisdiccion.pdf> (Last visited: February 28, 2009)

jurisdictional provisions contained in their legislation; and (iii) whether the current international conventions and recommendations provide a reliable framework for Latin-American countries in order to harmonize issues of adjudication of jurisdiction on Internet criminal conduct.

1. Jurisdiction in Cyberspace

1.1. Background

Jurisdiction in cyberspace has been addressed in a number of academic papers particularly at the time when cyberspace was in its initial stage of development and there were almost no international treaties or regulations governing it. For instance, Perry Barlow in his paper entitled: “*Selling Wine Without Bottles on the Global Net*” argues that the Internet is a new and separate jurisdiction in which the rules and regulations of the physical world do not apply. Further, he is of the opinion that a separate law of cyberspace should, and perhaps will be developed.¹⁶

One of the problems that cyberspace presents is that individuals, legal entities and corporations and their assets, as well as technical elements such as the computer and the communications equipment through which transactions are carried out, each have a real world existence and are situated in one or more physical jurisdictions worldwide. All these factors and actors in cyberspace provide a sufficient justification for national courts in claiming jurisdiction and the applicability of local laws to Internet conduct and activities on cyberspace.

1.2. Definition of Jurisdiction

Under common law, jurisdiction usually refers to the capacity of a court or tribunal to interpret and apply a specific rule of law; generally limited by both territory and subject matter.¹⁷

In the U.S., jurisdiction and applicable law has been determined on a case-by-case court analysis rather than applying strict written codified rules. The U.S. approach has traditionally considered notions of “reasonableness” and “fundamental fairness” to both plaintiffs and defendants; the “minimum contacts approach”¹⁸; and “the real and substantial connection with the forum”. The U.S. has a plethora of case law that has addressed the issue of jurisdiction in different areas of the regulation of the Internet.¹⁹

¹⁶ John Perry Barlow, “*Selling Wines Without Bottles. The Economy of Mind on the Global Net*”, available at: http://w2.eff.org/Misc/Publications/John_Perry_Barlow/HTML/idea_economy_article.html (Last visited: February 28, 2009).

¹⁷ Michael D. Scott, “*Internet and Technology Law Desk Reference*”, p.532, (Aspen Publishers 2005)

¹⁸ *International Shoe Co. V. Washington*, 326 U.S. 310, 316 (1945).

¹⁹ See David G. Post “*Personal Jurisdiction on the Internet- A Survey of the Cases*”, Cyberspace Law Institute (June 1998). See also the Internet Library of Law and Court decisions, which contains summaries of several important US cases relating to jurisdiction in Internet Law updated until May 2008, online: <http://www.internetlibrary.com/alldecisions.cfm#case33> (Last visited: February 28, 2009)

As a general rule, a defendant in the U.S. may be sued in the state where he resides, but when the defendant is not a resident of the state in which the suit is brought, a court may hear the case only when the court properly exercises personal jurisdiction over the defendant.²⁰

However in civil law jurisdictions, as a general rule, a defendant may be sued only in the state where he resides based on the subject matter and taking into account the rules of residence and domicile usually provided in the Civil Code.

1.3. Types of Jurisdiction

A. Personal Jurisdiction

The concept of personal jurisdiction usually refers to the capacity of a court to adjudicate a dispute involving a particular defendant. The court must find that the defendant has sufficient contacts with the jurisdiction to permit the court to adjudicate the claim.

The requirement that a court have personal jurisdiction over the defendant prevents a plaintiff from filing claims in a distant court to force the defendant litigate in an inconvenient location.²¹

B. Specific jurisdiction

This concept usually refers to when litigation occurs or arises out of the defendants' contacts with the forum state. In this particular type of jurisdiction, a court may assert jurisdiction over the defendant through the exercise of specific jurisdiction via a state's long-arm statute and taking into account the defendant's "minimum contacts" with the forum and that the defendant would reasonably have been able to anticipate being hauled into court of the forum state.²²

C. General jurisdiction

Under this concept, litigation does not occur or arises out of the defendants' contacts with the forum state. General jurisdiction is properly exercised over a non-resident defendant only when the defendant is present in the forum state or maintains "continuous and systematic" contacts with the state.²³

Since certain methods of analysis to cyberspace jurisdiction have emerged in the last decade, it is important to understand the traditional principles on jurisdiction, and how this concept works primarily in the U.S. in order to understand the general approach to cases dealing with jurisdiction on the Internet. For example, in the context of web publishing and commercial activities, U.S. courts have made a distinction between an 'active website'²⁴, which solicits those outside the jurisdiction to undertake a commercial transaction with the website owner and a 'passive website'²⁵, which only provides information.

²⁰ *Helicopteros Nacionales de Colombia S.A. v. Hall*, 466 U.S. 408 (1984).

²¹ Internet and Technology Law Reference, *supra* note.17, p.610.

²² *Worldwide Volkswagen Corp v. Woodson*, 444 U.S. 286, 291 (1980).

²³ *Helicopteros Nacionales de Colombia S.A. v. Hall*, 466 U.S. 408 (1984).

²⁴ See, *Zippo Mfr. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997), *supra* note 8.

²⁵ See *e.g. Cybersell Inc. v. Cybersell, Inc.* 130 F. 3d 414 (9th Cir. 1997) where the court held that the exercise of specific jurisdiction was not proper because the defendant's use of the "Cybersell" mark on its

D. Targeting Approach

This approach is often applied in the context of commercial transactions and copyright infringement on the Internet, and it usually refers to a particular action targeted towards a specific forum or jurisdiction. For instance, a defendant's actions that target a particular state may result in personal jurisdiction over the defendant in that state. Under this test, U.S. Courts examine the facts of each case to determine whether the defendant "purposefully availed" himself of the benefits of doing business in the state, or whether they "purposefully directed" their activities toward the forum state.²⁶

2. Cybercrime Jurisdiction

The transnational dimension of cybercrime requires a combination of efforts in different fronts, namely enactment of substantive and procedural legislation, effective law enforcement, policy recommendations and international cooperation. However, efforts in the legal field also bring a number of challenges for the legal systems of each country. One of the most important challenges is to resolve jurisdictional issues and application of national criminal legislation in order for authorities to investigate and prosecute offenders based in multiple jurisdictions, and affecting or harming nationals while respecting the principle of national sovereignty of states under public international law.

Many countries around the world do not have specific rules dealing with cybercrime jurisdictional issues and they have simply relied upon traditional rules to decide whether they have jurisdiction or not. Another important aspect for countries to consider is whether they assert territorial jurisdiction in a particular criminal case, considering the importance of the case concern, and whether they possess the financial and technical means, and fully trained staff in the enforcement front that can carry out an investigation successfully.²⁷

Among the results of a global survey on cybercrime and jurisdiction of 13 countries²⁸, which included two Latin American countries; Chile and Brazil, it was found that in the exercise of jurisdiction: (i) "*territoriality stills turns out to be a prime factor, despite the non-physical nature of the bits and bytes that usually constitute a cybercrime*"; and (ii) "*personality claims and protection claims occurs occasionally as well in relation to cybecrime.*" The global survey concludes that "*countries and states turned out to have varying scopes and bases in their cybercrime jurisdictional provisions and that such*

website was passive and the defendant conducted no commercial activity only displayed information in his website.

²⁶ See Michael Geist, "*Is There a There. Toward Greater Certainty to Internet Jurisdiction*", University of Ottawa (April 2001), an academic paper that explains the jurisdictional approaches to the Internet primarily in the US and Canada. This paper proposes the adoption of a 'targeting-based approach' in order to provide all parties with greater legal certainty and to conduct more effective legal risks analysis to Internet jurisdiction, available at: <http://aix1.uottawa.ca/~geist/geistjurisdiction-us.pdf> (Last visited: February 28, 2009)

²⁷ Bert Jaap Koops and Susan W. Brenner (Editors), "*Cybercrime and Jurisdiction. A Global Survey*". Information Technology & Law Series 11, Chapter One "Cybecrime Jurisdiction-An Introduction, pp.1-2, Leiden Center for Law in the Information Society, 2006.

²⁸ Bert Jaap Koops and Susan W. Brenner (Editors), *supra* note 27.

situation will probably lead to problems when jurisdiction conflicts emerge whenever a serious cross-border cybcrime that multiple states have an interest in prosecuting.”²⁹

The following section will analyze the current provisions on criminal jurisdiction contained in the legislation of three Latin-American countries: Mexico, Argentina and Chile.

3. Comparative Legislation of three Latin-American countries

3.1. Mexico

The legal foundation regarding conflict of law rules is established in Article 121 of the Political Constitution of the Mexican United States. Mexico does not have a comprehensive law that establishes conflict of laws rules. The Federal Civil Code and the Federal Code of Civil Procedure contains the principles and general rules regarding conflict of laws and choice of law.³⁰ It is worth mentioning that under the Mexican law³¹, separate rules on choice of law apply to individuals (*personas físicas*) and to legal entities (*personas morales*); therefore, these two subjects are treated separately under the Mexican legal system.³²

Choice of law rules under the Federal Civil Code follow a territorial approach and authorize Mexican courts to apply foreign law when prescribed by international treaties and conventions.³³ Article 13 of the Federal Civil Code provides guidance to Mexican courts in choosing the law applicable to disputes between parties located in different jurisdictions. Further, article 14 establishes the rules for the application of foreign law; and article 15 provides the grounds on which foreign law should not be applied for the purpose of evading fundamental principles of Mexican law, or if such application would be contrary to public policy.³⁴

Under Mexican law, the rules governing jurisdiction are usually referred to under the term “*competencia*”.³⁵ Rules relating to jurisdiction at the federal level are contained in the Federal Code of Civil Procedure (FCCP). The federal rules governing jurisdiction over the

²⁹ Supra note 27 at p.6.

³⁰ Stephen Zamora, Jose Ramon Cossio, Leonel Pereznieta, et.al, “*Mexican Law*”, pp. 676-677, Oxford University Press, (2005).

³¹ Mexico’s current 31 States and the Federal District have the power to adopt their own civil and criminal codes and to establish their own rules of judicial procedure, including judicial jurisdiction. The Civil and Criminal Codes for the Federal District, as well as the Federal Code of Civil Procedure and the Federal Code of Criminal Procedure have been used as model legislation for other state codes, supra note 30 at 684.

³² Supra note 30 at 677.

³³ See article 12 of the Federal Civil Code that reads as follows:

Article 12. Mexican laws apply to all persons within the Republic, as well as to acts and events that take place within Mexican territory or under its jurisdiction, and to those persons who submit themselves or their acts thereto, unless Mexican law provides for the application of a foreign law, or the application of foreign law is otherwise provided by treaties or conventions to which Mexico is a party.

³⁴ Supra note 30, pp.680-681.

³⁵ *Competencia* refers to the power of the court to assert jurisdiction over both the parties and the subject matter of the dispute before it. *Comptencia* in Mexico is determined in accordance with the Organic Law of the Judicial Power (*Ley Organica del Poder Judicial*) applicable to the particular court in question, as well as with specialized laws; *ibid* at 686.

parties, and over the subject matter, are set forth in Articles 23 to 38 of the FCCP. Articles 30 to 33 set forth the basic rules concerning the allocation of concurrent jurisdiction between federal and state courts of two or more states.³⁶

A. Jurisdiction under the Federal Criminal Code

The Federal Criminal Code (FCC) is the governing law on federal crimes committed in the Mexican Republic. Article 2 of the FCC specifies the scope and jurisdiction of that code under the following circumstances: *(i) Crimes committed or prepared abroad, which produce or are intended to produce effects within the Mexican territory, or by crimes initiated, prepared or committed abroad, as long as a binding treaty for Mexico provides the obligation to extradite or prosecute and no extradition of an offender to the State that might have requested him, and (ii) crimes committed in Mexican consulates or against Mexican consular personnel, when such crimes have not been judged by the courts of the country where they were committed.*

Articles 3 and 4 of the FCC provides the punishment of crimes committed abroad or in foreign territory as follows:

Article 3.- Continuous crimes committed abroad which continue being committed in Mexico, shall be prosecuted according to the Mexican law whether the offender is Mexican or foreigner.

Article 4.- Crimes committed in foreign territory by a Mexican against Mexicans or against foreigners, or by a foreigner against Mexicans, shall be punished in the Republic according to federal laws, if the following conditions are met:

I. That the accused is in Mexico;

II. That the defendant has not been definitely judged in the country where the crime was committed, and

III. That the infraction committed is considered as a crime in both, the country where it was committed and in Mexico.

The FCC, like most criminal codes in Latin America is based on the principle of territoriality and contains specific rules when the crime is committed in foreign territory by a national or by a foreigner against a national. The FCC goes even further and provides for the application of special laws and international treaties when a crime committed is not specifically punished under the FCC. Article 6 of the FCC reads as follows:

Article 6.- In cases of crimes not contemplated by this Code but contemplated by a special law or by an international treaty of compulsory observance in Mexico, the special law or the international treaty shall apply taking into account the provisions of the First Book of this Code and, if applicable, those of the Second Book.

B. Internet Related Offenses

³⁶ *Ibid.* at 686-687.

Some crimes and offenses committed through the use of the Internet, electronic means or with the support of computer equipment and systems are punished under the Federal Criminal Code (FCC) and the Law of Credit Institutions (LCI). For instance, the commercialization and misuse of credit and debit cards and payment instruments and the illegal transfer of funds are punished under article 112bis and 113 bis of the LCI. Corruption of minors and child pornography including its possession, distribution and commercialization on the Internet is punished pursuant to articles 202, 203 and 203 bis of the FCC. Also, the FCC contains a full chapter (*Arts. 211 bis 1-211 bis 7*) that prohibits and sanctions illegal access to computer equipment and information systems.³⁷

C. Cases

As of the date of submission of this paper, Mexican courts have not yet issued judicial decisions or established jurisprudence with regards to the application of Mexican law and the assertion of jurisdiction to criminal related conduct on the Internet³⁸ where a foreign resident has caused harm to a national individual, government agency or legal entity physically established in Mexico.

Mexican courts have, however, started investigating and prosecuting cases related to Internet criminal conduct where nationals are involved. For instance, in March 24, 2008, the District Court of the City of Cuernavaca in the State of Morelos issued a condemnatory sentence against a Mexican citizen who illegally distributed and commercialized copyrighted music, movies and TV series through his webpage. The District Court asserted jurisdiction and resolved to punish the individual with an imprisonment term of six years and a monetary fine for the equivalent of USD\$39,000.00.³⁹

3.2. Argentina

A. Jurisdiction

Unlike Mexico, Argentina has an independent legislation “Ley 48 (*Law 48*)”⁴⁰, which establishes the rules on jurisdiction and “*competencia*”⁴¹ of judicial tribunals in different areas including civil, commercial, administrative, maritime, criminal and international law. Criminal jurisdiction is established in articles 3, 7 and 12 section III of *Law 48*, and in Article 1 of the National Criminal Code (NCC). The said provisions are based in the

³⁷ For a detailed explanation of the legal framework on cybercrime and its enforcement in Mexico, see Cristos Velasco, “*General Summary of the Legal Framework concerning Cybercrime and Law Enforcement in Mexico*”, OCTOPUS Interface Conference 2007 of the Council of Europe, (June 11, 2007), available at: <http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Interface2007/567%20if%202007%20pres%20NACPECPresentation.pdf> (Last visited: February 28, 2009)

³⁸ The Federal Criminal Code contains a full title consisting of article 210-211 bis 7 that punishes the disclosure of secrets and illegal access to communication and computer equipment.

³⁹ See El Universal, “*Dan seis años de prisión a pirata cibernético*”, (May 20, 2008), available at: <http://www.eluniversal.com.mx/notas/508250.html> (Last visited: February 28, 2009)

⁴⁰ Law 48 (*Ley 48*) entitled: “*Jurisdiction and Competence of National Tribunals*” is available at: <http://www.infoleg.gov.ar/infolegInternet/anexos/115000-119999/116296/texact.htm> (Last visited: February 28, 2009)

⁴¹ *Supra* note 35.

principle of territoriality and its scope includes the investigation of criminal conduct committed, or the effects of which, are produced within the territory of Argentina or in the places subject to its jurisdiction; and as result of criminal conduct committed abroad by agents or authorities' staff in duty.

B. Cybercrime

On June 24, 2008 the Congress of Argentina enacted “Ley 26,388 (*Law 26,388*)”⁴² that punishes and sanctions Internet crimes. Law 26,388 amends and reforms the National Criminal Code and punish the possession and distribution of child pornography on the Internet (Article 128); the privacy of communications and electronic messages and the disclosure of personal data (Article 157 and 157 BIS); and criminal conducts like hacking (Art. 157 BIS), illegal access to computer systems (Articles 153 and 153BIS), identity theft, (Art. 173 section 16), damage to computer and communications systems (Article 183, 184), the creation and spreading of computer viruses, interception and interruption of public communications (Article 154, 155 and 197), and the falsification and destruction of legal evidence and records contained in digital systems (Art. 255).

C. Cases

The judicial courts in Argentina have been among the most active ones in prosecuting cases in the fields of cybecrime and data protection in Latin America. For instance, in a legal action on compensatory damages regarding the loss of a public document pertaining to an individual issued by a national government registry, a citizen in Argentina sued the State and the Province of Mendoza requesting monetary compensation for the financial damage incurred as a result of the lost of his identification that was subsequently misused to commit financial fraud. The judge in that case asserted jurisdiction and resolved that the State and the Province of Mendoza were responsible for the loss of such document and that both, the State and the Province should compensate the victim with a monetary fine plus interests within the term of 30 days.⁴³

Also, the Supreme Court of Justice of Argentina has issued decisions in the area of information credit reports and the legality of the Law of Credit Cards of that country.⁴⁴ However, it is important to mention that our research has shown that Argentina's national tribunals have pursued only cases involving national individuals and national institutions in that country. As far as the author is concerned, there has not yet been a cybercrime case pursued in the federal or local courts of Argentina where the defendant may be based in a

⁴² Bill 26,388 (*Ley 26, 388*) containing the reforms on cybercrime is available at: <http://infoleg.mecon.gov.ar/infolegInternet/anexos/140000-144999/141790/norma.htm> (Last visited: February 28, 2009).

⁴³ *Raul Alberto Serradilla vs. Provincia de Mendoza y Estado Nacional*, S.2790 XXXVIII (June 12, 2007), available in Spanish at: <http://www.habeasdata.org/pdfs/Serradilla.pdf> (Last visited: February 28, 2009).

⁴⁴ See *Organizaciones Veraz vs. c/ E.N. P.E.N. M° E. y O.S.P. s/ amparo ley 16.986*, available in Spanish at: <http://www.habeasdata.org/Caso-Veraz-v-Estado-Nacional> (Last visited: February 28, 2009).

foreign jurisdiction or cases dealing with extraterritorial cybercrime investigations affecting or damaging individuals, government or private entities in Argentina.

3.3. Chile

A. Jurisdiction

The general rules and ‘*competencia*’ of the Judicial Power and the administration of justice in Chile are contained in the General Courts Code (*Código Orgánico de Tribunales*).⁴⁵ Criminal jurisdiction is established under articles 5 and 6 of the National Criminal Code that textually provide the following:

“Article 5. Chile’s penal law is binding upon all the inhabitants of the Republic, including foreigners. Crimes committed within the territorial sea or adjacent shall be binding upon the provisions of this Code.”

“Article 6. Crimes or felonies committed by Chileans or foreigners outside of the Republic shall not be punished in Chile but solely in the terms prescribed by law.”

The procedural rules to investigate and prosecute criminals and offenders are contained in the Penal Procedural Code (*Código Procesal Penal*). Like Mexico and Argentina, the legal regime on criminal jurisdiction in Chile is mainly based on the principle of territoriality and does not specifically regulate extraterritorial jurisdiction.⁴⁶

B. Internet based Crimes

In Chile, sabotage of communication and information systems are punished under Law No. 19, 223 and the National Criminal Code. Law No. 19,223 was enacted in June 1993, and contains only four articles, which specifically punish the misuse and manipulation of data processing and information systems. Articles 1-3 punish the damage to, alteration of or interference with data-processing systems (*information sabotage*); and article 4 punishes the illegal disclosure or spreading of data contained in data processing systems (*spionage*). The National Criminal Code punishes such conducts with imprisonment terms from sixty-one days to five years depending on the circumstances of each case.⁴⁷

In addition, articles 374 bis. and 374 ter. of the National Criminal Code⁴⁸ punish the distribution, commercialization and exhibition of child pornography in any kind of support,

⁴⁵ The General Courts Code is available at the National Library of the Congress of Chile at: <http://www.bcn.cl/> (Last visited: February 28, 2009).

⁴⁶ For more on issues of extraterritorial jurisdiction, the ubiquity criterion doctrine and criminal offenses committed in Chile, see Rodrigo Zúñiga and Fernando Londoño, “*Cybercrime and Jurisdiction in Chile*” in Bert Jaap Kooops and Susan W. Brenner (Editors), “*Cybercrime and Jurisdiction. A Global Survey*”, supra note 27, Chapter Seven.

⁴⁷ An unofficial translation of Law 19, 223 in English is available at: [http://www.aladi.org/nsfaladi/ecomerc.nsf/cb1e8c4d2a4f8e4d03256da60046d248/982ee5236ab9f86303256b750062389c/\\$FILE/Chileley19223.pdf](http://www.aladi.org/nsfaladi/ecomerc.nsf/cb1e8c4d2a4f8e4d03256da60046d248/982ee5236ab9f86303256b750062389c/$FILE/Chileley19223.pdf) (Last visited: February 28, 2009).

as well as its acquisition, possession and stocking even when such conducts are made using a telecommunications system located abroad.

C. Cases

Like Mexico and Argentina, Chile has not yet issued jurisprudence or case law in the field of cybcrime. However, there have been a number of cases investigated in local courts since 2002.⁴⁹

The first case in Chile pursued under Law 19,223 was in the province of Talca in April 2003. The case involved a web-design and Internet host company (ATI-Chile) and a former employee who had been previously fired by ATI-Chile. The former employee hacked and damaged computer and data systems of the company on several occasions and accessed and damaged two websites hosted by ATI-Chile. The Court of the province of Talca asserted jurisdiction and resolved to punish and sanction the former employee with a series of criminal offenses contained in articles 1-3 of Law 19,223.⁵⁰

4. International Instruments

4.1. The Council of Europe Convention on Cybercrime

The use of ICTs and cybercrime have an obvious international component and dimension, and many governments, particularly from the developing world have recognized the need to ensure that legal protection is harmonized among nations.⁵¹ The most significant institutions in the field of cybercrime have been the Council of Europe and the European Union, which have been working together for more than a decade to address cybercrime and security issues at the regional and global level.

The Council of Europe adopted during its 109th Session of the Committee of Ministers the Convention on Cybercrime (COECC) and its Explanatory Report. The COECC was officially opened for signature in Budapest on 23 November 2001.⁵² The preamble of the Convention provides a set of objectives to be pursued with the ratification and implementation process. Among the most relevant objectives of the COECC are the following:

⁴⁸ The National Criminal Code of Chile is available in Spanish at: <http://www.bcn.cl/leyes/pdf/actualizado/1984.pdf> (Last visited: February 28, 2009).

⁴⁹ For a detailed explanation on the current lack of jurisprudence and case law in the area of cyberlaw in Chile, see Rodrigo Zúñiga and Fernando Londoño, “*Cybercrime and Jurisdiction in Chile*”, *supra* note 46, pp.146-147.

⁵⁰ See “*Chile: primer caso de hacking juzgado por la nueva reforma procesal penal*” (May 10, 2002), available at: <http://www.delitosinformaticos.com/noticias/102098246312064.shtml> (Last visited: February 28, 2009).

⁵¹ Marco Gercke, “*National, Regional and International Legal Approaches in the Fight Against Cybercrime*”, *Computer Law Review International. A Journal of Information Law and Technology*, pp.7-14 (Issue 1, 15 February 2008).

⁵² The Council of Europe’s Convention on Cybercrime (CETS 185) and its Explanatory Report are available at: <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG> (Last visited: February 28, 2009).

- “Supplement international treaties and conventions in the penal field in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence”⁵³;

“.... pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation.”⁵⁴

As of December 2008, the COECC has been ratified by 23 countries and signed but not yet ratified by 23 others, most of which are Member States of the Council of Europe. In addition, four Non-members States have signed the COECC; United States, Canada, Japan and South Africa, but they have not yet ratified it.⁵⁵

None of the Latin American countries have yet signed the COECC and its additional Protocol concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems.⁵⁶ However, Argentina⁵⁷ and the Dominican Republic⁵⁸ have recently enacted legislation following as a model the COECC.

Mexico and Costa Rica were invited by the Council of Europe to access the negotiation protocol of the COECC in March 2007, but as of March 2009, their corresponding Foreign Affairs Ministries have not formally done so. Furthermore, the Dominican Republic expressed its intention to access the COECC and its Protocol during the Octopus 2008 Conference on Cybercrime in Strasbourg in order to facilitate mutual assistance and international cooperation in the enforcement of its recently enacted legislation against cybercrime.⁵⁹

4.2. Jurisdiction under the Cybercrime Convention

⁵³ Paragraph thirteenth of the Explanatory Report of the COECC.

⁵⁴ Paragraph fourth of the Explanatory Report of the COECC.

⁵⁵ See Chart of Signatures and Ratifications, available at:

<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG>

(Last visited: February 28, 2009).

⁵⁶ The Additional Protocol (CETS 189) and its Explanatory Report are available at:

<http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=8&DF=&CL=ENG>

(Last visited: February 28, 2009).

⁵⁷ Supra note 42.

⁵⁸ See Ley Contra Crímenes y Delitos de Alta Tecnología (*Law Against Crimes and High Technology Criminal Conduct of July 23, 2007*), available in the website of Ciberdelincuencia.Org at: http://www.ciberdelincuencia.org/attachments/Ley_Contra_Crimenes_y_Delitos_de_Alta_Tecnologia.pdf

(Last visited: February 28, 2009).

⁵⁹ See Council of Europe’s news of April 17, 2008 entitled “Dominican Republic Accession to the Cybercrime Convention”, available at:

http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Default_en.asp (Last visited: February 28, 2009).

One of the most debated aspects of the COECC's provisions is Article 22 dealing with jurisdictional issues over criminal offences provided in Articles 2-11 of the Convention.⁶⁰ Article 22 of the Cybercrime Convention stipulates:

“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

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.”

The principle aim of article 22 of the Convention on Cybercrime is that the Parties establish a required level of extraterritorial jurisdiction in relation to information technology offenses by determining three relevant aspects: (i) the place where the offense was committed; (ii) which laws should accordingly apply in case of multiple jurisdictions; and (iii) how to solve positive and how to avoid negative jurisdiction conflicts.⁶¹

Paragraph 1 littera a of Article 22 is based upon the principle of territoriality.⁶² Under this paragraph, each Party is required to punish the commission of crimes established in the COECC that are committed in its territory.⁶³

⁶⁰ The offenses are: Illegal access (Art. 2); Illegal interception (Art. 3); Data interference (Art.4); System interference (Art. 5); Misuse of devices (Art. 6); Computer related forgery (Art. 7); Computer related fraud (Art. 8); Offences related to child pornography (Art. 9); Offences related to infringement of copyright and related rights (Art. 10) and; Attempt and aiding or abetting (Art. 11).

⁶¹ Henrik W. K. Kaspersen, “*Jurisdiction in the Cybercrime Convention*” in “*Cybercrime and Jurisdiction. A Global Survey*” (Ed. Bert-Jaap Koops & Susan Brenner), Chapter 2, Information Technology & Law Series 11, 2006 T.M.C. Asser Press, The Hague.

⁶² The territoriality principle provides legal authority for a state to exercise jurisdiction in a case, based on the location of the crime, *see* Henrik Kaspersen, *supra* note 61, pp. 1-11.

⁶³ See paragraph 233 of *Explanatory Report of the COECC*, available at: <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm> (Last visited: February 28, 2009).

There has been some criticism from the scientific academic community with regards to the legality of Article 22 under public international law. For instance, Spang-Hanssen mentions that “*the content of Article 22f section 1.d is not in accordance with international law and cannot become customary law as the rule suggested is contradictory to the main rule in international law that each State has the right to determine its own affairs and other states cannot intervene in Foreign States Legislation*” providing a citation of a relevant case in the field of international law.⁶⁴

Henrik Kaspersen, one of the drafters of the COECC is of the opinion that “*public international law does not protect the alleged perpetrator, because it only regulates the relation between sovereign states.*”⁶⁵

The comments of Spang Hansen and Kaspersen are particularly valid, if we analyze them in the context of public international law; however provided that cybercrime is an international problem of a global reach and dimension, and that the COECC is the only existing international treaty today for the fight against cross-border crime that provides for the harmonization of substantive and procedural criminal legislation and mutual and internal cooperation measures; member countries that have ratified this treaty recognize a ‘*standard jurisdictional approach*’⁶⁶ that should not be in conflict with their federal and local legislation when establishing jurisdiction over criminal offences committed in cyberspace.

Paragraph 1, littera d. is based upon the principle of nationality⁶⁷, a legal theory frequently applied by states with a civil law tradition. Under littera d., if a national commits an offence abroad, the party is obliged to have the ability to prosecute it, if the conduct is also an offence under the law of the state in which it was committed or the conduct has taken place outside the territorial jurisdiction of any state.⁶⁸

Another criticism of the Convention is that article 22 does not provide any definition of where a cyberspace acts occurs. According to Spang-Hanssen, *the Convention “allows exercise of Global Jurisdiction or “concealed” universal jurisdiction for the parties’ courts”* which in his view is prohibited by public international law, since Global Jurisdiction requires closeness and reasonableness between the jurisdiction and the alien in question.⁶⁹ Furthermore, the COECC does not provide rules or criteria on how to determine the place of the crime (*locus delicti*) with regard to cybercrime and thus leaves the matter

⁶⁴ Henrik Spang-Hanssen, “*Cyberspace & International Law on Jurisdiction. Possibilities of Dividing Cyberspace into Jurisdictions with help of Filters and Firewall Software*”, pp.379-380. (DJOF Publishing 2004).

⁶⁵ Henrik Spang-Hanssen, “*Public International Computer Network Law Issues*”, p.329, (DJOF Publishing 2006).

⁶⁶ See e.g. *People v. Lipsitz*, 174 Misc. 2d 571, 578, 663 N.Y.S.2d 468 (Sup Ct N.Y. Cty. 1997) where the court resolves that “traditional jurisdictional standards have proved to be sufficient to resolve all civil Internet jurisdictional issues”.

⁶⁷ The principle of “*nationality*” stipulates that nationals of a state are obliged to comply with domestic law even when they are outside its territory.

⁶⁸ See Paragraph 236 of the Explanatory Report of the COECC.

⁶⁹ Spang-Hanssen, *supra* note 65, p.329.

open to national law, case law and the interpretation of enforcement and judicial authorities.

In our view, the COECC was drafted in a general and abstract form, taking into consideration the internationally accepted principles on jurisdiction. We believe that if the convention contained a definition of cyberspace or more specifically mentioned ‘where’ and ‘when’ crime in cyberspace occurs, it would create controversy and polemic in the sphere of Internet governance since cyberspace is a definition not universally agreed upon within the academic community.⁷⁰

With regards to the establishment of the *locus delicti*, we believe that the lack of rules and criteria within the COECC would be troublesome, particularly when national courts and law enforcement authorities in Latin America apply their own laws and resolve where the place of the crime has occurred. On this issue, courts in Latin America would probably have to refer to what other courts in Europe are doing in order to establish the *locus delicti* under the COECC.

Further, pursuant to section 2 of Article 22 of the COECC, member countries have the right to make full or partial reservations in order to apply or not to apply the jurisdictional rules, only in specific cases or conditions provided in paragraphs 1.b through 1.d of Article 22. The scope of this provision responds to the fact that not all countries would be in the position to apply the jurisdictional principles contained in the COECC pursuant to their own domestic frameworks; therefore, such paragraph provides for a reservation possibility, and many countries have made full and partial reservations of the provisions of the COECC including the scope of Article 22.⁷¹

With regards to the last part of section 1.d. of Article 22 “*if the offence is committed outside the territorial jurisdiction of any State*” Spang-Hanssen mentions that “*unless the text is equal to what in international law is defined as res communis, then the text opens for many interpretations, as there in international law is no rule (s) as to where a cybercrime is “committed”*”.

We disagree with Hanssen’s statement in the sense that Article 22 of the COECC very clearly establishes four different scenarios when a country may be able to assert jurisdiction over a criminal offence committed through the use of computer systems network or through the Internet, and it even provides for a consultation mechanism in order for the parties to agree as to which one might be in a better position to claim jurisdiction and launch a criminal investigation.

Finally, effective exercise of jurisdiction over an individual committing a criminal offense under the COECC requires his extradition in the hands of a prosecuting state pursuant to

⁷⁰ See David G. Post, “*Against Cyberanarchy*” in *Who rules the Net?*, pp. 71-90, (2003, Cato Institute).

⁷¹ For a list of declarations and reservations made by different countries under the COECC, see the website of the Council of Europe, available at: <http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=185&CM=8&DF=&CL=ENG&VL=1> (Last visited: October 30, 2008).

Article 24 and the existent international extradition treaties; however, due to the extent of the topic, issues of extradition are out of the scope of analysis in this paper.

5. International Organizations Addressing Cybercrime

A. Council of Europe (CoE)

The CoE through the Economic Crime Division of the Directorate General of Human Rights and Legal Affairs has been the organization in charge of promoting the implementation and access to the COECC and its additional Protocol. The COE is currently developing a global “*Project against Cybercrime*”. The purpose of this project is very broad, but it includes the facilitation of mutual legal assistance and international cooperation between state institutions and the private sector. It also provides technical assistance to other countries in order to bring their legislations and institutions in line with the requirements of the COECC.⁷²

The CoE organizes every year the OCTOPUS Interface Conference on Cooperation Against Cybercrime in Strasbourg, France, where a large number of international organizations, justices and law enforcement officials, legal experts and researchers gather to discuss the latest cyber threats; share information concerning best practices in the implementation of the provisions of the COECC and its additional Protocol among their parties, international cooperation measures and points of contact, among other topics.

B. International Telecommunications Union (ITU)

On May 17, 2007, the ITU launched the Global Cybersecurity Agenda (GCA) as a platform to provide a framework within which the international response to the growing challenges to cybersecurity can be coordinated and addressed between member states in five key work areas or pillars.⁷³ Within the GCA, there is a High-Level Expert Group (HLEG)⁷⁴ that formulates proposals to the ITU Secretary General on possible strategies to promote cybersecurity. The HLEG comprises a sub-group working specifically on legal measures.

In a recent document issued by the HLEG, there was a wide debate on how to build on existent agreements in the legal area. The HLEG considered the example of the COECC and the Convention on the Prevention of Cyberterrorism of 2005. Some of the members of the legal measures sub-group, however, were against the COECC and mentioned that such instrument should not be proposed as the only global legal solution. In addition, some members recommended that the UN should elaborate strategies for the development of model cybercrime legislation as guidelines that can be globally applicable and interoperable

⁷² The CoE’s “Project on Cybercrime” is available at:

http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20Project/567-d-summary+workplan2008-2009c_14aug08.pdf (Last visited: February 28, 2009).

⁷³ The website of the Global Cybersecurity Agenda (GCA) is available at:

<http://www.itu.int/osg/csd/cybersecurity/gca/> (Last visited: February 28, 2009).

⁷⁴ The HLEG is a group comprising more than one hundred experts in the field of cybersecurity from a broad range of backgrounds in policy-making, ranging from government, academia and the private sector.

with existing national and regional legislative measures.⁷⁵ Further, the ITU has started to develop a Toolkit for Model Cybercrime Legislation, which aims to provide member countries with a set of guidelines that can assist in the establishment of a legislative framework to deter cybercrime. The Toolkit is expected to be available in 2009.⁷⁶

It is important to mention that the ITU through its HLEG has not yet issued studies or reports with regard to the challenges that aspects of cross-border jurisdiction and conflicts of law in the field of cybercrime among its members represent. Further, the ITU is in the process of drafting model cybercrime legislation that might create unintended legal consequences and would likely contradict some of the provisions already established in the COECC. The ITU Toolkit for Model Cybercrime Legislation would possibly lead to the creation of a double legal international standard on cybercrime and could create confusion among countries with regards to the most convenient instrument to follow and adapt to their own national legislation.

C. Organization of American States (OAS)

OAS is a regional government related organization comprised of 42 countries. OAS has an Intergovernmental Experts Group on Cybercrime conformed since 1999.⁷⁷ The Group of Experts has the following mandate: (i) complete a diagnosis of criminal activity which targets computers and information, or which uses computers as the means of committing an offense; (ii) complete a diagnosis of national legislation, policies and practices regarding such activity; (iii) identify national and international entities with relevant expertise; and identify mechanisms of cooperation within the Inter-American system to combat cybercrime; and (iv) to consider the preparation of pertinent Inter-American legal instruments and model legislation for the purpose of strengthening hemispheric cooperation in combating cybercrime, considering standards relating to privacy, the protection of information, procedural aspects, and crime prevention.

OAS' Group of Experts on Cybercrime organizes regional workshops on a regular basis with the aim of identifying the problems and strengthening the capacity and cooperation of OAS members in the development of substantive, procedural legislation and electronic evidence to combat cybercrime in the region.

On September 3-5, 2008, the U.S. Department of Justice, the Council of Europe and the Ministry of Foreign Affairs of Colombia organized a workshop on the development of

⁷⁵ Chief Judge Stein Schjølberg, ITU Global Cybersecurity Agenda (GCA), "*Report of the Chairman of HLEG*", p.6, available at: http://www.itu.int/osg/csd/cybersecurity/gca/docs/Report_of_the_Chairman_of_HLEG_to_ITU_SG_03_sept_08.pdf (Last visited: February 28, 2009).

⁷⁶ Information on the progress of the ITU's Toolkit for Model Cybercrime Legislation is available at: <http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html> (Last visited: February 28, 2009).

⁷⁷ The OAS General Secretariat through the Office of Legal Cooperation of the Secretary for Legal Affairs, serves as the Technical Secretariat to the Group of Experts on Cybercrime, pursuant to the resolutions of the OAS General Assembly. OAS Inter-American Cooperation website is available at: <http://www.oas.org/juridico/english/cyber.htm> (Last visited: February 28, 2009).

cybercrime legislation⁷⁸ with the participation of 17 countries which covered the following issues: (i) substantive and procedural laws required for an effective, comprehensive national legal framework against cybercrime; (ii) knowledge of best practices and reforms underway in the Americas and other regions of the world regarding cybercrime legislation; and (iii) steps countries can take toward strengthening national cybercrime legislation pursuant to the COECC and examples of how countries have implemented it through their national law. During the said workshop, the substantive and procedural national legislation of 17 countries was analyzed against the provisions of the COECC; however, it is worth mentioning that aspects of jurisdiction and applicable law under Article 22 of the COECC were not subject of a detailed analysis in that workshop.

D. Asia-Pacific Economic Cooperation (APEC)

APEC is a regional organization working and addressing policy issues in different areas of economic development, including ICT and telecommunications policy. Mexico, Chile and Peru are active members of that organization through their corresponding governments. APEC's Telecommunications and Information Working Group (APEC-TEL) issued the *APEC Cybersecurity Strategy*⁷⁹ during its 26th meeting in August 2002. Such initiative consists of a series of policy recommendations in order to further cooperation in six different areas of cybercrime, security and critical infrastructure protection within the APEC region. The six different areas are: (i) legal developments; (ii) information sharing & cooperation initiative; (iii) security and technical guidelines; (iv) public awareness; (v) training and education; and (vi) wireless security. The section on legal developments of APEC's Strategy contains the following recommendations:

“Member economies should, as soon as possible, adopt comprehensive substantive, procedural, and mutual assistance laws and policies that take into account the Council of Europe Cybercrime Convention.”

“APEC should facilitate member economies' efforts to develop comprehensive substantive, procedural, and mutual assistance laws and policies that take into account the Council of Europe Cybercrime Convention.”

“Economies should report on the status of their substantive, procedural, and mutual assistance laws as part of the Report on Economy Implementations of the Ten Measures included in U.N. General Assembly Resolution 55/63, “Combating the Criminal Misuse of Information Technologies.”

6. The Need for a Regional Legal Approach

⁷⁸ The report of the workshop by the Council of Europe is available at: http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20OAS/567%20oas%20col%20ws%20summary%20_8%20Sep%2009_.pdf (Last visited: February 28, 2009).

⁷⁹ APEC Cybersecurity Strategy, (August 2002) is available at: <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN012298.pdf> (Last visited: February 28, 2009).

After having analyzed the corresponding legal frameworks governing criminal jurisdiction of Mexico, Argentina, and Chile, it was found that certain similarities exist among them, particularly the fact that their approaches to jurisdictional issues strictly follow the principle of territoriality. Further, only two countries Mexico and Argentina, under very special circumstances, allow for the exercise of jurisdiction over foreign residents and nationals over criminal offenses affecting or harming their nationals. Only Mexico provides a specific rule for the prosecution of crimes pursuant to special laws or by international treaties of compulsory observance in its territory only when such crimes are not specifically punished under its federal criminal legislation.

Based on the previous findings, the similar approaches of jurisdictional issues in the field of criminal law in Latin America, as well as the current lack of specific rules on jurisdiction and competencia of national tribunals for crimes occurring in cyberspace, we recommend that a set of regional guidelines should be created in order to help and guide Latin American courts in the assertion of jurisdiction in the field of cyberspace and the application of criminal legislation for the prosecution of Internet crimes based on the principles and provisions contained in their corresponding legislations.

The guidelines could implement general accepted principles on jurisdiction regulated by public international law, and Article 22 of the COECC and its Explanatory Report. We strongly believe that such guidelines will not only harmonize jurisdictional issues and their approach by Federal and Local Courts on Internet related offenses at the regional level, but they could also be a ‘first step’ towards the implementation of cybercrime legislation and the subsequent negotiation and accession to the COECC and its Protocol.

7. Final Conclusions

Aspects of jurisdiction and applicable law in the field of cybercrime are still novel topics in Latin America and particularly among the judicial power and the entities in charge of the administration of justice. We firmly believe that Latin-American countries, through their corresponding judicial systems, will continue to claim jurisdiction on criminal conduct on the Internet pursuant to their current legislation, but only when a national interest or special motive in prosecuting a polemic case threatens to cause a serious economic damage in their own territories, and unfortunately not all cases pertaining to criminal conduct in cyberspace. This situation responds to several factors: (i) little legal knowledge of the judiciary and law enforcement on the current legal instruments and cooperation policies to combat cybercrime, both at the international and regional levels; (ii) scarce or not enough financial means, and especially the lack of training of the judiciary and law enforcement officials in using ICTs in order to determine the physical location of criminals, and the search of computer and communications equipment in order to investigate cross-border crime; and (iii) the complexity of the legal system in Latin-America in order to implement an international treaty or convention like the COECC that usually involves a long and very complex political process for its ratification and implementation at the national level. However, we believe that the COECC should continue to emerge as the only accepted model law or standard on cybercrime to be followed by Latin-American countries.

Lastly, international cooperation with the multilateral and regional organizations reviewed in this paper will continue to play a fundamental role in the creation of common policies and finding coordinated responses and viable solutions to deter cybercrime at the global level. However, more emphasis is needed in the legal field, particularly in the area of jurisdiction and applicable law in order for Latin American countries to investigate cybercrimes and prosecute offenders based within their territories and other jurisdictions.

Acknowledgements

The author would specially like to thank Professor Dr. Dr. h.c. Ulrich Sieber, Director of the Max-Planck Institute for Foreign and International Criminal Law for having provided support to carry out legal research at the Institute's library during August 2008. This paper was researched and drafted at the Max Planck Institute where I had access to a large collection of bibliography and current legal sources, as well as the chance to meet staff members, attorneys and visiting professors from all over the world. I enjoyed my academic stay and the great atmosphere of the city of Freiburg, and look forward to returning to the Max Planck Institute in the near future.

Bibliography References

Bert Jaap Koops and Susan W. Brenner (Editors), *“Cybercrime and Jurisdiction. A Global Survey”*. Information Technology & Law Series 11, (Leiden Center for Law in the Information Society, 2006).

Chris Reed, *“Internet Law. Text and Materials”*, (Cambridge University Press 2004).

Cristos Velasco, *“A Propósito de la Jurisdicción y el Derecho Aplicable en Internet”*, Entérate en Línea, Dirección General de Servicios de Cómputo Académico de la Universidad Nacional Autónoma de México (DGSCA-UNAM, November, 2005).

Cristos Velasco, *“General Summary of the Legal Framework concerning Cybercrime and Law Enforcement in Mexico”*, OCTOPUS Interface Conference 2007 of the Council of Europe, (June 11, 2007),

David G. Post, *“Against Cyberanarchy”* in Who rules the Net?, (Cato Institute, 2003).

Henrik Spang-Hannsen, *“Cyberspace & International Law on Jurisdiction. Possibilities of Dividing Cyberspace into Jurisdictions with help of Filters and Firewall Software”*, (DJOF Publishing 2004).

Henrik Spang-Hannsen, *“Public International Computer Network Law Issues”*, (DJOF Publishing 2006).

John Perry Barlow, *“Selling Wines Without Bottles. The Economy of Mind on the Global Net”*.

Marco Gercke, *“National, Regional and International Legal Approaches in the Fight Against Cybercrime”*, Computer Law Review International. A Journal of Information Law and Technology, (Issue 1, 15 February 2008).

Michael D. Scott, *“Internet and Technology Law Desk Reference”*, (Aspen Publishers 2005).

Michael Geist, *“Is There a There. Toward Greater Certainty to Internet Jurisdiction”*, (University of Ottawa, April 2001).

Stephen Zamora, José Ramón Cossío, Leonel Pereznieto, et.al, “*Mexican Law*”, (Oxford University Press, 2005).

Biography

Cristos Velasco San Martin is a Mexican attorney, holding specializations in Business Law from Instituto Tecnológico Autónomo de México (ITAM), and International Trade Law from Universidad Panamericana (UP), and an LL.M in International Trade Law from the James E. Rogers College of Law of the University of Arizona in Tucson, Arizona U.S.A. He is currently pursuing a PhD of Laws at Universidad Carlos III de Madrid (UC3M). He is a lecturer on topics related to the regulation of cyberspace, e-commerce, privacy, data protection and cybercrime law and policy at ITAM, and as a guest lecturer in other Mexican universities. He has been a visiting researcher at the Max-Planck Institute for Foreign and International Criminal Law in Freiburg, and at the Interdisciplinary Centre for Law and ICT (ICRI) of the Catholic University of Leuven in Belgium.

He is the founder and the current general director of the North American Consumer Project on Electronic Commerce (NACPEC <http://www.nacpec.org>), a not-for profit website that facilitates dissemination of information on policy and regulation of the Internet and e-commerce consumer protection.

He is also the director and coordinator of Ciberdelincuencia.Org (<http://www.ciberdelincuencia.org>) a website launched in September 2008, the purpose of which is to facilitate and promote the exchange of information in the field of cybercrime among legal and policy experts in Latin-America; and foster the share of best practices that come of each of the countries and government agencies that take part in the enforcement of cybercrime legislation. He currently lives in Madrid, Spain.