AIDP - CYBERCRIME
BRAZILIAN NATIONAL REPORT – SECTION I*

Artur de Brito GUEIROS SOUZA*

1. Introduction

Before we start our analysis of cybercrime, we must differentiate between proper cybercrime (*stricto sensu*) and improper cybercrime (*lato sensu*).

Improper cybercrime refers to those offences that have always existed in society and that are perpetrated in several ways, and which have found new ways of perpetration with technological development. Proper cybercrime, on the other hand, refers to the new forms of criminal activities that affect legal interests that did not exist before the emergence and development of information technology.

At present, both the opinion of Brazilian jurists and the case law in Brazil do not distinguish between these two modalities of cybernetic criminal activity, although the focus has been mostly on improper cybercrime, while proper cybercrime has taken a subordinate role. However, the Brazilian Legislative Power has recently shown a greater interest in creating specific definitions of crime to deal with proper cybercrime.

In this regard, one could highlight: **(i)** Bill nr. 2793/2011, which has already passed in the *Câmara dos Deputados* (Brazilian House of Representatives); **(ii)** Bill nr. 84/1999, passed in the *Comissão de Ciência e Tecnologia e Tecnologia e Informática da Câmara dos Deputados* (Chamber of Deputies' Commission for Science and Technology, Communication and Information Technology), however, its approval in plenary session, is uncertain at the time of writing; and finally, **(iii)** the Draft for the new Penal Code, whose final report has just been delivered by an expert commission to the Federal Senate, has paid special attention to the difference between proper and improper cybercrimes.

2. Criminalisation

The Brazilian legal system already criminalizes certain conducts related to cybercrime. They protect the following legal interests: **(i)** the integrity of the electronic voting system used in elections, pursuant to Law nr. 9504/97, article 72; **(ii)** confidentiality of traffic data, protected by Law nr. 9296/96 in addition to article 153, paragraph 1-A, and article 325, paragraph 1, both from the Penal Code; **(iii)** the reliability of computer data pursuant to Law nr. 8137/90, article 2, item V, in addition to articles 313-A and 313-B of the Brazilian Penal Code; **(iv)** software copyright, protected by Law nr. 9609/98, article 12; **(v)** the sexual dignity of persons under 18 years of age, confronting pedophilia and pornography, pursuant to Law 8069/90 (Children and Adolescents Act), article 241-A and its paragraphs, and amended by Law 11829/08.

In the opinion of Brazilian Jurists, there is a need to criminalize facts that result in damage or endangerment to Computer Systems and to information technology (IT) itself. An example from a Brazilian scientific work may suffice: in cybercrimes, "*a conduct may affect the natural state of the data (either its storage or its transmission) and the resources of the processing system, all of which apparently make it necessary for criminal protection to apply to immaterial and intangible components, that is, the software and the data available to the computer systems*." [1]

---

* Important notice: this text is the last original version of the national report sent by the author. The Review has not assured any editorial revision of it.

* Professor of Criminal Law at the State University of Rio de Janeiro (UERJ), Federal Prosecutor before the Court of Appeals of Rio de Janeiro, Ph.D in Criminal Law at University of S. Paulo (USP).

[1] SILVA, Rita de Cássia Lopes da. *Direito penal e sistema informático*. São Paulo: Revista dos Tribunais, 2003, p. 64/66

The same concerns can be seen in relation to *de lege ferenda* criminalization. The Draft of the Penal Code, already referred to, in its recitals states that in the so-called proper cybercrimes, one protects "*confidentiality – computer data is available solely to those individuals who were previously authorized by the computer system; integrity – the assurance that the electronic document and the computer data has not been manipulated in any way, by being destroyed or corrupted in whole or in part; and availability – the functioning and processing of the computer system (storage, retrieval, transmission)*".

In the draft of the Penal Code one recognizes the existence of a new legal interest in Brazilian Law: the "computer system". Thus, "*the election of this legal interest as worthy of criminal protection becomes necessary and legitimate by reason of the new harmful conducts that generate immediate damage to the computer system (proper cybercrime) and immediate damage to individual legal interests (improper cybercrime), justifying the anticipations of criminal protection as a first level of protection, with an aim to prevent, at the initial stage, the conducts that may cause more serious damage to social conviviality."* [2]

Even if one considers legal advances, with *de lege lata et ferenda* legal provisions for cybercrimes, the position adopted by Brazilian Courts turns out to be excessively conservative, that is, it has difficulties to recognize legal interests of an immaterial nature. In this regard, when trying a case involving the theft of values by means of Internet banking, the Brazilian Superior Court of Justice (*Superior Tribunal de Justiça*), demanded that the subtracted values be shown to have economic value, since the records entered in databases do not have "autonomous existence", being dissociated from the money value they represent. [3]

2.1 Typical examples of criminal laws concerning attacks against IT systems

Examples of the criminalization of conducts involving attacks against IT systems may be found in the legislation that governs the general elections in Brazil. In this regard, law nr. 9504/97 in article 72 punishes the following conducts with imprisonment for a term of five to ten years: **(i)** to obtain access to a system of automatic data processing used by the electoral service with the purpose of altering the polling or counting of votes; **(ii)** to develop or to introduce a command, instruction, or computer program capable of destroying, deleting, eliminating, modifying, recording or transmitting data, instructions or software, or capable of producing any other result than the expected in such an automatic data processing system used by the electoral service; **(iii)** to intentionally cause physical damage to the equipment, or its parts, used in voting, or in counting the votes.

Attacks against IT systems are provided for, *de lege ferenda*, in the draft of the Penal Code presently being analyzed in the Brazilian Federal Senate as can be shown by the crime definition provided in its article 210: "To interfere in any way, improperly or without authorization, in the functionality of a computer system or in the communication of computer data, so as to cause hindrance, impediment, interruption or serious disturbance, even if it is only partial. Penalty: one to two years imprisonment."

2.2 Typical examples of criminal laws concerning violation of IT privacy

A good example of the way violation of IT privacy has been criminalized is provided by Law nr. 9296/96, which governs judicial interceptions of telephone communications for the purposes of police investigation or production of evidence: "Article 10. It is a crime to intercept telephone communications, IT communications or Information and Communication Technology (ICT) communications, or to disclose Court proceedings closed to the public, without being authorized to do so by the Courts, or for purposes not authorized under the legislation. Penalty: two to four

[2] ANTEPROJETO DE CÓDIGO PENAL (*Draft for the Penal Code*), according to the final report of the Comission of Jurists. p. 334.
[3] CC 67.343. STJ. 3ª Seção. Rel. Min. Laurita Vaz, decision dated March 28, 2007, DJ dated Dec. 11, 2007, p. 170.

years imprisonment and fine."

The Penal Code currently in force, amended by Law 9983/00, likewise provides for conducts that violate cybernetic privacy: Article 153 (Disclosure of confidential information), paragraph 1-A: "To disclose, without cause, information that has been defined as confidential or restricted by the legislation, and which may or may not be stored in Government Computer Systems, or in Government databases: Penalty: one (1) to four (4) years imprisonment, and fine". Article 325 (Breach of confidentiality by public servants and employees), paragraph 1, item I: "To allow or to facilitate, access to Government computer systems or to Government databases to unauthorized individuals by attributing, revealing, or sharing passwords or in any other way; item II: to misuse restricted access. Penalty: six months to two years imprisonment or fine, if the fact does not constitute a more serious crime."

In the draft of the Penal Code legal concepts are provided, *de lege ferenda,* to criminalise violations of IT privacy in conformity with the following case: Article 209. Improper access: To access, improperly, or without authorization, by any means, a secured Computer System, putting computer data at risk of disclosure or misuse. Penalty: six months to two years imprisonment or fine. Paragraph 1 Anyone, who, without authorization, or improperly, shall produce, maintain, sell, obtain, import, or otherwise distribute the access codes, computer data or software, with the intent to produce the action described in the head provision of this article shall incur in the same penalty.

2.3 Typical examples of criminal laws concerning forgery and manipulation of digitally stored data

The Brazilian Tax System is fully computerized. Almost all annual tax returns of both natural persons and legal entities are made available to the *Receita Federal do Brasil* (Brazilian Inland Revenue) by Internet. Thus, in order to prevent possible events of tax evasion involving the taxpayer´s processing of data, Law nr. 8137/90, has criminalized, in its Article 2, item V, the following conduct: "to use or disclose software for data processing that allows the taxpayer to have accounting information that differs from the information that must be supplied by law to the Inland Revenue. Penalty: six months to two years imprisonment, and fine."

Sharing the same concerns with the preservation of the integrity of the public collection of taxes, the Penal Code, amended by Law 9983/90, has provided crime definitions for the *inputting of false data in Computer Systems*: Article 313-A: "to input or to facilitate, by an authorized employee, to input false data, to improperly alter or delete correct data in the Computer Systems or databases of the Government, with the intent of obtaining unfair advantage for oneself or for third parties, or to cause damage. Penalty: two (2) years to twelve (12) years of imprisonment, and fine."

2.4 Typical examples of criminal laws concerning criminalization of the creation and possession of certain virtual images, violation of copyright in the virtual sphere

In regard to violation of copyright in the virtual sphere, Law 9609/98, has been enacted in Brazil, providing for the protection of intellectual property of computer software. Article 10 of the aforementioned law, states that it constitutes a crime to "violate the copyrights of computer software", and stipulates a penalty of six months to two years imprisonment, or fine. In addition, paragraph 1 of article 12 states that if "the violation consists of the reproduction, by any means, of computer software, whole or in part, for purposes of trade, without authorization in writing from the author or its representative", the penalty shall consist of one to four years imprisonment, and fine. The same penalties shall apply to those who engage on the improper trade of the original software or its copies, produced under infringement of copyright.

As far as the creation and possession of certain virtual images go, Brazilian Law shows a special concern towards the protection of children (aged from zero to twelve years) and of adolescents (aged from 12 to 18 years), in cases of pedophilia and child pornography. Thus, Law nr. 8069/90 and amended by Law nr. 11829/08, provides for the

following crime: Article 241-A: to offer, exchange, make available, transmit, distribute, publish or otherwise disclose, included therein computer systems, Information and Communication Technology (ICT), photography, video or any other form of recording, any material that contains scenes of explicit sex involving children or adolescents. Penalty: three (3) to six (6) years imprisonment, and fine.

Those who ensure the means or services by which the photographs, scenes or images of sex or pornography involving children or adolescents are stored, as well as those who otherwise ensure access by a network of computers to the photographs, scenes or images of pedophilia or child pornography, are liable to prosecution for the same crime.

It is interesting to note that if the individuals in charge of the internet service provider fail to disable the access to the illicit content of pedophilia or child pornography once they have been formally notified to do so, they will also be actionable for this crime.

By the way, the Brazilian Supreme Court recognized, when deciding a petition for *habeas corpus*, that the internet was an appropriate conduit for making pedophilia content public, and therefore the conduct attributed to the defendant was contained within the crime definition under scrutiny (Law 8069/90, article 241-A).[4]

2.5 Typical examples of criminal laws concerning distribution of computer viruses

Given the seriousness of the issue, Brazilian Law has failed so far to criminalize the conduct pertaining to the distribution of computer viruses. However, new crimes have been provided for in the bills currently pending in the National Congress, like, for instance, the draft for the Penal Code.

In this regard the text of article 210 of the abovementioned draft defines the crime of those who, without authorization or improperly, engage in the production, storage, sale, acquisition, import or distribution of access codes, computer data or software designed to sabotage computer systems.

Along these lines, the Bill nr. 84/99, defines the crime of creating, developing or inputting data or software that is harmful to a computer, which imposes a penalty of one to four years imprisonment, and fine.

3. Issues relative to the structure of crime definition

Generally speaking, in Brazilian Law, a crime definition supplies a description of the conduct socially condemned, and is described thus: "*the set of objective and subjective elements contained in the incriminating penal norm. For a specific human conduct to have criminal relevance, it is necessary that the characters of the concrete fact mould themselves to the elements of the crime definition, to the abstract model contained in the Criminal Law; it is necessary, in short, that it is defined as a crime.*" [5]

These opinions of jurists are valid, as a matter of fact, to cybercrimes, and thus there is no specificity worth noting in the legislation pertaining to cybercrimes. Summing it up, the Brazilian legal system does not distinguish between the legal description of *cybercrimes* and the legal description of traditional crimes. Both are based on the description of the disapproved conduct, devoid of any specificity. However, one often notes, the use of open crime definitions [vagueness] for the definition of computer crimes, which is out of step with the generality of the typical description of traditional crimes.

In regard to the *object offence*, it would seem that both in the legislation currently in effect, and in the bills pending in

[4] HC 84561. STF. 2ª T. Rel. Min. Joaquim Barbosa, decision dated Oct. 05, 2004.
[5] SOUZA, Artur de Brito Gueiros & JAPIASSU, Carlos Eduardo Adriano. *Curso de Direito Penal*. Rio de Janeiro: Elsevier, 2012, p. 183.

the National Congress, the object offence in most cases seem to be *computer data*. This is, still, the opinion of Brazilian jurists when defining "computer crime" as: "*every procedure that attacks data, be it in the form they are stored, compiled, transmissible, or in transition. Hence one assumes the existence of two indissoluble elements: data (the material object), and hardware (the physical part of the system) and software (the logical part of the system) to carry out some sort of conduct with these data (means of executing).*"[6]

4. Active and passive subjects of cybercrimes

In regard to the author (active subject) of cybercrimes, the old belief that only individuals of sharp intelligence and vast technological knowledge – the so-called "hackers" or "crackers" – could commit such crimes, is now obsolete. In fact, with technological development and the greater diffusion of access to these technologies, cybercrime is now deemed to be a common crime, that is, a crime that does not require any specific qualification from its agent for its perpetration. This is also true for the victim (passive subject), that is, one cannot predict any particularity for the passive subject of the crime.

In this regard, Brazilian Criminal Law fails to provide for any crime definition that demands a special condition or quality from the agents so that they can be described as either passive or active subjects of cybercrimes. In other words, any given individual can equally be a criminal, or a victim of IT crime in Brazil. There is no legal limitation about this in Brazil. [7]

Along these lines, the bills pending in the National Congress, make no provision for crime definitions where the personal characteristics of either the criminal or the victim are required. There is, however, provisions for an increase of penalties in cases of crimes committed by public servants, or in the exercise of their profession (Bill nr. 84/99, article 15), as well as in cases where the victim is a government legal entity (draft for the Penal Code, article 209, paragraph 5 and article 210, paragraph 2).

In the scope of the Appellate Courts, it is worth mentioning a decision of the *Superior Tribunal de Justiça* (Superior Court of Justice), regarding an appeal from a defendant found guilty of the theft of values from bank accounts through the Internet. In that case, the Court decided that since the defendant had a "superior knowledge of IT within the criminal organization", and in addition, effected the conduct "from his own home, quietly and insidiously", he deserved a higher penalty than the other defendants. [8]

5. Provision for punishment for mere reckless conducts, or negligent conducts.

In Brazilian Criminal Law, there is no provision for the crime definition of recklessness or negligence in cybercrimes. The subjective element of intent (*mens rea*) must always be present, in order to frame the conduct in the Criminal Legislation.

6. Legislative technique of cybercrimes

Although the opinion of Brazilian jurists is critical of the use of the legislative technique of open crime definitions (vagueness) and open-ended crime definitions, criminal legislators often resort to these legal expedients. As mentioned before in regard to cybercrimes, one often adopts open crime definitions (vagueness), in order to avoid a lag between criminal law and technological evolution.

---

[6] FERREIRA, Lóren Formiga de Pinto. *Os "crimes de informática" e seu enquadramento no direito penal pátrio*. *In* Revista dos Tribunais, vol. 893/2010. p. 412.
[7] Along these lines, see ROSA, Fabrízio. *Crimes de informática.* Campinas: Bookseller, 2002, p. 59/61.
[8] HC 124.419. STJ. 6ª T. Rel. Min. Og Fernandes, decision dated May 19, 2011, DJe dated June 01, 2011.

One could refer, for instance, to Law 8069/90, amended by Law nr. 11829/08, article 241-A that criminalizes pedophilia and child pornography: "To offer, exchange, make available, transmit, distribute, publish or otherwise disclose through any means, included therein computer systems, Information and communication Technology (ICT), photography, video or any other form of recording that contains scenes of explicit sex involving children or adolescents. Penalty: three to six years imprisonment, and fine.

On the other hand, the Brazilian Criminal Legislation has no provision for the effects of *chilling* in the legitimate use of the internet. However, when discussing Bill nr. 2126/11, special attention was paid to the guarantee of neutrality of the Network as a form of protection to the legitimate distribution of content, given the control exerted by the copyright protection agencies.

Lastly, in regard to appropriate punishments, there is no provision other than imprisonment or the payment of fines, which specifically target cybercrime, be it on the legislation in force, be it on the pending bills which are supposed to govern the issue.

7. Scope of criminalization

In Brazilian law there are some crime definitions that criminalize merely preparatory conducts, such as the development of software or commands aiming at attacks to the electronic voting system (article 72, item II of Law nr. 9504/97), and the facilitation of access to IT systems or databases of the Government (article 325, paragraph 1, item I of the Penal Code).

Along these lines, the Draft of the Penal Code has paragraphs that show a particular concern with the preparatory acts for the future practice of cybercrimes, as the following text shows: "*the penalty is the same for cases of production, maintenance, acquisition, sale, import or distribution of certain devices or access data misused to commit, intentionally, the illicit conducts mentioned in the head provision. Such violations require the possession of means of access, or other devices, hence the need for the adoption of preventative measures, which will stop the proliferation of illicit networks for the production and distribution of these criminal ends, without requiring the effective consummation of any damage or attempt at producing them.*" [9]

There are, likewise, examples of crimes that punish the mere possession of data, as in Law nr. 8069/90 (Children and Adolescents Act) which article 241-B criminalizes the possession and storage of pornographic material involving children (from age 0 to age 12) and adolescents (from age 12 to age 18).

8. Limits of Criminal Liability

Besides the criminal liability incurred in by the direct authors of cybercrimes, Brazilian Criminal Legislation also caters for the possibility of criminal liability of site providers in the internet. In this regard the Children and Adolescents Act applies criminal sanctions against those in charge of site maintenance and data storage services, relative to the so-called child pornography. This criminalization, contained in Law nr. 8069/90, paragraphs of article 241–A, punishes the service provider for failing to withdraw from circulation the forbidden content, after being officially notified to do so.

On the other hand, Bill nr. 2126/11 ("*Marco Civil da Internet*" – *Civil Rights Framework for Internet*), which establishes principles, guarantees, rights and duties in the use of Internet in Brazil, and burdens Internet service providers with several obligations, will demand, among other measures, that connection records be kept for one year, as well as the obligation to provide the stored records when judicially requested to do so, in addition to civil liability in cases of

[9] ANTEPROJETO DE CÓDIGO PENAL. *Op cit.,* p. 336.

noncompliance with Court Orders to remove content deemed in violation of Brazilian Law.

In this regard on can easily find instances in case law, where service providers have been ordered by the Court to remove illicit content from the network, particularly in libel cases involving the so-called social networks or in relationship pages such as "Orkut" or "Facebook". [10]

9. Cyber crimes and constitutional guarantees

It would appear that the right to freedom of expression, the right to freely associate, the freedom of the press and similar rights guaranteed by the Brazilian Constitution are not a major concern in the cybercrime definitions currently in force, with the exception of Law nr. 9296/96, which in its article 10 criminalizes access without right to the contents of telephone or Information and Communication Technology (ICT) communications.

On the other hand, *de lege ferenda,* a main concern of the bills pending in National Congress are related to the right to privacy as evidenced by Bill nr. 84/91, articles 4 and 5, which protects personal information, forbidding its non-authorized collection.

There are other guarantees, provided in Bill nr. 2126/11 that stipulate rights and duties for the use of the Internet in Brazil, such as: **(i)** freedom of expression, communication and manifestation of thought, as guaranteed by the Brazilian Constitution; **(ii)** protection of privacy; **(iii)** protection of personal data as provided for in the legislation; **(iv)** the preservation and guarantee of the neutrality of the network, pursuant to the regulations; **(v)** the preservation of stability, safety and functionality of the net, by means of technical procedures compatible with international standards, and by encouraging good practices; **(vi)** liability of the agents in conformity with their activities as provided for in the legislation; and **(vii)** the preservation of the participative nature of the network.

In regard to the freedom of the press, the Brazilian Supreme Court (*Supremo Tribunal Federal*) ruled that Law 5250/67, passed during the Brazilian Military Dictatorship was unconstitutional in the terms of the Brazilian Constitution of 1988. This being the case, and given the criminalization gap, the illicit acts performed through the press, including those performed through the internet, are currently made to fit the traditional crime definitions of the Penal Code.

10. Alternatives to criminalization

Besides criminal liability, there is also non-criminal liability. In this regard it is worth of note that in Brazil, Internet civil liability is far more developed than criminal liability. However, future legislation strives to avoid any interaction between these two areas of law, as evidenced by the text of Bill nr. 2126/11, which does not approach any of the criminal aspects of Internet Regulation, making it clear that the Bill only covers the civil and administrative areas. In this regard, article 15 of Bill nr. 2126/11 expressly provides for the civil liability of the service providers that do not

[10] For instance, in a case involving offending remarks posted in the relationship page "Orkut", owned by Google Corporation, the Superior Court of Justice ruled that: "*Internet is, par excellence, a space dedicated to freedom, which is not to say that is a lawless universe and hostile to liability resulting from abuses therein. In the real world, as in the virtual one, the value of a person´s dignity is one and the same, since neither the environment where the transgressors dwell, nor the technological tools that they use can change or weaken the nature of the unwaivable, untransferable and imprescriptible principle granted by Brazilian Law. Whoever makes it technologically possible, whoever benefits economically and actively encourages the creation of communities and relationship pages in the internet has as much liability for the control of occasional abuses and for guaranteeing the personality rights of internet users and third parties, as the internet users themselves who generate and disseminate information deemed offensive to the simplest values of life in community, be it real or virtual* (…) (Appeal to the Superior court of Justice nr. 1117633. STJ. 2ª T. Rel. Min. Herman Benjamin, decision dated Mar. 09, 2010).

comply with a court order to withdraw from circulation any offensive material.

By the way, case law of the Brazilian Superior Court of Justice has already adopted the position that the administrator of the social network "Orkut", that is, Google Corporation, is liable for the immediate removal of its users´ offensive messages, even when the aggrieved party cannot supply a precise indication of the page where such information was posted. [11]

11. Extraterritorial application of Criminal Law

In regard to International Criminal Law, as a general rule, the territorial principle has been adopted by the Brazilian Penal Code in article 5: "*Brazilian Criminal Law applies to the crimes committed in Brazilian territory, without prejudice of the conventions, treaties and rules of International Law*." Paragraphs 1 and 2 of said article deal with the so-called "quasi-territory", consisting of: 1. public aircraft and ships wherever they may be located; 2. private Brazilian aircraft or ships that are in high seas on in the corresponding airspace, and 3. Private foreign aircraft and ships within Brazilian territorial waters / airspace.

Article 6 of the Penal Code, in turn, governs the "crime scene", encompassing the so-called "transnational crimes", that is, crime where the action and its results take place in different locations. According to this provision, "*a crime is deemed to have been committed in the location where the action or omission took place in whole or in part, as well as where the results were or should have been produced.*"

These general rules apply to cybercrime. Hence, in order to enforce Brazilian criminal law (domestic law), it is necessary that the conduct and / or result, in whole or in part, take place in Brazilian territory. However, if the action and / or result take place abroad, so that the cybercrime does not "touch" the Brazilian Territory, our criminal Law cannot be applied to concrete cases.

In regard to the principle of double criminality, it is assumed that said principle applies in cases involving international cooperation in criminal matters. In this regard, when requesting extradition from Brazil, so that a petition for delivery of a fugitive from justice being prosecuted for a cybercrime is granted, it is necessary to establish a correspondence between the crime for which the fugitive was convicted in the State of Origin, and Brazilian Criminal Law. This is the prevailing opinion in the Brazilian Supreme Court (*Supremo Tribunal Federal*) , which is competent to decide on petitions for passive extraditions, as it was found out when analyzing a petition for extradition of a person convicted of "IT fraud" (article 221 of the Portuguese Penal Code), since the facts corresponded to the crime of theft by deception (article 171 of the Brazilian Penal Code). [12]

On the other hand, in regard to existing cybercrimes, one notes that Brazil is not a signatory of a single treaty or international agreement which has as its specific object the fight against cyber crime. However, the recitals of the draft for the Penal Code, show that the "Budapest Convention on Cybercrime", dated 2001 and drawn up by the Council of Europe, and which entered in force in 2004, has strongly influenced the legislation being drafted in Brazil.

In the same way, and as far as one knows, the Brazilian Government has not taken part in international discussions about the harmonization or drafting of a multilateral convention on crime and the penalties applicable to cybercrime.

12. Final Considerations

According to research published by *IbopeNetRatings*, Brazil ended 2011 with 79.9 million people having internet

[11] Appeal to the Superior Court of Justice nr. 1175675. STJ. 4a T. Rel. Min. Luis Felipe Salomão, decision dated Aug. 09, 2011.
[12] Extradition nr. 1029. *Supremo Tribunal Federal*. Rel. Min. Cezar Peluso, decision dated September 13, 2006, publication on DJ dated Nov. 11, 2006.

access (37.4% of the population). By the end of 2010, 73.9 million internet users were active in Brazil; in 2009 this number was 67.5 million users. Brazil is now ranked 5th among the 20 countries with the highest number of internet users, behind only Japan, India, USA and China. In 2011, BRL18.7 billion were spent on online purchases, amounting to 1/3 of all retail sales made in Brazil.[13] Currently one out of three Brazilians owns a computer. In the business field, 95% of Brazilian Companies own computers.[14]

In 2011, American Company Symantec disclosed the results of a research enquiring on the dimensions and consequences of cybercrime, in which thousands of individuals were interviewed in 24 countries, including Brazil. According to those data, around 80% of the adult internet users in Brazil were victims of some sort of cybercrime, such as the invasion of profiles in social networks, phishing, and viruses among others, and one estimates that around 77 thousand Brazilians are conned on line every day.[15]

Along these lines the Brazilian Federation of Banks has released an estimate that in 2010, Banks would have to face around 900 thousand fraudulent operations, each with an average value of BRL1,000, that is, in that year alone, around BRL900 million would be subtracted from Brazilian bank accounts. [16]

On the subject of pedophilia or child pornography the situation in Brazil is alarming. According to information released by NGO SaferNet Brasil, there are 15,511 registered charges for child pornography in the internet, of which 35% were found in the social network "Orkut" (Google).[17] In this respect, on June 2012, 32 individuals were arrested as a result of an operation (Operation "Dirty Net") carried out by the Brazilian Federal Police with support from the Brazilian Public Prosecution Service and Interpol. This Police operation uncovered a network consisting of approximately 160 users of material of pornographic content involving children and adolescents, of which 97 users were foreign nationals and 63 Brazilians. The network under investigation was private and encrypted, and one could only enter by invitation after securing the approval of the network members.

Summing up, even though there is a significant number of cybercrimes in Brazil this report suggests that Brazilian Law regulates the issue in a fragmented and case-by-case manner, with a few articles within sparse Laws. Brazilian Law, therefore, lacks an extensive, systematic and up-to-date legislation, capable of confronting cybernetic delinquency in its multifarious forms, while doing so in a technically appropriate manner always respecting the scope of criminal law dogmas.

BIBLIOGRAPHY

CASTRO, Carla Rodrigues Araújo de. *Crimes de informática e seus aspectos processuais*. 2ª ed. Rio de Janeiro: Lumen Juris, 2003.

FERREIRA, Lóren Formiga de Pinto. *Os "crimes de informática" e seu enquadramento no direito penal pátrio*. Revista dos Tribunais, ano 99, vol. 893, São Paulo, março/2010.

INELLAS, Gabriel Cesar Zaccaria de. *Crimes na internet*. 2ª ed. São Paulo: Juarez de Oliveira, 2009.

ROSA, Fabrízio. *Crimes de informática*. Campinas: Bookseller, 2002.

SILVA, Rita de Cássia Lopes da. *Direito penal e sistema informático*. São Paulo: Revista dos Tribunais, 2003.

[13] In http://info.abril.com.br, accessed on August 03, 2012.
[14] In http://www.cetic.br/empresas, accessed on August, 2012.
[15] In http://br.norton.com/cybercrimereport/promo, accessed on August 27, 2012.
[16] In http://blogs.estadao.com.br, accessed on August 27, 2012.
[17] In http://www.safernet.org.br/site/indicadores, accessed on August 28, 2012

SOUZA, Artur de Brito Gueiros & JAPIASSU, Carlos Eduardo Adriano. *Curso de Direito Penal*. Rio de Janeiro: Elsevier, 2012.