

REGULATION AND WAYS OF CYBERCRIME: THE INTERNATIONAL CHALLENGE TO SOLVE THE EVERLASTING FREEDOM-SECURITY DICHOTOMY

By Celso Castanhêde, João Paulo J. de Oliveira, Máira Carvalho and Paulo F. Ferrari

Instantaneous global communications have given us a window on the world through which can be seen both the wonder of it all and the things that make us wonder about it all

John Naisbitt¹

1. Introduction: the new challenge

It is irresistible to make use of Naisbitt's quote highlighted by Chawki when analysing the contemporary phenomenon of cybercrime, once it expresses the modern challenge of expanding the freedom of knowledge without undermining security. This apparent, thought questionable, dichotomy between peace and freedom seems to be the main issue ever tackled by the international community, been present repeatedly in several levels and types of topics on the international agenda.

It could not be different in the recurrent and ever developing question of technology: in such field we also have to face new scenarios of State control under which equally new laws have to be created and measured in order to fit the principles that sustain the Democratic Rule of Law. Our society proves to become alarmingly more dependent on computers and the global interchange of information by them made possible. As individuals started to spend more time online it was only natural for the organized crime to dedicate their efforts to comprehend and manipulate such tools in order to improve their crime committing capacity, what generates the urge for proper governmental action, which demands severe caution not to harm the very foundations of democracy in name of a mere standard of protection.

Cybercrime is not a field just as delicate as any other legal area, it is indeed much more complicated to deal with due to the fact that it not only has its own nuances² and technical difficulties³, but also serves as a new vehicle or tool to commit more traditional offenses. Meaning that a computer network or system, or the data contained by them, can not only be direct objects of a crime, they may also serve as new, faster, and cheaper ways to perpetrate the same illicit actions committed in the physical space.⁴

Even when considering the simplest cases of cybercrime, the ones which only involve traditionally illegal behaviour executed by means of computers or computer networks, we still have to face the potential complications inherent to the very nature of cyber space:

Global computer-based communications cut across territorial borders, creating a new realm of human activity and undermining the feasibility-and legitimacy- of laws based on geographic boundaries. While these electronic

¹ (Naisbitt *apud* Chawki, 2005: 2)

² “[...]cybercrime’s ability to morph into new and different forms of antisocial activity that evade the reach of existing penal law creates challenges for legislations around the world.”(Chawki, 2005: 10)

³ “In fact, the different ways in which criminals can use computers has created many new challenges, not only for law enforcement, but for computer security professionals as well.”(Charney&Alexander, 2005)

⁴ “When speaking about cybercrime, we usually speak about two major categories of offences: In one, a computer connected to a network is the target of the offence; this is the case of attacks on network confidentiality, integrity and/ or availability. The other category consists of traditional offences- such as theft, fraud, and forgery- which are committed with the assistance of/by means of computers connected to a network, computer networks and related information and communications technology.” (Chawki, 2005: 7)

communications play havoc with geographic boundaries, a new boundary, made up of the screens and passwords that separate the virtual world from the “real world” of atoms, emerges. (Johnson & Post, 1996: 1367)

In others words, cybercrimes may be easily committed by individuals under a jurisdiction entirely distinct and miles away from the one where his victim is affected. This trans-boundary capability of a crime assisted by computer expertise is certain to create several situations of nebulous legitimacy and long inefficient international negotiations, hence the need to deeply analyse and vastly legislate over possible virtual acts, determining precisely what are the obligations and rights of one sovereign State to other when prosecuting cybercriminals, creating a minimum international system of common agreement and cooperation.

Law enforcement against computer crimes is becoming one of the main needs of our century⁵, requiring wider broaching by the international community in order to organize multifaceted coordinated actions. Bearing that in mind, the objective of this article is to approach the subject in its various possible forms, determining its international dimensions and indicating the basic legal principles involved in order to present the present development of international cooperation and determine what is still to be done and improved.

2. Cybercrime: a Theoretical Approach

For decades, cybercrime has been the stuff of Hollywood thrillers and pulp fiction novels. But the days when cybercrime was tantamount to a gaggle of teenage hackers creating viruses in their parents' basements have long since died. (Hoffman 2008, 1)

The crimes are moving faster than the legislation, thus loopholes in the legislation can be found, because the laws do not exactly apply. (Speer 2000, 9)

Common sense imagines cybercrime as the fruit of a teenager's immaturity and lack of things to do. As something small, punctual and unorganized, done in someone's basement. It is not seen as a mafia, as a lucrative industry, as a net with hundreds of members and a rigid hierarchy. The Internet has brought what some might call a revolution, yet to be understood.

Speer (2008) defines cybercrime as “activities in which computers, telephones, cellular equipment, and other technological devices are used for illicit purposes, such as fraud, theft, electronic vandalism, violating property right and breaking and entering into computer systems and networks”. In many cases, it represents an entirely new way of committing crimes, being used as a new tool for an old crime.

There are 4 major elements of cybercrime, according to Speer: location of the criminal in relation to the crime; the victim; the offender; and what is being done to eliminate the threat. Let's examine first the location of the criminal in relation to the crime, the element that gives cybercrime its uniqueness. It is not possible to arrest the criminal in the crime scene, and any investigation efforts demand cooperation between agencies. There's often a jurisdiction problem – the cybercriminal might be in one state, and the victim in other. With the necessity to cooperate, problems raise, such as competition between agencies, lack of efforts between governments, and communication failures, for an instance, making the fight against cybercrime even more difficult.

The victims also do not share a common profile. The major targets are governments and their agencies and organizations, but individuals are also victims – spam, data theft, financial crimes, viruses

⁵ For an overview of concepts and statistics related to cybercrime see Mukhtar, 2002.

and trojan horses affect millions. Laws concerning this type of crime suffer from the various and often opposite demands from the victims, which slows the process more and more. Internationally, countries such as the United States of America, that depend the most on technological devices and computers to support their infrastructure are the most vulnerable, even though they have the best security apparatus.

The offenders might have several reasons, and come from different backgrounds. They might be trying to prove themselves to someone, doing it for fun or to test their own abilities. There are also adults committing data theft to sell information, or committing financial crimes for their own benefit. Some belong to crime organizations, which have been growing in number and attacks. There are also those who, i.e., when downloading a song on the internet or copying a friend's DVD, are not aware that they are committing a crime. This variety poses the problem of monitoring possible offenders: they can be anyone. In companies such as Microsoft, Sun, and others, they might be their very own employees.

Cybercrime is a new and transforming issue. New threats are always emerging, motivated by new technologies, pushing the boundaries of security. It's a heterogeneous offense, with various actors, motivated by various reasons. Competing agendas within governments agencies, the various and often contradictory demands from victims and the problem of the right to privacy gives slows possible responses on the matter. The biggest multilateral action so far is the Council of Europe's Cybercrime Convention. However, the problem of territoriality remains ignored by States. International legislation is overall inexistent, as governments fear intervention on their national affairs and prefer to face the problem as on the domestic arena. There is much to be discussed in order to proper understand it, and many efforts to fight this new and transforming crime.

3. The many types of cybercrime

3.1 Data theft

We are addicted to information and knowledge, and our drugs are withheld from us. We are forced to seek our precious information and knowledge elsewhere. We have to find challenge somewhere, somehow, or it tears our very souls apart. And we are, eventually, forced to enter someone`s system.

Toxic Shock Group (1990, file 4)

'Why are viruses written?' This question was made in the Hacker and viruses' maker's convention in Argentina. The first answer was 'Because it's fun.'

Translated from Manual Completo do Hacker (2001, 16)

Originally, the word *hacker* describes a person with computer programming skills that modifies existing software in order to improve them, but that is not necessarily against law or the author's interests, once there are many free or open source softwares (softwares which you can modify freely). The specific term for a criminal hacker is 'cracker', but since the media often do not differ them, we will also use the term hacker to describe those who practice cybercrimes.

In *Hackers: crime in the digital sublime*⁶ (2001), Paul A. Taylor gives the reader a vast collection of quotes trying to elaborate a theory for the hackers' motivation to commit crimes. He specially explores

⁶ Hackers: crime in the digital sublime; by Paul A. Taylor, found at http://books.google.com.br/books?id=zHPT-Q1bbGwC&dq=Hackers:+Crime+in+the+Digital+Sublime&printsec=frontcover&source=bn&hl=pt-BR&ei=pW7iSqqYKMmyuAfLn-HcAQ&sa=X&oi=book_result&ct=result&resnum=5&ved=0CB4Q6AEwBA#v=onepage&q=&f=false

one motivation: addiction. And, if hacking abilities meets addiction and obsession, a new and dangerous criminal is born.

Saying hacking can be an addiction may seem a little too much, but many cases have already shown that excessive interest in computers can twist one's personality. There were even cases in which a criminal was excused from his actions because of that. An Edinburgh University student, Paul Bedworth used addiction as a defence in an incident known as the Bedworth case. *The Independent*, one of UK's biggest newspapers, wrote:

It was agreed that Mr Bedworth had broken into numerous computers in Britain and abroad by calling from the BBC microcomputer in his bedroom; that he had changed the data inside those computers; and that he had made more than 50,000 calls for which he had not paid. But his counsel found an expert witness to convince the jury that the hacker had no intent to commit the crimes, because he was so addicted to his computer that he was no longer responsible for his actions. (Harris 1993a:1)

When such addiction, or even curiosity, is held by someone with the abilities to break a system, data theft is one of the most common cybercrimes. The term applies to a great number of different actions, ranging from invading computers and mobile phones in order to obtain personal files - such as the notorious cases of private celebrities' information that are stolen and put on the web, violating their privacy - to big corporations, when the goal can be to obtain specific information or to modify them.

Between 2001 and 2002, Gary McKinnon made what some consider the biggest invasion in the United States' history. He alone invaded the government's system having access to NASA, Pentagon and military computers from his house at London. He claimed he was looking for extraterrestrial life evidences, but the US' officials said he left political messages on some of the computer he hacked into.⁷

Needless to say how dangerous is to have a country's confidential information stolen or changed. As our technology evolves, every day we have more and more important data being transmitted and stored in digital medias. For instance, Brazil has one of the most efficient voting systems in the world, which highly depends on microcomputers and intranet communication. Being so, their well functioning is a matter of national security once, if one manages to hack them, the elected president and other politicians can be changed. This scenario is not only a danger for the Brazilian people, but also a threat to democracy itself. To prevent this kind of situation, in November 2009 the country offered rewards for those who found breaches in the system or presented new ideas to improve it⁸.

Another aspect we have to consider is when the target is the media, case in which the cybercrime can also have enormous consequences. In August 2009, the hacking group entitled Skynet hacked the Brazilian TV channel Record website, changing the content of the site for various hours.⁹ They put all the website's original content down and displayed messages referring to a local scandal. Among their comments, Skynet called Record's owners thieves and showed their support to another TV channel.

⁷ <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1335485-6174,00.html>

⁸ http://www.tse.gov.br/internet/eleicoes/teste_seguranca.htm

⁹ <http://www1.folha.uol.com.br/fofha/informatica/ult124u610271.shtml>

Although the last examples were about big corporations, the most usual way of data theft is known as *phishing* and its goal are individuals, not organizations. The term comes from ‘fishing’ and implies the idea of an internet user being a fish ready to fall in an ambush. Basically, it is a fraud in which hackers pretend to be a certain company or person in order to persuade internet users to provide them information such as credit card numbers, bank passwords, usernames, id numbers, etc.

When combined with SPAM, which are unsolicited messages sent to a large number of people, they are a dangerous method, once is tricky to differ real corporation e-mails from phishing from what can be innocent publicity. Usually, hackers send the user an e-mail asking for the confirmation of any information or number. However, it has already occurred that an entire bank website was faked, leading the users to put all their account information in their hands.

3.2 Financial Crimes

It is impossible to discuss data theft without talking about money. When hackers’ motivation becomes more than just curiosity, finding challenges or proving they are capable of breaking a system, they usually go after profit. And, once their goal is money, their target can be a great number of users and their bank accounts or one big corporation’s. In these cases, not only great damage can be done to computers and data, but also great amounts of money can be involved in one single crime.

If they choose to attack numerous individuals, the *phishing* technique is usually the one chosen, since the same fake message or fake system can be sent for a large number of people. If only 1% of 100.000 users that received a scam do not notice it and enter their information, the hackers will still have total control over 100 accounts.

A less common situation was discovered by an American information technology (IT) and security company, CA¹⁰. Careless users had a hidden program named Gpcode¹¹ or LoroBot installed on their computers. The program finds common files, such as Word documents or JPG images, and encrypts them, making them inaccessible. The hackers charge \$100 to provide the user with the key to decrypt the files. This kind of ‘file kidnapping’ is a recent way of cybercrime known as *ransomware*. The text below is shown on the computer desktop after being infected, although CA says the new versions of LoroBot can already use with a 1024-bit encryption.

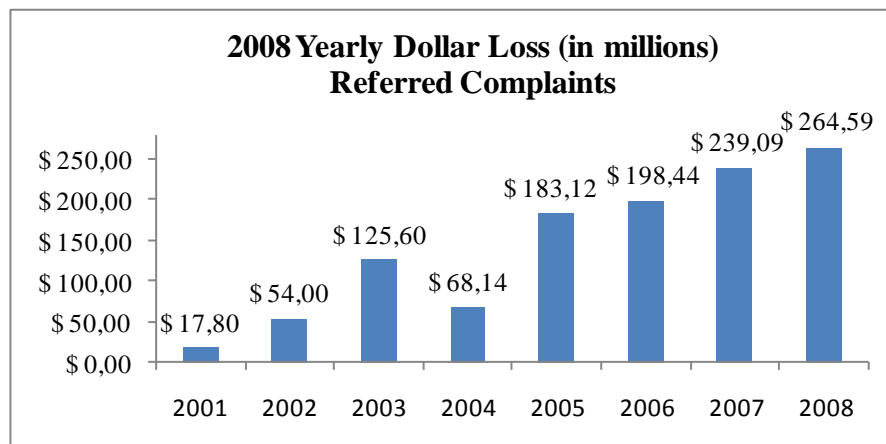
Semi-sincere apologies! Your files have been encrypted with 256-bit encryption.
For details of the encryption used, see: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard unlock price 100\$
This happened because you were infected with the LoroBot.
To recover your files, you must send an email to [...]
We have a very quick decryption file, and of course we alone know the encryption key that has been used to encrypt your files. There will be a charge for our decryption software. More details in email. And yes, this of course is blackmail, and you are being extorted. If you choose to lose your files, that's fine, if you choose to have is provide the quick and easy restore solution, you should contact us.
Ps. there is 0% chance that you will be able to manually decrypt the files without the encryption key.

¹⁰ <http://www.ca.com/us/>

¹¹ <http://www.ca.com/securityadvisor/pest/pest.aspx?id=453098767>

On the other hand, when a specific organization is chosen, although it will probably have a much more secure infrastructure, an enormous amount of money can be stolen in a single strike. Furthermore, this kind of cybercrime can be combined with the previous category: a company may be target in order to obtain private data of individual users. This type of crime happened between 2003 and 2006, when hackers invaded TJX Cos., the U.S. parent firm of Canadian retailers Winners and HomeSense. The TJX's system processes and stores data about credit and debit cards, checks and merchandise returns, but the hackers had even access to driver's licenses numbers. Just from January 2003 to November 2003 information from 45.7 million cards was stolen.¹²

To have an overall of the amount of money involved in cybercrimes, there are numerous sources that can be consulted. The Internet Crime Complaint Center¹³ (IC3) is an American organizations established as a partnership between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI). Every year, they release a report of the incidents in the US and the last of them¹⁴ (2008) provides a good range of statistics, giving an idea of the country's financial loss since 2001. As it can be seen in the graph bellow, just in 2008, more than 264 million dollars were lost in the US only because of cybercrimes.



Dollar loss of referred complaints from 2001 to 2008 in the United States. by the Internet Crime Complaint Center (IC3).

3.3 Intellectual Property Rights

In the last decades, our concept of what is valuable is changing rapidly. Money is no longer associated with gathering what is physical, what can be touched with our hands and seen with our eyes. We are learning that knowledge is untouchable yet powerful and a lucrative 'object', that it can be sold and bought as any other commercial product and that it is able to generate great fortunes.

Now, since it can be converted into expensive technology, goods or services, it is natural that knowledge is claimed by the authors as their belonging. The knowledge we are talking about can be a music or a theatre play, a technique to create a new device (like an iPod), a method to produce a medicine (like the expertise to produce anti-AIDS drugs), the code behind a new software (the new Windows 7, for instance) or many others. And when discussing about the knowledge's ownership, we

¹² <http://www.cbc.ca/money/story/2007/01/18/winnersbreach.html> and

<http://www.cbc.ca/money/story/2007/03/30/consumer-tjx.html>

¹³ <http://www.ic3.gov/default.aspx>

¹⁴ http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf

use the term Intellectual Property. Moreover, intellectual property generates great debates between countries or even within one and involves a whole field of law and rights to rule it.

According to the UN's World Trade Organization (WTO) (2009), "Intellectual property rights are the rights given to persons over the creations of their minds. They usually give the creator an exclusive right over the use of his/her creation for a certain period of time."¹⁵ Although we are going to focus on some specifics, the WTO considers Intellectual Property material ranging from machine inventions to artistic works, such as music and movies.

Even though one can think the protection of Intellectual Property is inevitable and fair, it also gives place to a lot of dilemmas and debates, even more with the access to the internet being easier day after day. For instance, if one buys an original software, one is paying the researchers and developers, recognizing their work and buying from them what they developed with a lot of effort. Even more, most companies offer great advantages, such as guarantees and updates when one purchases the original copy. On the other hand, a lot of programs are considered to be abusively overpriced, making the ease of downloading a cracked software (modified programs that can be used without buying the original) or buying a pirate copy a temptation for many. Furthermore, a regular computer user needs much more than a handful of software, making buying all of them really expensive.

In order to remain within the law, great progresses have been made in the development of open source or free software and also some prices have cheapen, but piracy of protected material is still largely practiced.

Basically, intellectual property rights can be divided in two areas: copyrights and patents. Since patents tend to be more for physical inventions, such as machines and devices, we shall concentrate upon copyrights.

3.3.1 Copyright

"[C]opyright is not about protecting authors or publishers, nor is copyright singularly about securing authors' welfare or consumers' welfare. Copyright is not about bolstering international trade balances, nor is it about protecting art, high or low. Copyright is about none of these things; and copyright is about all of them".

Goldstein (1992, 2-3)

"The natural right of an author to personally use her writings is distinct from the right, protected by copyright, to make her work public, sell it in a market, and then prevent others from making copies."

Hettinger (1989, 11)

The discussion of copyrights unravels many layers. Goldstein (1992) argues it is intrinsically related to authorship and the idea we have of it. Hettinger (1989), when discussing intellectual property, questions the labour as entitling one to copyrights, the relation to the market value, the publishers and how they are protected by copyright laws, among other subjects.

A general definition of copyright would be that it is a form of intellectual property that gives an author, for a certain amount of time, the exclusive right over his/her work. This right allows owners "to reproduce, prepare derivative works from, to distribute copies of, and to

¹⁵ http://www.wto.int/english/tratop_e/trips_e/intel1_e.htm#top

publicly perform or display the original work of authorship” (Hettinger 1989, 5). Poems, plays, drawings, paintings, sculptures, dances, theses, photographs, movies, computer programs, among many others, can be subject of it; on the other hand, it is not possible to copyright facts, ideas or concepts.

The opinions are diverse and often stand on the opposite sides of the question. There are those who see it as a monopoly, an undesirable tool that keeps prices high, refrains the transmission of information and overpays its creator. Others states that it is simply a property right, working as an incentive to creative work in general and assuring the survival of publishing companies, a fundamental tool to protect the author and publishers. There are also those who focus on punctual problems, such as the duration of the right, affirming it lasts too long and it benefits considerably more those who have the monopoly of the work than the author. According to the WTO, a patent usually lasts for 20 years and a copyright lasts for 50 years after the death of the author¹⁶.

Between the pro-copyright arguments, there's a powerful notion that supports it: that one is *entitled* to the result of one's labour. This goes back to John Locke's argumentation that the labour and the product are inseparable, being the human hand what creates the value in any object. This idea doesn't stand flawless, though: how much can we attribute to the author of a book, a movie or a play when he/she absorbs – consciously or not – an entire line of previous authors, contributions, techniques and schools? The intellectual labourer is not isolated in a room, free from any contact with society. Nozick (1974) questions why should one gain when mixing his/her labour with other's, and not simply lose it: when pouring a can of tomato sauce into the ocean, do we automatically own the ocean or did we just waste tomato sauce?

Secondly, there is a difference in being entitled to the result of one's own labour and being entitled to the market value of it. The right of a writer to use his writings might be obvious and clear, but it is distinct from his right to make them public, sell them and stop others from copying or distributing them. One cannot control the market value of products, being it merely the fruit of social and political decisions, sheer luck; why should it be attached to the notion of author rights? The value is not made by the labourer, and the market value doesn't rely only on the creator, but also in those who came before – even if they are deceased (Hettinger 1989, 10-11). How much to attribute to each author in this long line?

O'Hare (1985) points another important aspect: copyrights create a monopoly that is not necessarily the best nor the most efficient. “[I]t is not worthwhile for authors and publishers to pursue increased copyright protection for many kinds of media”, he affirms, concluding that “basic copyright protection is useful only for a subset of the intellectual property to which it now applies.” (1985, 12).

For instance, there are some companies that even thank piracy. Jamie Winans, director of the movie *Ink*, released in 2009, never expected his movie would get so much exposure as when it got ripped and made available for download. Winans sent an e-mail to the fans saying he knew the movie would at some point be pirated and it was inevitable. According to them, “what we didn't expect was that within 24 hours *Ink* would blow up. *Ink* became the number one most downloaded movie on several sites having been downloaded between 150,000 and

¹⁶ http://www.wto.org/english/tratop_e/trips_e/intell_e.htm

200,000 times as far as we can tell.” He ends the e-mail saying “We don’t know exactly where this will all lead, but the exposure is unquestionably a positive thing.”¹⁷

Of course this example is an exception and not the rule. Most companies do feel impaired by piracy, claiming their rights upon intellectual property. It is largely known how easy is to obtain music, movies and other media through the internet and that it drops drastically the author companies’ income.

Currently, there are many attempts going on to remove protected content from the web. The BREIN¹⁸ foundation is a Dutch organization against Intellectual Property theft and it is moving an action in the Dutch Court of Utrecht against the torrent tracker Mininova. They declare the website encourages piracy and makes money through advertisement and, being so, BREIN requires Mininova to remove all the under copyright links. The process is still going on, but the foundation asks for a fine of a thousand Euros for each link or torrent Mininova leaves online.¹⁹

On another perspective, companies and authors are also trying new approaches, attempting to find other profitable ways to explore their work. In the music field, there are plenty sites that are selling individual tracks instead of the entire CD. Some artists even put their work for free download in their official websites and concentrate on making money promoting shows and selling personalized accessories, such as t-shirts. Moreover, there are digital books to buy, cheap or free alternative software, free but limited versions of programs (which you have to pay to use the complete one) and new anti-copy protection methods are developed every day, though they are still inefficient since hackers always manage to crack them.

The debate becomes even more complicated when talking about cases between different countries. First of all, if some content is protected by copyright in a country, it is not necessary in others. Even though the process can be eased by existing international treaties, the author must ask for the copyright in each country he/she wants it to be protected. Second, what delimits the boundaries of a country when one is online? If one is in Brazil and is downloading a protected Japanese algorithm from an American server, which rules should apply and who should judge it, the Brazilian, the Japanese, the American, all of them or none?

Since there are still diverging opinions about copyrights, about to what extent internet’s content should be watched and limited, a solution to piracy or even to decide what should be considered piracy itself is a discussion that brings more questions than solutions. This fact shows alone the major importance of having an international authority debate it.

3.4 Child Sexual Exploitation

“At any one time there are estimated to be more than one million pornographic images of children on the Internet, with 200 new images posted daily. One offender in the UK possessed 450,000 child pornography images. It has been reported that a single child pornography site received a million hits a month... It has been estimated that there are between 50,000 and 100,000 pedophiles involved in organized pornography rings around the world, and that one-third of these operate from the United States”.

¹⁷ <http://www.jaminwinans.com/>

¹⁸ <http://www.anti-piracy.nl/english/english.asp>

¹⁹ <http://blog.mininova.org/articles/2009/08/26/mininova-considers-appealing-in-brein-case/>
<http://blog.mininova.org/articles/2009/05/18/trial-with-brein-postponed-until-june-2nd/>

Wortley and Smallbone (2006, 13)

The internet has brought both positive and negative changes to the rights of the child. It has been used as a tool to enhance children rights, through a larger exposition of their violations throughout the world to a wider public, through the greater interconnectedness between their defenders and, finally, through its usage as a tool to amplify the general awareness on the subject (HICK and HALPIN 2001, 67). Unfortunately, the opposite assertive is still a reality: it is used in manners that violate those rights, having in many ways facilitated those actions.

A basic overview would include in the concept of child sexual exploitation: sex tourism of children, child sexual molestation, child pornography, prostitution of children, among others. Online child sexual exploitation would be “exposing a child to unwanted sexual content or unwanted material via the Internet and to uninvited requests for sexual conversations. It includes employing, using, persuading, inducing, enticing, or coercing a minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct” (National Center for Missing & Exploited Children, 2008 *in* BURGESS and others, 2008).

Quayle (2008) categorizes the offenders according to several motives: situational offenders (those who aim to profit with the lucrative child pornography; adolescents or curious adults with recently discovered access to pornography; people with shaky morals and a history of violence), preferential offenders (pedophiles, being them exclusive or not; latent offenders) and miscellaneous offenders (media reporters in an investigation; pranksters; older boyfriends). Generally, offenders in all those categories are in a position of authority to the child - in the US, they are generally white men with some college education.

The crime classification is the following: traders, travelers and traffickers. Traders traffic or collect child pornography; many are teachers, clergy members, police officers and health care professionals. They are generally discovered by accident. By seeking to meet the child personally, the trader becomes a traveler. When the offender transports minors across states, it falls into the traffickers category.

The Internet provides a safe haven for those violators: “[b]ecause it is easy and anonymous to access the Internet, in the privacy of one’s own home, consumers of child pornography repeatedly search the Web for sexual images” (BURGESS and others 2008, 5). It has globalized child pornography, taking advantage of the easiness of p2p technology and the unruly new ground the cyberspace represents. It also benefits directly from the lack of critical thinking on the dangers the new technologies pose.

Privacy then enters the debate – how far can the State be allowed to delve into an investigation, and where does the limit imposed by the right to privacy become inflexible? How far does the right of privacy stretch when investigating a heinous crime? It's a complex balance between authority and liberty. The current situation is one that privacy takes complete precedence. As an instance, the Council of Europe’s Committee of Ministers stated that “any use of ICTs should respect the right to private life and private correspondence. The latter should not be subject to restrictions other than those provided for in Article 8 of the ECHR [Convention on Protection of Human Rights and Fundamental Freedoms], simply because it is carried in digital form.”²⁰ In police matters, the national regulations vary greatly among countries.

²⁰ Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society, CM(2005)56 final, 13 May 2005.

Specific new rights to Internet users are yet to be thought of, as “it is necessary to define the situation in which the exchange of personal data is deemed essential” (Rob van den Hoven van Genderen, 2008: 21).

Child sexual exploitation and abuse has existed long before the Internet has come to be. Still, this new technology has served as a mean to ease the access to pornographic material and to put in touch the offender and the victim. It can be said it reinvented and expanded these kind of violations. This section has focused on the offenders, but much can be discussed about the victim – what happens to a child who has access to pornography, who is the target of heinous crimes? Also, how can the right to privacy and police investigations live together? The debate has barely began.

4. International dimensions of cybercrime

4.1 Privacy

“Civilization is the progress toward a society of privacy. The savages' whole existence is public, ruled by the laws of his tribe. Civilization is the process of setting man free from men.”

Ayn Rand (Russian-American writer and novelist, 1905-1982)

When it comes to fighting crime, it's always good to make an observation about the limits of that fight. The right to freedom, being that civil, of possessing an individual inviolable space, being political, of participating in government, are stipulated rights in several articles of the Universal Declaration of the Human Rights. States have then the obligation to preserve these freedoms, respecting and searching for the continual improvement of the Declaration's content.

For the necessary protection of freedom, it's needed the protection of privacy, itself a human right, as stipulated in article 12 of the mentioned Declaration. Privacy is fundamental for the construction of individuality, that it is warranty for the formation of contrary opinions, in a way that it's not a surprise that privacy is among the first casualties of totalitarian regimes. In the words of Tatiana Cunha Vieira (2007:21), “You do not assure privacy without liberty, you do not exercise liberty without privacy”.²¹

Privacy is not just the warranty of freedom but it's also among the list of preconditions to the exercise of every rights of a person, here understood in the juridical broad sense as a body of rights and duties. When the Federal Constitution determines that an individual is a person, or that the Brazilian state is a person²², it is saying that they are holders of determined rights and duties. However, to the exercise of these rights, preconditions are needed, like the right to life, to freedom of thought and, as already said, to privacy, because to defend privacy is to defend personality, to defend the body of psychical characteristics that differentiate one person from the others. The right to have its personality assured derives from the human condition itself, and that is why it is necessary that these rights be formally recognized by law.

But what is the definition of privacy? First, it is needed to say that the distinction between public and private is socially and culturally constructed. An aborigine certainly does not feel ashamed for being naked in its tribe, but it would feel this way in the middle of a big city, because of the social reaction that he would feel. On the other hand, citizens of this big city certainly does not feel ashamed for being naked in a nudity beach as they naturally feel in their city. We see then how the public or private nature of human body is changed by the social and cultural context.

²¹ In the original, “não se assegura privacidade sem liberdade, não se exercita liberdade sem privacidade”.

²² It does not matter to us the difference between natural and juridical persons. Nevertheless, the reader should be aware that he is a natural person and that the state is a juridical person, and that the difference between them is that the holder of the rights and duties of a natural person is recognizable, while in the case of a juridical person, is indirect. In other words, the holder of the rights and duties of the reader is the reader itself, while in the case of the state, is the capacitated public agent.

Privacy is a concept source of great juridical debate, specially in its relation with the concepts of private life and intimacy. That's not our interest in here. We can however say that the oldest definition belongs to the American judge Thomas McIntyre Cooley, that defines the right to privacy as the right to be alone. This right is further popularized by Samuel Warren and Louis D. Brandell in their article *The Right to Privacy*, of 1890. We'll settle with the definition of privacy as the legal permission to hide from the public personal aspirations that are not to harmful to others. This definition is harmonized with the one of jurists like Brazilian Paulo José da Costa Júnior, that defines the right to privacy as “the right of the individual, if he wants, to be left alone, without the harassment of curiosity, or of indiscretion”²³, (Costa Júnior apud Silva Neto, 2001:20), or of José Afonso da Silva (Silva Neto, 2001:20), that conceptualize privacy as the body of information of the individual, that he can keep under his exclusive control, or communicate, deciding to who, when, where and in what conditions, without being able to be legally incriminated for that.

But why privacy is an cybercrime issue? As already studied, data theft is an important type of cybercrimes and directly involves the protection of privacy. The protection of personal data its the protection of privacy itself, since allowing it to be steal it's jeopardizing one's control over information that one should have exclusive control over.

Besides, privacy must be protected not just from offender's attacks but also from states itself. They must be bounded to protect privacy in the virtual space too, in order to protect freedom of its citizens, since, as we already saw, liberty and privacy walk together. Privacy must than be protected by the state and from the state. Not just states must act in order to protect its citizens' privacy in the cyberspace, it must not attack it, even in the name of cybercrime fight itself.

Chinese's Green Dam Youth Escort it's an example of state's attack on privacy. Allegedly for youth's protection of unappropriated content, Chinese government required domestic computer manufacturers and manufacturers that export computers to China to pre-install filtering software in their computers. Although retreating of it, Chinese government showed how much states are also a threat to privacy, and how not just cybercrimes, but the fight against cybercrimes, can be a threat to it.

4.2 *Fighting Cybercrime's Threat to Privacy*

Now that privacy is conceptualized and the importance of protecting it even in the fight against crime is understood, it is needed, in our study about cybercrimes, to find out how the privacy of personal data that flow among the virtual space are being defended in international politics. The concern with the protection of personal data started already in the sixties, with the control of the few gigantic computational centers that stored it. With the popularization of new communication technologies, this kind of control became impossible, and now we're already in the third generation of laws concerning that protection²⁴, in which are ways to regulate principles of treatment of personal data and the measures and safety procedures to be adopted during the collection and storage of these informations when needed.

It's in Europe that we see the greatest normative progress regarding cybercrimes, since it is involved in a longest time with new communication technologies than other continents, with the exception of America, that has not made any progress in the subject as only Canada and the USA have significant historical technological progress in the continent. Africa has no cooperation on the subject, neither does Asia . The Organization of the American states²⁵ have published an Convention on the subject, the American Convention on Informative Self-

²³ In the original, “o direito do indivíduo, querendo, de ser deixado em paz, sem o importúnio da curiosidade, ou da indiscrição”.

²⁴ The first generation of laws was the control of that few computational centers, that could only operate with permission and due control of governmental agencies. With the popularization of new technologies, came the second generation of laws, where little centers where controlled by simple notification of existence to that agencies. Due to the great spread of these technologies and to the inefficiency of these laws, it came the third, and present, generation.

²⁵ The OAS was established to achieve among its member states, as stated in Article 1 of its Charter, “an order of peace and justice, to promote their solidarity, to strengthen their collaboration, and to defend their sovereignty, their territorial integrity, and

Determination, recognizing the danger of exposition of personal data if the necessary measures of control are not taken and assuring the necessity of creating similar protection systems around the world since the problems of new technologies don't see boundaries, but has taken no step further than that.

We should see now how Europe deals with this subject. A consultive commission was established by the Council of Europe²⁶ in 1967. This commission led to two resolutions of this Council, relating personal data flow and protection of individual data, in the years of 1974 and 1976. In 1981, Convention 108 was agreed upon, a milestone because it stimulated legal harmonization not just among European countries, but any country wanting to be part of it. However, due to the non-binding character of the treaty, the European Union published Directive 95/46/CE, which obliged European countries to harmonize its legislations with the recommendations and guidelines of Convention 108. Today, European legislations are impressively harmonized, and data privacy is protected by administrative ways, by agencies, commissions and departments in each European country, responsible for inspection in accord with the directive.

4.3 International Law

"He who does not prevent a crime when he can, encourages it".

Seneca, Roman philosopher of the first century AD

As we can draw even from common sense, in order to prevent a crime, we must create a rule prohibiting it and giving warranties that this rule shall be followed. That means we have to use law to prevent crimes. But we must go further than common sense and first answer two basic questions: what is a rule and what is law?

Rules are, in a simple concept, mandatory statements that exist to avoid bad practices and to stimulate good practices amongst the ones under its control. We must stress here that we're dealing with juridical rules, which differ from moral, religious or other kinds of rules by coercion, that it's the threat or actual use of legitimate force in order to apply them. It is necessary to remember, since we'll be dealing with International Law, that a rule is only real if coercion is believable and possible.

A law is a body of juridical rules. Expanding our concept, we can define law as a body of regulatory rules of human behavior that aims to avoid bad practices and stimulate good practices with the possibility of using coercive means to reach its objectives. What would International Law then be? It would be, according to Hans Kelsen, the body of rules that regulate the conduct and relations between states. Accioly (2009:12) follows a similar thought, less focused in the State, defining international Law as "the body of juridical rules that conduct the international community, (...) specially in the mutual relations between the states and, secondarily, of other international actors, such as some international organizations, and individuals"²⁷.

International rules are rules like any other, if exists the real possibility of a international person being coerced by another in a legal way, or in other word, of happening an coercive reaction against a delict²⁸ in name of

their independence." Today it comprises the 35 independent states of the Americas and has granted permanent observer status to 63 states, as well as to the European Union. The Organization of American states constitutes the principal political, juridical, and social governmental forum in the Hemisphere.

²⁶ The Council of Europe, based in Strasbourg (France), now covers virtually the entire European continent, with its 47 member countries. Founded on 5 May 1949 by 10 countries, the Council of Europe seeks to develop throughout Europe common and democratic principles based on the European Convention on Human Rights and other reference texts on the protection of individuals. The primary aim of the Council of Europe is to create a common democratic and legal area throughout the whole of the continent, ensuring respect for its fundamental values: human rights, democracy and the rule of law.

²⁷ In the original, "o conjunto de normas jurídicas que rege a comunidade internacional, (...) especialmente nas relações mútuas entre os Estados e, subsidiariamente, das demais pessoas internacionais, como determinadas organizações, bem como dos indivíduos".

²⁸ Delict is not a violation of law, since a violation means an act of violence and law, being something abstract, can not be violated. It's not also a denial of the law, an unlawful act, since it's foreseen in law. The definition of delict it is of a conduct that is sanctionable by law.

the international legal community²⁹. As said by Kelsen (1952:15): “it is a characteristic feature of law to constitute a force monopoly of the legal community”, which means that force can only be used legally, in name of the legal community.

Force is actually used by the international community in name of the law, and the possibility of an international person being coerced to follow a rule exist, and the main evidence of this is that the International Law exists. If it was not followed, if it was but void rules, it would be soon abandoned. The mere existence of States is an evidence of International Law’s supremacy over the international community. It is certainly not the Brazilian Constitution, that created and regulated the Brazilian State, that forces the United States of America to recognize it. Only the International Law can explain the prevalence of the principles of identity and continuity of States. International Law is respected, and international rules are created because it is respected. But how it is created?

Law have sources, “documents and speeches from which rights and duties come”³⁰ (Aciolly, 2009:120), and International Law have several sources, being customs and treaties the main ones, and jurisprudence, equity and the general principles of Law as minor sources. We should focus on treaties, being then main sources of law and, by definition, easier to create, since customs differentiates from treaties by not being knowingly created and by not being created by a specific institution.

Treaties are deals, confluence of wills between two or more subjects of International Law stipulating rights and duties. Since the Vienna Convention on the Law of Treaties, of 1969 and 1986, not just states but also other international persons, such as international organizations, can sign treaties. Treaty is a generic expression, and for the International Law, equivalent to other names such as protocol, convention, declaration, among others.

So, by signing a Treaty, States create international rules, mandatory statements for the signatories to avoid bad practices and stimulate good ones. It is the possible for States to create Treaties in order to prevent cybercrimes and stimulate cooperation in the fight against these crimes. In fact, some few steps in this path have already been taken, and some treaties have already been signed.

4.4 Cooperation

Cyberspace is a concept created by science fiction author William Gibsons, meaning the “place” between two modems. It's not a physical place, and that brings several problems for countries dealing with crimes executed in it. As pointed out by Chawki(2005, 5):

Cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location. The rise of the global computer network is destroying the link between geographical location and: (1) the power of local governments to assert control over online behaviour; (2) the effects of online behaviour on individuals or things; (3) the legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply.

Not being physical, questions around the jurisdiction of states about the crimes that are committed there arouse. Let's say a businessman owns an illegal service, as a gambling website, in a country and his client is in another country. Who is to judge then? And what if gambling it's not illegal in one of these two countries, can the one that consider illegal to judge the foreigner for its actions, being that playing an illegal game or hosting a website for illegal games? In other words, what it is the jurisdiction of each country in this situation? And first, what is jurisdiction?

Jurisdiction comes from Latin, *jurisdictio*. In a simple way, it's the power of a court to compel you to physically appear before a forum for a lawsuit. Jurisdiction problems of cybercrimes are problems happening over doubts about witch state would have the it when a certain cybercrime involves several countries. It may happen when two state claim jurisdiction over the same offender, raising the question of where he must be trialled, or when

²⁹ Legal community is the body of individuals authorized to effectuate sanctions foreseen in law.

³⁰ In the original, “documentos e pronunciamentos de que emanam direitos e deveres”.

state A claim jurisdiction over a citizen of state B, and they enter in a conflict if state B refuses to deliver its citizen to be trialled by state A. Since it involves several countries, international cooperation is needed to tackle this issue.

The necessity of cooperation has long been understood, and several international organizations already have taken initiative in dealing with the issue of cybercrimes and its jurisdictional problem. They usually focus in harmonization of legislation and in coordination and cooperation of law enforcement agencies, in order to provide to its parts training, equipping and trading of information. Also, several of them stimulate security awareness in international and in national level, to clarify the importance of the subject. Lastly, some few direct anti-cybercrime actions are coordinated focusing on prevention or in investigation of cybercrime.

We must stress some examples of international organizations initiatives³¹, starting with Council of Europe's effort, being the most significant one today and finishing with other international organizations efforts like OAS³² (Organization of the American states), or APEC's³³ (Asia-Pacific Economic Cooperation). It is also necessary to recognize Interpol's Working Parties on Information Technology Crime work, which brokers efforts of specialists on regional patterns aiming for intercontinental harmonization in both legal and technical issues involved on counter-cybercrime task.

The Council of Europe created an historic landmark for the fight against cybercrimes in 2001, when the Convention on Cybercrimes became open for signatures. The Convention is the apex of nearly four years of continued negotiations and research, it discusses and recommends substantive procedural and international rules and jurisdictional issues, in other words, the totality of the legal problems regarding cybercrimes. It is considered a historical landmark because it permits countries outside of Europe to be part of it, making the global issue of cybercrimes possible to be tackled by any willing nation and also because of the range of its recommendations. In addition to that, the Council of Europe made other efforts, as the Convention 108 on personal data protection, and, more recently, in 2006, the Project against Cybercrimes, created to train judges, prosecutors and other law-enforcement officers in how to deal with cybercrimes.

APEC deals with cybercrimes recommending that the most advanced economies of the organization help the other ones, looking for law enforcement training and legal harmonization. Unfortunately, because of the great differences between the economies and legal systems involved, development in legal harmonization hasn't been satisfactory. In 2005, in the sixth APEC Ministerial Meeting on Telecommunications and Information Industry, Lima Declaration was published, encouraging members to study the Council of Europe's Convention on Cybercrimes.

The OAS, in its forum for the Ministers of Justice, in 2006, recognized the importance of sound legal framework to fight cybercrimes and urged members to endorse and harmonize cybercrime laws to make international cooperation possible. The Commonwealth³⁴ created in 2002 the Model Law on Computer and

³¹ For a complete panorama on this matter see: Li, (2007).

³² The OAS was established to achieve among its member states, as stated in Article 1 of its Charter, "an order of peace and justice, to promote their solidarity, to strengthen their collaboration, and to defend their sovereignty, their territorial integrity, and their independence." Today it comprises the 35 independent states of the Americas and has granted permanent observer status to 63 states, as well as to the European Union. The Organization of American states constitutes the principal political, juridical, and social governmental forum in the Hemisphere.

³³ Asia-Pacific Economic Cooperation, or APEC, is the premier forum for facilitating economic growth, cooperation, trade and investment in the Asia-Pacific region. APEC is the only inter governmental grouping in the world operating on the basis of non-binding commitments, open dialogue and equal respect for the views of all participants. Unlike the WTO or other multilateral trade bodies, APEC has no treaty obligations required of its participants. Decisions made within APEC are reached by consensus and commitments are undertaken on a voluntary basis.

³⁴ The Commonwealth is a voluntary association of 53 countries that support each other and work together towards shared goals in democracy and development. The world's largest and smallest, richest and poorest countries make up the Commonwealth and are home to two billion citizens of all faiths and ethnicities – over half of whom are 25 or under. Member countries span six continents and oceans from Africa (18) to Asia (8), the Americas (2), the Caribbean (12), Europe (3) and the South Pacific (10). The Commonwealth, with roots as far back as the 1870s, believes that the best democracies are achieved through partnerships – of governments, business, and civil society. This unique association was reconstituted in 1949 when Commonwealth Prime Ministers

Computer Related Crimes, as a guideline for its members. It also encouraged members to sign, ratify and implement Convention on Cybercrimes of the European Commission.

Lastly, the United Nations. As stressed by Li (2007, 10), the U.N. is a global organization and for so has unique advantages in coordinating international positions. The United Nations' General Assembly published some resolutions dealing with the issue of cybercrimes, such as resolution 55/63 (2000), and resolution 56/121 (2001)³⁵. Among the measures taken by this committee, we may list law enforcement cooperation and training, security awareness and warranties for the protections of liberty and privacy.

There are still problems that hold advance in cooperation against cybercrimes. First these are recently created crimes, new challenges to mankind, with still a lot of study to be made about how to fight them. Second, Internet is everywhere, so, any coordination not supported by every State will remain ineffective and insufficient. Thirdly, there are several coordination processes going on, leading to different solutions that may enter in conflict with each other. Despite these problems, States must take the subject seriously and focus on how to cooperate over this issue. There would be only two ways of dealing with it: breaking Internet in national networks in a way that facilitates the identification of jurisdiction, or adapting legislation to a transnational reality such as Internet. The first solution seems technically impossible and largely invasive, leaving only International cooperation in order to adapt each national legislation for this international locus that is the Internet.

5. Conclusion: what may and what must be done

The application of pertinent agreements in specific courts has demonstrated that an international forum can acquire certain achievements prior to legislation at the national level. Traditional international criminal law has aimed at harmonizing substantive law and coordinating procedural law on offences that have existed in society since the coming into being of humankind. Presently, what the countries are eager to realize is an international agreement on offences with a history of only several decades. The anxiety for success, the absence of trial practice, the lack of an accumulation of experience and knowledge, the alienation between the legislature and general public, and the different interests between the various countries, all deliver an international consensus in its lowest form. It is inevitable that during the drafting stage and particularly after the Convention on Cybercrime has been opened for signature, many commentators have published their evaluation and criticism. Combined with other progress made in international harmonization, the most important unsolved problem may be the limited participation and the limited consensus. (Li, 2004)

For many times the International Community faced the challenge of dealing with the need of juridical control of international crimes such as war crimes and crimes against humanity, but such issues were firstly addressed by supranational authorities and are almost exclusively limited to the global scenario, usually obeying to the traditional relations peculiar to physical interactions, facts that allowed the international authorities to build a solid basis for nations to work on therefore avoiding legal gaps and incoherencies. Cybercrimes, on the other hand, have already been domestically tackled in many of its forms much before the international community could properly determine the pillars and principles to be followed, this delay created mismatches amongst regional legislations³⁶; this new offenses may also work

met and adopted what has become known as the 'London Declaration' where it was agreed all member countries would be "freely and equally associated."

³⁵ Also, for more specialized guidelines, Tenth United Nation Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, and April 2000. Available at <<http://www.uncjin.org/Documents/congr10/4r3e.pdf>> (visited 13/11/2009)

³⁶ "[...]each organization and the authors of each piece of legislation have their own ideas of what cybercrime is-and isn't. These definitions [of cybercrime] may vary a little or a lot.[...] Laws in different jurisdictions define terms differently, and it is important for law enforcement officers who investigate crimes, as well as network administrators who want to become involved in prosecuting cybercrime that are committed against networks, to become familiar with the applicable laws."(Chawki, 2005: 07)

in several different levels of interaction, involving old types of victims and objects and new insubstantial and highly valuable targets, having great economical impacts and demanding a deep specialized effort to confront it.

The many ways in which cybercrime may present itself³⁷ turns it into a Hydra to modern law enforcement, and, just as the mythological been, it demands cooperation for the complete extermination of its many heads. Only through extensive international cooperation the sources of organized cybercrime may be directly confronted, once the intangible transnational linkage constituted by the World Wide Web knows no physical barriers and provides a vast variety of possible malicious acts able to be committed with relative little resources and knowledge compared to the large achievable damage, not to mention the high levels of impunity due to the difficulties involved in the process of tracking the origin of the threat and to the jurisdictional gaps which impedes proper prosecution once the responsables are located.

However, as usual in security matters, cybercrimes also requires the classical debate about how far may a State go to maintain order, the question of how much freedom is peace worth. Governments must decide if privacy must or must not be overlapped by security measures that intend to prevent economical impact, company loss, data invasion or even the threat of cyberterrorism.

Bearing in mind such properties of these new mutant forms of criminal behaviour, it is unavoidable to think of the United Nations key role in brokering national points of view towards global harmonization, generating an effective net of data interchange and legal and executive cooperation. Even though many other international organisms, such as the Council of Europe and Interpol have made significant progress in such direction, the United Nations is the one capable of combining the already produced international jurisprudence into a new, broader and deeper protocol to serve as fundamental stone for nations to base their own laws upon, minimizing disharmonies which sustain several areas of impunity. The UN abiding capability and incomparable influence must be profusely exploited if to solve the raising menace of cyber mayhem.

Bibliography

ACCIOLY, Hildebrando. (2009). **Manual de direito internacional público**. Editora Saraiva.

ALGEO, John; ALGEO, Adele. (1994). **Among the New Words**. *American Speech*, vol 69 no. 4. pp 398-410.

ASIA-PACIFIC ECONOMIC COOPERATION. *What is Asia-Pacific Economic Cooperation?*. Available in: <http://www.apec.org/apec/about_apec.html>. Accessed at 19/10/2009.

ATHENIENSE, Alexandre. (2003). *A jurisdição no ciberespaço*. Available in: <<http://www2.cjf.jus.br/ojs2/index.php/cej/article/viewFile/524/705>>. Accessed at 22/10/2009.

³⁷ “In addition to the increased scale of criminal activity the cybercrime offers, it also has a tendency to evade traditional offence categories. While some of its categories consists of using ICTs to commit traditional crimes, it also manifests itself as new varieties of activity that cannot be prosecuted using traditional offence categories.” (Chawki, 2005: 10)

BERNE CONVENTION FOR THE PROTECTION OF LITERARY AND ARTISTIC WORKS. July 24, 1971

BREIN FOUNDATION (2009). Available in <<http://www.anti-piracy.nl/english/english.asp>>. Accessed at 22/09/09.

BURGUESS, Ann Wolbert; MAHONEY, Meghan; VISK, Julie; MORGENBESSER, Leonard. **Cyber Child Sexual Exploitation**. (2008). *Journal of Psychosocial Nursing* • Vol. 46, No. 9. pp 38-45.

CA (2009). *Detalhes sobre o spyware Gpcode*. 04/06/06. Available in <<http://www.ca.com/securityadvisor/pest/pest.aspx?id=453098767>>. Accessed at 22/09/09.

CBC (2009). *TJX says hackers stole data from 45 million cards*. 30/05/07. Available in <<http://www.cbc.ca/money/story/2007/03/30/consumer-tjx.html>>. Accessed at 22/09/09.

CBC (2009). *Owner of Winners, HomeSense says hackers stole costumer info*. 18/01/07. Available in <<http://www.cbc.ca/money/story/2007/01/18/winnersbreach.html>>. Accessed at 22/09/09.

COMMONWEALTH OF NATIONS. *The Commonwealth*. Available in: <http://www.thecommonwealth.org/Internal/191086/191247/the_commonwealth/>. Accessed at 22/10/2009.

COUNCIL OF EUROPE. (2008) *Cybercrime investigation and the protection of personal data and privacy*. Discussion paper prepared by Rob van den Hoven van Genderen. France.

COUNCIL OF EUROPE. *Our objectives*. Available in: <<http://www.coe.int/aboutcoe/index.asp?page=nosObjectifs&l=en>>. Accessed at 19/10/2009.

COUNCIL OF EUROPE. *Who we are*. Available in: <<http://www.coe.int/aboutcoe/index.asp?page=quisommesnous&l=en>>. Accessed at 19/10/2009.

DUBIN, Joseph S. **The Universal Copyright Convention**. (1954). *California Law Review*, Vol. 42, No. 1, pp. 89-119.

ESPOSITO, Lesli C. **Regulating the Internet: The new battle against child pornography**. (1998). *Case Western Reserve Journal of International Law*; Vol. 30, No. 2, pp. 541.

FASS, Paula. (2003). **Children and Globalization**. *Journal of Social History*, Vol. 36, No. 4. pp 963-

977.

FINKELHOR, David; ARAJI, Sharon. **Explanations of Pedophilia: A Four Factor Model.** (1986). *The Journal of Sex Research*, Vol. 22, No. 2, pp. 145-161.

FOLHA DE SÃO PAULO (2009). *Piratas virtuais invadem site da Record e chamam bispos de ladrões.* 15/08/09. Available in [in <http://www1.folha.uol.com.br/folha/informatica/ult124u610271.shtml>](http://www1.folha.uol.com.br/folha/informatica/ult124u610271.shtml). Accessed at 22/09/09.

G1 (2009). *Hacker que invadiu Pentagono perde última chance de apelar contra extradição.* 09/10/09. Available in [in <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1335485-6174,00.html>](http://g1.globo.com/Noticias/Tecnologia/0,,MUL1335485-6174,00.html). Accessed at 22/09/09.

GOLDSTEIN, Paul. **Copyright.** (1992). *Law and Contemporary Problems*, Vol. 55, No. 2. pp. 79-91.

HARVARD LAW REVIEW. (2007). *Developments in law: the law of the media.* Available in: [in: <http://www.harvardlawreview.org/issues/120/feb07/DEVO/DEVO_intro07.pdf>](http://www.harvardlawreview.org/issues/120/feb07/DEVO/DEVO_intro07.pdf). Accessed at 22/10/2009.

HETTINGER, Edwin C. **Justifying Intellectual Property.** (1989). *Philosophy and Public Affairs*, Vol. 18, No. 1, pp. 31-52.

HICK, Steven; HALPIN, Edward. (2001). **Children's Rights and the Internet.** *Annals of the American Academy of Political and Social Science*, Vol. 575. pp. 56-70.

HOFFMAN, Stefanie. **The New Face Of Cybercrime.** (2008) . *Jericho*, Iss. 1275, pp. 16.

HUMAN RIGHTS IN CHINA. (2009). *Chinese government orders computer manufacturers to pre-install filtering Software.* 08/06/2009. Available in: [in: <http://www.hrichina.org/public/contents/press?revision_id=170097&item_id=169820>](http://www.hrichina.org/public/contents/press?revision_id=170097&item_id=169820). Accessed at 15/11/2009.

KELSEN, Hans. (1952). *Principles of international law.* Rinehart.

INTERNET CRIME COMPLAINT CENTER (2009). *2008 Internet Crime Report.* Available in [in: <http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf>](http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf). Accessed at 22/09/09.

LEMLEY, Mark A. **Place and Cyberspace.** (2003). *California Law Review*, Vol. 91, No. 2, pp. 521-542.

LI, Xingan. (2007). *International actions against cybercrime: networking legal systems in the networked crime scene.* Available in: <<http://www.webology.ir/2007/vb4n3/a45.html>>. Accessed at 22/10/2009.

MAX PLANCK INSTITUTE FOR FOREIGN AND INTERNATIONAL CRIMINAL LAW. (2009). *Extraterritorial prosecution of cybercrime.* Available in: <<http://www.mpicc.de/ww/en/pub/forschung/forschungsarbeit/strafrecht/jurisdiction.htm>>. Accessed in 22/10/2009.

MININOVA (2009). *Mininova Considers Appealing in BREIN case.* 26/08/09. Available in <<http://blog.mininova.org/articles/2009/08/26/mininova-considers-appealing-in-brein-case/>>. Accessed at 22/09/09.

MININOVA (2009). *Trial with BREIN postponed until June 2nd.* 18/05/09. Available in <<http://blog.mininova.org/articles/2009/05/18/trial-with-brein-postponed-until-june-2nd/>>. Accessed at 22/09/09.

O'HARE, Michael. **Copyright: When Is Monopoly Efficient?** (1985). *Journal of Policy Analysis and Management*, Vol. 4, No. 3, pp. 407-418.

ORGANIZATION OF AMERICAN STATES. (2009). *Who we are.* Available in: <http://www.oas.org/en/about/who_we_are.asp>. Accessed at 19/10/2009.

QUAYLE, Ethel; LOOF, Lars; PALMER, Tink. (2008). **Child Pornography and Sexual Exploitation of Children Online.** ECPAT International.

SILVA NETO, Amaro Moraes e. (2001). *Privacidade na internet: um enfoque jurídico.* EDIPRO.

SPEER, David L. **Redefining borders: The challenges of cybercrime.** (2000). *Crime, Law and Social Change*, Vol 34, No. 3, pp. 259.

SPYMAN, *Manual Completo do Hacker* (2001), Editora Book Express.

TAYLOR, Paul A., *Hackers: crime in the digital sublime* (2001). United States of America: Routledge.

TRIBUNAL SUPERIOR ELEITORAL (2009). *Teste de segurança do sistema eletrônico de votação*. Available in [in <http://www.tse.gov.br/internet/eleicoes/teste_seguranca.htm>](http://www.tse.gov.br/internet/eleicoes/teste_seguranca.htm). Accessed at 22/09/09.

VIEIRA, Sônia Aguiar do Amaral. (2002). *Inviolabilidade da vida privada e da intimidade pelos meios eletrônicos*. Editora Juarez de Oliveira Ltda.

VIEIRA, Tatiana Malta. (2007). *O direito à privacidade na sociedade de informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação*. UNB/FD.

WORLD TRADE ORGANIZATION (2009). *What are intellectual property rights?*. Available in [in <http://www.wto.int/english/tratop_e/trips_e/intel1_e.htm#top>](http://www.wto.int/english/tratop_e/trips_e/intel1_e.htm#top). Accessed at 22/09/09.

WUNDERLICH, Gene. **Property Rights and Information**. (1974). *Annals of the American Academy of Political and Social Science*, Vol. 412, pp. 80-96.