

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

By Celso Cantanhêde, João Paulo J. de Oliveira, Maíra Carvalho and Paulo F. Ferrari

### **Latin America**

Even though there are efforts to unify these countries, such as Mercosul, the formation of one single, unified and strong bloc has still not become reality. Being so, not many combined attempts have been made against cybercrime and each country is facing it individually. There are several differences between each internal policy, but all of the countries have a tendency: the increase of cybercrime and cybercriminals as the internet evolves and becomes accessible to everyone.

Computers, cell phones and other equipment become cheaper with the economic growth; as well the revolution in the last years in internet technology also makes easy to anyone access the web. This scenario brings a lot of issues together with the advantages. According to Misha Glenny, BBC's reporter and author of *McMafia: A Journey Through the Global Criminal Underworld*, "Brazil produces more cyber-criminals than any other nation" as "more and more people become computer literate"<sup>1</sup>. Furthermore, there are problems ranging from pedophilia in social networks such as Orkut to data and bank information theft, besides piracy of material protected by copyrights.

On the other hand, there are digital inclusion policies that intend to raise the education level, reducing misinformation and crime. Some countries are engaged in that ideal, lowering computer taxes and fabrication costs and managing to distribute really cheap computers. Argentina, Peru, Mexico, Haiti, Brazil, Colombia and Paraguay are some of those, but the country that seems most into the operation is Uruguay, which is working together with organizations such as One Laptop per Child<sup>2</sup> and the Inter-American Development Bank for that. Uruguay is implementing the so-called Ceibal plan (Conectividad Educativa de Informática Básica para el Aprendizaje en línea, in the original) and it is claimed to be the first country in the world to achieve one laptop per child. The One Laptop per Child organization also acts in all the other continents, especially in Africa and Asia.

### **Western Europe**

Mostly composed by the European Union (EU) but also involving other countries, the bloc is quite homogenous in fields as economy and technology. Regarding the EU, the European Commission has been developing policies to fight cybercrime as a whole and have specific operations against child sexual abuse material on the Internet, massive attacks to information systems and identity fraud.

The Commission action can be resumed in four categories: achieving a certain degree of harmonization of relevant criminal law between the EU's members; encouraging cross-border law enforcement cooperation within the EU; promoting public-private cooperation to fight cyber crime, in particular

---

<sup>1</sup> [http://www.bbc.co.uk/worldservice/documentaries/2008/05/080512\\_how\\_crime\\_took\\_on\\_four.shtml](http://www.bbc.co.uk/worldservice/documentaries/2008/05/080512_how_crime_took_on_four.shtml)

<sup>2</sup> <http://laptop.org/en/>

cooperation between law enforcement authorities and private companies; and playing a coordinating role at international level, proposing adequate legislation to EU level matters.

In the continent, enormous discussions are lying upon intellectual property rights for two of the world's greatest trackers (websites where you can download almost anything using the BitTorrent technology) have their offices in The Netherlands (Mininova) and Norway (The Pirate Bay). Both sites have hosted links that were protected by copyrights, angering local and foreign companies as well as governments. The difference between the countries' legislations created a good deal of debates, involving local and international organizations. There are legal processes still going on about both trackers.

### **United States of America, Australia, Canada and Japan**

Although these countries do not form a specific political group, they do have similarities, especially when it comes to technology and internet. To begin with, they are extremely advanced in microelectronics, which involves computers, cell phones and all kinds of hardware and software. Some of the biggest computer companies are place in their territory (if not the manufacturing plant, at least, their head offices). Secondly, but in consequence of the first, a great share of the population have access good quality computers and fast internet connection, making the access to the web an easy and popular day a day habit.

As well as in others, cybercrime also shows itself in its many forms in these countries. It is even discussed in some of the G8 meetings (Australia does not make part of the G8) as a way to perform terrorism and organized crimes and, for that, has to be avoided and combated. Even more, cases of illegal access to confidential information, data theft and privacy invasion (both of ordinary people and celebrities) are also present. Since it is particular easy to accept these acts as crimes, the governments are trying to avoid them and punish cybercriminals, but the subject becomes quite troublesome when the cybercriminal is not in the same country where the crime occurred.

Furthermore, there are other complicated issues ranging from intellectual property rights, as it occurs in Europe and also it's worsened by territoriality, to industrial spying, since the technology companies are always competing, and hacker attacks to economy institutions, for a big part of the global stock market is operated with computers.

### **Eastern Europe**

Due to its recent common soviet history, this part of the world still has a similar international position. In the issues of cybercrime, two facts are important, the great number of cybercriminals in these areas and the fragility of democratic institutions, which leads to authoritarian police methods and insufficient cybercrime combat.

Russia, being the most important country of the region, is a model for the rest of it. Internet freedom is far from being complete in the country. It is known that Russian internet providers have being blocking access to an opposition aggregate news site. Furthermore, Russian involvement in the attack on the website twitter in august of 2009 is suspected, since it's known that the attacked was directed to a pro-Georgia blogger.

Besides of the cybercrimes committed by the state, there are also a great number of hackers in the region. According to the newspaper Pravda,

The issue of Russian hackers was touched upon at the recent e-Crimes Congress in London. Head of the RF Interior Ministry's department for special technical activities Lieutenant-general Boris Miroshnikov spoke at the congress. He said, the police provided reliable data proving that Russian hackers are better than their foreign "colleagues." This is quite understandable, he says, because the Russian mathematics school is known as one of the world's best schools; today programmers from Russia successfully work all over the world. This is the reason why Russian hackers perform so wonderfully.

The Interior Ministry is anxious over the increasing number of hackers in this country. In the mid-1990s, hackers were just mere net hooligans who cracked websites of banks or informational systems of governmental structures just for fun. But today, hackers form virtual gangs and earn much money cracking important websites.

Normally aimed at western countries, these hackers have already spread losses in the region. In 1999, Ukraine lost around 20 million dollars of its Reserve Fund for unauthorized access to its National Bank. Legislation efforts on the fight against cybercrimes are still not enough in the region. Though Ukraine have signed and ratified the Convention on Cybercrime of the European Council, Czech Republic, for instance, have not yet ratified and Russia have not even signed it, and so did several other neighbor countries.

As for copyright infringements, Eastern Europe countries have been updating its legislations in order to make copyrights infringements combat easier, and have been compromising in enforcing these legislations. In this scenario we can see Part IV of the new modern Russian civil code, with a chapter on the subject. Yet, polish legislation on the subject is already 15 years old, and so it's the case in other states. According to David Martin, head of anti-piracy of the British Phonographic Industry, Eastern Europe is a focus of piracy to be fight. According to BBC,

The BPI is working with a global body, the International Federation of Phonographic Industries, to tighten up copyright laws in other parts of the world. Mr. Martin said they were also trying to crack down on commercial CD plants in the former USSR and Eastern Europe, who often copy CDs on an industrial scale without paying royalties to artist and publishers.

## **Autocracies**

Countries identified here as autocracies are ones with what we may call pervasive censorship on Internet. This censorship severally defines the way that these countries fight and even define cybercrime. Some of them are listed in the Internet enemy list of the Reporters Sans Frontières, others are just well known for its restrictions. In common, not just cybercrimes as the ones studied but also political opposition is targeted by the police in the web, retaliating violations of such kind with imprisonment or other sanctions.

An example of these policies is the creation of a special police unit for cybercrime monitoring by the Iranian government, in November 2009. Although not only for, it's know that this unit will aim at the political opposition of the government, since the web was heavily used by then after the elections of mid 2009. It is known that the Iranian police already monitor the Internet, and that have already banned several pornography websites and even some political opposition ones.

As for cybercrime in general, these countries are, like most of the underdeveloped world, catching up with legislation efforts. Saudi Arabia recently ratified laws against cybercrime with sanctions of 1 year of imprisonment for criminals or even fines of around U\$ 130,000. These laws were proposed by the nation's advisory council, the Shura, in 2006 in order to expanded already existing laws regarding pornography and were ratified by King Abdullah in the following year. China has also created new regulations recently, in

November 2009. It proposed that state agencies and telecommunication operators were created to better monitor the web in order to catch cybercriminals. China have been facing great problems with botnets, computers infected with softwares that let the attackers control them remotely, with up to one million computers infected in 2008.

In the copyrights agenda, these countries face similar problems. They're safe heavens for piracy, due to its weak and/or corrupt police institutions that cannot fight copyrights and infringements properly, let aside its government's compromises and wishes of cooperating with record, movie and software industries. For instance, the Chinese government has signed in 2007 a memorandum of understanding with Motion Picture Association of America, the Business Software Alliance, the Association of American Publishers and the Publishers Association of the UK, among other industry associations, to help fight piracy and protect on line copyright. Still,

According to IDC, a research firm doing annual studies country by country, the piracy rate of software in China reached 86 percent last year and resulted in more than three billion dollars in losses by 2005. Piracy in China extends well beyond software with China believed to be the world's leading source of pirated goods in general. American officials say Chinese piracy costs legitimate producers up to \$50 billion a year in lost potential sales.

### References

3 ARANTES, Silvana. (2009). *Plano de distribuição de laptops é trunfo em eleição no Uruguai*. Available in <<http://www1.folha.uol.com.br/folha/mundo/ult94u640997.shtml>>. Written at 10/21/09. Accessed at 12/19/09.

• BBC NEWS. (2002). *Music piracy in UK soars*. 18/12/2002. Available in: <<http://news.bbc.co.uk/2/hi/entertainment/2588013.stm>>. Accessed at 26/12/2009.

• BBC NEWS.. (2003). *Iran steps up net censorship*. 12/05/2003. Available in: <<http://news.bbc.co.uk/2/hi/technology/3019695.stm>>. Accessed at 26/12/2009.

4 BBC RADIO. (2009). *How Crime Took Over the World*. Broadcasted on 05/19/08. Available in <[http://www.bbc.co.uk/worldservice/documentaries/2008/05/080512\\_how\\_crime\\_took\\_on\\_four.shtml](http://www.bbc.co.uk/worldservice/documentaries/2008/05/080512_how_crime_took_on_four.shtml)>. Accessed at 12/19/09.

• COMPUTER WORLD. (2009). *China toughens cybercrime rules*. 19/05/2009. Available in: <[http://blogs.computerworld.com/china\\_toughens\\_cybercrime\\_rules](http://blogs.computerworld.com/china_toughens_cybercrime_rules)>. Accessed at 26/12/2009.

• COUNCIL OF EUROPE. (2007). *Cybercrime legislation – Country Profile: Russian Federation*. Available in: <<http://www.coe.int/T/DG1/LegalCooperation/Economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Russia%20april%202008.pdf>>. Accessed at 26/12/2009.

• COUNCIL OF EUROPE. (2007). *Cybercrime legislation – Country Profile: The Czech Republic*. Available in: <[http://www.coe.int/T/DG1/LegalCooperation/Economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Czech%20Rep%2030%20May%202007\\_En.pdf](http://www.coe.int/T/DG1/LegalCooperation/Economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Czech%20Rep%2030%20May%202007_En.pdf)>. Accessed at 26/12/2009.

• COUNCIL OF EUROPE. (2007). *Cybercrime legislation – Country Profile: Ukraine*. Available in: <<http://www.coe.int/T/DG1/LegalCooperation/Economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Ukraine%208Oct07.pdf>>. Accessed at 26/12/2009.

5 EMBASSY OF JAPAN. (2009). *G8 Justice Ministerial Meeting Concludes in Washington*. Available in: <<http://www.us.emb-japan.go.jp/english/html/pressreleases/2004/040517.htm>>. Written at 05/17/04. Accessed at 12/20/09.

6 EUROPEAN COMMISSION (2009). *Fight Against Cybercrime*. Available in <[http://ec.europa.eu/justice\\_home/fsj/crime/cybercrime/fsj\\_crime\\_cybercrime\\_en.htm](http://ec.europa.eu/justice_home/fsj/crime/cybercrime/fsj_crime_cybercrime_en.htm)>. Accessed at 12/19/09.

7 FELITTI, Guilherme e LUCA, Lygia de. (2009). *Senado detém suposto lobista do Google Brasil na CPI da Pedofilia*. Available in <<http://idgnow.uol.com.br/internet/2008/06/26/senado-detem-suposto-lobista-do-google-brasil-na-cpi-da-pedofilia/>>. Written at 06/26/08. Accessed at 12/19/09.

• GOLUBEV, Vladimir. (2003). *Fighting Cybercrimes in Ukraine*. Available in: <<http://www.crime-research.org/news/2003/06/Mess0801.html>>. Accessed at 26/12/2009.

8 INTER-AMERICAN DEVELOPMENT BANK. (2009). *Uruguay to expand laptop availability for students with IDB assistance*. Available in <<http://www.iadb.org/news-releases/2009-12/english/uruguay-to-expand-laptop-availability-for-students-with-idb-assistance-6095.html>>. Written at 12/09/09. Accessed at 12/19/09.

9 NARCELLI, Rita. (2009). *Azaredo apresenta ao Parlamento do Mercosul projetos sobre crimes de informática*. Written at 08/06/07. Available in <<http://www.senado.gov.br/comunica/agencia/mercosul/not39.htm>>. Accessed at 12/19/09.

• PRAVDA. (2005). *Russian hackers recognized best in the world*. 14/04/2005. Available in: <[http://english.pravda.ru/main/18/90/362/15287\\_hacker.html](http://english.pravda.ru/main/18/90/362/15287_hacker.html)>. Accessed at 26/12/2009.

• REPORTERS SANS FRONTIÈRES. (2006). *List of the 13 Internet enemies*. Available in: <<http://www.rsf.org/List-of-the-13-Internet-enemies.html>>. Accessed at 26/12/2009.

• THE EXILE. (2008). *Russia Toying With Internet Censorship?*. 29/02/2008. Available in: <[http://exile.ru/blog/detail.php?BLOG\\_ID=17285&AUTHOR\\_ID](http://exile.ru/blog/detail.php?BLOG_ID=17285&AUTHOR_ID)>. Accessed at 26/12/2009.

10 THE OLPC WIKI. (2009). Available in <[http://wiki.laptop.org/go/The\\_OLPC\\_Wiki](http://wiki.laptop.org/go/The_OLPC_Wiki)>. Modified at 12/19/09. Accessed at 12/19/09.

• THE SIDNEY MORNING HERALD. (2009). *Iran creates Internet crime unit*. 14/11/2009. Available in: <<http://news.smh.com.au/breaking-news-technology/iran-creates-internet-crime-unit-20091114-if0k.html>>. Accessed at 26/12/2009.

11 TORRENT FREAK (2009). *Behind the Scenes at Mininova*. Available in <<http://torrentfreak.com/behind-the-scenes-at-mininova-090316/>>. Written at 03/16/09. Accessed at 12/19/09.

• VIRUSLIST.COM. (2007). *Saudi Arabia toughens stance on cybercrime*. 30/03/2007. Available in: <<http://www.viruslist.com/en/viruses/news?id=208274060>>. Accessed at 26/12/2009.

• WEB TV WIRE. (2006). *Chinese Government promises to help fight online piracy*. 19/12/2006. Available in: <<http://www.webtvwire.com/chinese-government-promises-to-help-fight-online-piracy>>. Accessed at 26/12/2009.