

Status in 2013 of the legislation to fight cybercrime in Brazil and protection of the internet

As I discussed here in 2009, the Brazilian Senate approved, on 9 July 2008, a bill of law to typify cybercrimes and to stipulate the corresponding penalties. The bill was forwarded to the Chamber of Deputies for a review of the amendments included.

Finally, in November 2012 we made an agreement and approved two Laws, the first¹ expanding “The Anti-Racism Act” and creating specialized Police to fight cybercrime and the second² with some of the original typifications transferred to it, typifying the fraudulent creation of credit and debit cards, the invasion of electronic devices, and its resultant crimes such as diffusion of malicious code causing harm, capture of passwords, and destruction or capture of electronic data. This Law also expands the provision of “Disruption of public utility services”.

Some autonomous or independent cybercrimes were left to further discussions, because consensus was not achieved, such as the dissemination of malicious codes to steal passwords (phishing) and attacks against the computer network (DoS, DDoS, DNS etc.).

The Brazilian Federal Constitution provides that a law must exist to compel individuals to act or not act in a certain way. It also determines that a law must be created to typify crimes and determine penalties.

Brazil has specific pieces of legislation to deal with Copyright, proprietary software rights and rules to fight piracy in music and videos, as well as child pornography, including a Special Agreement with Google. So, the country has significant and appropriate legislation to address cybercrime.

Unfortunately, the decision to send a letter of interest to the Council of Europe expressing the wish to take part in the signing of the Convention of Budapest on Cybercrime is still waiting for consideration. However, there is an internal document to the Ministry of External Relations, which will support this decision, produced in the last quarter of 2008, by a working group composed of additional Brazilian authorities related to Brazilian legislation on cybercrime, comparing it, article by article, to the Convention on Cybercrime.

Nevertheless, on 24 August 2011 Madame President sent Congress a new bill named “Civil Mark of the Internet”. A part of the old bill about cybercrime was transferred to Civil Mark. This part determined network providers to ensure preservation of connection data as well as access data and permits disclosure of that information, including data for auditing purposes, provided there is express judicial authorization.

Civil Mark is going to be approved this year, if consensus is reached. The main difficulties are about network neutrality and local operation of datacenters that hold Brazilian citizens’ data. Concerning neutrality, the government says that the only parameters to be used are speed and the amount of data transferred. No additional charges will be allowed based on content such as e-mail, videos, sound, social networks, etc. However, the majority of the Chamber wants to leave these questions to be considered on an individual basis between consumers and providers. With regard to local operation datacenters, the government will likely withdraw.

“Civil Mark of the Internet” was suggested at the UN by the Brazilian Government to be discussed by other nations because of recent USA (NSA) affairs, involving the President of Brazil, the Prime Minister of Germany and the President of France, as well as many other persons, as published by the press.

In September, President of Brazil said:

“I would like to bring to the consideration of delegations a matter of great importance and gravity. Recent revelations concerning the activities of a global network of electronic espionage have caused indignation and repudiation in public opinion around the world.

In Brazil, the situation was even more serious, as it emerged that we were targeted by this intrusion. Personal data of citizens was intercepted indiscriminately.

¹ Law 12.735, approved on 7/11/2012, signed by Madame President on 30/11/2012, enforced as of 1st April 2013.

² Law 12.737, approved on 7/11/2012, signed by Madame President on 30/11/2012, enforced as of 1st April 2013.

Corporate information - often of high economic and even strategic value - was at the center of espionage activity.

Also, Brazilian diplomatic missions, among them the Permanent Mission to the United Nations and the Office of the President of the Republic itself, had their communications intercepted.”

And Brazilian Ambassador at UN, former Minister of Foreign Relations of Brazil, H.E. Antonio Patriota, said:

“Brazil and Germany introduced the text on which action will be taken in a few minutes. Since 7 November, the list of co-sponsors has consistently grown, from the initial 10 co-sponsors to the current close to 50 Members.

Co-sponsors to document L.45/Rev.1 represent a wide spectrum of the UN Membership, including countries of all regions of the world and levels of development. The breadth of support clearly signals the importance of the issue.”

He also said:

“We expect that resolution L.45/Rev.1 will launch a debate that is central to our times on surveillance and respect for human rights in cyberspace.”

I hope that this brief presentation was enough to keep you updated on the recent developments of the Brazilian legislation to fight cybercrime in the country.

Thank you for your attention.

Federal Deputy **EDUARDO AZEREDO**