

## Status of the legislation to fight cybercrime in Brazil

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. The country did not have, however, appropriate legislation to address cybercrime. The legislation to fight cybercrime in Brazil is therefore the core of this presentation.

The Brazilian Senate is now discussing a bill of law to typify cybercrimes and to stipulate the corresponding penalties. This bill brings together three other bills, one of which is from 1996. The bill was first approved by the Senate Committee on Education (CE) in May 2005. Next, it was approved by the Senate Committee on Science and Technology (CCT) in December 2007. At present, the bill is awaiting a review by the Senate Committee on Economic Issues (CAE), after which it will be sent to the Committee on Constitution and Justice (CCJ). The bill will then be forwarded to the House of Representatives for a review of the amendments included.

The Brazilian Federal Constitution provides that a law be created to typify crimes and determine penalties. It also determines that a law must exist to compel individuals to act or not act in a certain way. Hence the need for the present bill of law, which both typifies cybercrimes and determines that network providers ensure preservation of connection data. Providers will only be allowed to disclose information, including data for auditing purposes, provided there is express judicial authorization.

The bill of law modifies and expands **eight** pieces of Brazilian legislation: *1-The Criminal Code; 2-The Criminal Procedural Code; 3-The Military Criminal Code; 4-The Consumer Protection and Defense Code; 5-The Federal Police Act on Uniform Repression; 6-The Telephone Interception Act; 7-The anti-Racism Act; 8-The Statute of the Child and Adolescent.* The anti-Racism Act and the Statute of the Child and Adolescent were included in the last review.

Following are the **thirteen** crimes to be typified in both Criminal and Military Criminal Codes: *1-The dissemination of malicious codes to steal passwords (phishing); 2-Credit card fraud; 3-Cell phone cloning; 4-Stipulation of increased penalties for offenses of libel, slander, and defamation; 5-Creation, insertion and dissemination of malicious codes to cause harm (viruses, Trojans, worms etc.); 6-Unauthorized access to a computer network, if authorization is required; 7-Unauthorized access to information and unauthorized possession, transportation or provision of such information, if authorization is required; 8-Unauthorized disclosure of a databank, if authorization is required; 9-Compound larceny with the use of computer systems; 10-Disruption of public utility services; 11-Attacks against the computer network (DoS, DDoS, DNS etc.); 12-Racism on the internet; and 13-Keeping digital files with pedophile content.* Racism on the internet and Keeping digital files with pedophile content were included in the last review.

In the Criminal Procedural Code, preventive detention is included to apply to cybercrimes. The Act on Uniform Repression by the Federal Police is also going to cover interstate and international offenses using IT. The Telephone Interception Act will comprise cybercrimes; and the Consumer Protection and Defense Code will incorporate a security alert for the ordinary consumer.

In the near future and after consultation with other Brazilian authorities, the Ministry of External Relations will send a letter of interest to the Council of Europe expressing the wish to be a party in the Budapest Convention. I have presented the contents of the Convention to the Mercosur Parliament, of which I have the honor to be a member. Last year Mr. Alexander Serge, from CoE, presented the contents of the Convention to the members of the Brazilian Internet Steering Committee (CGI.br).

The Senate recently approved a bill of law to prohibit spamming. A system will be created which is a cross between the opt-in and opt-out methods: it will only accept emails if previous contact existed between sender and recipient. If not, the email will be classified as a spam. Spammers will have to pay a fine and if proven that false names or addresses were used, they will be charged with misrepresentation. The Senate has also recently approved the creation of a Special Investigation Committee (CPI) to inquire into pedophilia on the internet and its link to the organized crime.

I hope that this brief presentation was enough to bring you updated on the recent developments of the Brazilian legislation to fight cybercrime in the country. Thank you for your attention.

Senator **EDUARDO AZEREDO**