www.coe.int/cybercrime

International workshop on cybercrime legislation

(Bogota, Colombia, 3-5 September 2008)

More than 60 representatives from 17 countries of Latin America[1] participated in an international workshop aimed at strengthening national legislation in line with the Convention on Cybercrime of the Council of Europe. The workshop was organized by the Government of Colombia, the Organization of American States, the Council of Europe and the United States Department of Justice.

By the end of the workshop, draft profiles had been prepared for each of the 17 countries analyzing existing or draft national legislation against the provisions of the Convention and identifying needs for further legislative work.

In general terms, a considerable number of provisions is already in place in different countries.

Regarding substantive criminal law, that is, the conduct to be criminalized, several countries cover child pornography on the internet in the comprehensive manner of Article 9 of the Convention on Cybercrime. The illegal access to computer systems (Article 2) and data interference (Article 4) are also provided for in one way or the other in most countries.

On the other hand, the legislation of several countries was unclear with regard to the difference between data interference (Article 4) and system interference (Article 5), and thus it is not certain whether a botnet or denial of service attack would constitute a criminal offence. The same is true for the misuse of devices, that is, the production, sale or distribution of tools for illegal access (hacking tools), illegal interception, and data or system interference.

In terms of procedural law (expedited preservation, search and seizure, production orders and other measures in Articles 16 to 21) most countries seem to rely on omnibus provisions applying to real-life situations. These appear to work to some extent but limit the effectiveness of investigations and the gathering and use of electronic evidence in the course of criminal proceedings.

Further work is thus required in most countries. Some countries recently adopted (such as Argentina) or are about to adopt cybercrime legislation (such as Brazil). The legislation adopted in the Dominican Republic in 2007 appears to be fully in line with the Convention on Cybercrime.

Participants pointed at the need for the cooperation of Internet service providers with law enforcement and criminal justice authorities. In this connection the "Guidelines for law enforcement – Internet service provider cooperation in the investigation of cybercrime" adopted by the Council of Europe global conference in April 2008 should be helpful.

Concerning international cooperation – a key issue considering the transnational nature of cybercrime – the alignment of national legislation with the Convention on Cybercrime will be an important step towards an international harmonization of legislation and help countries meet the requirement of dual criminality. Accession to the Convention would in addition provide countries with a legal framework for effective police and judicial cooperation. It should be mentioned that Costa Rica and Mexico have already been invited to accede to the Convention.

---

[1] Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru and Uruguay.