By Luis C. Schmidt, Partner

Computer und Recht International, April 2002

In Mexico there is no equivalent to the so-called US »Anti-wiretapping“ Law. However, amendments to the Federal Penal Code (published on May 17, 1999, in the Federal Official Gazette) implement, among others, criminal provisions concerning disclosure of confidential information and illegal access to information equipment and systems with jail sanctions ranging from one to eight years of prison.

1. BACKGROUND

Criminal provisions as those referred to above, were not considered as relevant for Mexico, as there was a believe that in Mexico hacking and other informatics crimes were not common.

Notwithstanding the foregoing, different local Congresses in Mexico (i.e. Sinaloa's Congress) incorporated in their local Penal Codes criminal provisions concerning disclosure of confidential information and illegal access to information equipment and systems.

Even though these regulations represented a legal conflict in connection with applicable jurisdiction to these kind of criminal actions (due to the fact that even if the offence had taken place in the State of Sinaloa, applicable venue to informatics and software in general belonged to Federal Courts; likewise applicable law was Federal law); these efforts to regulate criminal provisions on privacy issues were the first step in the incorporation of anti-wiretapping provisions in the Federal Code.

2. ANTI-WIRETAPPING PROVISIONS

According to these new provisions, sanctioned conducts can be classified as follows:

Modification, destruction, triggering or loss of information pertaining either to particulars, Government or Mexican Financial System.

Wrongful misappropriation or copy of information pertaining either to particulars, Government or Mexican Financial System.

In order to be sanctioned, the conduces shall:

Rely on information contained in systems or information equipment, protected by any security mechanism or media.

Be based on unauthorized access.

Notwithstanding the above, in case of information pertaining to the Government or Financial System, sanctions would increase if the person had authorization to access the information but nevertheless modified it. In addition, the penalties above shall be higher if crime is committed by personnel of financial institutions.

3. CONSEQUENCES

It can be concluded that anyone including ISPs, may be held liable of a criminal misconduct if it either has triggered a loss of information in a system pertaining to a private, government or financial entity or if it misappropriates or copies that information without proper authorization.

On the other hand, the wording of new provisions is not clear as to the way of enforcing and accepting evidence for this purpose. In this respect it is necessary to highlight that although in Mexico evidence in electronic support is recognized, Criminal Courts do not have enough experience as to admit that kind of evidence, which if admitted will not be duly considered by the judges.

In addition, there is nothing indicated in the new provisions of the Federal Penal Code, as to a prohibition to transmit or send private information via Internet or by any other means. In this respect an amendment to articles 173 and 174 of the Federal Penal Code as to include a sanction to whomever opened a private communication transmitted by electronic, electromagnetic or optical means was proposed to the Federal Congress; which up to this date has not been approved.

Local Congresses and IT lobby groups are now pushing for new modifications to local and Federal Penal Codes as to classify illegal access to information supported in electronic means as a “grave crime” (crimes sanctioned with penalties with a ratio of imprisonment of more than 5 years).