MINISTERIO PUBLICO

THE FIGHT AGAINST CYBERCRIME IN CHILE

Veronica Rosenblut G.
Consultant Lawyer.
Specialized Unit on
Economic Crime, Money Laundering and Organized Crime.
Public Prosecutor´s Office of Chile.

I. LEGAL FRAMEWORK.

- In 1999 was published in Chile Law N° 19.223 (**cybercrime law**), by which it is possible to punish cyber attacks against the correct functioning and protection of privacy of the informatic systems and the data that contains it (espionage and sabotage typologies).

- The Chilean Congress has been working, since the year 2003, in **two different bills** which objectives are to modify both the Law and the Penal Code, by the incorporation of new offences relating to phishing, electronic document´s forgering and informatic fraud.

I. LEGAL FRAMEWORK.

- It has also been enacted Law N° 19.799, which regulates **electronic documents and digital signature.** It was published in 2002. Legal instructions ordering public institutions to use this tools complement this legal regulation.

- Chilean legislation also punishes **cyber laundering, child pornography and child abuse by internet.** Cyber laundering can be punished as a form of money laundering by Law N° 19.913 of 2003. Child pornography and child abuse by internet can also be punished using new and broader sexual offences incorporated in the Penal Code in 2004.

I. LEGAL FRAMEWORK.

- To follow criminal money, search for assets and investigate cyber laundering and any other kind of cybercrime, the **Chilean procedural system** allows, since 2000, the **interceptation** of electronic and physical correspondence, phone conversations and any other mechanisms of communication.

- The Chilean Procedural Law also indicates that is the **ISP duty** to conservate for six months the IP register of the virtual communications of their clients. That information can be used in the investigations conducted by the PPO.

II. PREVENTION, INVESTIGATION & PUNISHMENT OF CYBERCRIME.

- Cybercrimes are investigated in Chile by **especial divisions** inside the PPO and the Police. They have been trained to deal succesfully with this kind of criminal activity.

- In addition, the PPO established in 2003 the **Specialized Unit on Economic Crime, Money Laundering and Organized Crime**. It is integrated by lawyers, engineers and other professionales, who give support and assistance to the prosecutors in the investigation of cybercrime and financial investigation.

II. PREVENTION, INVESTIGATION & PUNISHMENT OF CYBERCRIME.

- In the year 2004, the Chilean Government developed a “Digital Strategy”, by which it is the reponsability of the Minister of Interior to create a **public system of prevention and reaction** against cyber attacks.

- To prevent cyber laundering, the new Casino´s Law (N°19.995), published in 2005, **forbids the institutions operating as Casinos, to use the internet as a means to gambling.**

II. PREVENTION, INVESTIGATION & PUNISHMENT OF CYBERCRIME.

- To follow criminal money from cyber or economic offences, since 2006 the PPO has developed a **cooperation network** with other public institutions which can provide financial information to prosecutors on-line.

- Following the same objectives, since 2007 the PPO has been coordinating actions **with many email service´s providers**. Through this mutual cooperation, the latter gives the PPO information about email users and can also immediately freeze accounts and keep its content for future use by the prosecutors.

II. PREVENTION, INVESTIGATION & PUNISHMENT OF CYBERCRIME.

- In this context, the PPO has agreed with several **national and international companies** like Google, Microsoft and Orange, mechanisms of mutual cooperation.

- The PPO has also developed an important **cooperation system with Chilean ISPs**, creating an efficient mechanism to exchange, by email, information concerning the identity and address of internet users.

III. ACHIEVEMENTS.

- As a **result** of the work done together by the Chilean Government, the PPO and the Police, it has been possible to investigate and prosecute an important part of cyber offences committed since 2000.

- **Examples of successful prosecutions** include cases of credit card numbers´ traffic on the internet, on-line fraudulent banking operations performed with data obtained by phishing and cyber attacks against private and public web pages of the Chilean government and other countries, among others.

THANK YOU

Verónica Rosenblut G.
vrosenblut@minpublico.cl
Phone: 56-2-6909130
Fax: 56-2-6909126

Specialized Unit on
Economic Crime, Money Laundering and Organized Crime.
Public Prosecutor´s Office of Chile.