









 Instituto Federal de Acceso a la Información y Protección de Datos

# ***Data Protection and Cybercrime Challenges***

***(Preliminary Presentation)***

Sigrid Arzt  
Commissioner  
IFAI, Mexico  
*Octopus Conference*  
6 - 8 June 2012  
Strasbourg , France

 Instituto Federal de Acceso a la Información y Protección de Datos

## **DATA PROTECTION IN MEXICO: A BRIEF OVERVIEW.**










**THE FEDERAL INSTITUTE OF ACCESS INFORMATION AND PERSONAL DATA (IFAI).**- Is a body that belongs to the Federal Public Administration, which has operative, budget and decision making **autonomy**. It is in charge of:

- Promoting the use of the right of access to information.
- Deciding if a request of access to information is accepted or denied.
- Protecting all personal data at the Federal Public Administration and private entities.

Hence, two **critical mandates** which are set from the very top legal framework, the Mexican Constitution:

- Warranty **access to information**.
- **Protect personal data** collected by government and entities of the Federal Public Administration and by the private sector.

2



## Legal Framework for the Public Sector.

On June 11, 2002 the **Federal Law of Transparency and Access to Public Government Information** was published. It regulates the right of access to information and the protection of personal data held by the departments and entities of the Federal Public Administration (FPA), and it is only mandatory at the federal level. Mexico is a federal system, so each of the 32 states of the country has their own regulation, which are close to the federal law.

A number of guidelines have been published for the implementation of the law, such as the **Guidelines for the Protection of Personal Data**<sup>1</sup>. Those guidelines establishes the mandate of all departments of the federal government to register their databases of personal information in a system called “Sistema Persona”.

1. These guidelines contain a whole chapter of security measures that should be considered for the protection of personal information contained in those databases.



## “Sistema Persona”

- The purpose of this system is to **control the registry of all the databases** of personal information held by the departments and entities of the FPA.
- Information that should be submitted for registration: name of the database, **purpose of the collection** of the data, **legal basis** for processing it, name of the **person in charge** of such processing and the specification if **transfers** are carried out.
- Modifications or cancellations of the databases should be informed through the system.
- **Today, only at the Federal level, we have a total of 3097 databases** has been registered. Around 97% of those databases contain only basic **ID information** and the other 3%, have gathered **sensitive personal data** (ethnic origin, health or genetic information, religion, sexual preference, political beliefs among other data).



## Legal Framework for the Private Sector.

As of July 5th, 2010, with the publication of the **Federal Law on Protection of Personal Data Held by Private Parties**, Mexico joined the group of countries that have specific legislation for data protection in hands of private sector. This law is mandatory in all the Mexican territory. It has many **aspects of international data protection models: European model and APEC privacy framework**.

This law seeks a **balance** between **protecting personal data** and, at the same time, allowing markets to develop with **free flow of information across borders**.

5




## CYBERCRIME IN MEXICO: A BRIEF OVERVIEW.

Now, with respect to cybercrime, the legal framework, that is the Federal Criminal Code, establishes among other crimes:

- *Secret information disclosure* (using or publishing secret information or images, without consent or legal cause, in order to damage a person);
- *Hacking* (the illegal access to computer equipments or systems);
- *Cracking* (the commercial manufacturing of a device or system in order to break electronic security systems of copyright software);
- *Underage pornography* (Publishing and transmission of files, thru a public net or private telecommunications system of any kind of underage pornography);
- *Fraud* (cheating or taking advantage of other people to illegally get lucrative gains).

6


 Instituto Federal de Acceso a la Información y Protección de Datos

The Mexican Deputies Chamber approved, on March 2012, an Initiative to reform the Federal Criminal Code, in order to punish and increase the penalties related to:

- Cyber bullying (Threats and intimidation thru digital systems and the use of images as mean of blackmailing.)
- Cyber fraud or identity theft.
- Phishing (illegal practice used to attempt to gather personal, financial and other sensitive information by e-mail).
- Cyber crimes related to sexual tourism and prostitution.

This Initiative has been sent to the Mexican Senate, where it will be reviewed.

7


 Instituto Federal de Acceso a la Información y Protección de Datos

### Cybercrime Investigation.

While, the legal framework gets underway, the Federal Police is in charge of cybercrime investigation. In that regard, the Federal Police set under the *Scientific Division* a force with the following mandate:


- a) Identify, monitor and track the public net of internet, in order to prevent criminal behavior.
- b) Manage cooperation with internet service suppliers to neutralize sites and electronic pages that attempt against the public security, as well as to prevent and to fight crimes in which electronic means are used.
- c) Promote the culture of crime's prevention in which electronic means are used, as well as the diffusion of the legal framework that sanctions them.


8

 Instituto Federal de Acceso a la Información y Protección de Datos

- *The National Center to Cybernetic Incidents Response*, a branch of the *Scientific Division* is the office in charge to deal with cybersecurity issues.
  - a) Receive denounces of attacks to technological asset's infrastructure;
  - b) Monitor security of the network and systems, and
  - c) Coordinate the response to incidents to victims of cybernetic attacks.
- Since its creation (May 2010) to the first semester of 2011, the *Scientific Division* attended 4.991 denunciations in the matter of cybernetic crimes, the majority related to fraud thru electronic commerce and phishing.
- As a result of the cabinet investigation, identification, preservation and presentation of digital evidence, of at least 23 cases were presented to the Public Prosecutor. By February of 2011, the first federal sentence by the crime of child pornography by a judge, who condemned a Canadian citizen that, from the city of Tijuana, Baja California, operated at least 36 web sites.


Source: MEXICO GOVERNMENT 2011 9



 Instituto Federal de Acceso a la Información y Protección de Datos

## ***Challenges Ahead***

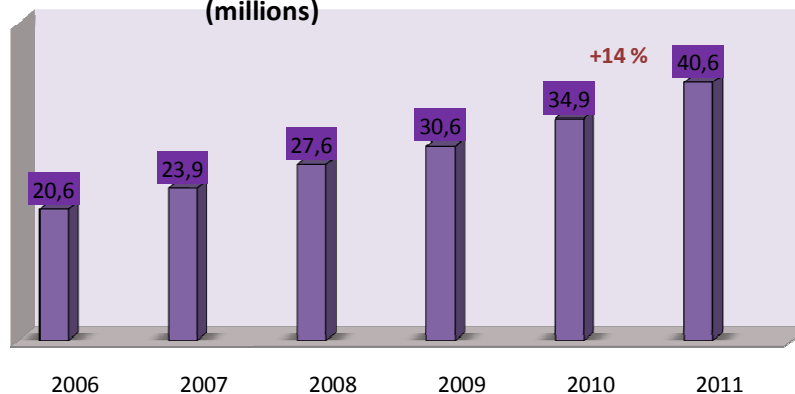
## ***Cybercrime and Data Protection***





## Numbers about internet in Mexico

Number of internet users in Mexico 2006-2011  
(millions)



Source: AMIPCI, 2011

Mexico has a total population of more than 110 million people. According to recent studies, 40.6 have access to internet.

11



## Some information about internet and personal data in Mexico...

In 2011, the number of internet users reached 40.6 millions (37% of the total population), which represents an increase of 14% compared to 2010. The most used device for connection to internet are PC's and Laptop.

The use of smartphones to access internet (58%) doubled compared to 2010 (26%), thus the use of PC and Laptop decreased.

The average time of connection to internet is 4 hours.

The main online activities in Mexico are: the use of e-mail, social networks and searching of information.

The main entertaining activities are: the use of social networks, reading news and downloading videos and music. The number one social network in Mexico are Facebook (90% of Mexican internet users have an account); Youtube (60%) and Twitter (55%).

Source: AMIPCI, 2011

12



In Mexico, social network (79%), online banking (65%) and online shopping (62%) sites are mainly where internet users give personal data.

9 out of every 10 Internet users have provided identification data (name, photograph, age, address, gender, Federal Taxpayer's Code (RFC) and Sole Code of Population Registration (CURP) and almost 4 out of every 10 have provided sensitive data (ideology, political affiliation, religion, ethnicity and sexual preference).

76% of internet users have enabled the privacy settings offered in the social networks, and 61% do not know how will their personal data will be processed in these networks.

The Mexican internet users who do not access to social networks is because they are not interested or because they want to protect their personal data.

Source: AMIPCI, 2011  
13



## **In a Global context, cybercrime and personal data protection become a critical challenge for any authority.**

We now know that Symantec Internet Security Threat Report of April 2012, shows that Mexico is in the 4th place of America's countries with greater malicious activity (phishing, spam, net attacks) in the internet, and in the 29th position, of more than 200 countries, at world level.

Worldwide, an average of 1,1 million identities were robbed as a result of violations or data leaks in 2011. Hacker incidents represented the main threat, exposing 187 million identities in 2011.

The most frequent cause of data leaks that facilitated the identity theft was the robbery or loss of computers or other gadgets where data is stored or transferred, e.g. smart phones, USB's or endorsement devices.

14



## Globalization

The global interconnectivity demands cybersecurity to become a **national policy priority**, therefore, a new generation of public policies called “cybersecurity strategies” are emerging.

National policies requires **governmental** coordination, **public-private** cooperation and respect of **fundamental values**.

Key Priority Areas need to be developed and highlighted in action plans. Government security, protection of information **infrastructures**, fight against **cybercrime**, **protection of vulnerable groups** such as children; development of **cybersecurity skills** and creation of **cyber security incident response group** at a national level are areas that need to be followed and learned from of those who have already walk that road.

A high level of cybersecurity can provide a competitive economy.

15



**Cybercrime** is not confined to a single nation, and cybersecurity strategies of one country can affect citizens of another country due to the **cross-border** nature of communications.

**Cooperation between security agencies** is required because the jurisdictions have boundaries, but there are **extra-territorial effects** that should be taken into account.

**Cybersecurity** should be based on globally accepted standards, best practices, and international programs.

Governments must take actions in the legal field, and they should enforce national laws related with cybercrime.

Cybersecurity and data protect policies must be consistent with **fundamental rights of citizens**, which are essential to democratic societies.

\*According to OECD. 16







## Conclusions

Even though it is true that in the actual global world connectivity is fundamental, and information technologies have become a catalyst element to countries' economic growth and development, it is also true that pursuant to the use of telecommunications new threats have arisen, against persons, businesses and governments that may compromise the confidence and safety when using these technologies.

Even when it should be a priority to develop a solid cybersecurity policies at a national and international level, as well as, legislative obligations to secure information systems and software for everyone, this can not oversee data protection as a key component.

17



One of the fundamental issues of the Mexican national agenda is safety, and the one referred to information and data protection is no exception, therefore work has been undertaken in order to strengthen national regulation and, at the same time, international cooperation is vital to generate trust and safety in information society.

Over the last ten years, Mexico has been constructing a legal framework on **privacy and security**, but the country faces many **challenges** in those matters as a result of **technological development** in the field of telecommunications, social networks and many others. Mexican government is aware that data protection is one of the fundamental rights that has to be preserved in a digital world and will keep working to protect that persons' right. In doing so, it is critical we educate people on the threats and benefits while providing personal data users while using technologies.

18

Instituto Federal de Acceso a la Información y Protección de Datos

# Thank you