Cooperation with multinational internet service providers

The Brazilian experience

Brazilian Civil Rights Framework for Internet
Marco Civil da Internet

- **Marco Civil da Internet – art. 11**

Any ISP providing services to people on Brazilian territory has an obligation to comply with Brazilian law.

subscriber information

traffic data

content

Three situations where Brazilian law apply

- ISPs with physical presence in Brazil (headquarters or branches)
- ISPs with no physical presence in Brazil but targeting people on its territory and pertaining to an economic group with physical presence
- ISPs with no physical presence in Brazil but targeting people on its territory

When Brazilian law does not apply

- ISPs with no physical presence in Brazil and Not targeting people on its territory

...

International Judicial Cooperation - MLAT

How to compel ISPs to comply with Brazilian law

- **ISPs with physical presence in Brazil (headquarters/ branches or same economic group):**
  - **Fines up to 10 per cent of the turnover (freeze the money)**
  - **Prohibition of contracting with public institutions**
  - **Suspension or interruption of activities**

How to compel ISPs to comply with Brazilian law

- **ISPs with no physical presence in Brazil, but targeting people on its territory:**
  - **Freezing of any possible economic gain through application stores**
  - **International Judicial Cooperation**
  - **Suspension or interruption of activities**

WHY BUDAPEST CONVENTION ?

- **For the cases where we need International Judicial Cooperation**

More and more criminals, even located in Brazil, are using foreign services to commit crimes in Brazil.

Budapest Convention has tools to speed the exchange of information and evidence such as POCs 24X7 and judicial authorities and prosecutors direct request for MLA and communications in urgent situations (art. 27.9 BC).

The 2nd Additional Protocol to the Convention will bring even greater agility and efficiency.

CASE STUDY

Vulnerabilities in the computer systems of public institutions in Brazil and abroad were being offered in forums for cybersecurity topics. The first step was to seek IP data and information about the forum hosting services, the servers that supported those services and also the IPs of the emails that the criminal displayed in the forum for contact, in order to obtain the data that would lead to the identity of the person who had provided the vulnerabilities for illegal access.

CASE STUDY

All these initial contacts were urgent and ended up being made either by the MPF or the police contact network, which served to preserve the data and decide which path would be worth following to obtain a successful MLA. Even so, with the need for traditional MLAs to guarantee the status of evidence for information to proceed with the investigation, valuable time is lost, often making it unfeasible.

GOOD PRACTICES

- Cybercrime specialized Points of Contact at the Prosecution Service to get in touch with a point of contact in each ISP.
- Knowing the procedure to obtain data from each ISP, how to use their platform, when the case, and what can be obtained from them.
- Keeping this information in an organized way and easy access.

THANK YOU !!

Fernanda Teixeira Souza Domingos

Federal Prosecutor

Coordinator of the Advisory Group on Cybercrime at the Criminal Chamber of the Federal Prosecution Service (Brazil)