Daniela Dupuy

Synopsis of the presentation

In criminal investigations in cyberspace prosecutors often need and require data from suspects, that is, digital evidence that is lodged in strange jurisdiction.

That can be achieved if international service providers store that data for a certain period of time and if there are measures in place that allow law enforcement to access that evidence across borders.

The main challenge is the different legal systems between the countries, variations in national criminal and procedural laws on cybercrime and different rules of evidence. Variations in the range and geographical applicability of regional and multilateral treaties on cybercrime, approaches to protection data and respect for human rights, also represent important challenges.

The harmonization of criminal and procedural provisions, especially regarding the treatment, collection and exchange of evidence, and the drafting of specific protocols, could guarantee that digital evidence in a country is admissible in other countries.

In this sense, on May 14, 2022, the Second Additional Protocol to the Budapest Convention was signed, within the framework of the Council of Europe, Strasbourg, France, whose main objective is to establish common international rules to strengthen international cooperation in matter of Cybercrime and obtaining digital evidence hosted in other countries, so that collaboration between states and with the private sector is constant and efficient.