BRAZIL ITEM 5

The migration of many criminal offenses to digital platforms has demanded important efforts towards updating proper legislative, law-enforcement and judicial response to the new threats. Their geographical amplitude has also challenged the traditional mechanisms through which Brazil has provided and received international police cooperation and mutual legal assistance.

Challenges are tremendous. Internet service providers, which hold important information needed to investigate cybercrime and collect electronic evidence, frequently have physical headquarters in one country, provide services in different continents and store their information on servers anywhere else on the planet. In this scenario, law enforcement strives to identify and duly address whoever has jurisdiction over the data and direct access to it. Additional difficulties in gathering evidence have been posed by anonymizing networks, as certain VPN providers claim not to keep access logs.

Brazil has been sensitive to the peculiar nature of digital evidence and cybercrime. Our Civil Framework for the Internet provides that Brazilian law must be applied in the collection, storage and processing of data when one of the computer terminals is located in Brazilian territory. Foreign companies that have branches in Brazil or that provide services to Brazilian users and which collect, store, maintain or process data obtained from these users must therefore comply. This framework allows Brazilian authorities to have access to electronic evidence and data collected from services provided in the country without having to activate international legal cooperation channels.

In spite of the transnational nature of the phenomenon at hand, whenever a link between investigation and jurisdiction is enabled internationally, the legal development of a case is often decelerated by divergences over the meaning of privacy protection, which is reflected in the various national requirements for data disclosure. That cooperation is further challenged by the extreme volatility of digital evidence. A more cohesive international distribution of jurisdiction would be an important step forward in persecuting cybercrime. More and better cooperation is needed.

In their traditional form, mutual legal assistance requests have been slow to process and tend to be innocuous, given the extraordinary pace of digital disposal. We are ready to cooperate with jurisdictions which are also striving to find digital solutions for our digital challenges in facing current cybercrime.