Permanent Mission of the Federative Republic of Brazil

UNODC/91/2016

The Permanent Mission of the Federative Republic of Brazil to International Organizations in Vienna presents its compliments to the United Nations Office on Drugs and Crime and, with reference to note CU 2016/133/DTA/OCB/CSS, has the honor to convey comments of the Brazilian government regarding the Comprehensive Study on Cybercrime.

2. A significant question raised in the executive summary of the study relates to the right to privacy and the access to information. According to the study, "While technical possibilities exist for filtering of internet content by service providers, restrictions on internet access are subject to foreseeability and proportionality requirements under international human rights law protecting rights to seek, receive and impart information." In this sense, it should be mentioned that filtering of internet content and restrictions of internet access are against the principle of net neutrality, foreseen in the Brazilian law.

3. Regarding chapter 4, on criminalization, it should be noted that the study does not reflect important changes made in Brazilian law since 2012, such as law 12.737/12, which included in the Penal Code articles dealing with the invasion of electronic devices, and law 12.965/14, which defined the principles for the functioning of the internet in Brazil and established the bases for law enforcement authorities to obtain access to data on internet connection and applications.

4. The study emphasizes the need for harmonization of legislations, which is an extremely important point. Although there is a basic set of legal similarities among countries, small

Pestalozzigasse 4 / 2. Stock, 1010 Wien – **brasemb.viena@itamaraty.gov.br** – Tel.: +43 1 512 0631

variations in the description of criminal offences may hinder international cooperation, create gaps that obstruct punishment of certain crimes or even impose disproportionate sentences.

5. These variations have even graver consequences in the prosecution of crimes related to child pornography and other crimes involving children and adolescents. As there is no consensus regarding the age limit of victims for the criminalization of the conduct, the production and publishing of child pornography may simply be outsourced to countries where that limit is lower, disseminating, from these countries, material that would violate the laws of others.

6. A solution to the issues related to harmonization pointed out by the study, through the establishment of a basic set of offences by an international instrument, is interesting, as it guarantees an international legal framework while respecting national characteristics. Evidently, the extent of the openness to national characteristics cannot allow for a conflict with the general set of offences.

7. In what regards to chapter 6, on electronic evidence, it is clear that the unique features of this kind of evidence engender specific challenges, particularly in relation to the technical capacity of countries. One solution to this issue may be a model similar to the one adopted by the Budapest Convention, with the sharing of knowledge and good practices among member states. Therefore, any international instrument on cybercrime should also foresee such a mechanism, so that its members have not only the legal framework, but also effective practical means for the criminal prosecution of cybercrime. The objective of avoiding the creation of "safe havens" for cybercriminals will not be fulfilled if prosecution is not equally effective in all member states.

8. One question that the study does not touch upon is the current – and growing – use of encryption in instant messaging applications. End-to-end encryption is currently the rule among the major companies that offer instant messaging services, and it is impossible to be broken without assistance or intervention from the company. Encrypted messaging apps have been used, for instance, for coordinated terrorist attacks and have been the object of frequent questioning, including via attempts to approve legislation that forbids encryption or creates access mechanisms for authorities when investigating serious crimes.

9. Given the current situation, any international instrument on cybercrime, when dealing with electronic evidence, will need to address the question of encryption. In Brazil, there is still no consensus on the issue: there are ongoing discussions regarding whether the law authorizes the encrypted communication currently offered and also if it authorizes courts to determine the breaking of encryption.

10. With regards to international cooperation, the current international legal framework does not have the adequate mechanisms for the solution of the issues generated by the need for quick access to movable evidence, while duly preserving sovereignty. One possible path towards improvement in this area, mentioned by the study, could be the "(re)-conceptualization of the extent to which 'data location' can still be used as a guiding principle". This path may even reduce the need for international cooperation.

11. It is important to stress that electronic evidence is not used only in the prosecution of cybercrime, since crimes carried out in the "real world" also produce electronic evidence. In this sense, any convention that contains regulations on electronic evidence must take into account the fact that they are also used for the prosecution of regular crimes. The issue of international cooperation and jurisdiction, therefore, goes beyond the sphere of cybercrime.

12. Traditionally, the country where the evidence is located has jurisdiction and thus access to it, being able to provide it to other interested countries. For electronic evidence, however, this concept cannot be applied fully, for a variety of reasons. The evidence may be moved almost instantly, changing the country which would have jurisdiction over it. It may be stored in different countries at the same time. It is often impossible to determine where exactly it is stored (technologies such as "cloud computing" make it growingly difficult to pinpoint the location of storage). Moreover, the ease with which data can be transferred across borders allows for companies to "choose" their jurisdictions without regard to their level of protection of the interests of users or victims (allowing for a kind of "jurisdiction shopping").

13. Initial efforts regarding trans-border access to data (including those by the Budapest Convention, from 2001) have been gradually expanded throughout the world. Currently, it is common to use the concept of control and service provision to determine jurisdiction. This

concept derives, to some extent, of a wider interpretation of article 18 of the Budapest Convention.

14. Countries that have implemented similar provisions in their national legislations have been expanding it to allow for direct access to any data or electronic evidence controlled by a company that provides services in its territory, irrespective of the location where the evidence is stored. In a survey from 2012, the company Hogan Lovells noted that several countries adopt the criteria of control/service provision and, in another study, from 2014, the same company noted that many countries in the Americas, including Brazil, use similar mechanisms.

15. In Brazil, article 11 of law 12.965/14 uses this concept, which determines that the country that has jurisdiction over the company that controls the evidence has jurisdiction over the evidence, independently of where that evidence is stored. Therefore, a company is under Brazilian jurisdiction in case it provides services for customers in Brazil, even if it is established elsewhere.

16. This shift of paradigm would require that a multilateral convention on cybercrime approaches, aside of traditional issues of international cooperation, mechanisms for the direct access to evidence that include the concept of control/service provision instead of the purely territorial concept for the definition of jurisdiction.

17. Regarding chapter 8 of the study, about prevention, it would be positive to deepen the debate on minimum security requirements for "big data" and "cloud computing", given the challenges faced by information security in these segments, with vulnerabilities that allow both citizens and the state to be exposed to criminal activities. The effective strengthening of cooperation between states in the identification and responses to such activities would also be of high relevance. Wider use of the repository on cybercrime by countries too would be beneficial to improve the exchange of lessons learned in the matter.

18. As a final consideration, it should be reiterated that the harmonization of criminal offences related to cybercrime through bilateral or regional agreements is insufficient and that traditional mechanisms of international cooperation need to be improved, due to the movable

nature of electronic evidence, which demands quick and effective cooperation to guarantee its preservation.

19. There is a need for a global instrument, given that the existing regional instruments are not sufficient to promote effective cooperation in combatting cybercrime. Brazil concludes, from the study, that the most appropriate option to be followed is the negotiation of a comprehensive multilateral convention on cybercrime that incorporates the provisions that are consensual for countries of all regions, even though this may be a challenging process. It is important to emphasize, also, that a comprehensive multilateral convention and instruments of a more limited regional or international scope would not be mutually exclusive.

The Permanent Mission of the Federative Republic of Brazil to International Organizations in Vienna avails itself of this opportunity to renew to the United Nations Office on Drugs and Crime the assurances of its highest consideration.

Vienna, 2 September 2016.

e-mail: untoc.cop@unodc.org.

Permanent Mission of the Federative Republic of Brazil

UNODC 98 /2016

The Permanent Mission of the Federative Republic of Brazil to International Organizations in Vienna presents its compliments to the United Nations Office on Drugs and Crime and, with reference to note CU 2016/133/DTA/OCB/CSS, has the honor to convey updated comments of the Brazilian government regarding the Comprehensive Study on Cybercrime.

Executive summary

2. Access to extraterritorial data during collection of evidence, without the State's consent, may be damaging to State sovereignty in some circumstances, especially in cases where disclosing data may affect national interests.

3. According to the study, "investigators may, on occasion, obtain data from extra-territorial service providers through an informal direct request". Although this is a statement of reality by the authors, it must be taken into account that this type of data collection must be fully compatible with national legislation.

4. Other important issues are the guarantee of privacy of citizens and access to information. According to the study, "While technical possibilities exist for filtering of internet content by service providers, restrictions on internet access are subject to foreseeability and proportionality requirements under international human rights law protecting rights to seek, receive and impart

Pestalozzigasse 4 / 2. Stock, 1010 Wien – **brasemb.viena@itamaraty.gov.br** – Tel.: +43 1 512 0631

information". It should be noted that, in Brazil, the filtering of internet content and restrictions of access are, in essence, contrary to the principle of net neutrality, provided for in Brazilian internet law.

Chapter 4: Criminalization

5. Chapter 4 of the study analyzes the various legislations on cybercrime and the degree of harmonization among them, emphasizing that there is a certain basic consensus, but many differences.

6. In the case of Brazil, two important laws were enacted after 2012: Law 12.737/12, which included articles 154-A and 154-B, dealing with the invasion of electronic devices, in the Penal Code; and Law 12.965/14 (called "*Marco Civil da Internet*"), which defined the principles for the operation of the internet in Brazil and established the basis for law enforcement authorities to access network connection data and applications. Therefore, some of the information regarding the legislation in Brazil used in the study is outdated.

7. In general, the study emphasizes the need for harmonization of the different national laws, which is an extremely important point. Although there is a basic core of similar legislation, slight variations in description of the various types of offences and, in particular, on the type's element of intent, could hinder cooperation between countries, opening gaps that hinder the punishment of certain crimes or impose disproportionate penalties.

8. These variations could have yet more serious consequences in pursuing crimes related to child pornography and other crimes involving children and adolescents. As there is no consensus on the maximum age of the victim to the criminalization of these acts, the production and publication of child pornography can simply be transferred to countries where the maximum age is lower, spreading to the prohibited material from there in violation of the laws of several countries, but not of the country where the material is produced.

communications of criminals and terrorists. The use of encrypted instant messaging applications assisted, for instance, in the execution of recent terrorist attacks and has been the subject of constant questioning from authorities, including through the discussion of legislation to prevent encryption or create access mechanisms for authorities investigating serious crimes.

14. In the current context, any international convention on cybercrime, when addressing electronic evidence, should also address the issue of encryption. In Brazil, there is no consensus on the theme, with doubts regarding whether legislation authorizes encrypted communications being offered to the public and whether it allows courts to determine the breaking of encryption.

Chapter 7: International Cooperation

15. Chapter 7 of the study deals with international cooperation, describing the challenges and difficulties faced in prosecuting cybercrime, time-consuming mechanisms of international cooperation and also some of the efforts for direct access to evidence.

16. Cybercrime is, in essence, transnational. The expertise of criminals and the multiplication of international black markets accessible from anywhere around the globe lead to all offences comprising acts in different countries. It is not uncommon for the criminal action to be developed in a country, with victims in another and electronic evidence stored in a third. Also, there are services offered in one country with products and marketing strategies specific for its inhabitants, but with equipment and operations kept elsewhere.

17. The current international legal framework has no suitable mechanism for the solution of the challenges generated by the need to quickly obtain volatile electronic evidence while preserving sovereignty. The path sought by many countries, which is mentioned by the study when it discusses the need to rethink the concept of "local data", is the change in the criteria for identification of the country which has jurisdiction over the electronic proof. This path would even diminish the need for international cooperation and could be explored in a new convention on the subject.

18. Initially, it is important to note that electronic evidence is used not only in the criminal prosecution of cybercrime itself. With the widespread use of computer systems, common crimes

9. The proposed solution to the issues of harmonization indicated by the study, through the establishment of a basic set of offences in international instruments and leaving for the domestic level to establish aggravating and mitigating circumstances, is interesting. It would ensure a minimum international legal framework, but at the same time preserve local peculiarities. Evidently, the extent of the openness to national characteristics cannot allow for a conflict with the general set of offences, such as changing the maximum age for identification of victims of child pornography. Defining this basic set may, however, be a challenging task.

Chapter 6: Electronic Evidence and Criminal Justice

10. Chapter 6 deals with electronic evidence and its singularities, such as its fragility and the need to preserve all its elements for possible further control. It is evident that the singularities of this kind of evidence bring up particular challenges, especially referring to the technical capacity of countries that may adhere to a universal convention on cybercrime.

11. A solution to this issue could be the adoption of a model similar to the one of the Budapest Convention, with the dissemination of knowledge and "best practices" among member countries. Thus, a United Nations convention should also contain mechanisms for sharing technologies and best practices in investigation and prosecution, so that its members are provided not only with the legal framework, but also with effective means for the practical criminal prosecution of cybercrime (investigation and judicial proceedings). The objective of avoiding the creation of "safe havens" for cybercriminals will not be fulfilled if prosecution is not equally effective in all member states.

12. One issue that is not addressed in the study but has now become essential is the increasingly widespread use of encryption in instant messaging applications. End-to-end encryption is currently the rule among the major companies that offer instant messaging services, and it is impossible to be broken without assistance from or intervention (invasion) in the company.

13. This issue opposes, on the one hand, experts in security and stricter privacy advocates, who defend encryption as a way to ensure safe communications, and, on the other hand, law enforcement authorities, who see the encryption mechanism as preventing access to

- committed in the "real world" – now also involve electronic evidence. Thus, any convention that is willing to discipline electronic evidence must take into account the fact that they are also used in proceedings regarding common crimes. The issue of international cooperation and jurisdiction over electronic evidence goes, therefore, beyond the limits of cybercrime.

19. Traditionally, the country where the evidence is located has jurisdiction and thus access to it, being able to provide it to other interested countries. For electronic evidence, however, this concept cannot be applied in its entirety. Firstly, because electronic evidence can be moved from one place to another immediately and effortlessly. A country may lose jurisdiction on electronic evidence in a matter of minutes.

20. Secondly, because, as pointed out by the study, the electronic evidence can be stored simultaneously in different countries to meet the specific interests of companies.

21. Thirdly, because it is often impossible to determine where the evidence is stored. With the proliferation of "cloud" data storage services, it has become increasingly difficult to determine exactly in which country are kept the machines that store electronic data.

22. Fourthly, because as electronic evidence can be easily moved and stored, focus on the territorial concept of jurisdiction allows enterprises to choose the jurisdiction that suits them to store the data. That jurisdiction is not necessarily the one that better protects the interests and rights of users and victims of crimes, creating the possibility of a "jurisdiction shopping" that has been opposed by courts of several countries.

23. The Budapest Convention, in its article 32, foresees mechanisms for cross-border access to data. Recognizing that international cooperation in electronic evidence is not effective and that territory is not the best way to determine the jurisdiction over the electronic evidence, that Convention foresees that, in limited situations, its members can access data stored in other countries signatories.

24. This first effort of the Budapest Convention, which dates from 2001, was gradually expanded by its members and other countries. Currently, it is increasingly frequent to use of the concept of control and service provision to determine jurisdiction, as does article 11 of the

Brazilian law 12.965/14. According to the concept of control/service provision location, the jurisdiction over the electronic evidence rests with the country that has jurisdiction over the company controlling such evidence, regardless of where the data is effectively stored. As a complement to the concept, a country will have jurisdiction over a parent company in case it provides services to its residents, even if it is based in another location.

25. This new concept is derived to some extent from a broad interpretation of article 18 of the Budapest Convention. Originally thought to allow access to data controlled and maintained in the territory of the requested country, when implementing this article in their domestic legislation countries have expanded the provision to allow for direct access to any data or electronic evidence controlled by a company providing services in its territory, regardless of where the evidence is effectively stored.

26. In a survey conducted in 2012, the company Hogan Lovells found that several European countries adopt the criteria of control/service provision. In another study, held in 2014, the same company found that several countries in the Americas use similar mechanisms, such as Brazil. Another country has defended the possibility of direct access to data controlled by national companies, even if physically kept abroad.

27. Proposals for new international instruments should take into account the evolution of the practice in international cooperation for the effectiveness and promptness of obtaining electronic evidence, as well as the feasibility of access mechanisms involving the concept of control/service provision.

The issue of harmonization of crimes that are not strictly cybercrime

28. As for the question of whether it would be appropriate or not for a future convention to deal with crimes that are not strictly cybercrime, such as child pornography and crimes against honor, it has to be understood that an increase in the scope of a convention can generate more discussion and greater delays in its implementation.

29. Of the two examples cited, as discussed above and highlighted in the study, there is some consensus among several countries for the crime of child pornography, although there are

variables on the maximum age of victims. However, there is no consensus on crimes against the honor, which could prolong the discussions. Thus, before proposing to expand the scope, it could be necessary to ascertain which crimes could be included in a consensual basis, so as to not create protracted discussions.

30. What is important to note, however, as stated above, is that any provisions on electronic evidence affect the collection and production of evidence not only in cases involving cybercrime itself, but for all kinds of offenses that may be committed with the use of computer systems or with the storage of documents in computer systems. Thus, it should be borne in mind that a convention, when disciplining electronic evidence, would affect the prosecution of all offenses.

Chapter 8: prevention

31. It would be appropriate to deepen the debate on the minimum security requirements for "big data" and "cloud computing", given the challenges faced by information security in these segments, with vulnerabilities that allow both citizens and the state to be exposed to criminal activities. The effective strengthening of cooperation between states in the identification and responses to such activities would also be of high relevance.

32. There should, in addition, be a wider use of the "cybercrime repository", created for sharing experiences and lessons learned related to cybercrime.

Final considerations

33. As a final consideration, it should be reiterated that the harmonization of criminal offences related to cybercrime through bilateral or regional agreements is insufficient to face the need of observing the principle of dual criminality.

34. The traditional mechanisms of international cooperation need to be improved, given that the volatility of electronic evidence demands rapid and effective cooperation so that the preservation of such evidence can be ensured.

35. There is a need for a global instrument, since regional ones are now insufficient to promote effective cooperation in combating cybercrime.

36. Brazil considers that the study provides sufficient basis for the conclusion that it would be convenient to begin negotiations on a comprehensive and universal instrument on cybercrime that can include consensual provisions agreed upon by various regions, despite the challenges that may eventually arise in this process.

37. Nothing would prevent a comprehensive convention to coexist with specific regional instruments on the subject, given that there are countries whose domestic legal systems are incompatible with regional conventions open to members of other regions.

The Permanent Mission of the Federative Republic of Brazil to International Organizations in Vienna avails itself of this opportunity to renew to the United Nations Office on Drugs and Crime the assurances of its highest consideration.

Vienna, 14 September 2016.

e-mail: untoc.cop@unodc.org.