UNIO - *EU Law Journal*. Vol. 5, No. 2, July 2019, pp 136-145.

School of Law – University of Minho

Obtaining digital evidence in the global world

Pedro Verdelho*

ABSTRACT: Gathering evidence in criminal proceedings is becoming more complicated each day. Cases are no longer merely national in nature. Nowadays most of the cases require obtaining evidence from global Internet service providers. This means that evidence from a crime may be found anywhere. The Budapest Convention addresses this issue, in Article 32, allowing the competent authorities of a State Party to seek data in another's Party territory, in limited circumstances. The Portuguese law goes beyond those limited cases, allowing Portuguese authorities to extend searches beyond the physical and political borders of Portugal, no matter where the data may physically be stored. The drafting process of a Second Additional Protocol to the Budapest Convention is currently ongoing. It is expected that this exercise will allow State Parties to the Budapest Convention to seek an agreement on a number of issues regarding obtaining evidence from the cloud, such as loss of location, or transborder searches, or direct cooperation with providers in other jurisdictions, amongst others.

KEYWORDS: Digital evidence – loss of location – transborder access to data – informal cooperation with providers.

* Public Prosecutor at the Prosecutor General's Office - Cybercrime Office

A) "*Here*" is "*nowhere*"

1. The Internet has taken over our daily life and our routines: we work, live, consume, have fun on the Internet and with the help of the Internet.

On the other side, the Internet is no longer a simple set of computers and servers whose location is well-known and where our contents and information are stored. It is now a complex framework of networks and services. In there, we store our data and we look for other data or information we may need, or we may want to obtain.

These days, without the need for computer technical knowledge and sophisticated resources, merely using common equipment, we can store or obtain server-supported information hosted anywhere in the globe. This banal statement is simply a consequence of the expansion of the famous *cloud*, the ethereal and mysterious entity to whom we all entrust our informational lives. This famous *cloud* is accessible from anywhere, at any time, from any device and by anyone, provided the person owns the proper credentials. It can, therefore, be said that it is *everywhere*. That is, the information we make available and seek is globally disseminated and globally available.

2. Nevertheless, this informational globalization was not followed by a globalization in the criminal justice action. Indeed, citizens manage their information globally, using as daily routine online services (email, social networks, hotel or airplane booking services or payment services) from distant countries. Similarly, criminals enjoy the advantages of globalization.

On the contrary, the action of the law enforcement entities is, as it was a century ago, limited to the political and geographical boundaries of their own State. That is, if they find in their investigations facts that have occurred in other countries or if they need to obtain evidence in other countries, as a rule, in order to pursue their investigation, they must respect the sovereignty of those other countries and therefore have to submit a request for international assistance.

With exceptions, namely at the European Union level, the rule, remains that international cooperation in criminal investigations related to more than one country should be requested.

3. This new globalised reality poses serious difficulties for criminal investigations, whether substantive or procedural.

By hosting content in the *cloud*, if that content may itself qualify as a criminal offense, it raises the prior question of determining where the crime is committed. Content or facts that may qualify as criminal offenses in a jurisdiction may not have such a qualification in another jurisdiction. The most recurring example in the European judicial practice in this respect is that of the crimes of defamation and others regarding harm to honour and consideration: being qualified as crimes in some countries, while not being illegal acts in others (where they may fall under the right to freedom of expression).

Thus, without determining the place where the crime occurred, it is not possible to determine which criminal law is applicable and, therefore, to whom the jurisdiction belongs. In a *cloud-hosting* environment where data and information are an unknown, sometimes even undetermined or undeterminable location, this problem is difficult to solve in the absence of legislative initiative.

B) The Budapest Convention

4. In fact, international law is still quite unprepared for this globalized crime. From the perspective of most international treaties and conventions, the dominant view is still the prevalence of sovereignty of each State over the facts that occur in its territory, excluding the possibility of any action within their borders by authorities of other States. This perspective clashes head-on with the enormous demands that digital evidence imposes on criminal investigation authorities.

5. However, it is important to mention an exception to this general rule, which is enshrined in Article 32 of the Budapest Convention[1] (the Council of Europe Convention on Cybercrime).

In fact, according to this provision, the competent authorities of a State, Party to the Budapest Convention, may obtain evidence digitally stored in the territory of another State Party, in two different situations: *i)* when that digital evidence is open to public access (open source); *ii)* when that digital evidence is not open to free access but the lawful and voluntary consent of the person who has the lawful authority to disclose the data was obtained. In both cases, the competent authorities of the first State may access or receive, through a computer system in its territory, stored computer data located in the other Party.

6. This legal approach, binding several States,[2] is an important move forward, since it allows, even if in limited circumstances, access to evidence stored abroad, namely in the *cloud*. Nevertheless, as stated, this provision is limited. Furthermore, some legal issues regarding its interpretation have been raised.

In this juncture, it is important to consider the opinion of the Cybercrime Convention Committee (hereinafter "T-CY"), who issued a Guidance Note referring to it.[3] According to this Guidance Note, it is recognised that the provisions of Article 32 are exceptions to the principle of territoriality, because it permits, without the need for mutual assistance, access data stored abroad.

The provision of Article 32(a) did not raise any specific issue: it is commonly understood and accepted that the competent authorities from one State may access data that the public free and openly may access.

But with Article 32(b) the issue is not as clear. Parties to the Budapest Convention support the implementation of the provision, while some countries oppose it. One country[4] refused to join the Convention because of this Article.

---

[1] Article 32. Trans -border access to stored computer data with consent or where publicly available. A Party may, without the authorisation of another Party: Access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b) Access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

[2] In fact, it is supposed that all the Parties to the Budapest Convention have implemented domestically this provision. The Budapest Convention has currently (September 2019), 64 Parties, while another 3 signed but did not ratify it yet and 5 others were invited to access (https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185).

[3] Guidance Notes of the (T-CY) are informal opinions that, nevertheless, represent the common understanding of the Parties to the Convention, regarding the use of the treaty, aiming at facilitating the effective use and implementation of the Budapest Convention, also in the light of legal, policy and technological developments. A Guidance Note on the question of transborder access to data under Article 32 Budapest Convention is publicly available here: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a.

[4] Russia.

7. As said, in short, according to Article 32(b), the competent authorities from one Party are authorised to access data stored in the territory of another Party with consent of the person legally authorised to consent. As the Guidance Note underlines, it is clear that the consent needs to be lawful (thus not illegal) and voluntary (thus, free – not forced).

From this approach, one must also conclude that this consent cannot be provided by a national authority (for example a judge), even if in case that authority has the legal power to override the lack of authorisation.

Examples of this situation may occur, for instance, where the owner of an email account stored abroad allows authorities of his own country, where he is present, to remotely access that email account. Or the situation where the holder of a Facebook profile provides authorization to the authorities of his own country to access his profile.

8. Article 32(b) is not a mutual legal assistance toll. In fact, it seems more a unilateral action, from a State, not requiring the intervention of the other State. Thus, for example, a notification to that State is not foreseen in Article 32 – albeit it is true that it is also not precluded.

9. Another perspective, it is also clear that Article 32 of the Budapest Convention only applies within the territory of the contracting Parties to the Convention: since it is a treaty, the Budapest Convention only binds those countries that ratified it or acceded to it.

This obvious conclusion constitutes a strong limit to its scope. In fact, on the one hand, the number of Parties to the Budapest Convention, even if constantly growing, is still limited, and does not include yet a number of relevant States regarding the real cybercrime world. On the other hand, due to the limits of applicability of the physical borders of the Parties, this excludes the possibility to apply Article 32 when the location of data is unknown – since in that case, it is not possible to determine if the data are, or not, within the territory of a State Party. It will be, for instances, the case of data stored in different pieces (packets), in multiple locations, or data in undetermined location or, generically, data on the *darkweb*.

10. Thus, even if this is an interesting approach, it is clear that Article 32 of the Budapest Convention is not useful in most of the investigations regarding obtaining evidence in the *cloud*, or on the *darkweb*.

That notwithstanding the text of the Budapest Convention does not preclude or limit the adoption of other solutions at national level. However, such unilateral domestic measures have neither the recognition nor the legitimacy of international law. This factor has crucial importance: in many jurisdictions, the conducting of criminal investigations by foreign entities is not only prohibited but even criminally relevant.

C) Investigation in the *cloud* and the Portuguese law

11. As already emphasised, the methods used by criminals have modernized while legal procedural tools remain tied to the geographical and political boundaries of States. Similarly, substantive criminal law rules confer jurisdiction on States on the same basis as they did in the pre-Internet world. It may occur that a criminal makes available in the *cloud*, digital materials with criminal content (for example child pornography) and, nevertheless, the State where he lives does not have jurisdiction regarding the case, because the location of the data is unknown and might be outside of the frontiers of the State.

In this scenario, fighting cybercrime remains really difficult, since criminals live and act globally, while criminal justice authorities are limited to their national borders.

12. In this regard, Portuguese national law moved somewhat forward: the Cybercrime Law (Law No. 109/2009 of 15 September) introduced an extension to the general rules for the application of Portuguese criminal law. In general, the Portuguese criminal law applies, as occurs in many other States, to national citizens and to facts occurring on the national territory. In addition, it also applies to facts occurring abroad, when practiced by Portuguese or against Portuguese citizens.

Moreover, the Cybercrime Law, in its Article 27, states that, besides the general cases, the Portuguese criminal law is still applicable to facts; (a) practised by Portuguese citizens, if no other law is applicable; (b) committed for the benefit of legal entities established in the Portuguese territory; (c) acts physically committed in Portuguese territory, even if they relate to computer systems located outside that territory; and (d) facts related to computer systems located in the Portuguese territory, regardless of where these facts are physically practised.

This extension of jurisdiction is intended to allow courts to apply Portuguese criminal law to acts which in some way relate to the country and, in particular, if no other national law applies to them.

13. It is also important to mention the mechanism and criteria provided for in number 2 and number 3 of the same Article 27, which apply to situations in which it is found that both Portuguese law and that of another State are applicable. This legal provision provides rules in view of deciding which one of the States should centralize the procedure.

14. However, substantive criminal law issues do not exhaust the difficulties caused by informational globalization. As mentioned before, another one of the serious difficulties with criminal investigations is the procedural limitation imposed on investigators from acting outside their national borders.

It has been said that the famous *cloud* is everywhere, spread globally. That is, to put it another way when there is evidence of crimes in the *cloud*, that evidence can be physically stored anywhere. It can even be said that, in most cases, these days, any investigation may need evidence stored in the *cloud*, i.e. it may be *anywhere*. In fact, for this purpose, purely national investigations no longer exist, since any investigation may need evidence stored elsewhere, in any place on the other side of the planet (potentially).

Nevertheless, the truth is that for the purposes of criminal investigation, the *cloud*, which is *everywhere*, is also *nowhere*: it has no seat or headquarters, no postal address, or any physical premises or offices. This diffusion poses a serious difficulty to criminal investigations because it makes it difficult to clarify which criminal law and criminal procedure law should apply in the activity of obtaining information in the *cloud*.

This difficulty is compounded, as said when the data is stored on multiple servers, or on servers whose physical location is unknown or undetermined, or on *darkweb* servers, whose physical location is usually impossible to determine.

15. Also in this regard, the Portuguese Cybercrime Law introduced and interesting approach: Portugal authorizes its criminal justice authorities to act virtually outside the borders of the country, while allowing the authorities of other States (third countries) to act virtually on servers physically located in Portugal, in view of obtaining evidence.

After the ratification of the Budapest Convention by Portugal (again, the reference is Article 32(b) of the Convention), the Portuguese criminal justice authorities are allowed to access data stored on a computer physically present in another State (Party

of the Convention), remotely, without the permission or any intervention of the other State, as already explained above.

Correspondingly, according to Article 25 of the Cybercrime Law, it is allowed to the competent foreign authorities, without prior request to the Portuguese authorities or any other kind of authorization, in accordance with the rules on data protection, to "*access, through a computer system located in its territory, to computer data stored in Portugal, with the legal and voluntary consent of a person legally authorized to disclose it*".

16. But probably, the most interesting and innovative procedural approach of the Cybercrime Law regards the extension of computer searches.

Article 15 of the Cybercrime Law provides for the search for computer data, an expression that the law adopted for what could also be referred to as computer search. Basically, the provisions of the article have the common aim of adapting to the digital environment and to computer systems' classic procedural measure of search. Thus, this procedural tool, described in Article 15 of the Cybercrime Law, is a form of coercive access to a computer system. To this end, the rules for the execution of the searches, provided for in the Code of Criminal Procedure also apply to computer searches, unless expressly provided for and *mutatis mutandis*, according to Article 15, paragraph 6 of the Cybercrime Law. The same would already be inferred from the rules on paragraphs 2 to 4, which contain substantive provisions of the same nature as the correspondent rules on searches, within the Code of Criminal Procedure.

17. Those are general and common rules. But the same is not true for the particular rule introduced by Article 15, paragraph 5, which allows the extension of the search to other computer systems.

Paragraph 5 states that when "*in the course of a computer search, reasons arise to believe that the data sought is in another computer system, but that such data is legitimately accessible from the initial system, the search can be extended.*" That is, criminal justice authorities are allowed to access a remote computer system, departing from a local computer system, if during a lawful search to this last, they find out that from this particular computer system it is legitimately permitted to access the remote system. This legal possibility includes, for example, where the search subject uses an Internet-based e-mail (a webmail), the possibility to access that account if it is lawfully requested, is usually accessed from the computer under search.

This is a quite powerful tool, allowing authorities to access data in the *cloud*, by the means of computer systems belonging, for example, to suspects. In fact, in a number of cases, no one other than the intended person can access a certain remote system, as he is the only holder of the access credentials. Eventually, there is no other way to access it, except by intervening directly with the server/host of that system, which is not always possible.

18. The provision of Article 15, paragraph 5, is clearly inspired by Article 19, paragraph 2 of the Budapest Convention, which already provides for extension of searches when, during a search, there are grounds to believe that the data sought is stored in another computer system. However, according to the Budapest Convention, this provision only allows the extension of the search to remote systems physically located within the territory of the State that carries out the investigation.

On the contrary, Article 15, paragraph 5 of the Cybercrime Law allows the extension regardless the location of the remote system. In fact, this extension of computer searches is indifferent to the physical location of the remote system. That is, the search can be extended to either systems located within the Portuguese territory or

to systems located elsewhere, abroad or even in an unknown location. The criterion for the extension is solely the legitimacy of the access, departing from the system under investigation (under search).

19. Another interesting procedural tool of the Portuguese legal system is enshrined in Article 14 of the Cybercrime Law, which provides for the so-called injunction to present or grant access to data.

It is an innovative provision in the context of the Portuguese law, inspired directly by Article 18 of the Cybercrime Convention. The underlying reasons are the fact that, sometimes, the criminal investigation process requires obtaining information stored in computer systems with a large storage capacity, where access to which might be enormously complex. In such types of situations, difficulties arise in coercively accessing information: in the immense storage space of modern digital media, it can be very difficult and time consuming to find the sought information without the collaboration of those to whom data is available on the system. On the other hand, the various possibilities of hiding information or blocking access to it (e.g. by the use of encryption techniques or entering passwords for access to folders or documents) can make the search for information an unsuccessful activity, if carried out without the collaboration of the controller of it.

20. Thus, an injunction is an order, served by a judicial authority to anyone to whom data is available or has control over certain computer data, in view to communicate or give access to the data in question. Such an order must be complied with and cannot be refused. Because of that, it is, therefore, clear from the text of the law that the injunction cannot be addressed to suspects or defendants. Otherwise, the provision would clash with the right to non-self-incrimination.

In fact, this procedure is specifically intended to enable information to be obtained from computer systems belonging to other than suspects or defendants. This will be the paradigmatic case of service providers. But this will not be the only case. This provision also makes it easier, for example, to gain access to computers within corporate structures where suspects are employees and whose systems kept evidence of their unlawful activities.

21. Article 14 of the Cybercrime Law is clearly inspired by Article 18 of the Budapest Convention. This is quite relevant since according to the Convention, Article 18 applies both to domestic providers and providers based (with its seat or headquarters) in other States if they provide services in the territory of the investigative State. That is, according to Article 18, one State may address directly a provider in other State, seeking data.

In this matter, it is also relevant to consider a Guidance Note issued by the T-CY, the Cybercrime Convention Committee.[5] According to it, "*Article 18.1.b, may include a service provider that has its headquarters in one jurisdiction, but stores the data in another jurisdiction*". The key point at this respect is that the provider "*offers its services in the territory of the investigating State. The storage of subscriber information in another jurisdiction does not prevent the application of Article 18 Budapest Convention as long as such data is in the possession or control of the requested service provider*". On the other side, the Guidance Note also states that 'possession or control' refers to data "*in the service provider's physical possession and to remotely stored subscriber information under the service provider's control*".

22. Thus, according to the Portuguese legal framework (including both the Budapest Convention and the Cybercrime Law), criminal investigation authorities are

[5] This Guidance Note is available here: https://www.coe.int/en/web/cybercrime/guidance-notes.

entitled to issue injunctions directed to foreign service providers if they provide services to customers or subscribes in Portugal. And this is still valid, even if the provider does not have an office, or an establishment, or a legal representative in the country.

23. As abovementioned, Article 14 is applicable to obtaining information in possession of service providers, namely costumer or subscriber information.[6] In fact, this legal provision is the regular and most common legal basis used to request information from service providers.

In this respect, it is an obvious conclusion that in modern criminal investigations, the importance of evidence in possession of Internet service providers has grown substantially. Increasingly, these private entities store personal data, communications records, and content data that may be of great importance and, often, most precious in identifying suspects and demonstrating the perpetration of crime. This is valid regarding providers based in the investigative State, but also regarding providers based in other jurisdictions, with costumers or subscribers spread all over the world.

24. Those were the legal grounds that motivated the Portuguese Prosecution Service to approach a number of foreign service providers, in view of facilitating the communication, with the purpose that Portuguese prosecutors could issue injunctions directed to those providers and that they reply to them in an efficient manner.

As a result of this approach, it became quite frequent to Portuguese Prosecutors to serve injunctions to entities like Facebook, or Google, or Microsoft and be responded to directly by them, without the need to use the regular mutual legal assistance channels.

According to a publicly available report[7], this mechanism has proved to be of great practical effectiveness because it facilitates the timely obtaining of essential information for criminal investigations without the bureaucratic complexities of the mutual legal assistance mechanisms. On the other hand, the possibility of directly obtaining subscriber information allowed them to obtain certain types of information easier because, before, in practice, it was not possible, at all, to obtain information in this manner.

D) Remaining challenges

25. Despite the national and international mechanisms, the truth is that cybercrime keeps growing. Everyday, more crimes occur online, by the means, or with the help of the communications networks. Those crimes produce digital evidence that remains stored in a number of countries – sometimes, maybe unknown or unidentified countries.

The development of the technologies, the constant growth of the possibilities to remain anonymous online, cloud computing, the simultaneous use of multiple devices and platforms, or encryption, render the gathering of electronic evidence for

[6] Subscriber information is defined, at this respect, in Article 14, paragraph 4 of the Cybercrime Law: 4 - The provisions of this Article will apply to service providers, who may be ordered to report data on their customers or subscribers, which would include any information other than the traffic data or the content data, held by the service provider, in order to determine: a) the type of communication service used, the technical measures taken in this regard and the period of service; b) the identity, postal or geographic address and telephone number of the subscriber, and any other access number, the data for billing and payment available under a contract or service agreement, or c) any other information about the location of communication equipment, available under a contract or service agreement.

[7] Such as this annual report of the Cybercrime Office of the Prosecutor General's Office: http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/relatorio_anual_gabinete_cibercrime2015_02-03-2017.pdf.

criminal justice purposes highly complex. Besides, mutual legal assistance procedures are inefficient, in the face of the natural volatility of digital evidence. Thus, criminal investigations related to *online*, or *digital* cases is becoming less efficient each day.

These conclusions, among others, can be further explored in two important reports, from two working parties of the Council of Europe, the *Ad-hoc Subgroup on Transborder Access and Jurisdiction* and the *Cloud Evidence Group,*[8] both of them developing their work in the context of the Committee of the Cybercrime Convention (T-CY).

Both reports raised difficult questions and challenges to criminal justice regarding the location of a crime (thus, which is the applicable substantive law, and which is the competent jurisdiction, for prosecutorial purposes). On the other side, these reports express concerns in view of the limits to criminal investigation, posed by the jurisdictional issues, regarding, for example, cross border investigations, or investigations *in the cloud*.

26. Certainly, the solution to these difficult problems is neither easy nor obvious. It requires international dialogue, understanding, and concertation. In the search for solutions to ensure rule of law and justice, respect for human rights and the interests of victims, it clashes with other superior interests, sometimes conflicting with the previous, such as respect for the legality or sovereignty and independence of States.

This general concern drove the *Cloud Evidence Group* to propose the drafting of a new international treaty: an Additional Protocol to the Budapest Convention. This proposal was addressed to the T-CY Committee of the Council of Europe, which, on its 17th Plenary Meeting, on 8 June 2017, approved it.[9] Moreover, the T-CY Committee also issued the Terms of Reference[10] for the Preparation of a *Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime*.

According to the Terms of Reference, a special working group was committed to discuss and draft the terms of the Second Additional Protocol to the Budapest Convention. This drafting process should have been finished by December 2019 but, due to the complexity of the ongoing work, the term was extended until December 2020.

27. The general purpose of this future Second Additional Protocol to the Budapest Convention is to fulfil the gaps on international law posed by the new challenges of obtaining digital evidence from the *cloud*. In substantive terms, one of the first options of the protocol is to include provisions to make more efficient international cooperation. It is clearly assumed that, regarding digital evidence, the current international cooperation model is not being efficient enough and needs less formality and some flexibility. For example, one of the points to explore regards the language of the requests.

On the other side, the future Protocol should address informal cooperation between States and Internet service providers. Currently, a number of States have in place informal mechanisms of obtaining information from their side. However, only a few of them have proper regulation in place at this respect. Moreover, at the international level, in general, there is no coercive mechanism to make these requests compulsory – thus, all the process depends on is the good will of the providers. Moreover, it

[8] The final report of the *Ad-hoc Subgroup on Transborder Access and Jurisdiction* is available here https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726e, and the final report of the Cloud Evidence Group is available here https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e.

[9] The report of this meeting is available here https://rm.coe.int/t-cy-17-meeting-report-/168072366d.

[10] The Terms of Reference are available here https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b.

is expected the future protocol to provide a legal framework to this existing current practice will make the request a prerequisite.

The same can be said regarding the current practices, developed by some States, to access and obtain digital evidence across the borders. Some States already introduced into domestic frameworks provisions allowing the national competent authorities to access data physically stored outside the borders of the State. However, at the international level, this practise has no recognition yet.

As said, this is the case of Portugal, as described above these lines.

Another important component expected from the Protocol is a set of provisions on procedural guarantees and safeguards, including referring to data protection.

28. In practice, it is expected that this future additional protocol to the Budapest Convention considers issues such as a simplified regime for mutual legal assistance, requests for subscriber information, or international production orders, or direct cooperation between judicial authorities in mutual legal assistance requests, or joint investigations and joint investigation teams. Loss of location and existing transborder accesses should also be discussion, during the drafting process.

The ongoing process and the provisions under negotiation by the State Parties to the Budapest Convention can be followed on the web page of the T-CY Committee,[11] where all the published reports of the drafting groups are also available.

[11] https://www.coe.int/en/web/cybercrime/t-cy-drafting-group.