PRACTICAL NOTE No. 1/2012

The IP address and the identification of the user

The Protocol signed on 9 of July of 2012 between the Prosecutor General's Office and the major telecommunications operators (ISP) created practical mechanisms to facilitate the obtaining of information requested by the prosecution, in criminal proceedings.

Among that information, it is the identification of the IP address used by a particular customer of the ISP and, in the opposite sense the identification of the costumer that has used a given IP address, which time of use was already determined. It is described below the legal reasoning implicit in the option to include this kind of information in the requesting form.

1

There is not, in the law, a general status of the IP address. It is not also expressly provided in any legal text if the IP address is or is not, "traffic data". Nevertheless, this discussion has been important in the jurisprudence, as it raises important consequences on the possibility of obtaining such information in criminal proceedings.

2

Within criminal investigations, obtaining traffic data of electronic communications is subject to the rules of Article 18 of the Law on Cybercrime, which also applies to obtaining content data communications (Article 18, paragraph 1 and paragraph 3). In short, that possibility depends on obtaining judicial authorization and it is only allowed at the stage of investigation, in similar cases to those where it is possible to obtain telephone interceptions.

The remaining data computer (other than traffic or content) can be obtained at all stages of procedure in accordance with Article 14 of the Law on Cybercrime, by the means of the procedure order. This order, during the investigation, can be issued by

the prosecutor, whenever obtaining the data in question is necessary for the discovery of the truth.

In practical terms, considering the IP address as traffic data, has the consequence, on the one hand, that obtaining it requires authorisation by the judge; on the other hand, this is not permitted in all cases and is restricted only to serious crimes - is only permitted to obtain such data in situations where it could also be authorised a telephone interception - to which rules refers the Law of Cybercrime (Article 18, paragraph 1, subparagraph b) and paragraph 4). Moreover, this possibility is legally limited to the investigation stage.

It should be noted that if the IP address is submitted to the traffic data rules, it is not possible to obtain this kind of information in a statistically and sociologically very significant number of criminal investigations. In other words, in that case, it would have an important legal obstacle to the investigation in a very wide range of the existing criminality committed in or via the communication networks. This would cover, for example, frauds or scams with Internet sales, or defamation by email, or in blogs or other web pages or in social networks, or even threats transmitted by electronic communication.

3

The identification of a particular IP address, together with the identity of the person who used it in a particular day and time, does not disclose any information about the route of this communication or any other traffic information of the person concerned. It just proves that the communication (and only that communication) was effectively established by that technical number access. So this information, just establishes the connection between a particular communication, which is already known, and its origin. The same does not occur when information is required referring to an extended period of time or to multiple communications established by a suspect: in this case, the information required is clearly traffic information and must be submitted to the competent rules.

In conclusion, if the request of information refers only to obtaining the identification of the user of an IP address or the identification of an IP number used by an already identified person, this is not likely to disclose private or confidential information. In

practical terms, those who provide this kind of information just will confirm that an already identified communication was established – it is just a confirmation of the identity of someone that the law enforcement agents already knew, but whose name and details didn't knew.

4

The legal concept of traffic data for criminal purposes (Article 2, paragraph c) of the Law on Cybercrime), is very broad and comprehensive. Moreover, as noted, the requirements for obtaining traffic data within criminal investigations are much narrower than those of obtaining all remaining data (other than content data). Therefore, the jurisprudence has insisted on discussing the nature of the IP address.

However, this theoretical discussion about whether the IP address is or is not traffic data, is not decisive for the definition of its the status within criminal procedures: as Article 14 of the Law on Cybercrime expressly lays down the rules that law enforcement must follow when obtaining the IP address from ISP - via the special procedure modality of the production order.

By the means of the production order, within a criminal investigation, the prosecutor can issue and order to the service provider to obtain computer data stored in its system, excluding however, traffic data and content data (in this case, the rules for obtaining are stated under Article 18). However, although not including it in any of the categories of data described on paragraph 4, subparagraph b) of Article 14 of the Law on Cybercrime, this act expressly regulates the procedure of requesting IP address information to communications providers. This is a special and independent categorization of data defined by law.

Thus, on paragraph 4 it is allowed to the judicial authority to obtain data "relating to their customers or subscribers, which would include any information other than the traffic data or content contained in the form of computer data (...) and in order to establish, "among others," any number of access ". This "access number" to which the law refers to is precisely IP address. In digital communications there is no other "access number" or some kind of reality that can correspond to this concept, being legitimate and safe to conclude that this reference was expressly stated in the law to refer to IP address.

The legal solution described in the Law on Cybercrime was directly translated from Article 18, paragraph 3 of Budapest Convention on Cybercrime, of which Portugal is a Party (http://conventions.coe.int/Treaty/ en/Reports/Html/185.htm). In that international instrument it is mentioned the obtaining, by the means of the production order, of "subscriber's identity, postal or geographic address, telephone and other access number". In the Explanatory Report of the Convention (paragraph 179 - http://conventions.coe.int/Treaty/en/Reports/Html/185.htm) it is explained that this refers to all technical measures that "enable the subscriber to enjoy the communication service offered. Such provisions include the reservation of the technical number or address (telephone number, web site address or domain name, email address, etc.)." The Explanatory Report adds (paragraph 180) that "subscriber information (...) also means any information, other than traffic data or content data, by which can be established the user's identity, postal or geographic address, telephone and other access number". And it concludes (paragraph 182) that "for example, on the basis of the provision of a particular name (...) a particular associated telephone number or private e-mail address may be requested. On the basis of a particular telephone number or email address, the name and address of the subscriber concerned may be ordered ".

In this context, it is irrelevant whether it is a fixed IP address, assigned permanently to a single user, or a dynamic address, successively assigned to multiple users: both of them are a "access number" and in none of the cases the law enforcement agency will obtain data which would disclose personal or intimate information. For these purposes, the difference between them is in how the operator gets the information which is sought: in the case of the dynamic IP address, the service provider needs to see traffic data. However, since the requested data are other than those that are kept for imposition of Law No. 32/2008 (for which there are specific obligations of confidentiality and limited access - Article 7, paragraph 1, subparagraph d) and Article 8, paragraph 1) then the providers are not, at all, prohibited from accessing those data, if they don't disclose the data to third parties. Indeed, service providers are even required to monitor traffic across their networks, so as they can ensure, as required by Article 3 of Law 41/2004, safety and security in the services they provide and in the network itself. Moreover, it is inevitable that operators obtain access to traffic data, in

the normal course of their business - they need to charge their customers by the use of the services provided. This possibility is permitted by Article 6, paragraph 2 of Law No. 41/2004. Therefore, nothing prevents ISP to provide information about a particular IP address, or who used it on a particular day and time, even if they need to consult traffic data.

As mentioned, this particular aspect of the Portuguese law follows the text of Budapest Convention. None of these normative sources includes a specific status of the IP address - but it is established in both of them a particular rule that aims to regulate obtaining information related to it in criminal proceedings.

5

In short: by the specific reference made in subparagraph b) of paragraph 4 of Article 14 of the Law on Cybercrime, in the particular conditions mentioned, the IP address belongs to the set of computer data that may be requested by a production order.

The order must be issued by a judicial authority and can be issued if "it becomes necessary for the production of evidence in order to ascertain the truth." Issued the order, "who has control or availability of such data" should report them to the investigation, under penalty of punishment for disobedience (Article 14, paragraph 1).

Thus, during the investigation, the production order is the proper way for the prosecutor to ask service providers to identify the IP address used by a particular individual and, on the other side, the identification of the customer who used a certain IP address under certain circumstances of time. As said, this particular information is treated with specificity in the law (regardless of discussion about the nature of data traffic or not) and is subtracted to the limitations of Article 18 of the Law on Cybercrime.