RASCÃO
SANTOS PEREIRA
ADVOGADOS

ADMISSIBILITY OF DIGITAL EVIDENCE

Portuguese Regulations

Portuguese Law n.32/2008 of 17th of July according to the Directive 2006/24/CE of the European Parliament and Council of 15th July 2006

Brief Considerations

The Law n-º 32/2008 of 17th of July rules the preservation and transference of data of traffic and localization related to singular and collective people, as well as connected data necessary to identify the subscriber or registered user, for investigation purposes, detections and repression of serious crimes by the competent authorities, transposing for the internal juridical order the Directive n.º2006/24/CE, from the European Parliament and Council, of 15th of March, related to the preservations of fata generated or treated in a context of electronic communication services offer publically available or to private communications network, which alters the Directive n-º 2002/58/CE, from The European Parliament and Council, of 12th of June, related to the treatment of personal data and to the protection of privacy of the electronic communications sector.

By **Digital Evidence** it is consider all and any type of information to which is conceded a probative value that is, however, filed and transference in a digital way. In this category Evidence we can conclude:

- Files data in the hard disk of a computer;
- Digital vídeo;
- Digital Audio;
- Packs transfered by networks;
- Email;
- Communications through instant messages services
- Private conversations in instant messages services;
- Etc.

Legal Notes:

Regarding the prevision of the article n.º 151º of the Portuguese Criminal Procedure Code (PCPC) the expert regime as a Evidence method which goal is the evaluation of traces of practiced crime based on technical, scientific or artistic knowledges. There are no motives that lead us to the non-application of this regime to the digital Evidence.

It is further more disposed in the article n.º 189 of the PCPC an extension regime of the provisions of the articles n. 187º and 188º to all communications or conversations by any technic method different from a phone, existing a clear and undisputed reference to the transferences of fata by email or by any other method of transference by telematics way, even if they are stored in digital format.

Should even be applied to a part of the digital Evidence, such as, email, the disposed in the article n.º 179º of the PCPC. So, the judge is competent to authorize or demand, by order, its consultation by the competent bodies.

In principle, there is only one requirement in order to include the email in this regime, the messages must be sent to a determined receiver.

The present Law transpose to the Portuguese legal order the Directive n.º 2006/24/CE, of the European Parliament and Council, of 15th of March, related to the preservation of data generated or treated in a context of offer of electronic communications services publically available or public networks of communications.

This Directive has proceed to the harmonization between the European Members and it is applied to the data of traffic, data of localization and related data, aiming to help the internal ruling of each European Member. Portugal was not an exception and it has proceed with the transposition to the internal juridical order through the Law n.º 32/2008 of 17th July

In this manner, the mentioned purposes to rule:

1. The **preservation and transference of data of traffic and localization** related to:
    a) Single People;
    b) Collective People:

The first though of the Directive in question refers that should be demanded to the European Members on the treatment of this data that the rights and freedom involved must be assured considering that, during its treatment, they are obliged to proceed to their extinction once they became unnecessary.

2. The related data necessary to identify the registered **subscriber** or **user** for purposes of (article 3º, n.º1)
    a) Investigation:
    b) Detention
    c) Reprehension of serious crimes.

We are dealing with a type of Evidence that constitutes an extremely crucial and useful element on the continuation of the mentioned aims, considering that all technologies related to these communications of this nature have a rapidly evolution. Therefore, emerges legitimately the need to see the consequent evolution of the authorities as well.

Any restriction that occurs within the continuation of the aims above mentions must constitute ineludibly a necessary measure, adequate and proportional to a democratic society, according to reason that should be ruled, such as motives of public nature, national security, etc.

The internal Law as well as the Directive start by clarifying some undetermined concepts. According to the n.º 2 of the article 2º should be understood by data all data of traffic, localizations and related damages necessary to identify he subscriber or user;

The concept of telephonic service, for effects of the mentioned Law, should include: Services of local calls, teleconferences, data transference, supplementary services (call forwarding and call transfers) and also messages services and multimedia (services of short messages, services of multimedia messages and services of improved messages and multimedia services)

By code of user identification we should understand the unique code given to the users since the moment that they became subscribers or subscribe any service with access to the interne or in a communication service through the internet.

The **identifier of the cell** should be the identification of the cell of origin and destiny of a telephonic call within a mobile network.

All the communication between the telephonic connection that has been established without reply or if there has been an interception by the network manager should be considered a telephonic call failed.

The use of data must respect the **principle of utility**, therefore, we must distinguished localization damages from basis and content. On the first group enter all data that allows tracing geographically a specific user, within the group of basis data we include all personal data, such as, phone number, the identity, the address of the service subscriber, the detailed list of communication movements, which means, everything that allows the competent authorities to have access to some beginning point in order to be able to continue the investigation process. Last, by content data we understand all the data related to the content of the communication *per si* or of the message, for example, the matter of an email message, the matter of a private conversation in the MSN, a sent image by phone, etc.

The legal **competence** for the practice of this regime is given to the following **juridical authorities** and **criminal police authorities**:

a) The Judiciary Police (Criminal Investigation Police);
b) The National Republican Police (Law Enforcement *strictu sensu*)
c) The Police of Public Security (Law Enforcement *strictu sensu*)

d) The Military Judicial Police
e) The Foreign and Borders Service
f) The Maritime Police

Consequently, it is celebrated by the disposed in the article 17º of the refered Legal order considering that it is a responsibility of the European Members to implement legal procedures to assure that only data preserved are transferred to the competent authorities in order to avoid violations of fundamental rights and freedom.

In the article 4º of the Directive it is also added the obligation of the European Members to take action in order to assure that the data are only transferred to the competent authorities and that this fact only occurs in situations legaly established.

From the internal Law it is so concluded that its content will be only applied in the following legal types:

a) Terrorism Crimes;
b) Violent Criminality;
c) Criminality Highly Organized;
d) Abduction;
a) Kidnapping;
b) Hostage taking;
c) Crimes of cultural identity;
d) Crimes against personal integraty;
e) Crimes against the State Security;
f) Currency falsification;
g) Falsifications of titles similar to currency;
h) Crimes covered by convention about security of aerial or sea navigation.

According to the jurisprudence of the Court of Second Instance of Lisbon, on 13th of October of 2004, has been decided that the constitutional demand authorizing or ordering the housing search by a judge it is a consequence of the house be seen as, by excellence, a space of privacy and intimacy.

As a result of this demand the fact of a personal computer where on it can be found "information of personal character" nothing alters the nature of the damaged rights done by a housing search.

The authorization conceded to realize a housing search allows the OPC to acknowledge the content of the hard disk of a computer eventually there found. However, the same cannot be applied to the email filed on it.

As to the email should be applied the legal regime predicted to the apprehension of correspondence (articles 179º and 252º) and not what the PCPC reserves concerning the interception of the communications once it is only directed to the interception of conversations or communications taking place:

1) There must be an authorization, by legal and justified order of the instruction judge;
2) The diligence must be consider crucial for the discovery of the truth, being impossible achieve it by other means:
3) Has legitimacy to require: the MP and the competent criminal police authority;
4) Can only be authorized a transference of data **concerning**: the **suspect** or the **defendant, to a person as intermediary**, to whom is considered fundament reasons to believe that such person receives or transfers messages to or from the suspect or defendant and to the crime victim.
5) On the final decision of the judge of instruction must be conveniently though the **principles of adequacy, necessity and proportionality**;
6) These requirements can be kept away any time there is the need to avoid threat to the life or serious offense of physical integrity (article 252º PCPC)

The Court end up deciding, according to the article 167º of the PCPC, that they cannot be constituted Evidence.

Hence, regarding the legal requirements predicted to the Portuguese legal organization Thus, must be considered **inadmissible digital Evidence**:

a) All Evidence that has no kind of relevance to the concrete fact, so without contributing, in any way, to the discovery of the truth;
b) All Evidence merely unnecessary, considering that there are other types of Evidence that sustain the judge decision, allowing such types the knowledge of the truth.

The **criteria of admissibility of digital Evidence** must attend to the relevance and the essentiality in the process, though by the judge of instruction for the concrete case.
The Portuguese mentality joined the Directive. In the n.º9 argument can be found the disposed the fact that any person has the right to their own private life and their correspondence. Although the public authorities can interfere on the exercise of this right whenever its assembled necessary within a democratic society avoiding the violation of ECHR, fulfilling all the requirements of its article 8º.

According to the importance of this type of data, the Directive has opted to rule and grant that in an European level the regime of preservation was clearly defined. So, the suppliers are obliged to preserve the data as well as it to them imposed minimum and maximum temporal periods.

The suppliers of services to access communications networks preserve the data to minimize the negative effects on the possibility of "anonymous utilization" of the internet and by the lack of control of local places of free access. It is predicted in the article 6º of the internal Law a deadline between a temporal space to be defined by the European Members by a period never lesser than 6 months and never superior than 2 years counting from the communication date.

It is also an obligation of the suppliers of these services to assure the quality of these data and the confidentiality and security of its treatment during the temporal period, imposed by the internal Law, that obliged the suppliers to preserve them.

According to the article 7.º of the Directive, the preserved data should have the same quality and must be subject of the same protection and security of the network data. Should even be an object of technical procedures that protects them from accidental or illicit destruction. To these, obviously, should only have access people with legal competence to do so.

The suppliers of services of access to the communications networks preserve data in order to minimize the negative effects of the possibility of anonymous utilization of the internet and by the lack of control of locals of free access. A period of one year of it is the preservation deadline predicted in the article 6º of the mentioned Law.

Hence, **any time** that is required a specific information, should this information be given in perfect conditions against the prejudice of disobeying crime.

If the judge of instruction decides the transference of data, he should determine the **destruction** of the data in questions from the moment they stop to fulfill the requirement of essentiality in the process.

The **impulse** can came from other then the judge, thus, any interested can direct a requirement that requests the destruction of data on the hands of the competent authorities above mentioned, when one of the following conditions are verified:

i. Definitive filling of penal process;
ii. Acquittal, final rendered;
iii. Condemnation, final rendered;
iv. Prescription of the penal proceeding;
v. Amnesty.

Concerting the duties resulting from the category “competent entities”, they are obliged to:

a) **Preserve** data so they can be transferred immediately and according to the judge authorization;
b) **Grant** that they are submitted to the same protection and security of the data in the network**;**

c) **Avoid** in an active away the **accidental** or **ilicit destruction, lost** or **accidental transformation** and filling, treatment, access and divulgation **non-authorized** or ilicit;

d) **Grant** that only some people specially authorized have access to the data**;**

e) Proceed to the destruction of the data immediately after judge order;

f) **Preserve** the data between the period that the judge authorizes its transference and orders its destructions;

If there is a violation of the rules above mentioned, the article 13º of the referred Law predicts the constitution of crime, punished with prison until 2 years or fee until 240 days.

The Directive predicts the necessity of each Member State appoint one or more public authorities to control the application, in each national territory, the dispositions adopted by the Member States. This authority must act with absolute independence on the exercise and control of the application of the Directive as well as the internal laws.

It was, then, decided in Portugal, that the National Commission for Data Protection has competence to control the application of the mentioned above and should maintain an electronic registry permanently updated of the people specially authorized to have access to the data.

To this authority should be addressed, electronically, the necessary data to identify everyone specially authorized to accede the data by the suppliers of electronic communications services or of a public network of communications.

It is also a **competence** of the **National Commission of Data Protection** the instruction of the process of infringement proceedings and the subsequent applications of fees related to the violations above mention, considering that the amount charged is distributed by the State (60%) and the NCDP (40%).

Every year the NCDP is in charge of communicate the statistics related to the preservations of the data generated or treated in the context of offer of electronic communications services publically available or in a public network of communications, the deadline to send is until 1st of March of each year, excluding any type of personal data:

The Directive disposes that the Member States must ensure that they communicate the statistics about the preservations of data generated or treated. Following this though, the Portuguese law imposes that each year the NCDP must be in charge of communicate the statistics related to the preservation of the data generated or treated in the context of offer electronic communication services publically available or in a public network of communications, having until 1st March of each year to send the, excluding any type of personal data:

a) The **number of cases** in which there was information transference to the competent national authorities.
b) The period of time occurred between the time from which the data were preserved and the time in which the competent authorities requested its transference;
c) The number of cases in which the requests could not be fulfilled.

Against the annual analysis of this statistics it is also a competence of the NCDP, in cooperation with the Institute of Communications of Portugal – National Authority of Communication:

1. To **evaluate** all the proceedings predicted in the mentioned law;
2. **Elaborate** a biannual report in detail;
3. Include eventual recommendations

The content of the report must be communicated to the Portuguese Parliament and the Government.