Proc.

0186

Senhor Director-Geral,

Em resposta ao Questionário da Comissão Europeia referente à Directiva 2006/24/CE (Retenção de Dados), junto tenho a honra de remeter a V.Exª respostas enviadas pela Ministério da Justiça e da Comissão Nacional de Protecção de Dados.

Restantes respostas, particularmente dos operadores de telecomunicações, cujos contributos não estão traduzidos para nenhuma das línguas de trabalho da Comissão Europeia, serão encaminhadas oportunamente.

Queira aceitar, Senhor Director-Geral, os protestos da minha alta consideração.

O Representante Permanente

J.L.S. SCANNED

03 FEB. 2010

Exmº Senhor
Jonathan FAULL
Director-Geral
Direcção-Geral da Justiça, Liberdade e Segurança
Comissão Europeia
Bruxelas

MCS/IRC
Questionnaire with a view to take stock of the operation of the retention of data generated or processed in connection with the provision of publicly available electronic communications services or networks and amending directive 2002/58/EC

As a general and previous remark to the whole of the questionnaire, it should be stressed that in relation to Portugal most of the questions have to be considered premature, bearing in mind that Law 32/2008, which transposes the Data Retention Directive, dates from the 17th of July 2008 and that the framework set by the law required further regulation, which was implemented through Portaria 469/2009, of May 2009. Moreover, between August and the end of November 2009, a trial period set forth in Portaria 916/2009 of the 18th of August took place, during which competent authorities could use the software in a voluntary manner.

The use of the electronic system developed in order to request retained data has become mandatory since the 1st of December 2009, meaning that an evaluation of the implementation will obviously be more accurate from this date on. So far, the Institute for Justice Information Technologies (ITIJ) does not have information on requests made by competent authorities using the new system and it is predictable that training sessions both for competent authorities, judges and network and service providers will be required. Therefore, as far as quantitative replies are concerned, the information we can provide at this stage is necessarily scarce.

1. Questions to Member States and non-EU EEA States

1.1. Qualitative and quantitative aspects of the application of Directive 2006/24/EC, taking into account further developments in electronic communications technology and the statistics provided pursuant to Article 10.

1.1.1. Law enforcement issues

1.1.1.a. Total number of requests that are issued by year to obtain data retained under DRD.

Not applicable. Due to the fact that both the Law transposing the Data Retention Directive and the Regulation that implements the law have been into force for less than one year, the competent authorities have not yet registered requests in its application.

1.1.1.b. Number/percentage of these requests that are generated by type of requesting authority: 1. Police; 2. Judicial, and 3. Other authorities (please specify as relevant).

Not applicable.

1.1.1.c. The time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data, or if unavailable, the average age of the data that are requested? The answer to this question may already have been provided in the context of the statistics of Article 10 DRD.

Not applicable. This question can only be answered when there are any registered requests.

1.1.1.d. Which communication channels are used to exchange information between law enforcement authorities and service providers (e-mail, fax, secure network, or other
channels? If certain channels are required to be used, please provide information about the channels to be used.

The competent authorities submit the requests through a specifically designed software placed by the Ministry of Justice; the request is authorised or commanded by a judge and then submitted to the service providers concerned by the search through private network communications.

I.A.1.e Type of crimes

I.A.1.e.1 For what type of crimes does the national law authorise the acquisition and use of retained data? Please provide a list of these crimes.

According to Law 32/2008, data retention is limited to serious crime and encompasses the following criminal offences: terrorism, violent crime, highly organised crime; abduction, kidnapping and taking of hostages, crimes against cultural identity and personal integrity; falsification of currency and equivalent titles, criminal offences set forth in conventions on aerial or maritime navigation security.

According to the Portuguese Criminal Procedure Code, the expression «violent crime» refers to intentional conduct against life, physical integrity or personal freedom punishable with an imprisonment penalty of five or more years.

«Highly organized» crime refers to conduct encompassed by the crimes of criminal association, trafficking in persons, arms trafficking, drug trafficking, corruption, influence peddling and money laundering.

Additionally, Law 109/2009 of 15th September (Cybercrime Law), allows for the expedited preservation of data stored in a computer system in relation to the crimes of computer-related fraud, data interference system, computer-related sabotage, illegal access, illegal interception and illegal reproduction of protected computer software, crimes committed by means of a computer system or to the collection of evidence in electronic form of a criminal offence. The expedited preservation of data is ordered by the competent judicial authority to whoever possesses or controls the data, including the service provider.

What is the average age of the data that has been requested for the different types of crime mentioned under I.A.1.e.1?

This question cannot be answered at this stage. The Portuguese legislation foresees a maximum period for the retention of data of 1 year.

I.A.1.e.3 - Does the national law allow for or prohibit acquisition of data from communications providers of data subservient of the Directive and/or related serious crime (e.g. copyright infringements). If so, please provide details about the alternative purpose(s) or laws prohibiting such acquisition.

The Law that transposes the Directive (Law 32/2008 of 17th of July) allows data retention exclusively for the purposes of investigation, detection and prosecution of serious crime to competent authorities and following a judicial mandate (despatch). Retained data are transmitted to competent authorities only if there is reason to believe that they are fundamental to uncover the truth or that proof would be impossible or very difficult to obtain in the context of the investigation,
detection and repression of serious crime. In this context, the only exception is the obtaining of cellular location data in order to repeal a danger to life or a serious offense to physical integrity. However, we can consider that the scope of application is wider in relation to traffic data stored in a computer system, as the Cybercrime Law allows the expedited preservation of data stored in a computer system in relation to crimes of computer related fraud, data interference system, computer related sabotage, illegal access, illegal interception and illegal reproduction of protected computer software, crimes committed by means of a computer system or collection of evidence in electronic form of a criminal offence.

1.A.1.e.4 - Assessment of the data to be retained (the meaning of this question is not clear)

1.A.1.e.5 - Does the national law transposing the Data Retention Directive or a related instrument, require the retention of other categories of data in addition to the data contained in Article 5 of the Directive? If so, please provide details about the additional data as well as the instrument in which this obligation is enshrined.

No. Portuguese Law requires the retention of the exact same categories of data that are listed in the Data Retention Directive (data necessary to trace and identify the source of a communication; data necessary to identify the destination of a communication; data necessary to identify the date, time and duration of a communication; data necessary to identify the type of communication; data necessary to identify the location of mobile communication equipment).

1.A.1.e.6 - Adequacy and law enforcement relevance of the data retained under Article 5 of the Data Retention Directive.

Please indicate whether the data the service providers must retain under Article 5 of the Directive are relevant and sufficient from a law enforcement perspective, and mention which data either should be removed from the list of Article 5 where redundant or be added where relevant data is not yet retained. Member States are invited to motivate their answer and provide examples of situations that demonstrate the redundancy or the law enforcement requirements.

At this stage it is not possible for Portuguese competent authorities to assess the relevance and sufficiency of the data to be retained.

1.A.1.f. Details of the requests that are issued.

1.A.1.f.1 The kind of information that service providers are requested to retrieve; please provide information about typical search parameters (information selection criteria) contained in requests for the acquisition of retained data, e.g., listing of the communications made from or to a given phone number, or at a certain hour, or listing of all calls made from a certain location, or of all numbers used by an identified user.

The search parameters are:

1) Mobile communications: Phone nr.
2) Access communications to the mobile internet: IP.
3) Fixed telephone or VOIP communications; Phone nr.

4) Access to internet via fixed network communications; IP; USERNAME; PORTID.

5) E-mail services – account activity; E-MAIL ADDRESS.

6) Communications by cell/hour; Search by cell; LOCATION INFO.

7) Phone Communications and ISP Services; Phone nr.; IP; USERNAME; PORTID.

8) E-mail service – Client’s data; EMAIL ACCOUNT; EMAIL ADDRESS.

9) Voice communications/Mobile Network data – pre-paid cell ID; Phone nr.

10) MEI phone number identification; Phone nr.;IMEI.

<table>
<thead>
<tr>
<th>Description</th>
<th>PHONE NR</th>
<th>IP</th>
<th>USERNAME</th>
<th>PORTID</th>
<th>EMAILACCOUNT</th>
<th>EMAILADDRESS</th>
<th>IMEI</th>
<th>LOCATION INFO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile communications</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access communications to the internet via mobile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fixed telephone or VOIP communications</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access to internet via fixed network communications</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail services – account activity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Communications by cell/hour; Search by cell</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Phone Communications and ISP Services</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail service – Client’s data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice communications/Mobile Network data – pre-paid</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
1.A.1.f.2 - Did your country standardise or is seeking to standardise the format for the acquisition and disclosure of communications data between public authorities and communications service providers (for instance in service level agreements, or by making reference to relevant ETSI standards)? If so, please provide information about the standard (form or format) for requests, the message format, the technical modalities and/or interface.

We did not standardise the format for the acquisition and disclosure of communications data between public authorities and communications service providers through any service level agreements or ETSI standards.

In Portugal both the request of data, the judicial mandate commanding or authorising the transmission of data and the reports containing the data that satisfy the request were formatted according to two patterns: an XML grammar, which models and encompasses the parameters for all possible searches; a PDF file, digitally signed, with a valid digital certificate.

Moreover, the answer report is cyphered through public-key encryption that can only be decrypted with a secret key owned by the information system of the Institute of Justice Information Technologies.

1.A.1.g - Details of the replies to the requests mentioned under 1.A.1.g.

The reply of the service providers is sent in PDF format, digitally signed, containing a mandatory set of informations, but without a rigid structure of reply.

1.A.1.h - Does the national law governing the acquisition of communications data enable the public authority to specify the time period within which data must be disclosed, as referred to in the Directive as "without undue delay". If so:

1.A.1.h.1 - Please provide examples of time frames enforceable within the context of national legislation or by service level agreements between competent authorities and communication providers.

The legal instrument that regulates Law 32/2008 of 17th July (Portaria 469/2009 of 6th May) does not mention a specific time frame. According to its article 3, upon the reception of the request, the communications provider must perform the data research immediately, by order of reception of requests or according to the degree of urgency determined in the judicial mandate.

1.A.1.h.2 - What measures do competent authorities avail of to ensure the respect of the time period within which they request the reply to be given?

According to article 12 of Law 32/2008, non compliance with the obligation to transmit the requested data is considered an infringement (of non criminal nature) punishable with a fine of €1500 to €50000 for physical persons and €5000 to €10 000 000 for legal persons.
1.1.h.3 – Where relevant, do competent authorities distinguish between time periods within which they require the disclosure of data by communication providers and the type of request or type of data they need? If so, please provide examples of such differentiation.

No, the only differentiation made is that based on the urgency of the request, defined in the judicial mandate.

1.1.i – Reimbursement of costs

1.1.i.1 – Does your country reimburse CAPEX and/or OPEX incurred by service providers? If so, please provide information about the type of costs that are reimbursed, as well as about the modalities and amount or ratio of reimbursement.

Law 32/2008 does not provide for any reimbursement of costs incurred in by the network and service providers. Therefore, each provider will support the costs of adapting its own system to ensure compliance with the obligations imposed by the law. However, costs regarding the development of the application to be used by the competent authorities for the sending of the requests and receiving of data are supported by the Ministry of Justice.

1.1.i.2 – Does your country make the reimbursement of costs conditional on the respect of certain conditions, such as, for instance, guaranteeing a certain quality of service (request profiles, amount of requests to be handled, speed of retrieval)? If so, could you please provide information about the conditions that service providers have to meet and the link between reimbursement scheme.

There is no reimbursement of costs.

1.1.j – Effectiveness – What is the success rate of the use of retained data.

At this stage it is not possible to answer to this question.

1.1.j.1 – Did the use of retained data assist in crimes being detected and/or prosecuted within the courts that otherwise would have failed? If so, please provide examples.

At this stage it is not possible to answer to this question.

1.1.j.2 – How much does the use of retained data cost in terms of deployment of Human Resources and acquisition & maintenance of dedicated equipment? What are the typical cost drivers?

The answer to this question is premature.

1.1.j.3 – How can cost effectiveness of the acquisition and use of retained data be increased?

The answer to this question is premature.

1.2 – National and transnational requests and answers.
1.A.2.a - Within this questionnaire, a "transnational request" means a cross-border request for the acquisition of communications data between EU Member States and non-EU EEA States as appropriate where:

The software is not prepared to receive transnational requests or to send requests to non-national authorities. Transnational requests are made via regular cooperation channels.

1.A.2.c. Which authority takes the decision in your country to issue a transnational request? Are all law enforcement authorities entitled to make or prompt to make a transnational request?
As in national requests, the decision to issue a transnational request is taken by a judge, following a request by a competent authority or commanded by the judicial magistrate.

1.A.2.d. Does your country have a central point that issues outgoing requests or receives incoming requests? If so, please provide details about these central points.
The request point in charge of data retention is not mentioned.

1.A.2.e Costs

1.A.2.e.1 - There is no reimbursement foreseen.

1.A.2.f Language.

1.A.2.f.1 Does your country impose linguistic conditions to incoming requests? If so, please provide details about those conditions.
(to be completed)

1.A.2.f.2 What means does your country deploy to comply with linguistic conditions imposed by other countries to outgoing requests? Do you have a central facility to provide linguistic support?
(to be completed)

1.A.2.g - Data Security
Which measures (rules, procedures, audit provisions) are enforced to protect data against misuse?

The security of information is ensured through a set of procedures: the encryption of all electronic communications by the electronic systems, the encryption of the file containing the reply, meaning that the information can only be seen through that specific software; the digital signature of the judicial mandate and of the reply file of the provider; the electronic register of all the requests sent; the storage of the reply files in a special section created for each provider, equipped with security mechanisms in order to avoid data interconnectivity; security audits to the application.
Additionally, access to the application is made through usernames and passwords and at the end of the retention period, the data are destroyed, except those whose conservation was determined by the
judge. Another relevant security measure is the blocking of the data since the beginning of the conservation period and subsequent unblocking only for transmission purposes.

1.B – At the moment Portugal does not deploy measures to ensure traceability of users of prepaid SIM cards.
Reply from Portuguese Data Protection Authority

(Comissão Nacional de Protecção de Dados - CNPD)

Questionnaire with a view to take stock of the operation of on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

V 30.09.2009

3) The Data Protection Authority in Portugal (CNPD) is the only national supervisory authority for all data protection matters, either according to the Data Protection Directive, the e-Privacy Directive or the Data Retention Directive.

At this point, since Law 32/2008, which transposes the Directive 2006/24/EC, only entered into force in August 2009, there is no possibility to make the assessment of its application yet.

Indeed, as far as we know, the electronic platform, by secure network, set up to transmit data between the providers and the competent authorities has not being used yet. Therefore, we are not able to analyse whether this situation is due to the lack of necessity in terms of criminal reality or whether that platform is not in full activity.

Concerning the statistics provided for in article 10 of Directive (article 16 of Law 32/2008), the DPA is the competent authority to provide them to the European Commission.

However, only next year we will be able to communicate this information to the EC, once the Portuguese law will only be applicable for 4 months of the current civil year.

According to the Portuguese law, the service providers have to transmit this information to the DPA, each year, until the 1st of March.

3.A.1) Yes, the DPA has powers of authority, including investigative and sanction powers, and powers to collect all the information necessary for the performance of its supervisory duties (article 22 of Law 67/98, Data Protection Law). This include the possibility to inspect in loco, with free access to all computer systems and documentation deemed necessary.
As stated above, once this law on data retention has only 3 months in force, the DPA has not received any complaint.

Apart from the general competence of the DPA, Law 32/2008 disposes in its article 7 (transposing article 9 of the Directive 2006/24/CE) that the DPA is the competent supervisory authority.

3. A. 2) The DPA has the same powers towards private and public bodies. In fact, the Data Protection Law applies equally to 1st and 3rd pillar data. The DPA also supervises data processing in the police sector. Portugal did not use the derogation foreseen in article 13 of the Data Protection Directive.

Regarding complaints, the situation is the same as described in the previous question.

3. A. 3) Yes, the DPA has the power to audit compliance of providers, and we will do so.

For the time being, that practice is prejudiced by the fact that the law has only been in force since August 2009.

3. A. 4) Not applicable for the reasons described above.

3. A. 5) There have been no specific problems concerning the data storage by service providers. First of all, the data is retained for a shorter period than now resulting from dispositions of Directive 2006/24/EC. On the other hand, the service provider didn’t have to store so much data as they are obliged currently.

The obligation to retain all the traffic data for a maximum period of 1 year (in Portugal) means that there will be huge amounts of data stored, related to one single person. This information is, according to the Portuguese Constitution and law, considered sensitive data. Therefore, it should be better protected. Moreover, the use of such data for police purposes puts upon the data an added value.

Therefore, the possibility of the service providers to recourse to outsourcing companies to process this data presents specific concerns.
Furthermore, when the data process could be in a third country, therefore subjected to particular rules (or laws) imposed from outside.

This situation poses serious problems for supervisory authorities, who are not able to fully control the data flows and subsequent use. This is a very delicate matter, once it deals with criminal investigations, judicial secrecy and action. It is very difficult for a DPA to oppose to such outsourcing (based on data Protection Directive) when the law does not mention this question or prevent this situation. However, we consider that the potential information leakage or misuse is highly increased. It would be almost the same as law enforcement authorities outsourced their investigations to private companies based on third countries.

3.A.6) Not applicable yet. There is some jurisprudence concerning the violation of telecommunications, but no specifically on data retention.

3.B) The traceability of users of pre-paid SIM cards was never set forth by the Government. Indeed, in the draft law transposing the Directive 2006/24/CE, the pre-paid cards users are not obliged to identify themselves to the operators. Therefore, the DPA did not raise any considerations on that. Nevertheless, though the anonymity would better serve privacy, the fact the application of the Data Retention Directive leaves out such users, which represent in Portugal around 80% of the market consumers, raises the question of pertinence and accomplishment of the purposes of the Directive itself. How efficacious could this Directive be if the great majority of the mobile phone users is left out. We suppose criminals are not well behaved subscribers. As the law stands now, it is our opinion that the purpose of the Data Retention Directive is far from being reached. On the other hand, “inlaw” citizens have their communications data retained for longer period, increasing the risks of undue access and misuse. This reality is also quite negative form a data protection point of view.

CNPD, 11th of November 2009