EUROPEAN AFFAIRS COMMITTEE

## Opinion COM(2011)225

COMMISSION REPORT TO THE COUNCIL AND TO THE EUROPEAN PARLIAMENT - Evaluation report on the Data Retention Directive (Directive 2006/24/EC)

EUROPEAN AFFAIRS COMMITTEE

PART I - INTRODUCTION

Pursuant to Article 7 of Act No 43 of 25 August 2006, as amended by Act No 21 of 17 May 2012 on the monitoring, examination and issuing of opinions by the Assembly of the Portuguese Republic in the context of the European Union integration process and in accordance with the arrangements for the scrutiny of EU Initiatives approved on 20 January 2010, the European Affairs Committee received the REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT - Evaluation report on the Data Retention Directive (Directive 2006/24/EC) [COM(2011)225].

Given its subject matter, the above-mentioned initiative was forwarded to the Committee on Constitutional Affairs, Rights, Freedoms and Guarantees, which analysed it and approved the report annexed to this Opinion, of which it is an integral part.

**PART II – GROUNDS**

**1. General**

For the purpose of investigating, detecting and prosecuting serious crimes, Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data requires Member States to oblige providers of publicly available electronic communications services or public communication networks to retain traffic and location data for between six months and two years.

The Commission carried out an evaluation of its application by Member States and its impact on economic operators and consumers, taking into account further developments in electronic communications technology and statistics provided to the Commission, with a view to determining whether it is necessary to amend its provisions, in particular with regard to its data coverage and retention periods.

Further to a brief mention of the background, objectives and legal basis of the Directive, the report points to the ‘complex legal relationship between the Data Retention Directive and the e-Privacy Directive (Directive No 2002/58/EC), combined with the absence of a definition in either of the two directives of the notion of 'serious crime', which makes it difficult to distinguish, on the one hand, measures taken by Member States to transpose the data retention obligations laid down in the Directive and, on the other, the more general practice in Member States of data retention permitted by Article 15(1) of the e-Privacy Directive.

2. Main aspects

As regards transposition of the Directive, the report notes the transposition of the Data Retention Directive by 25 Member States: Belgium (only partially), Bulgaria, Czech Republic, Denmark, Estonia, Ireland, Greece, France, Spain, United Kingdom, Italy, Cyprus, Romania, Slovenia, the Netherlands, Lithuania, Luxembourg, Poland, Hungary, Slovakia, Finland, Germany, Latvia, Malta and Portugal, which transposed the Directive with Act No 32/2008 of 17 July 2008.

It also notes the fact that, following the initial notification of transposition by Czech Republic, Germany and Romania, their respective constitutional courts annulled the domestic legislation transposing the Directive, and they are considering how to re-transpose the Directive.

It mentions too the very different solutions found by Member States to comply with the objectives of the Directive.

Another aspect which should be noted is the role of retained data in the judicial system. To this end, it notes that both the volume of telecommunications traffic and the request for access to traffic data are increasing, despite the very different situations between Member States, with the most frequently requested type of data being related to mobile telephony.

It should also be noted that, according to most Member States, the use of retained data older than three and even six months is less frequent but can be crucial.

Its use has tended to fall into three categories:

1. Internet-related data tend to be requested later than other forms of evidence in the course of criminal investigations. The reason for this situation is that analysis of fixed network and mobile telephony data often generates potential leads which sometimes result in further requests for older data.

2. Investigation of crime tends to rely on older data, in particular, data relating to the period of preparation and planning of these crimes, in order to identify patterns of criminal behaviour and relations between accomplices to a crime and to establish criminal intent. It is often the case that activities linked to complex financial criminality are detected only after several months.

3. Some Member States have requested traffic data held in another Member State, which can usually only release these data with judicial authorisation in response to a letter rogatory issued by a judge in the requesting Member State.

It is also observed that the Member States report data retention to be at least relevant and, in some cases, indispensible for preventing and combating crime, including the protection of victims and the acquittal of the innocent in criminal proceedings. The report also states that successful convictions rely on guilty pleas, witness statements or forensic evidence. Retained traffic data, it was reported, have proven necessary in contacting witnesses to an incident who would not otherwise have been identified, and in providing evidence of, or leads in establishing, complicity in a crime. Certain Member States further claimed that the use of retained data helped to clear persons suspected of crimes without having to resort to other methods of surveillance, such as interception and house searches, which could be considered more intrusive.

It is also considered that there is cause for concern at the ways of circumventing the measures deriving from the application of the Directive, such as using unregistered pre-paid SIM cards or other forms of technologically more advanced or increasingly used communication such as virtual private networks in universities.

3. Relevant issues

As regards the impact of data retention on operators and consumers, the report intended to assess the effects of the application of the Directive on economic operators and consumers, taking into consideration the technological development of electronic communications and the statistics submitted to the Commission, in order to assess the need to amend its provisions, particularly as regards the data covered and the period during which they must be retained.

According to the Commission’s assessment, ‘most operators were unable to quantify the impact of the Directive on competition, retail prices for consumers or investment in new infrastructure and services.

It also noted that ‘there is no evidence of any quantifiable or substantial effect of the Directive on consumer prices for electronic communications services’.

In relation to the implications of data retention on fundamental rights, the report analysed the implications of the Directive for fundamental rights, taking into consideration several judgments of the European Court of Justice (which laid down guidelines) and taking into account the criticism of data retention, as well as various calls for stronger security and data protection rules.

a) Legal basis

The Directive is based on Article 95 of the Treaty establishing the European Community (replaced by Article 114 of the Treaty on the Functioning of the European Union) concerning the establishment and functioning of the internal market.

b) The principle of subsidiarity

The principle of subsidiarity does not apply as the document being analysed is not a legislative initiative.

PART III - CONCLUSIONS

Overall, the Commission considered that the evaluation has demonstrated that data retention is a valuable tool for criminal justice systems and for law enforcement in the EU.

However, the Commission still considers that the contribution of the Directive to the harmonisation of data retention has been limited in terms of, for example, purpose limitation and retention periods, and also in the area of reimbursement of costs incurred by operators, which is outside its scope.

Given the implications and risks for the internal market and for the respect for the right to privacy and the protection of personal data, the EU should continue through common rules to ensure that high standards for the storage, retrieval and use of traffic and location data are consistently maintained.

PART IV - OPINION

In the light of the information set out above and the Report of the relevant committee, the European Affairs Committee's opinion is as follows:

1. No issues have been raised concerning the issue of compliance with the principle of subsidiarity.

2. Concerning the questions raised in the grounds, the European Affairs Committee will continue to monitor the legislative process relating to this initiative, specifically by exchanging information with the Government.

Palácio de São Bento, 19 February 2012

| Rapporteur | President of the Committee |
| --- | --- |
| (Rui Barreto) | (Paulo Mota Pinto) |

ASSEMBLY OF THE PORTUGUESE REPUBLIC

EUROPEAN AFFAIRS COMMITTEE

ANNEX 5

Report and Opinion of the Committee on Constitutional Affairs, Rights, Freedoms and Guarantees

ASSEMBLY OF THE PORTUGUESE REPUBLIC

COMMITTEE ON CONSTITUTIONAL AFFAIRS, RIGHTS, FREEDOMS AND GUARANTEES

REPORT

**COM(2011)225 final** - Report from the Commission to the Council and the European Parliament - Evaluation report on the Data Retention Directive (Directive 2006/24/EC)

1 – Introduction

Pursuant to Law No 43/2006 of 25 August 2006 on the monitoring, examination and issuing of opinions by the Assembly of the Portuguese Republic in the context of the process of EU integration, the Committee on Constitutional Affairs, Rights, Freedoms and Guarantees received initiative COM(2011)225 final – Report from the Commission to the Council and the European Parliament - Evaluation report on the Data Retention Directive (Directive 2006/24/EC) given its subject-matter and in order to issue an opinion if applicable.

2 - Grounds

Taking into account that Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data requires Member States to oblige providers of publicly available electronic communications services or public communication networks to retain traffic and location data for between six months and two years for the purpose of investigating, detecting and prosecuting serious crimes, the Commission carried out an assessment of its application by Member States.

Further to a brief mention of the background, objectives and legal basis of the Directive, the report points to the 'complex legal relationship between the Data Retention Directive and the e-Privacy Directive (Directive No 2002/58/EC), combined with the absence of a definition in either of the two directives of the notion of 'serious crime', which makes it difficult to distinguish, on the one hand, measures taken by Member States to transpose the data retention obligations laid down in the Directive and, on the other, the more general practice in Member States of data retention permitted by Article 15(1) of the e-Privacy Directive.

Transposition of the Directive

The report notes the transposition of the Data Retention Directive by 25 Member States: Belgium (only partially), Bulgaria, Czech Republic, Denmark, Estonia, Ireland, Greece, France, Spain, United Kingdom, Italy, Cyprus, Romania, Slovenia, the Netherlands, Lithuania, Luxembourg, Poland, Hungary, Slovakia, Finland, Germany, Latvia, Malta and Portugal, which transposed the Directive with Act No 32/2008 of 17 July 2008.

It also notes the fact that, following the initial notification of transposition by Czech Republic, Germany and Romania, their respective constitutional courts annulled the domestic legislation transposing the Directive, and they are considering how to re-transpose the Directive.

It mentions too the very different solutions found by Member States to comply with the objectives of the Directive.

Role of retained data in the judicial system

The report notes that both the volume of telecommunications traffic and the request for access to traffic data are increasing, despite the very different situations between Member States, with the most frequently requested type of data being related to mobile telephony.

It also shows that around 90% of the data accessed by competent authorities in 2008 was six months old or less and around 70% three months old or less when the (initial) request for access was made.

Furthermore, according to most Member States, the use of retained data older than three and even six months is less frequent but can be crucial.

Its use has tended to fall into three categories:

*1- Firstly, internet-related data tend to be requested later than other forms of evidence in the course of criminal investigations.* The reason for this situation is that analysis of fixed network and mobile telephony data often generates potential leads which sometimes result in further requests for older

data. *'For example, if during an investigation a name has been found on the basis of fixed network or mobile telephony data, investigators may want to identify the Internet Protocol (IP) address this person has been using and may want to identify with whom that person has been in contact over a given period of time using this IP address. In such a scenario, investigators are likely to request data allowing the tracing also of communications with other IP addresses and the identity of the persons who have used those IP addresses'.*

2- Secondly, investigation of serious crime tends to rely on older data, in particular, data relating to the period of preparation and planning of these crimes, in order to identify patterns of criminal behaviour and relations between accomplices to a crime and to establish criminal intent. Activities connected with complex financial crimes are often only detected after several months.

3- Thirdly, and exceptionally, Member States have requested traffic data held in another Member State, which can usually only release these data with judicial authorisation in response to a letter rogatory issued by a judge in the requesting Member State. This type of mutual legal assistance can be a lengthy process, which explains why some of the requested data was in these cases over six months old.

It is also observed that the Member States report data retention to be at least relevant and, in some cases, indispensible for preventing and combating crime, including the protection of victims and the acquittal of the innocent in criminal proceedings. The report also states that 'successful convictions rely on guilty pleas, witness statements or forensic evidence. Retained traffic data, it was reported, have proven necessary in contacting witnesses to an incident who would not otherwise have been identified, and in providing evidence of, or leads in establishing, complicity in a crime. *Certain Member States further claimed that the use of retained data helped to clear persons suspected of crimes without having to resort to other methods of surveillance, such as interception and house searches, which could be considered more intrusive'. (our underlining)*

It is also considered that there is cause for concern at the ways of circumventing the measures deriving from the application of the Directive, such as use of unregistered pre-paid SIM cards or other forms of technologically more advanced or increasingly used communication such as virtual private networks in universities.

Impact of data retention on operators and consumers

The report also tried to assess the impact of the Directive by Member States on economic operators and consumers, taking into account further developments in electronic communications technology and statistics provided to the Commission, with a view to determining whether it is necessary to amend its provisions, in particular with regard to its data coverage and retention periods.

In its assessment, the Commission concluded that 'most operators in their reply to the Commission's questionnaire were unable to quantify the impact of the Directive on competition, retail prices for consumers or investment in new infrastructure and services'.

It also considered that 'there is no evidence of any quantifiable or substantial effect of the Directive on consumer prices for electronic communications services'.

Implications of data retention for fundamental rights

The report also attempted to analyse the implications of the Directive for fundamental rights, taking into consideration several judgments of the European Court of Justice and taking into account the criticism of data retention, as well as various calls for stronger security and data protection rules.

Findings

Overall, the Commission considered that the evaluation has demonstrated that data retention is a valuable tool for criminal justice systems and for law enforcement in the EU.

However, the Commission considers that the contribution of the Directive to the harmonisation of data retention has been limited in terms of, for example, purpose limitation and retention periods, and also in the area of reimbursement of costs incurred by operators, which is outside its scope.

Given the implications and risks for the internal market and for the respect for the right to privacy and the protection of personal data, the Commission considers that the EU should continue through common rules to ensure that high standards for the storage, retrieval and use of traffic and location data are consistently maintained.

The Commission therefore intends to suggest alternatives to the Directive on the basis of the following conclusions and recommendations:

1- the EU should support and regulate data retention as a security measure;

2- transposition has been uneven;

3- the Directive has not fully harmonised the approach to data retention and has not created a level-playing field for operators;

4- operators should be consistently reimbursed for the costs they incur;

5- ensuring proportionality in the end-to-end process of storage, retrieval and use.

3 - Principle of subsidiarity

As the document under examination is a non-legislative initiative there is no need to assess it for compliance with the subsidiarity principle.

4- Rapporteur's opinion

The fight against crime - particularly serious, organised and economic and financial crime - which obviously benefits from scientific and technological advances, must be a priority in Member States' concerns, not only at the legislative level and at the level of the options available in criminal justice policy but also in terms of allocating means to comply with this objective.

The Commission's report dealt with in this opinion, highlights the inappropriateness of some of the mechanisms or means of judicial cooperation, particularly in light of its slowness compared to the speed with which crime is prepared and carried out.

The inability to combat efficiently financial crime prepared or carried out from a computer with internet access by using the IT platforms made available by financial institutions across the world and even under cover of non-cooperating off-shore operations is obvious when, for their part, the judicial authorities depend on rogatory letters to request information, which, when they obtain it, arrives at best several months after the request or sometimes years after the crime was perpetrated.

This fact, however, cannot justify the creation of mechanisms that invade the privacy of citizens, including even data relating to their communications.

The issue of data retention, involving aspects that clearly fall within the scope of citizens' private lives, is an issue whose constitutional nature within the scope of Constitutional Affairs, Rights and Freedoms and Guarantees implies specific concerns in respect of the possibility of its repression or restriction.

Law No 232/2008, which transposes in Portugal the Directive which is the subject of the Commission's above-mentioned assessment report, caused wide concern and criticism for the manner in which it failed to reconcile this need to create efficient mechanisms to fight serious crime and the duty to protect citizens' privacy.

The report notes that such concern and criticism could be seen across the EU as the Directive was being transposed. It even mentions countries where its transposition (even patchier than that carried out in Portugal) could not even become effective because of these concerns (examples of the Czech Republic, Germany and Romania).

On the other hand, the report notes (with concern) the use of mechanisms provided for by the Directive as 'preventive' mechanisms, noting the advantage (?) of thereby avoiding using other means of more intrusive surveillance such as telephoning tapping or house searches.

What therefore appears to be legitimised is, ultimately, the incomprehensible (and unacceptable) advantage of continuous surveillance of the lives of all those people who are not guilty of any crime in comparison with the 'laborious' collecting of evidence which could justify surveillance of the lives of those who are suspected of involvement with crime.

It should also be noted that there is not, in any of the annexes to the report, any detailed reference to Portugal; we are not aware of any reason for this situation.

5- Opinion

In view of the above, the Commission for Constitutional Affairs, Rights, Freedoms and Guarantees in relation to COM(2011)225 final - Report from the Commission to the Council and the European Parliament - Evaluation report on the Data Retention Directive (Directive 2006/24/EC) has decided:

1. As the document under examination is a non-legislative initiative there is no need to assess it for compliance with the subsidiarity principle.

2. to take note of COM(2011)225 final - Report from the Commission to the Council and the European Parliament - Evaluation report on the Data Retention Directive (Directive 2006/24/EC).

3. to pass on this report to the European Affairs Committee.

Palácio de São Bento, 19 December 2012

Rapporteur