Electronic communications: personal data protection rules and availability of traffic data for anti-terrorism purposes

2005/0182(COD) - 15/03/2006 - Final act

PURPOSE : to harmonise Member States' provisions concerning the obligations of providers of publicly available electronic communications services with respect to the retention of certain data.

LEGISLATIVE ACT : Directive 2006/24/EC of the European Parliament and of the Council 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.

CONTENT : the Council adopted this Directive with the Irish and Slovak delegations voted against. The Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The Directive applies to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It does not apply to the content of electronic communications, including information consulted using an electronic communications network.

The following categories of data must retained with regard to fixed network telephony and mobile telephony, as well as Internet access, Internet e-mail and Internet telephony:

- data necessary to trace and identify the source of a communication;

- data necessary to trace and 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 communication device;

- data necessary to identify the location of mobile communication equipment.

The types of data to be retained under these categories of data are specified in the Directive. With regard to an "unsuccessful call attempt", this is defined as a communication where a telephone call has been successfully connected but is unanswered or there has been a network management intervention. This will include the retention of data in relation to unsuccessful call attempts where that data is generated or processed, and stored (as regards telephony data) or logged (as regards Internet data) by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communication services concerned. The Directive shall not require the retention of data in relation to unconnected calls. Data on an unsuccessful call attempt only has to be retained if the company already stores such data.

No data revealing the content of the communication may be retained pursuant to this Directive.

Member States must ensure that the categories of data specified are retained for periods of not less than six months and not more than two years from the date of the communication. A Member State facing particular circumstances that warrant an extension for a limited period of the maximum retention period may take the necessary measures. That Member State shall immediately notify the Commission and inform the other Member States of the measures taken and state the grounds for introducing them. The Commission shall, within a period of six months after the notification, approve or reject the national measures concerned, after having examined whether they are a means of arbitrary discrimination or a disguised restriction of trade between Member States and whether they constitute an obstacle to the functioning of the internal market. In the absence of a decision by the Commission within this period the national measures shall be deemed to have been approved.

The Directive goes on to make provision for data protection and data security. Each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, certain prescribed data security principles with respect to data retained in accordance with the Directive. Each Member State must designate a supervisory authority to be responsible for monitoring the application within its territory of the provisions adopted by the Member States regarding the security of the stored data. Those authorities may be the same authorities as those referred to in Article 28 of Directive 95/46/EC. The supervisory authority must act with complete independence.

No later than 15 September 2010, the Commission must submit an evaluation of the application of the Directive and its impact on economic operators and consumers, taking into account further developments in electronic communications technology and the statistics provided to the Commission with a view to determining whether it is necessary to amend the provisions of this Directive, in particular with regard to the list of data and the periods of retention.

TRANSPOSITION : 15 September 2007. Until 15 March 2009, each Member State may postpone application of the Directive to the retention of communications data relating to Internet Access, Internet telephony and Internet e-mail. Any Member State that intends to make use of this provision must notify the Council and the Commission to that effect by way of a declaration. The following Member States have made such a declaration postponing application for differing lengths of time: the Netherlands, Austria, the United Kingdom, Estonia, Cyprus, Greece, Luxembourg, Slovenia, Sweden, Lithunia, Latvia, Czech Republic, Belgium, Poland, Finland, Germany.

ENTRY INTO FORCE : 03/05/2006.