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

2005/0182(COD) - 14/12/2005 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted a resolution on data retention by 378 votes in favour, 197 against and 30 abstentions. The final text negotiated beforehand with the Council aims to facilitate judicial co-operation in criminal matters by approximating Member States' legislation on the retention of data processed by telecommunications companies.The amendments finally adopted were a compromise between the PES and EPP groups with the Council and differed in some key points to the draft directive adopted initially by the Civil Liberties Committee. (Please see the document dated 24/11/2005.) The GUE, Greens and UEN groups and some members from the ALDE group voted against the directive in the final vote. Alexander Nuno **ALVARO** (ALDE, DE) was unhappy with the result of the compromise adopted and withdrew his name as rapporteur.

The main amendments are as follows:

-Purpose: the aim is 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 Commission had included the objective of “prevention” which was deleted by Parliament. Members felt that the concept of prevention is too vague and could lead to abuse of the system from national authorities. Parliament also deleted the words “serious criminal offences such as terrorism and organised crime” preferring to use the term “serious crimes”.

-Period: The directive will provide for data to be retained by the telecommunications companies for a minimum of 6 months and a maximum of 24 from the date of communication. The Commission had proposed the period of one year

-Unsuccessful calls: An "unsuccessful call attempt" 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. In a recital, Parliament stated that, “considering that the obligations on providers of electronic communications services should be proportionate, the Directive requires that they only retain such data which are generated or processed in the process of supplying their communications services; to the extent that such data is not generated or processed by those providers, there can be no obligation to retain it. This Directive is not intended to harmonise the technology for retaining data, the choice of which will be a matter to be resolved at national level.”

Reimbursement of costs: Parliament decided to delete the paragraph in which it was mandatory for Member States to reimburse telecom companies for all additional costs of retention, storage and transmission of data. In the draft directive adopted by the Civil Liberties Committee, Members had initially called for the full reimbursement of costs.

-Content: A new clause is inserted stating that no data revealing the content of the communication can be retained pursuant to this Directive.

-Type of data: Parliament tightened up the provisions on types of data to be retained, in Article 4. This includes the registration of location data on calls, SMS and internet use.

-Supervisory authority: There is a new clause on supervisory authority. Each Member State must designate one or more public authorities 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. These authorities must act with complete independence in exercising their functions.

-Data protection and data security: A new clause states that 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.

-Push system: Member States must ensure that data retained in accordance with the Directive are only provided to the competent national authorities, in specific cases and in accordance with national legislation.

-Sanctions: Unauthorised access or transfer of data will be punished by “effective, proportionate or dissuasive” penalties, either administrative or criminal.

-Future measures: A new clause has been introduced permitting derogation from the time period. A Member State facing particular circumstances warranting an extension for a limited period of the maximum retention period may take the necessary measures. The Member State shall immediately notify the Commission and inform the other Member States of the measures and indicate the grounds for introducing them. The Commission shall, within six months after the notification, approve or reject the national measures involved after having verified whether or not they are a means of arbitrary discrimination or disguised restriction of trade between Member States and whether or not they shall 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.