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

2005/0182(COD) - 24/11/2005

The committee adopted the report by Alexander Nuno ALVARO (ALDE , DE) amending the proposal under the 1st reading of the codecision procedure:

- Article 1 (purpose of the directive) was amended so that data could be retained for the investigation, detection and prosecution, but not the "prevention", of serious criminal offences, on the grounds that the concept of prevention was too vague and could lead to abuse of the system. Moreover, whereas the proposal had simply given examples of serious offences ("such as terrorism and organised crime"), the committee preferred to refer to the definition given in Article 2(2) of the European Arrest Warrant;

- new provisions in Article 1 specified that one of the aims of the directive should be to ensure "respect for private life" and the protection of personal data when data is retained. The scope of the directive should be limited to traffic and location data and the data necessary to identify the subscriber or registered user. It should not apply to "related" data;

- data retained under the directive should only be provided to the competent national authorities responsible for the investigation, detection and prosecution of serious criminal offences "following the approval of the judicial authorities and of other competent authorities according to national legislation";

- two new articles introduced provisions governing access to retained data and data protection and data security. These sought to ensure inter alia that access to retained data would be granted only for specific purposes, on a case-by-case basis, and would be restricted to the "relevant and proportionate" data necessary for a specific investigation. It should not include "large-scale data mining in respect of travel and communications patterns" of people unsuspected by the competent national authorities. Data should be erased when no longer necessary and also when inaccurate. Any accessing of data should be recorded. Lastly, the data should only be forwarded to third countries (such as the USA) by means of an International Agreement under Article 300 of the Treaty, to which Parliament had given its assent;

- another new article provided for Member States to lay down "effective, proportionate and dissuasive" sanctions for infringements of the national provisions adopted to implement the directive;

- MEPs wanted all data (i.e. from telephony and internet) to be retained for a period of 6-12 months and then erased, whereas the proposal had simply provided for telephony data to be retained for one year and internet data for 6 months;

- the committee restructured the proposal so as to place the Annex (listing the types of data to be retained) into the main body of the text (in Article 4);

- while supporting the registration of location data on successful calls, SMS and internet use, MEPs preferred to leave it up to the Member States to decide whether to request telecom companies to retain data on unsuccessful calls. They introduced a new definition - "unsuccessful call attempt" - into the directive;

- telecom companies should be fully reimbursed by the Member States for all extra costs incurred in order to comply with obligations imposed on them as a result of the directive, including investment and operational costs as well as the extra costs resulting from further modifications of the directive, whereas the proposal had only provided for the reimbursement of "demonstrated additional costs";

- finally, the directive should be reviewed after 2 years, and every 3 years thereafter, with attention being focused in particular on the types of data retained and the retention periods.