English translation of Belgian proposal for Third Pillar legislation

Draft framework decision on the retention of traffic data and on access to this data in connection with criminal investigations and prosecutions

THE EUROPEAN COUNCIL

In view of the European Union Treaty, and in particular article 29, article 34, paragraph 2, point b);

In the light of the proposal by .....

In the light of the opinion of the European Parliament,

Considering the following:

1. Offering a high level of protection in an area of liberty, security and justice requires that criminal investigations and prosecutions be carried out in an adequate manner.

2. The use of telecommunications services has grown to the extent that the data relating to this use, and principally those relating to traffic are very useful tools for investigating and prosecuting criminal offences.

3. The conclusions of the Council of 20 September 2001 call for care to be taken to ensure that the forces of law and order are able to investigate criminal acts which involve the use of electronic communications systems and to take measures against the perpetrators of these, while maintaining a balance between the protection of personal data and the need of the law and order authorities to have access to data for criminal investigation purposes.

4. Access to traffic data is particularly relevant in the case of criminal investigations into cybercrime, including the production and diffusion of paedophile or racist material. The plan of action of the Council and the Commission on the best ways to implement the provisions of the Treaty of Amsterdam on the establishment of an area of liberty, security and justice, the conclusions of the European Council at Tampere on 15-16 October 1999, the European Council at Santa Maria del Feira on 19-20 June 2000, the European Commission in its scoreboard and the European Parliament in its resolution of 19 May 2000 call for an intervention in the area of cybercrime.

5. It is necessary to allow the authorities responsible for criminal investigations and prosecutions to have access to traffic data; the legislation of Member States permits in certain cases access to such data in the context of criminal investigations in progress.

6. 6. The retention of traffic data in the absence of a criminal investigation in progress (a priori retention), whether by the telecommunications service providers or by a third party, is technically possible. Many Member States have passed legislation making such a priori retention compulsory for the purpose of criminal investigations or prosecutions. Work in this area is under way in other Member States. The content of this legislation varies considerably.

7. These differences present problems for the provision of telecommunications services beyond the territory of a single Member State and are prejudicial to cooperation in criminal matters. A harmonisation of legislation is therefore desired both by the authorities responsible for criminal investigations and prosecutions and by the providers of telecommunications services.

8. The purpose of this present framework decision is to make compulsory and to harmonise the a priori retention of traffic data in order to enable subsequent access to it, if required, by the competent authorities in the context of a criminal investigation.

9. Such a priori retention of data and access to this data constitutes an interference in the private life of the individual; however, such an interference does not violate the international rules applicable with regard to the right to privacy and the handling of personal data contained, in particular, in the European Convention on the Protection of Human Rights of 4 November 1950, the Convention of the Council of Europe no.108 on the protection of persons in respect of the automated handling of personal data of 28 January 1981, and the Directives 95/46/ce and 97/66/CE, where it is provided for by law and where it is necessary, in a democratic society, for the prosecution of criminal offences.

10. It is necessary to establish certain procedures for the retention of and access to data in order to guarantee their effectiveness and their harmonious application in Member States. These procedures concern the minimum period for the a priori retention of traffic data, the minimum list of types of data that may be retained, and the minimum list of offences for the prosecution of which access to retained data shall be possible.

11. In drawing up other procedures relating to the retention of and access to data, it is important to strike a balance between, on the one hand, the need to allow Member States ample room to make their own individual assessments given the differences that exist between criminal justice systems, and on the other the positive effect of a harmonisation of procedural guarantees for the creation of an area of liberty, security and justice.

12. A period of a minimum of 12 months and a maximum of 24 months for the a priori retention of traffic data is not disproportionate in view of the needs of criminal prosecutions as against the intrusion into privacy that such a retention would entail. [...]

13. The content of the minimum list of types of data to be retained will have an impact on certain sectors, particularly the telecommunications service providers. It is preferable, therefore, that the drawing up of this list of types of data to be retained should be made by

further decisions of the Council after the Commission has engaged in the necessary consultations.

14. The drawing up of the minimum list of types of data to be retained must also take into account the invasion of privacy which such a retention entails. Member States must keep this balance in mind should they ever draw up a more extensive list. It should be emphasised that the invasion of privacy would be disproportionate if the data retained related to the content of messages exchanged or of the information sources consulted under whatever form, within the framework of communications.

15. The framework decision would fail in its aim to harmonise procedures for and improve the effectiveness of criminal investigations and prosecutions if access to the retained data were not possible for the prosecution of offences inevitably linked to the use of telecommunications systems or regarded as serious offences in all Member States.

16. The framework decision shall not apply to access to data at the time of transmission, that is by the monitoring, interception or recording of telecommunications.

HAS ADOPTED THE PRESENT DECISION:

Article 1 - Definitions

The following definitions shall apply in this present framework decision:

a) "traffic data": all data processed which relate to the routing of a communication by an electronic communications network;[1]

b) "communication": all information exchanged or routed between a finite number of parties via an electronic communications network accessible to the public. [This does not include information routed in the context of a radio service to the public via an electronic communications network except insofar as a link can be established between the information and the subscriber or identifiable user who receives it;[2]

c) "Telecommunications service": services which consist in total or in part of the transmission and routing of signals on telecommunications networks, with the exception of radio and television.[3]

---

1 See article 2, point 2b) of the draft directive of the European Parliament and Council on the handling of personal data and the protection of privacy in the electronic communications sector. (version 15396/2/01 REV 2 ECO 395 CODEC 1375). Initial draft: COM(2000) 385 final - JO C 365 E of 19.12.2000. Article 1 point d) of Convention COE 185 on cybercrime is more specific.

2 See article 2, point d) of the draft directive (above)

3 Article 2, point d) of Directive 97/66/CE. Convention COE 185 on cybercrime offers a definition of "service provider".

Article 2 - Access to traffic data

Member States shall take adequate measures to allow the authorities responsible for criminal investigations and prosecutions to have access to the traffic data needed to accomplish their task.

Article 3 - Retention of traffic data and access to data retained

1. The measures envisaged in article 1 include in particular the obligation to retain for the purpose of criminal investigations and prosecutions, either on the part of the telecommunications service provider who holds the data in question, or on the part of a trusted third party, for a period of 12 months minimum and 24 months maximum, the following categories of traffic data:

   a) Data necessary to follow and identify the source of a communication;
   b) Data necessary to identify the destination of a communication;
   c) Data necessary to identify the time of a communication;
   d) Data necessary to identify the subscriber;
   e) Data necessary to identify the communication device.

2. Each Member State shall take the necessary measure in order to determine with the appropriate precision the exact types of data which must be retained in application of paragraph 1. These types of date shall be limited to what is necessary in a democratic society for criminal investigation and prosecution. These types of data shall not concern the content of the exchanged correspondence or the consulted information, in any form, in the framework of telecommunications.

3. In implementing paragraph 2, Member States inform each other on the avancement of their work and collaborate with the Commission.

4. The measures envisaged in article 1 shall also include access by the authorities responsible for criminal investigations and prosecutions to data, the retention of which occurred in application of this article. Each Member State determines the offences for the prosecution of which access to traffic data will be possible. In doing so, he makes sure that these offences are sufficiently serious taking into account the limitation of the right to privacy which constitutes this access. He also makes sure that the following offences as defined in national law are at least included :

   - offences under the Convention of the Council of Europe no.185 on cybercrime of 23 November 2001;
   - participation in a criminal organisation ,
   - terrorism,
   - trafficking in human beings,
   - sexual exploitation of children and child pornography,

- illicit trafficking in narcotic drugs and psychotropic substances,
- illicit trafficking in weapons, munitions and explosives,
- corruption,
- fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests,
- laundering of the proceeds of crime,
- counterfeiting of the euro,
- computer-related crime,
- environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,
- facilitation of unauthorised entry and residence,
- murder, grievous bodily injury,
- illicit trade in human organs and tissue,
- kidnapping, illegal restraint and hostage-taking,
- racism and xenophobia,
- organised or armed robbery,
- illicit trafficking in cultural goods, including antiques and works of art,
- swindling,
- racketeering and extortion,
- counterfeiting and product piracy,
- forgery of administrative documents and trafficking therein,
- forgery of means of payment,
- illicit trafficking in hormonal substances and other growth promoters,
- illicit trafficking in nuclear or radioactive materials,
- motor vehicle crime,
- rape,
- arson,
- crimes within the jurisdiction of the International Criminal Tribunal,
- unlawful seizure of aircraft/ships,
- sabotage.

Article 4 – Procedural rules and data protection

1. In implementing article 3, Member States take the necessary measure to make sure that :

   - Access to retained traffic data is given only to judicial authorities or, in the extent that they have autonomous power in criminal investigation prosecution, to police authorities;

   - Access to retained traffic data is not authorised when other measures are possible which are less intrusive in terms of privacy and leading to similar results regarding criminal investigation and prosecution;

   - The process to be followed in order to get access to retained traffic data is defined with

precision;

- Confidentiality and integrity of retained traffic data are ensured;
- Data to which access has not been asked at the end of the period of mandatory retention are destroyed ;
- Providers of telecommunication services respect the obligation of data retention.

2. Rules mentioned in paragraph 1 are without prejudice to the rules applicable in national law to access to data during their transmission, including tracking, interception and recording of telecommunications.

Article 5 – Obligation to execute a decision of access to retained traffic data

Member States shall undertake to execute, in conformity with this framework decision and on the basis of the principle of mutual recognition, any decision of access to retained traffic data taken by a competent authority of a Member State on the ground of provisions adopted in this Member State in order to implement articles 3 and 4 and transmitted in accordance with article 6 to 8.

Article 6 – Determination of the competent authorities

1. The issuing authority shall be the authority of the issuing State which is competent to issue a decision of access to retained traffic data by virtue of the law of the issuing State.

2. The executing authority shall be judicial authority of the executing State which is competent by virtue of the law of the executing State.

3. Each Member State shall inform the General Secretariat of the Council of the competent authorities under its law.

Article 7 – Transmission of the decision of access to retained traffic data

1. A decision of access to retained traffic data may be transmitted by the issuing authority to the executing authority of a Member State in which the provider of telecommunications services which must have retained the concerned traffic data is located.

2. The decision is accompanied with the following information, in the form of certificate mentioned in paragraph 3:

   a) the issuing authority;

b) information allowing to identify the provider of telecommunication services which must have retained the traffic data;

c) the criminal conduct under investigation;

d) indications allowing to select the searched data among all retained data.

3 The Council determines the form of the certificate which will contain information provided for in paragraph 2, taking into account the evolution of the work of the Member States related to the implementation of article 3 paragraph 2.

4. The executing authority may request any further information necessary to enable it to decide whether access to retained data would be authorised in a similar national case.

5. The United Kingdom and Ireland, respectively, may, before the date referred to in Article 9, state in a declaration that the decision of access to retained trafic data together with the certificate must be sent via a central authority or authorities specified by it in the declaration. Any such declaration may be modified by a further declaration or withdrawn any time. Any declaration or withdrawal shall be deposited with the General Secretariat of the Council and notified to the Commission. These Member States may at any time by a further declaration limit the scope of such a declaration for the purpose of giving greater effect to paragraph 1. They shall do so when the provisions on mutual assistance of the Schengen Implementation Convention are put into effect for them.

6. If the competent authority in the executing State is not known to the competent authority in the issuing State, the latter shall make all necessary inquiries, including via the contact points of the European judicial network in order to obtain the information from the executing State.

7. If the issuing authority so wishes, transmission may be via the secure telecommunications system of the European Judicial Network.

8. The issuing authority may forward the decision of access to retained traffic data by any secure means capable of producing written records under conditions allowing the executing Member State to establish its authenticity.

9. All difficulties concerning the transmission or the authenticity of any document needed for the execution of the decision of access to retained traffic data shall be dealt with by direct contacts between the judicial authorities involved, or, where appropriate, with the involvement of the central authorities of the Member States.

10. If the authority which receives a decision of access to retained traffic data is not competent to act upon it, it shall automatically forward it to the competent authority in its Member State and shall inform the issuing authority accordingly.

Article 8 – Conditions of execution

The issuing authority may make the execution subject to conditions which would be applicable in a similar national case.

Article 9 – Implementation

1. Member States shall take the necessary measures to comply with this Framework Decision by 31 December 2003.

2. They shall communicate to the Council and to the Commission the text of any provisions they adopt to comply with this Framework Decision.

3. The General Secretariat of the Council shall communicate to the Member States and to the Commission the information received pursuant to Article 6 (3) and Article 7 (6). It shall also have the information published in the Official Journal of the European Communities.

Article 10 – Entry into force

This Framework Decision shall enter into force on the twentieth day following its publication in the Official Journal of the European Communities.

Done at Brussels,

For the Council
The President