EUROPEAN PARLIAMENT

2004 *2009*

Committee on Civil Liberties, Justice and Home Affairs

21.1.2005

WORKING DOCUMENT

on the draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Alexander Nuno Alvaro

I. Background

At the Justice and Home Affairs Council meeting on 29/30 April 2004 France, the United Kingdom, Ireland and Sweden submitted a joint proposal[1] for a framework decision on the retention of communications data. This initiative follows up to a declaration on combating terrorism[2], adopted by the European Council on 25 March 2004, in which the Council was instructed to examine measures for establishing rules on the retention of communications traffic data by service providers.

The objective of the proposal is to facilitate judicial cooperation in criminal matters by approximating Member State legislation on the retention of data processed and stored by providers of publicly available electronic communications services for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences, including terrorism.

Traffic and location data generated by the following communications methods, including subscriber and user data, would be covered[3]:

- telephony, excluding short message services, electronic media services and multimedia messaging services;

- short message services, electronic media services and multimedia messaging services provided as part of any telephony service;

- Internet protocols, including e-mail, voice-over-Internet protocols, worldwide web, file transfer protocols, network transfer protocols, hyper text transfer protocols, voice-over-broadband and subsets of Internet protocol numbers - network address translation data.

Communication content would not be covered.

The proposal makes provision for a minimum and maximum retention period of 12 and 36 months respectively. With regard to the second and third categories of the above communications methods, Member States would be able to derogate from the retention period provided for.

A Member State would be able to have access, in connection with requests for legal assistance, to retained data available in other Member States.

The proposal contains no reimbursement rules to cover costs arising.

[1] Council doc. 8958/04 of 28 April 2004.
[2] Council doc. 7764/04 of 28 March 2004.
[3] cf. Article 2(3) in Council doc. 8958/04.

II. Assessment of the proposal

1. Legal basis

It is debatable whether the legal basis indicated would actually allow adoption of the framework decision. The Council cites Articles 31(1)(c) and 34(2)(b) of the Treaty on European Union.

The rapporteur does not share this legal interpretation; he is of the opinion, rather, that the proposal is made up of measures which should be classified as coming under the Union's first pillar (e.g. as regards time periods and data to be retained) or under the third pillar (e.g. as regards enhanced judicial cooperation).

To clarify this fundamental issue, the Committee on Civil Liberties, Justice and Home Affairs has asked the Committee on Legal Affairs for its opinion pursuant to Rule 35(2) of Parliament's Rules of Procedure.

If necessary, it should be suggested to the Council that the framework decision be split, to reflect the pillars concerned, so that there can be discussion of two documents whose legal basis would be beyond doubt.

2. Proportionality of the measures

The measures provided for must be proportionate; that will be the case only if the arrangements are suitable and necessary and are not unreasonably harsh for the parties concerned.

(a) Suitability, i.e. the measures should at least be conducive to realising the desired objective
Given the data volume to be retained, in particular Internet data, it is debatable whether appropriate analysis of the data would be at all possible.

(aa) Scope for circumventing the measures
Individuals in organised crime and terrorism milieus will know how to easily prevent their data from being traceable, possible ways being to have 'front men' acquire telephone cards or to switch between mobile telephones from foreign providers, to use public call boxes, to change the IP or e-mail address when using an e-mail service, or right from the outset to use non-European Internet service providers not subject to data retention obligations.

(bb) Data availability
If all traffic data covered by the decision, including Internet data, actually had to be stored, the accumulated data volume within the network of a large Internet service provider, even at current traffic levels, would amount to 20 000 to 40 000 terabytes. That is equivalent to roughly four million kilometres worth of full lever-arch files; that is equivalent, in turn, to 10 gigantic stacks of files, each of which would stretch from the Earth to the Moon!

Given that monumental volume of data, a single search operation using current technology, without additional investment, would take 50 to 100 years. It is therefore a moot point whether the data requested would be available.

(b) Necessity, i.e. equally suitable but less stringent measures are possible to achieve the same objective

By comparison with the present proposal for 'blanket' data retention, storage for a specified purpose could be both equally suitable and less stringent; this is also the model laid down by the Council of Europe Convention on Cybercrime[1].

With regard to the Council's reasons for rejecting that alternative[2], the inevitable question is to what extent the project data retention arrangements are compatible with the principle of presumption of innocence.

(c) No unreasonably harsh measures for the parties concerned

The proposal does not address the possible strains on the parties concerned. The danger is, in addition to the serious infringement of the protection of individuals' personal data, that enormous burdens would be placed on the European telecomms industry and on small and medium-sized telecomms firms.

Costs would arise principally because of:

- technical changes to systems for data generation and storage,
- changes to firms' in-house processes for secure data archiving, and
- action to process and analyse security authorities' inquiries.

According to estimates by a wide variety of fairly large firms in Member States, the investment this would require within traditional circuit-switched telephony would total some € 180 m a year, per firm, with annual operating costs of up to € 50 m. Small and medium-sized firms' ability to trade would be bound to be in jeopardy.

According to estimates, the Internet-related burden would be many times greater than the investment within traditional circuit-switched telephony.

The Article 36 Committee therefore proposes that only data which are generated as things stand at present should continue to be covered[3].

The Council's proposal lacks arrangements, harmonised on a pan-European basis, for spreading the cost burden it would create, resulting, in turn, in distortions of competition that would jeopardise competition structures that are viable in the long term and thus preventing completion of a single European internal market.

[1] CETS No 185, 8 November 2001.

[2] Council doc. 8958/04 ADD 1.
The explanatory note on the framework decision on data retention simply states that storage for a specified purpose 'will never aid in the investigation of a person who is not already suspected of involvement with a criminal or terrorist organisation'. It 'is therefore not sufficient to meet the needs of the security, intelligence and law enforcement agencies in the fight against modern criminals including terrorists'.

[3] Council doc. 15098/04 of 23 November 2004.

III. Compatibility of the framework decision with Article 8 of the European Convention on Human Rights (ECHR) and Article 15 of Directive 2002/58/EC

The draft does not discuss Article 8 of the ECHR (right to respect for private life and correspondence).

Data monitoring and storage/retention arrangements must be rejected unless they fulfil three fundamental criteria in accordance with Article 8(2) of the European Convention and the European Court of Human Rights' interpretation of that provision: a legal basis, the need for the measure in a democratic society and conformity with one of the legitimate aims listed in the Convention[1]. As has been verified, it would appear debatable, at the very least, that the present Council draft fulfils all necessary criteria[2].

Nor does Article 15 of Directive 2002/58/EC stipulate that, of the possible measures set out, consideration can be given to mandatory data retention across Europe. What Directive 2002/58/EC does stipulate is that 'Member States may ... adopt legislative measures' regulating the retention of data for a limited period[3].

Clear answers are needed to other unresolved questions such as the burden of proof where state authorities incorrectly analyse data, the obligation to notify citizens concerned in the event of unwarranted data inquiries, or the right of citizens to information on retained data relating to them.

It must in addition be regarded as constitutionally debatable, at the very least, whether, specifically as regards Article 2(4) of the framework decision, the principle of normative clarity has been taken into account.

IV. Summary

With regard to the framework decision set out in Council document 8958/04, the rapporteur has doubts as to:

- the choice of legal basis,
- proportionality,
- compliance with the principle of presumption of innocence,
- compatibility with Directives 2002/58/EC and 95/46/EC plus the ECHR,
- the normative clarity of Article 2(4), and
- whether the financial implications have been taken into consideration.

In connection with the framework decision set out in Council document 8958/04, the rapporteur proposes that:

[1] Article 29 Data Protection Working Party, Council doc. 11885/04 of 9 November 2004.
[2] The European Court of Human Rights has stressed that the contracting states do not have unlimited discretion to subject individuals within their territory to clandestine surveillance. Given that corresponding powers, conferred on the ground that the intention is to defend democracy, threaten to undermine or destroy democracy, the Court stresses that contracting states are not allowed to adopt any measure they deem appropriate in order to combat espionage or terrorism.
[3] Cf. Article 15(1) of Directive 2002/58/EC.

- the framework decision be split into two documents, to reflect the measures it contains, which can then be classified as coming under the relevant Union pillar,
- the shortcomings in connection with data storage for a specified purpose be eliminated, instead of introducing data retention, and cross-border cooperation be improved,
- the data storage/retention period be limited, throughout Europe, to six months,
- the extent of data to be stored/retained should not go beyond what is commercially necessary.
- reimbursement rules, harmonised on a pan-European basis, be devised,
- a data protection directive be developed for the Union's third pillar.

The rapporteur asks that, as part of further work on the framework decision, he be given an opportunity:

- to invite both the Committee on Industry, Research and Energy and the Committee on the Internal Market and Consumer Protection to deliver an opinion on the framework decision set out in Council document 8958/04,
- to invite the Commissioner responsible, a representative of the Council and law enforcement agency representatives to a meeting of the Committee on Civil Liberties, Justice and Home Affairs.