ARTICLE 29 Data Protection Working Party

1868/05/EN
WP 113

Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005)

Adopted on 21st October 2005

EXECUTIVE SUMMARY

The European Commission's Proposal for a Directive on the retention of data is confronting us with a historical decision.

Traffic data retention interferes with the inviolable, fundamental right to confidential communications.

Any restriction on this fundamental right must be based on a pressing need, should only be allowed in exceptional cases and be the subject of adequate safeguards.

Providers of publicly available communication services would be forced unprecedentedly to store billions of data relating to the communications of any and all citizens for investigational purposes.

Terrorism presents our society with a real and pressing challenge. Governments must respond to this challenge in a way that effectively meets their citizens need to live in peace and security while not undermining their individual human rights – including the right to data privacy- which are a cornerstone of our democratic society.

The European Commission's initiative might ultimately result in setting out maximum retention periods that are shorter than those envisaged in other recent proposals.

The Working Party questions whether the justification for an obligatory and general data retention coming from the competent authorities in Member States is grounded on crystal-clear evidence. The Working Party also doubts whether the proposed data retention periods in the draft Directive are convincing.

As just mentioned above, the justification for any compulsory and general data retention must be clearly demonstrated and backed up with evidence. This also applies to the maximum periods that should apply in such a case. In any case, the conditions under which the competent authorities could access and use such data in order to combat the threat of terrorism should also be clearly spelled out.

The purposes of data retention should be stated clearly in the Directive by having regard to the fight against terrorism and organised crime rather than against any undetermined "serious crime".

Account should be taken that there are less privacy-intrusive approaches (e.g. the quick-freeze procedure).

The retention period of the data, if any, should be as short as possible and represent the maximum retention threshold applying to all Member States, even though they will be free to lay down shorter retention periods. The measures possibly introduced should be broadly publicized.

The evidence supporting these measures should be evaluated periodically. Based on a periodical assessment, to be performed at least every two or three years and made public, the envisaged data retention measures should be time-limited pursuant to the "sunset legislation" concept. A three-year term is considered suitable.

In any case, imposing the said data retention obligations on communication service providers without having first realised adequate, specific safeguards is not to be accepted within the existing European legal framework.

Finally, the Working Party set out twenty specific safeguards to be envisaged with particular regard to the requirements applying to recipients and further processing, the need for authorisations and controls, the measures applying to service providers also in terms of security and logical separation of the data, the determination of the data categories involved and their updating, and the need to rule out contents data.

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS
WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 (1)(a) and (3) of that Directive and 15(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002,

having regard to its Rules of Procedure, and in particular Articles 12 and 14 thereof,

has adopted the following Opinion:

I. Background

Within the framework of the European initiatives to fight terrorism and organised crime, on the last 21st of September the European Commission presented a "*Proposal for a Directive on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC* [1]".

The issue in question is of considerable importance to all citizens.

Freedom and confidentiality of correspondence and all other forms of communication are among the pillars of modern democratic societies. Their inviolability has been set forth in several instruments, including constitutional charters, as well as being specifically safeguarded in the European Convention on Human Rights which Community law has set as its own foundations.

The proposed Directive is confronting us with a historical decision. It is aimed at introducing, for the first time, the Europe-wide obligation to retain, for investigational purposes, billions of data relating to the communications of any and all citizens. Under Community law, such data are currently not stored or else are retained only on a temporary basis by electronic communications service providers - and if so, exclusively for contractual purposes.

Traffic data retention interferes with the fundamental right to confidential communications guaranteed to the individuals by Article 8 of the European Convention on Human Rights. In a democratic society, any interference with this fundamental right can be justified if it is necessary in the interests of national security. It can ultimately result in keeping track of and charting all contacts and relationships held by individuals as well as the places in which this happens and the means used for such purposes The European Court of Human Rights has also stressed that secret surveillance poses a danger of undermining or even destroying democracy on the ground of defending it; additionally, the Court has affirmed that States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate. [2]

[1] [COM (2005) 438 final], 21.9.2005, *not yet published in O.J.*

This is why any restrictions of this fundamental right must be based on a pressing need, should only be allowed in exceptional cases and be the subject of adequate safeguards. The retention of traffic data -including location data- for purposes of law enforcement should meet strict conditions, [3] in particular it must take place only for a limited period and when necessary, appropriate and proportionate in a democratic society.

The powers available to law enforcement agencies in the fight against terrorism must be effective, but they cannot be unlimited or misused. A proportionate balance must be struck to ensure that we do not undermine the kind of society we are seeking to protect. This balance is especially necessary when forcing communication service providers to store data that they themselves have no need for. In this manner, one could eventually achieve the unprecedented, continued, pervasive monitoring of all kinds of communication and movement of the totality of citizens in their daily life. A huge amount of information would be stored that is actually useful for investigational purposes in a limited number of cases.

Consideration should also be given to the circumstance that such a sweeping data retention obligation impacts on some communications that raise delicate issues in connection with certain categories of professional and/or investigational secrecy, or certain activities by particular institutions, that are protected specifically by the law.

For this reason, for some years now the view of both the Article 29 Working Party and the Conference of European Data Protection Authorities has been firm and clear. Upon several occasions since 1997, the Working Party [4] and the European Conference [5] have questioned the necessity of general data retention measures.

---

[2] Klass and others v. Germany, para. 49.

[3] See, in particular, article 15(1) of Directive 2002/58/EC.

[4] See (*all documents are available at http://europa.eu.int/comm/internal_market/privacy*):

-**Opinion 9/2004** on a draft Framework Decision [..] (Document of the Council 8958/04 of 28 April 2004). A summary of the following statements can be found in the annex to this opinion;
-**Opinion 1/2003** on the storage of traffic data for billing purposes;
-**Opinion 5/2002** on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data;
-**Opinion 10/2001** on the need for a balance approach in the fight against terrorism;
-**Opinion 4/2001** on the Council of Europe's Draft Convention on Cyber-crime;
-**Opinion 7/2000** on the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 COM (2000) 385;
-**Recommendation 3/99** on the preservation of traffic data by Internet Service Providers for law enforcement purposes;
-**Recommendation 2/99** on the respect of privacy in the context of interception of telecommunications;
-**Recommendation 3/97** on Anonymity on the Internet.

[5] See the statements adopted in Stockholm (April 2000) and Cardiff (April 2002).

II. PRELIMINARY ASSESSMENT AND GENERAL PRECONDITIONS

1. Retained data may provide a useful tool for investigators, but the above mentioned conditions should be clearly demonstrated and substantiated.

Firstly, the aim of such a measure should be stated very clearly. Secondly, the justification for compulsory and general data retention must be clearly demonstrated and backed up with evidence. This also applies tot the maximum periods that should apply in such a case. Thirdly, the conditions under which the competent authorities could access and use such data in order to combat the threat of terrorism should be clearly spelled out.

That evidence should at least be evaluated periodically and the results published, taking also into account that introducing means of general surveillance of citizens might cause strategies on the side of terrorism and organized crime not to use certain means. This would result in the necessity to develop new methods of even stricter surveillance thus setting into motion a spiral of possible infringements of the fundamental rights of citizens which will be hard to stop. Furthermore, this would change the character of the society we are striving to preserve.

The Working Party acknowledges that some conditions have changed in our societies as for the risks posed by terrorist threats, and has been informed that some data may at times be helpful and justifiably used in certain investigations. Additionally, the Working Party notes that the European Commission's initiative might ultimately result into setting out maximum retention periods that are shorter than those envisaged in the past, on which the Working Party expressed itself unfavourably – lastly via Opinion no. 9/2004 adopted on 9 November 2004, WP 99.

However, the circumstances justifying data retention, even though they are said to be based on the requests coming from the competent authorities in Member States, do not appear to be grounded on crystal-clear evidence. Accordingly, the proposed terms do not appear convincing as yet.

There exist other useful measures to be taken into account for investigational purposes, which infringe to a lesser extent upon the basic right positions of the citizens, e.g. the "quick freeze-procedure" where neither the communication providers nor the Internet service providers are obliged to store traffic data. For instance, in well-founded cases, the law enforcement agencies consult the companies and request the storage of certain data. After those data have been stored, the agencies are given some weeks to collect evidence in order to obtain a judicial order. Then, based on this order, they can access the data.

In any event, a general retention period must be clearly regulated. Such retention period should be as short as possible and should be as close as possible to the retention period for the original purposes for which communication service providers recorded those data.

2. The harmonisation of Member States' legislation currently proposed by the Commission should clarify that the provision for a binding data retention period at European level is based on a proportionality assessment carried out at European level by taking also account of the transnational character of organised crime as well as of the maximum security requirements of all Member States.

Then, it will have to be clarified that the data retention period referred to in the Directive is to be regarded as the maximum harmonised threshold applying to all Member States.

Therefore, it should be made clear that Member States will not have to provide for longer data retention periods than the Directive – even though they will be free to lay down shorter retention periods. It should also be recalled that the data are to be erased at the end of the said periods. Given this context, the current wording of Article 11 in the draft Directive is not satisfactory.

The Article 29 Working Party welcomes that the proposal contains an article on an evaluation (Article 12), to be carried out periodically at least every two years.

This evaluation should include the necessity of the traffic data used by law enforcement authorities in specific and well identified cases, and should involve the data protection authorities. The result of these evaluations should be published.

However, it should be pointed out that the said evaluation should not be performed with regard to an undetermined amount of time, given that the proposal is based on the concrete assessment of the assumptions and prerequisites it refers to. Therefore, the envisaged data retention measures should be time-limited pursuant to the "sunset legislation" concept. A three-year term is considered suitable by the Working Party. Upon expiry of this term, the national implementing measures mandating data retention should cease to be effective - without prejudice to the possibility of starting the analysis required to prepare a new decision by the Council and the European Parliament endorsing a new Directive also prior to the expiry of the three-year term.

With regard to the principle of proportionality, the Article 29 Working Party also welcomes the limitation of the set of data to be retained with regard to the use of Internet. Moreover, a maximum set of data to be retained has to be preferred over a minimum list. Generally, the data to be retained should be restricted to those collected by the providers for technical and billing purposes.

It is essential to determine the access to data and purposes of use, to ensure that any general data retention measures are accompanied by the strongest safeguards, and to submit such measures to audit.

3. The safeguards available within the existing legal framework on data protection in the first pillar (Directives 95/46/EC and 2002/58/EC) should be further specified for the particular law enforcement context of traffic data retention. Specified safeguards are vital to ensure that the protection offered by Directive 2002/58/EC, in particular to the right of the confidentiality of the use of publicly available electronic communication services, is not substantially undermined.

Additionally, the Working Party is of the opinion that adequate safeguards should be in place regarding data processing operations in sectors that at present fall outside the scope of these directives.

This is why the Working Party holds the view, inter alia, that the draft Directive should itself provide for these safeguards, or otherwise be evaluated and adopted jointly with other adequate legal instruments. In particular, the Working Party considers that the "Framework Decision on

the protection of personal data processed in the framework of police and judicial cooperation in criminal matters" shall be carefully assessed also within this context.

Finally, given the impact on fundamental rights and freedoms of the citizens concerned, the Working Party believes that the measures possibly introduced should be broadly publicized.

III. OTHER SPECIFIC SAFEGUARDS

In addition, the Working Party considers that the following issues should at least be addressed:

1. PURPOSES

The data should only be retained for specific purposes of fighting terrorism and organised crime, rather than with regard to any other undetermined "serious crime". This limited purpose should be also referred to in the title of the proposed Directive.

2. RECIPIENTS

The Directive should provide that the data be only available to specifically designated law enforcement authorities where necessary for the investigation, detection, prosecution and/or prevention of terrorism. A list of such designated law enforcement authorities should be publicly available.

3. DATA MINING

Prevention of terrorism should not include large-scale data-mining based on the information referred to in the Directive in respect of the travel and communication patterns of people unsuspected by the law enforcement authorities. Access must be restricted to those data that are necessary in the context of specific investigation.

4. FURTHER PROCESSING

Any further processing of retained data by law enforcement authorities for other related proceedings should be ruled out or limited stringently on the basis of specific safeguards, and any access to the data by other government bodies should be prevented. The rules set out in previous European legal instruments concerning the electronic communications sector may not be applied in a manner that is inconsistent with this principle.

5. ACCESS LOGS

Any retrieval of the data should be recorded. The records should only be available, upon request, to the authority and/or body mentioned below in point 6 as well as to data protection authorities in case of control, and have to be deleted one year after being produced.

6. JUDICIAL/INDEPENDENT SCRUTINY

Access to data should, in principle, be duly authorised on a case by case basis by a judicial authority without prejudice to countries where a specific possibility of access is authorised by law, subject to independent oversight. Where appropriate, the authorisations should specify the particular data required for the specific cases at hand.

7. ADDRESSEES

The Directive should clearly define which providers of publicly available communication services are concerned by the obligations. In the case of the Internet, a limitation on access provider and one-to-one communication (e-mail services, voice over IP) is necessary.

8. IDENTIFICATION

It is important to clarify also in this Directive that there is no obligation for identification in cases where the identification is not necessary for billing purposes or other purposes to fulfil the contract.

9. PUBLIC ORDER PURPOSES

Providers of public electronic communication services or networks should not be allowed to process data retained solely for public order purposes for their own purposes.

10. SYSTEM SEPARATION

In particular, the systems for storage of data for public order purposes should be logically separated from systems that are used for the business purposes of providers and protected by more stringent security measures (for instance by means of encryption) in order to prevent unauthorized access and use.

11. SECURITY MEASURES

The Community measures should provide for minimum standards for technical and organisational security measures to be taken by the providers, specifying the general requirements regarding security measures established in Directive 2002/58/EC.

12. THIRD PARTIES

The Community measures should specify that access to retained data by any other third parties is illegitimate.

13. DEFINITIONS

There should be a clear definition of the data categories and a limitation on traffic data.

14. LIST OF DATA AND MECHANISMS FOR ITS REVISION

It is necessary for the Directive to directly specify the list of personal data to be retained. This is important in order to accurately gauge the impact on fundamental rights and freedoms of the citizens concerned, by having regard to the risks for their personal sphere and taking also account of the issues related to ensuring accuracy and updating of the retained data. Any proposals for changes to the list of the types of data to be retained should be subjected to a strict necessity test. In the light of the impact of these measures on fundamental rights and freedoms, the revision of the said list should be carried out only with the approval of the European Parliament and by involving data protection authorities. The participation of representatives from consumer and user associations, other relevant non-governmental bodies, and the European associations of the electronic communications industry should also be envisaged. In this perspective, it does not appear to be appropriate to carry out the revision of the said list merely according to the comitology procedure as envisaged in the Directive.

15. NO CONTENTS DATA

Since the scope of the proposal is meant to exclude contents of communications, specific guarantees should be introduced in order to ensure a stringent, effective distinction between contents and traffic data – both for the Internet (i.e., only log-in/log-off data, or else any information, including mail server logs, web cache logs and IP flow logs) and for telephony (conference calls, fax, sms, voice).

16. UNSUCCESSFUL COMMUNICATION ATTEMPTS

The different categories of traffic data related to unsuccessful communication attempts should not be included, failing an in-depth adequacy assessment in the light of the principles mentioned above.

17. LOCATION DATA

Storing location data should not go beyond the cellID at the start of a communication.

18. EFFECTIVE SUPERVISION

There should be effective controls on the original and on any further compatible use (including duplication), by judicial authorities within and for the purposes of a criminal procedure and, concerning data protection regardless of the existence of a judicial proceeding, by data protection authorities.

19. PUBLICITY

The Directive should envisage the obligation to adequately inform all citizens with regard to any and all processing operations to be possibly performed further to the implementation of its measures.

20. COSTS

The Article 29 Working Party notes that additional costs upon providers of public electronic communication services or networks are to be compensated by Member States. The Working Party would like to stress the importance of this issue exclusively with regard to the features that are directly related to data protection. Data retention measures should also involve both reimbursement for investments in the adaptation of the communication systems, for the disclosure of data to law enforcement authorities and about security measures. A comprehensive view is required in order to prevent any negative effects from being produced both on the data protection level and on the economic sphere of citizens, who might be charged some of the costs incurred by providers. In this context, it might also be considered whether a provider's entitlement to reimbursement for costs should be subject to fulfilment of the minimum standards and should take place on a case-by-case basis.

The Working Party is confident that the considerations made in its Opinion will be taken into due account, and recalls that all the safeguards mentioned above should be in place prior to putting into practice data retention obligations.

Done at Brussels, on 21st of October 2005

For the Working Party

The Chairman

Peter Schaar