11885/04/EN
WP 99

Opinion 9/2004
on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. [Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)]

Adopted on 9th November 2004

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

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 to Articles 12 and 14 thereof,

has adopted the present Opinion:

In recent years, the Working Party has repeatedly commented on the issue of retention of communication traffic data[2], and the European Conference of Data Protection Commissioners has issued several joint statements on the same subject[3]. The proposal for a draft Framework Decision on the retention of such traffic data presented by four member states in the Council of the European Union once again calls for an opinion of the Working Party. In view of the early stage of discussion in the relevant working party of the Council, this opinion has a preliminary character. The Working Party intends to reconsider the subject, on the basis of a revised draft, at a later stage.

The Working Party has examined whether the draft is in conformity with the standards of Article 8 of the European Convention on Human Rights.

In this context it is essential to take into account that citizens increasingly perform daily activities and transactions using electronic communications networks and services. The data generated by these communications - so called 'traffic data' - possibly including details about time, place and numbers used for fixed and mobile voice services, faxes, e-mails, SMS and other use of the Internet, therefore also increasingly reflect a range of details concerning the way in which these citizens conduct their daily lives.

In its *Recommendation 2/99 on the respect of privacy in the context of interception of telecommunications, adopted on 3 May 1999* the Working Party defined interception as the act of a third party acquiring knowledge about the content and/or data relating to private telecommunications between two or more correspondents, and in particular of traffic data concerning the use of telecommunications services. On that occasion the

---

1 Official Journal no. L 281 of 23/11/1995, p. 31, available at: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

2 See: Recommendation 3/97 on Anonymity on the Internet; Recommendation 2/99 on the respect of privacy in the context of interception of telecommunications; Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes; Opinion 7/200 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; Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime; Opinion 10/2001 on the need for a balance approach in the fight against terrorism; 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 1/2003 on the storage of traffic data for billing purposes. A summary of these statements can be found in the annex to this opinion. All documents are also available at http://europa.eu.int/comm/internal_market/privacy.

3 See statements adopted in Stockholm (April 2000) and Cardiff (2002).

Working Party stated that each telecommunications interception (including monitoring and data mining traffic data) constitutes a violation of individuals' right to privacy and of the confidentiality of correspondence. It follows that interceptions are unacceptable 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 this 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.

The Working Party takes the view that the same fundamental criteria apply to the retention of traffic data beyond what is needed for the delivery of communications services and other legitimate business purposes, and to any subsequent access to these data for law enforcement purposes[4].

The Working Party again has considerable doubts whether these fundamental criteria are fulfilled in the Draft framework decision. To start with the first criterion (legal basis), considering the preliminary status of the discussions in the Council, the Working Party does not consider it opportune to deal with this at this moment. With regard to the third criterion (conformity with a legitimate and listed aim) the Working Party questions the very aim of the Draft. Would that aim indeed solely be the prevention, investigation, detection and prosecution of criminal offences as was stated in the draft (Ground 7), while excluding other aims listed in Article 8? This aim must be clear in the first place.

With regard to the second criterion (need in a democratic society), according to the ECHR's interpretation the interference must respond to a "pressing social need" (e.g. the judgement in Klass v. Federal Republic of Germany of 18 November 1977, European Court of Human Rights, Series A No 28). The Court of Human Rights recognised the right of the Contracting States to carry out secret surveillance on personal correspondence and telecommunications in exceptional cases and under specific conditions. At the same time, it added:

[4] This is supported by the case law of the European Court of Human Rights. For example, in the Amann judgement (pp. 30) the storage by the authorities of information alone was held to be an interference, whether that data are used against the individual or not. In the Rotaru judgement as well, the storing of historical information by the secret services constituted an interference. In the PG v. UK judgement the Court stated (pp.42) that metering does not per se offend against Article 8, for example if done by the telephone company for billing purposes. Obtaining information from the provider relating to numbers called on a telephone by the police, however does interfere with the private lifes or correspondence. In the Malone case (pp. 84) too the Court ruled that the transfer of metering data from an operator to the police was an interference with 'correspondence' in Article 8. From these cases one might conclude that the mandatory storage of traffic data by providers of telecommunication does in itself not constitute an interference with Article 8, while the transfer of such data to the authorities or the further processing does. That conclusion would be wrong. In MM v. The Netherlands the Court ruled that authorities cannot avoid liability by making use of private persons when they make a crucial contribution to the execution of the surveillance scheme. Consequently, this would mean for instance that data retention and data mining in their own systems by telecommunication operators for public order purposes will constitute an interference too.

"... this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such as law poses of undermining or even destroying democracy on the ground of defending it, confirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate" (Klass, p. 3).

The routine, comprehensive storage of all traffic data, user and participant data proposed in the draft decision would make surveillance that is authorised in exceptional circumstances the rule. This would clearly be disproportionate. The draft framework would apply, not only to some people who would be monitored in application with specific laws, but to all natural persons who use electronic communications. Additionally all the communications sent or received would be covered. Not everything that might prove to be useful for law enforcement is desirable or can be considered as a necessary measure in a democratic society, particularly if this leads to the systematic recording of all electronic communications. The framework decision has not provided any persuasive arguments that retention of traffic data to such a large-scale extent is the only feasible option for combating crime or protecting national security. The requirement for operators to retain traffic data which they don't need for their own purposes would constitute a derogation without precedent to the finality/purpose principle.

Analysis carried out by telecommunication companies in Europe reveal the biggest amount of data demanded by law-enforcement were not older than six months. This shows that longer periods of retention are clearly disproportionate.

It should be noted that representatives of the law enforcement community have failed to provide any evidence as to the need for such far reaching measures. Indeed, they have been totally and conspicuously absent at recent workshops organised with a view to consider the background and the consequences of the present proposal for a draft Framework Decision.

The Convention on Cybercrime provides only for individual secure storage on the "fast-freeze – quick thaw" model which, by contrast with the views of the four proposing Governments, is entirely adequate for the prevention or prosecution of criminal offences. It is characteristic of current legal discussions that the present proposal is being seriously discussed before the Convention on Cybercrime has entered into force in most signatory states and its practical consequences can be assessed. The Article 29 Working Party has already stated (Opinion 5/2002) that the retention of traffic data for purposes of law enforcement should meet strict conditions under Article 15(1) of Directive 2002/58/EC, i.e. in all cases, only for a limited period and when necessary, appropriate and proportionate in a democratic society. Also the European Data Protection Commissioners at their International Conference in Cardiff (9-11 September 2002) have made a statement on mandatory systematic retention of traffic data. It was pointed out that the

systematic retention of all kinds of traffic data for a period of one year or more would be clearly disproportionate and therefore unacceptable.

Not only does the draft Framework Decision fail to cover those conditions, it expressly seeks to nullify them by not requiring definite grounds of suspicion and a reliable basis in fact in individual cases and providing for comprehensive data storage as precautionary measure in future legal proceedings against any users of electronic communications systems.

The Working Party is of the opinion that the mandatory retention of all types of data on every use of telecommunication services for public order purposes, under the conditions provided in the draft Framework Decision, is not acceptable within the legal framework set in Article 8.

Done at Brussels, on 9th November 2004

For the Working Party

The Chairman

Peter Schaar

ANNEX

Summary of statements of the Article 29 Working Party on the issue of retention of communication traffic data

RECOMMENDATION 3/97 ON ANONYMITY ON THE INTERNET

In Recommendation 3/97 on Anonymity on the Internet the Article 29 Working Party (WP29) stated that although transactional data may in some jurisdictions enjoy a degree of protection under rules protecting the confidentiality of correspondence, the massive growth in the amount of such data is a cause of legitimate concern. As on-line services develop in terms of their sophistication and their popularity, the problem of transactional data will grow. As more and more aspects of our daily activities are conducted on-line, more and more of what we do will be recorded.

Identifiable transactional data by its very existence will create a means through which individual behaviour can be surveyed and monitored to a degree that has never been possible before. According to WP29, the ability of governments and public authorities to restrict the rights of individuals and monitor potentially unlawful behaviour, should be no greater on the Internet than it is in the outside, off-line world.

RECOMMENDATION 2/99 ON THE RESPECT OF PRIVACY IN THE CONTEXT OF INTERCEPTION OF TELECOMMUNICATIONS, ADOPTED ON 3 MAY 1999

How human rights principles relate to measures concerning the surveillance of telecommunications (including monitoring and data mining traffic data) has been indicated by WP29 in its Recommendation 2/99 on the respect of privacy in the context of interception of telecommunications, adopted on 3 May 1999. On that occasion WP29 defined interception as the act of a third party acquiring knowledge about the content and/or data relating to private telecommunications between two or more correspondents, and in particular of traffic data concerning the use of telecommunications services. WP29 pointed out that each telecommunications interception constitutes a violation of individuals' right to privacy and of the confidentiality of correspondence. It follows that interceptions are unacceptable unless they fulfil three fundamental criteria in accordance with Article 8 (2) of the European Convention and the ECHR's interpretation of this 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.

In this legal context, exploratory or general surveillance on a large scale must be proscribed. Reference was especially made by the WP29 to the Leander and Klass cases: effective guarantees against abuse are needed in view of the risk that a system of secret surveillance for the protection of national security, poses the risk of undermining or even destroying democracy on the ground of defending it. In the Klass case, German legislation did not contravene Article 8 since, inter alia, the surveillance might only cover the specific suspect or his presumed 'contact-persons'. In this recommendation (paragraph 9) the Working Party issued a list of demands to be met by national law with regard to interceptions.

RECOMMENDATION 3/99 ON THE PRESERVATION OF TRAFFIC DATA BY INTERNET SERVICE PROVIDERS FOR LAW ENFORCEMENT PURPOSES, ADOPTED ON 7 SEPTEMBER 1999.

The obligation to erase traffic data or make them anonymous is motivated by the sensitivity of traffic data revealing individual communication profiles, including information sources and geographical locations of the user of fixed or mobile telephones and the potential risks to privacy resulting from the collection, disclosure or further uses of such data.

Concerning the period during which traffic data may be stored, WP29 observed significant divergence in Member States. WP29 recommended that traffic data should not be kept for the sole purpose of law enforcement and that national laws should not oblige to keep traffic data for a period of time longer than necessary for billing purposes. The length of such a period could be further harmonised within the EU.

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, ADOPTED ON 2ND NOVEMBER 2000.

Traffic data such as URLs might reveal an individual's personal interests e.g. indications about religious beliefs, political opinions, health or sex life. Those data should in addition enjoy the confidentiality provided for communications.

According to WP29, an additional aspect that would need further discussion is that some of these data could also be considered sensitive data in the sense of Article 8 of the general Data Protection Directive 95/46/EC, the processing of which is in principle prohibited.

Given the wide definition of traffic data, WP29 deemed it is not necessarily acceptable to treat all items in the same way. Some types of traffic data may need more protection than others.

OPINION 4/2001 ON THE COUNCIL OF EUROPE'S DRAFT CONVENTION ON CYBER-CRIME, ADOPTED ON 22 MARCH 2001

If procedural law is to be harmonised, the harmonisation of safeguards and conditions that shall apply to the measures envisaged is to be considered as well. Again, WP29 emphasised that a general surveillance obligation consisting in the routine retention of traffic data, as originally proposed in the Cybercrime Convention (Version no 25), would be an improper invasion of the fundamental rights guaranteed to individuals by Article 8 of the European Convention on Human Rights.

Furthermore, business may need more legal certainty in case it is not clear when and to whom access has to be given to confidential information and communications and when.

OPINION 10/2001 ON THE NEED FOR A BALANCED APPROACH IN THE FIGHT AGAINST TERRORISM, ADOPTED ON 14 DECEMBER 2001

In *Opinion 10/2001 On the need for a balanced approach in the fight against terrorism, adopted on 14 December 2001* WP29 stated that the objective of democratic societies to

engage in a fight against terrorism is both necessary and valuable. Nevertheless, in this fight certain conditions have to be respected, that form also part of the basis of our democratic societies. With full knowledge of the serious problem of terrorism -since this phenomenon has been known for quite some time in Europe- long term reflection is necessary, on measures which are simply 'useful' or 'wished', such as the prior and generalised retention of telecommunication data. The measures to be taken shall not restrict the fundamental right and freedoms. A key element in the fight against terrorism involves ensuring that we preserve the fundamental values which are the basis of our democratic societies and the very values that those advocating the use of violence seek to destroy.

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, ADOPTED ON 11 OCTOBER 2002

WP29 gravely doubted the legitimacy and legality of the mandatory systematic retention of traffic data, in order to permit possible access by law enforcement and security bodies.

The outcome of lengthy and explicit debate on the issue in Directive 2002/58/EC was that retention of traffic data for purposes of law enforcement should meet strict conditions under Article 15 (1) of the Directive: i.e. in any case for a limited period only and where necessary, appropriate and proportionate in a democratic society. WP29 stated that systematic retention of all kinds of traffic data for a period of one year or more would be clearly disproportionate and therefore unacceptable in any case.

Furthermore, WP29 expected to be consulted on measures that may emerge from third pillar discussions before they are adopted.

OPINION 1/2003 ON THE STORAGE OF TRAFFIC DATA FOR BILLING PURPOSES, ADOPTED 29 JANUARY 2003

In *Opinion 1/2003 on the storage of traffic data for billing purposes, adopted 29 January 2003* WP29 gave guidance in the harmonisation of the period during which traffic data may lawfully be processed for billing purposes. Storage for billing purposes should normally involve a storage period of 3-6 months at most. Only traffic data that are adequate, relevant and non-excessive for billing and interconnection purposes may be processed. Other traffic data must be deleted or anonymised.

Practices that are inconsistent with these principles as well as practices that are not clearly authorised by legislative provisions under the conditions of Article 15 of Directive 2002/58/EC are, prima facie, incompatible with the requirements of EC Data Protection Law.