Représentant les avocats d'Europe
Representing Europe's lawyers

CCBE RECOMMENDATIONS FOR THE IMPLEMENTATION OF THE DATA RETENTION DIRECTIVE

Conseil des barreaux européens – Council of Bars and Law Societies of Europe
association internationale sans but lucratif
Avenue de la Joyeuse Entrée 1-5 – B 1040 Brussels – Belgium – Tel.+32 (0)2 234 65 10 – Fax.+32 (0)2 234 65 11/12 – E-mail ccbe@ccbe.org – www.ccbe.org

CCBE RECOMMENDATIONS FOR THE IMPLEMENTATION OF THE DATA RETENTION DIRECTIVE

In this paper, the CCBE publishes recommendations to its member bars in relation to the implementation of the data retention directive (Directive 2006/24/EC of the European Parliament and the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC).

During the legislative passage of the directive, the CCBE vigorously expressed its concerns regarding a number of issues, described below. The directive has been in force since 3 May 2006 and will have to be implemented by the Member States into national law by 15 September 2007, with the possibility to postpone the application regarding internet traffic data until 15 March 2009.

The CCBE calls upon its members to urge their national legislators to respond to the concerns of the legal profession when transposing the directive. To this end, the CCBE has issued recommendations which could support its members in this task.

Introduction

The CCBE supports the fight against terrorism and crime. However, it is worried by the growing initiatives taken at the European level which, under cover of the fight against terrorism, are serious infringements to fundamental freedoms and rights.

The data retention directive aims to harmonise laws of Member States on the retention of data generated or processed by publicly available communications services providers or providers of a public communications network. It obliges all Member States to have a legal framework providing for retention of traffic data as well as localisation data for a fixed period of at least six months, but no longer than two years. Information obtained through traffic and localisation data are important matters, hence the interest of such legislation for governments. The fact of being able to know when, where, how and how many times a person consults his/her lawyer seriously challenges the confidentiality of the lawyer-client relationship and even the exercise of the right of defence itself.

The CCBE was opposed to the data retention directive which, on the one hand, infringes professional secrecy since it does not differ between various data, and on the other hand, includes numbers of gaps and uncertainties (please see below for further background information). The two particular concerns of the CCBE have been: (1) that professional secrecy is not guaranteed when governments have eventual access to the retained data; and (2) that prior judicial authorisation is not required before governments have access to the data.

In support of the CCBE's stance on professional secrecy, the European Parliament passed a legislative resolution at the same time as it passed the data retention directive. The relevant part of this resolution of 14 December 2005 (P6_TA (2005)0512, A6-0365/2005) stressed the need to safeguard professional secrecy:

> *The European Parliament (…) 4. Considers that the Member States have the right to apply their national constitutional principles and considers especially that **professional secrecy** will also be respected in the application of the present directive;*

Regarding prior judicial authorisation, the background note below lays out in great detail the vagueness and shortcomings of the directive which make prior judicial authorisation imperative for the protection of citizens' rights.

Accordingly, the CCBE calls upon its members to safe-guard in particular professional secrecy and prior judicial authorisation when their national legislator transposes the data retention directive into national law.

Recommendations

The CCBE calls upon its members to urge their national legislators:

1. **to ensure that lawyers' professional secrecy is guaranteed when retained traffic and communication data is accessed by governments and other competent authorities;**

2. **to ensure that access to retained data is granted under the legislation only with prior judicial authorisation;**

3. **to ensure that once the government or law enforcement authority has accessed the data, it should only be used and stored as long as this is necessary for the purpose for which the data was originally supplied as protected under Article 6 of the Directive 95/46/EC[1] and Article 6 Para 1 of the Directive 2002/58/EC[2];**

4. **to ensure that a high level of protection measures safeguarding the principle of respect for privacy and confidentiality of communications as protected under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union and Article 8 of the European Convention of Human Rights are inserted into the legislation.**

Background information:

It should be noted that until now Community law aimed at protecting natural persons with regard to processing of personal data (Directive 95/46/EC). This Directive forbids storage of communications and related traffic data by persons others than the users, or at least sets as a preliminary condition the obligation to make the data anonymous (Directives 95/46/EC and 2002/58/EC) when they are stored for a limited period of time, notably for invoicing. Under Directive 2002/58/EC, the retention of data is,

---

[1] Article 6
1. Member States shall provide that personal data must be:
(a) processed fairly and lawfully;
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
2. It shall be for the controller to ensure that paragraph 1 is complied with.

[2] *Article 6*
Traffic data
1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

in any case, an exception and is strictly limited by the provisions of Article 15 of the Directive 2002/58/EC[3].

From now on, and under the terms of this new directive, the retention of data would become standard, and no longer remain an exception. The CCBE concerns refer to (1) the protection of professional secrecy and (2) judicial authorisation, as well as legal certainty regarding the access to data.

1/ Professional secrecy

The legal profession is concerned by the consequences of the directive which departs from the principle of respect for privacy and confidentiality of communications (infringements of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union and of Article 8 of the European Convention on Human Rights[4]). The directive ignores as well the right to the protection of personal data (Article 8 of the Charter of Fundamental Rights of the European Union). It denies the confidential character of the lawyer-client relationship and in general professional secrecy.

Everyone has the right to consult a lawyer in order to ask advice which can be provided on the basis that the citizen is assured that what is said to the lawyer remains confidential. This right is part of fundamental freedoms and rights and derives from the principle of the rule of law. Denying this right would lead to serious infringement of the rights of defendants. The obligation of a lawyer to professional secrecy serves the interest of judicial administration and in general of the State. Professional secrecy is a right for the client and a duty for the lawyer. Without ensuring confidentiality, there cannot be trust and the lawyer cannot play his/her specific role in society.

The European Court of Justice expressly mentioned in its decision in the AM&S[5] case: "*that confidentiality serves the requirements, the importance of which is recognized in all of the member states, that any person must be able, without constraint, to consult a lawyer whose profession entails the giving of independent legal advice to all those in need of it*" [6]It added that "*the principle of the protection against disclosure afforded to written communications between lawyer and client is based principally on a recognition of the very nature of the legal profession, inasmuch as it contributes towards the maintenance of the rule of law and that the rights of the defence must be respected"*. The duty of the lawyer to respect "*strict professional secrecy*" was asserted again by the Court in the Wouters[7] case as being a generally recognised principle in all Member States and an "*essential rule to ensure the proper practice of the legal profession*" that bars try to keep to.

Information obtained through traffic and localisation data are important matters, hence the interest of such legislation for governments. The fact of being able to know when, where, how and how many times a person consults his/her lawyer seriously challenges confidentiality of the lawyer-client relationship and even the exercise of the right of defence itself. Therefore, confidentiality should benefit from protection by the State, and increased protection should be expected from a European law.

---

[3] *"Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction "constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system". "To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph."*

[4] ARTICLE 8

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[5] Judgement of the Court of 18 May 1982, AM & S Europe Limited v Commission of European Communities, case C-155/79

6 For an important national case, also well known in an international context, please see: Three Rivers District Council and Others v Governor and Company of the Bank of England [2004] UKHL 48.

[7] Judgement of the Court of 19 February 2002, Wouters, Case C-309/99

2/ The need of prior judicial authorisation and legal certainty regarding the access to data

In the directive, retention is generally authorised for the investigation, detection as well as the prosecution of *serious crime* (Article 1(1)). Serious crime as a term is not defined and is open to varying interpretation.

The European Data Protection Supervisor (EDPS) in its opinion on the draft directive of 26 September 2005 stressed the fact that an adequate availability of certain traffic and location data can be a crucial instrument for law enforcement agencies and can contribute to the physical security of persons. However, in the same opinion, the EDPS mentioned that this does not automatically imply the necessity of the new instruments, as foreseen in the present proposal. According to the EDPS, the necessity of this new obligation to retain data — in its full extent — had not been adequately demonstrated.

Article 7 on "*Data Protection and data security*" does not contain any serious protection measures above an absolute minimal technical and operational level. It speaks of "…*appropriate technical and organisational measures to protect data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure"*. On the contrary, Member States have latitude, and no parameter is set despite what is mentioned in the preamble of the directive.

There are no safeguards for persons concerned by data retention but only a vague reference to Directive 95/46/EC and the opportunity to have judicial remedies. This again is left to the discretion of the individual Member States.

Article 4 on "*Access to data*" delegates the entire responsibility of necessity and proportionality requirements to the discretion of the Member States. It appears wrong to establish such an invasive legal instrument as the data retention directive at European level without giving it any boundaries or an adequate level of legal safeguard and protection at the same time.

Nothing is foreseen for judicial proceedings to be respected as far as access to data is concerned, but there is only the requirement of "*data (..) are provided only to the competent national authorities in specific cases and in accordance with national law, …in accordance with necessity and proportionality requirements … subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights"*. This is too vague and leaves retained data subject to numerous interpretations. There should be in any case an authorisation given by a judge for the extension of the period for the retention of data.

There are no provisions on the conditions under which the retention is operated, or on the supervising authorities.

Furthermore, there are no limitations on duration for data once they have been accessed and preserved. Article 7 (d) sets out that all data shall be destroyed at the end of the period for retention (two years according to Article 6) "*except those data which have been accessed and preserved*". In contrast to this, and in line with Article 6 of the Directive 95/46/EC and Article 6 Para 1 of the Directive 2002/58/EC, the national law that transposes the data retention directive should ensure that data submitted by an operator to the government or law enforcement authority according to a proper judicial process should be kept only as long as this is necessary for the purpose which allowed the data to be submitted in the first place. The data may not be used by the government or law enforcement authority for any other purpose than for which it was originally submitted.

According to Article 11, conditions set out in Article 15 of the Directive 2002/58/EC, which contain the provisions of Article 8(2) of the European Convention for Human Rights, are explicitly excluded for the application on data regulated in the data retention directive. The text of Article 11 does not clarify sufficiently that the Member States are no longer competent to adopt legislation in relation to criminal

offences, additional to the present proposal. This creates ambiguity on the Member State's remaining competences to adopt legislation as regards the retention of data.

For these reasons, the CCBE strongly believes that that access to the data should be subject to prior judicial authorisation in all cases.