Conseil des barreaux européens
Council of Bars and Law Societies of Europe
Association internationale sans but lucratif
Rue Joseph II, 40 /8 – 1000 Bruxelles
T. : +32 (0)2 234 65 10 – F. : +32 (0)2 234 65 11
Email : ccbe@ccbe.eu – www.ccbe.eu

CCBE Recommendations concerning the annulment of the Data Retention Directive

12/09/2014

Introduction

The Council of Bars and Law Societies of Europe (CCBE) represents the bars and law societies of 32 member countries and 13 further associate and observer countries, and through them more than 1 million European lawyers.

In this paper, the CCBE publishes recommendations to its member Bars and Law Societies in relation to the recent annulment of the Data Retention Directive (2006/24/EC) by the EU Court of Justice (CJEU) on 8 April 2014 (Joined Cases C-293/12 and C-594/12).

During the legislative passage of the Data Retention Directive, the CCBE vigorously expressed its concerns regarding, inter alia, professional secrecy of communications between lawyer and client (known in some jurisdictions as legal professional privilege), prior judicial authorisation before data is accessed, duration and purpose of data retention.

The directive has been in force since 3 May 2006, and had 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.

In September 2006, the CCBE published a set of recommendations to its members regarding the implementation of the directive into national law. In view of the recent judgement the question arises to what extent these national laws comply with the proportionality concern raised by the CJEU.

Overview of the CJEU judgment

Serious interference with the rights to respect for private life and protection of personal data

The Court observes that the data to be retained make it possible to: (1) know the identity of the person with whom a subscriber or registered user has communicated and by what means; (2) identify the time of the communication as well as the place from which that communication took place; and (3) know the frequency of the communications. This data, taken as a whole, may provide very precise information on the private lives of the persons whose data are retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, activities carried out, social relationships and the social environments frequented.

The Court takes the view that, by requiring the retention of those data and by allowing the competent national authorities to access that data, **the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data**.

Furthermore, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the persons concerned a feeling that their private lives are the subject of constant surveillance.

Non-compliance with the principle of proportionality – potential incompatibility with professional secrecy obligations

The Court considers that retention of data for the purpose of their possible transmission to the competent national authorities genuinely satisfies an objective of general interest, namely the fight against serious crime and, ultimately, public security.

Although the retention of data required by the directive may be considered to be appropriate for attaining the objective pursued by it, **the wide-ranging and particularly serious interference of the directive with the fundamental rights at issue is not sufficiently circumscribed to ensure that that interference is actually limited to what is strictly necessary.**

First, the directive covers, in a generalised manner, all individuals, all means of electronic communication and all traffic data without **any differentiation, limitation or exception** being made in the light of the objective of fighting against serious crime. In this respect, the Court points out that in general, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made under the objective of fighting against serious crimes, applies even to persons whose communications are subject, according to rules of national law, to the obligation of **professional secrecy**.

Secondly, the directive fails to lay down any objective criterion which would ensure that the competent national authorities have **access to the data** and can use them only for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights in question, may be considered to be sufficiently serious to justify such an interference. On the contrary, the directive simply refers in a general manner to 'serious crime' as defined by each Member State in its national law. In addition, the directive does not lay down substantive and procedural conditions under which the competent national authorities may have access to the data and subsequently use them. In particular, the access to the data is not made dependent on the prior review by a court or by an independent administrative body.

Thirdly, so far as concerns **the data retention period**, the directive imposes a period of at least six months, without making any distinction between the categories of data on the basis of the persons concerned or the possible usefulness of the data in relation to the objective pursued. Furthermore, that period is set at between a minimum of six months and a maximum of 24 months, but the directive does not state the objective criteria on the basis of which the period of retention must be determined in order to ensure that it is limited to what is strictly necessary.

The Court also finds that **the directive does not provide for sufficient safeguards** to ensure effective protection of the data against the risk of abuse and against any unlawful access and use of the data. It notes, inter alia, that the directive permits service providers to have regard to economic considerations when determining the level of security which they apply (particularly as regards the costs of implementing security measures) and that it does not ensure the irreversible destruction of the data at the end of their retention period.

Lastly, the Court states that **the directive does not require that the data be retained within the EU**. Therefore, the directive does not fully ensure the control of compliance with the requirements of protection and security by an independent authority, as is, however, explicitly required by the Charter. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data.

As a result, the Court is of the opinion that, by adopting the Data Retention Directive, the EU legislature has **exceeded the limits imposed by compliance with the principle of proportionality**.

Impact of invalidation

Since the Data Retention Directive has been invalidated in its entirety this text is deemed to have never existed. Given that the Court has not limited the temporal effect of its judgment, the declaration of invalidity takes effect from the date on which the Data Retention Directive entered into force. As a result, it is no longer applicable. The judgement does not, however, apply to nationally implemented laws, and at this stage it still remains to be seen what measures will be taken in response to the judgment by the EU institutions as well as by individual Member States.

The European Commission so far has stated in a FAQ published on the date of the judgment that "National legislation needs to be amended only with regard to aspects that become contrary to EU law after a judgment by the European Court of Justice. Furthermore, a finding of invalidity of the Data Retention Directive does not cancel the ability for Member States under the e-Privacy Directive (2002/58/EC) to oblige retention of data."

Nevertheless, it seems likely that the CJEU ruling opens the door to legal challenges against data collection in national courts, especially in relation to the proportionality concern raised by the CJEU.

Recommendations

Considering the outcome of CJEU ruling, the CCBE now recommends the taking of appropriate action as follows:

1. If the national legislation does not comply with the proportionality concern raised by the CJEU, as well as the CCBE's concerns on
   - professional secrecy of communications between lawyer and client,
   - prior judicial authorisation before data is accessed,
   - duration and purpose of data retention,

it is proposed that the CCBE members should take the following actions:

   a) Identify strategies to initiate a change in national legislation where it is necessary (e.g. lobby parliamentarians, launch a public-awareness campaign, etc.).

   b) Publicise any individual cases where clients/lawyers are negatively affected by the non-compliance and seek legal advice on possible remedies with reference to the CJEU ruling.

   c) Bring non-compliance to the attention of the government bodies (i.e. data protection authorities, ministry, departments etc.) responsible for data protection. Furthermore, wherever appropriate, CCBE members should seek to initiate legal challenges against any national legislation that can be argued to be contrary to the CJEU ruling, including by supporting individual lawyers or law firms in such legal challenges (e.g. through amicus briefs if available).

   d) Make specific reference to the CJEU ruling in any document, public statement and letter to government and elected officials which is sent regarding the issue of data protection in the context of data retention.

   e) Bring the concerns to the attention of the European Commission (DG Justice - Directorate C Fundamental rights and Union citizenship – 3 Data Protection) and the Working Group established under Article 29 of Directive 95/46/E[1] , the national data protection commissioner or the European Data Protection Supervisor[2].

   f) Inform the CCBE about the state of implementation of the Data Retention Directive in the respective Member State and let the CCBE know how it can support the CCBE member's actions towards a change in national legislation where it is necessary.

   g) Consider possible claims challenging the law implementing the Data Retention Directive before the relevant constitutional body (e.g constitutional court or other relevant constitutional body, ordinary courts, etc. as local law provides) or other appropriate Court.

2. Based on the conclusions in the CCBE Comparative Study on Governmental Surveillance of Lawyers' Data in the Cloud, the CCBE at the same time invites the European Commission to ensure that whatever regulatory regime is in place in a Member State for the interception of communications, that regime should guarantee the inviolability of data and other evidence falling under the principle professional secrecy.

For this reason:

   a) There should be a harmonised, minimum level of protection for professional secrecy, regardless of the data being traffic data, other metadata or content data, and irrespective of which governmental body requires access to a given data, and whether the purpose is for national security, fighting, or preventing crime.

   b) The minimum level of protection of communications containing professional secrecy should be the same in the electronic world as it is in the paper world.

---

[1] European Commission: DG JUST - Justice, Marie-Helene.Boulanger@ec.europa.eu (Head of Unit - Data protection), +32 229-69408. Art.29 Working Group: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.

[2] For contact details of the national data protection commissioner, please see : http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm; Contact details of the European Data Protection Supervisor: http://ec.europa.eu/justice/data-protection/bodies/supervisor/index_en.htm.

a) This minimum level of protection has to ensure in the Member States a more explicit and consistent protection of professional secrecy of communications between lawyer and client, with prior judicial authorisation and clear requirements on purpose and duration of data.

3. In view of the European Parliament's resolution of 12 March 2014 on the 'US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI))', the CCBE also invites the European Parliament to undertake urgent action to establish 'A European Digital Habeas Corpus - protecting fundamental rights in a digital age' including the protection of confidentiality of lawyer-client relation, as stipulated in Action 6 of the resolution.