Chapter 18

The Implementation of the Data Retention Directive: A Comparative analysis

Anna Pateraki
Humboldt University of Berlin, Germany

ABSTRACT

This paper aims to provide a comparative analysis regarding the implementation of the EC Data Retention Directive (2006/24/EC) in the most important Member States including Germany, Great Britain and France in order to provide the reader with the necessary information on the current controversial matters relating to it and display the differences in the speed, intensity and form of its implementation.

I. INTRODUCTION

Data retention has been the most controversial legal and political issue in the recent years in relation to data protection in Europe. As already analyzed in the previous papers the Data Retention Directive (2006/24/EC) refers to the obligation of providers of publicly available electronic communications services or of public communications networks to retain without occasion – which means without initial suspicion – traffic and location data of communications through fixed, mobile and internet telephony, internet access and e-mail for the purpose of investigation, detection and prosecution of serious crimes, as defined by the national law. The period of retention shall range between 6 months and 2 years; the content of the communication shall be exempted from the above obligation. The retained data shall be transferred to the competent authorities upon request and without undue delay, while certain data security principles are to be respected during the period of retention.

Ireland, supported by Slovakia, brought an action for the annulment of the Data Retention Directive before the European Court of Justice in 2006. Ireland’s action related solely to the choice of legal basis and not to any possible infringement by the Directive of fundamental rights resulting from interference with the exercise of the right to privacy. In particular, the choice of Art. 95 EC former version (internal market) as the Directive’s
legal basis had been questioned. Nevertheless, the European Court of Justice dismissed this action on February 10, 2009 (C-301/06) and did not accept the argument made by Ireland that the “centre of gravity” of the Directive does not concern the functioning of the internal market, as its principal objective is the investigation, detection and prosecution of crime, and it should therefore be subjected to the third pillar and not to the Community competence under Article 95 EC former version. In fact, the Court held that the Directive was correctly adopted on the basis of the EC Treaty as it relates predominantly to the functioning of the internal market, with the argument that data retention has significant economic implications for service providers in so far as they may involve substantial investment and operating costs. Besides the Data Retention Directive amended the provisions of the Directive 2002/58/EC, which was itself based on Article 95 EC former version. In those circumstances, in so far as it amends an existing Directive which is part of the acquis communautaire, the Data Retention Directive could not be based on a provision of the EU Treaty.

This judgment was treated with criticism among commentators, since it contradicts an older decision (C-317/04) where the European Court of Justice annulled the Commission’s Decision 2004/535/EC on the adequate protection of personal data contained in the Passenger Name Records (PNR) of air passengers transferred to US authorities on the grounds that it was not validly adopted on the basis of Art. 95 EC former version (Simitis, 2006). This decision made a crucial distinction between the purpose for which personal data are collected and processed and their further processing for public security purposes. The basic argument was that the processing of data collected for commercial purposes falls within the protective ambit of the data protection Directive, but when the same data are later transferred for public security reasons, they no longer enjoy the same protection (Kosta/ Dumortier, 2007). Nevertheless, the Court did not follow the same reasoning in the Ireland case. Moreover, it did not answer the compatibility question of the data retention obligation and the data protection principles such as the principles of necessity and proportionality, the finality principle or else purpose limitation and Art. 8 ECHR. At this point it is worthy of mention that if the European Court of Justice had accepted Ireland’s action for annulment then many national constitutional courts of the Member States would have acquired the competence to question the compatibility of data retention with the above mentioned rights and principles.

Thus, since the primary aim of the Directive was to combat terrorism and serious crime, the unexceptional implementation of this measure on all citizens has been questioned. Further, as this legal framework contradicts in some cases the traditional national level of privacy protection, significant oppositions and contradictions have been raised in many Member States with respect to the proportionality of this measure. In Germany, for instance, several administrative courts have decided that data retention is incompatible with the principle of proportionality. On the other hand, strong legislative debates aiming at the application of retained data also to civil copyright cases in the future have also arisen.

Nevertheless, in this context it is worth noting that according to the legislation of the European Court of Justice Member States have to specify a time-limit for storage of personal data for as long as it is necessary for the purposes for which the data has been collected or for which it is further processed, in order to guarantee the right of access of the data subjects to their data as stated in Art. 12 lit. a) of the Directive 95/46/EC (ECJ C-553/07). In this respect, Article 12 lit. a) of the Directive 95/46/EC provides for a right of access to basic data and to information for the recipients or categories of recipients to whom the data has been disclosed. As stated in recital 41 in the preamble to the Directive 95/46/EC, the data subjects must have a right of access to the data
Related Content

A Unified Use-Misuse Case Model for Capturing and Analysing Safety and Security Requirements
[www.igi-global.com/article/unified-use-misuse-case-model/62313?camid=4v1a](www.igi-global.com/article/unified-use-misuse-case-model/62313?camid=4v1a)

The Impact of IoT on Information Warfare
[www.igi-global.com/chapter/the-impact-of-iot-on-information-warfare/206782?camid=4v1a](www.igi-global.com/chapter/the-impact-of-iot-on-information-warfare/206782?camid=4v1a)

Content Filtering Methods for Internet Pornography
[www.igi-global.com/chapter/content-filtering-methods-internet-pornography/13459?camid=4v1a](www.igi-global.com/chapter/content-filtering-methods-internet-pornography/13459?camid=4v1a)

Secure Communication: A Proposed Public Key Watermark System
[www.igi-global.com/article/secured-communication/111272?camid=4v1a](www.igi-global.com/article/secured-communication/111272?camid=4v1a)