Data Retention in Europe and Germany

Thilo Weichert, Kirsten Bock

In Europe a controversial discussion on data retention of communication and related traffic data is lead now for almost 10 years. Following the attacks of September 11, 2001 in the USA, but particularly after the attacks in Madrid on March 11, 2004 for which mobile communication was used to activate the explosive device, in particular the law enforcement authorities have demanded to retain traffic data from telecommunication providers in order for the police, public prosecutors and intelligence services to gain access whenever needed. These efforts were intensified after the terrorist attack on July 7, 2005 in London.

A respective initial national legislative draft introduced in Germany in 2004 failed. Subsequently, politicians successfully tried to establish an obligation for data retention of telecommunication data by way of a European Union (EU) regulation. On March 15, 2006 a directive\(^3\) (hereafter the Directive) was constituted to oblige all EU Member States to retain traffic and location data for the purposes of investigation, detection, and prosecution of criminal offences for a time period of a minimum of six month and a maximum of two years. This directive restricts the Directive on privacy and electronic communications\(^4\) of 2002 which ensures confidentiality of communications and which allows retention of related traffic data only for the transmission of a communication and for billing purposes.

On April 18, 2011 the European Commission presented a report\(^5\) on the transposition of the Directive into the national laws of the Member States. According to this report the majority of Member States implemented data retention into their national laws. In Austria and Sweden, which until now did not know an obligation for data retention, legislative drafts are under discussion. In the Czech Republic, in Germany and in Romania the Directive was implemented at first; yet, declared void by the respective constitutional courts.

According to the Directive, the following data are to be retained: Source, address, date, time and duration, kind of communication, identification and for mobile devices its location. There are considerable differences between the transposing legislation in the Member States. The retention periods determined by the Directive in its Article 6 are between not less than 6 months and not more than two years, whereby the internet data are sometimes subject to shorter respites than those for telephone networks.

\(^1\) Findings of this text have been presented at the 21st annual Computers, Freedom and Privacy Conference, Law Center Georgetown University, Washington DC/USA on June 14, 2011.

\(^2\) Thilo Weichert is Data Protection and Freedom of Information Commissioner of the German Land Schleswig-Holstein and Head of ULD, Kirsten Bock is Head of EuroPriSe at ULD.

\(^3\) Directive 2006/24/EC of the European Parliament and the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks and amending Directive 2002/58/EC.


In some countries (Finland and UK) small providers are not obliged to retention. In all Member States access is possible for public prosecutors and the police. In fourteen Member States intelligence services are allowed access. In six Member States tax and customs authorities can obtain traffic data. In eleven Member States it is necessary to have judicial authorisation to gain access.

The German Federal Constitutional Court decided in its judgement of March 2, 2010\(^6\) that the national transposition of the Directive constitutes an infringement of Art. 10 of the German Basic Law (GG) which safeguards the secrecy of communications. To be sure, a six month groundless retention period of communications and related traffic data could be tolerable. But the Federal Constitutional Court found sufficient warranties for data security missing. Moreover, the Federal Constitutional Court asked for better regulations on transparency and legal protection. According to the Court data shall only be used in case of a sufficiently evidenced cause of a serious crime or the warding off of concrete danger for life, limb or freedom of a person or for the safety of the state but not in the forefield of criminal offences or dangers by way of precaution. Therefore, the access possibilities of intelligence services were subject to objection.

Also the Czech Constitutional Court (Judgement of March 22, 2011)\(^7\) and of the Rumanian Constitutional Court (Judgement of October 8, 2009)\(^8\) were of the opinion that data retention encroaches fundamental rights.

An Irish civil society organisation filed suit against data retention before the Irish High Court. The Court has addressed the European Court of Justice and asked for a preliminary ruling. Neither the European Court of Justice nor the European Court of Human Rights has ruled in substance until today.

According to the report of the European Commission only 67% of requests for data from security authorities are older than three months, further 19% are up to six months old and another 12% are up to one year old. Only in 2% of the cases requested data were older than one year.

The question, whether retained data are necessary for prosecution purposes is argued controversially. The prosecution services argue the data are absolutely necessary especially to investigate and resolve cyber crime. On the other side the German Interior Minister of Lower Saxony had to admit that even though data retention stopped in Germany as a result of the decision of the Federal Constitutional Court, the crime solution rate in cyber crime did not drop.

On European as well as on German level there is a political debate ongoing about the proportionality of data retention. In Europe the Commissioner of Home Affairs Cecilia Malmström is of the opinion that it is an absolutely necessary instrument whereas Commissioner Viviane Reding in charge of justice, fundamental rights and citizenship has asked for limits. The conflict in Germany is similar: The christian democratic Interior Minister Hans-Peter Friedrich would like to re-introduce data retention as fast as possible, whereas the liberal Minister of Justice Sabine Leutheusser-Schnarrenberger favours a combination of a short data retention period and a so called quick-freeze procedure. In the quick-freeze procedure the provider will be obliged to freeze the traffic data on short notice if there is probable cause of a crime. The data can be used for investigational purposes after a judge


\(^8\) Decision No. 1258.
has ordered to defreeze the data. The position of the Minister of Justice goes back to a suggestion made by the Federal Data Protection Commissioner and the office of the Data Protection Commissioner of Schleswig-Holstein (ULD).

However, there are many data protection officers and organisations of civil society who utterly reject data retention and who would only accept a quick-freeze procedure.

The report of the European Commission declares data retention to be necessary. Due to the different handling of the Directive, a harmonisation of the pre-requisites and procedures is envisaged. One reason for harmonisation is that telecommunications provider should find preferably uniform conditions for competition on the European market. The European Commission declared that it aspires to balance the interest of effective prosecution and effective fundamental rights protection.

In an opinion of March 31, 2011 the European Data Protection Supervisor\(^9\) comes to the conclusion that the Directive does not meet the demands of fundamental rights protection. The necessity of the measure taken has not been sufficiently demonstrated. This goal could have been regulated in a less privacy-intrusive way. Moreover, the Directive lacks foreseeability. The European Data Protection Supervisor Peter Hustinx therefore requested the Commission to further check potential alternatives and to only adopt a harmonized data retention directive if purpose, procedure and prerequisites are defined in a precise and distinct manner.

The discussion about data retention of telecommunication data needs to be seen in a broader context. Also in other sectors private companies are obliged to retain data and to make them available to security authorities. This is especially true for storing of international bank transaction data by the Belgium based SWIFT service to make it available to US authorities in the frame of the Terrorist Finance Tracking Program and for passenger name records.

Against plans to establish such data retention also within Europe, there is much opposition in the European Parliament. At the same time there are attempts in the European Parliament to terminate existing agreements between the EU and the USA or to at least limit them in scope and put them under better control mechanisms that are not yet sufficiently implemented in the current system.

Financial transaction, the use of air traffic or the use of telecommunication and the Internet – all of this entails the exercise of explicitly guaranteed fundamental rights and liberties. The German Federal Constitutional Court has clarified explicitly in its judgement of March 2, 2010 that the exercise of the fundamental liberties of people may not be totally captured and monitored. The prohibition of surveillance was found to be part of the “constitutional identity of the Federal Republic of Germany”.

The Treaty of Lisbon, effective since December 1, 2009, brought about two important changes for data protection in Europe. It put in place a Fundamental Rights Charta that not only includes an explicit right to privacy but also in its Article 8 a fundamental right to data protection. Moreover, the treaty provides for police and judicial cooperation of the Member States to be within the competence of the European Union, so that there will be further harmonisation taking place in this area. Both give reason for hope among data protection activists in Europe that the protection of informational self-determination in the security area in Europe and also in exchange with the USA will play a more important role in the future.

and that this will be highlighted by the actions of the European Parliament as well as by the European Court of Justice.