DATA PRIVACY

AND DATA RETENTION IN EUROPE

Rainer Kaspar and Hermann Hansmann • PHH Prochaska Havranek Rechtsanwälte GmbH

THE BEGINNING AND THE END

The issuance of the EU Directive RL 2006/24/EC (***Directive***) by the EU legislator was triggered, in addition to the 9/11 attacks, by the terrorist attacks in Madrid 2004 and London 2005.

The objective of the Directive was to improve the fight against crime, in particular organized crime and terrorism. With the conflict between freedom and security always having stood at the heart of the Directive, the stringent and comprehensive rules of the Directive on data retention was from the outset heavily criticized and opposed.

With the Wikileaks and Snowden incidents having raised enormous public interest and opposition, it came as no real surprise that the European Court of Justice (ECJ) struck down the Directive with its decision of April 8, 2014, on cases C-293/12 and C-594/12, thus repealing the Directive with retroactive effect.

WHAT DOES DATA RETENTION MEAN?

Data Retention within the meaning of the Directive meant the storage of all call data (communication data), and thus encompassed for example the following: Who called whom for how long and from where? Who sent whom an e-mail? Which IP address was used for browsing the Internet and how long did that browsing take place? Retention of data was to be done without any particular cause, and thus "for retention." However, the content of the communication was not retained.

The required data was collected by private telecommunication companies, which were subjected by the Directive to a duty to retain. The data was to be kept available on their servers for a "second step," the access by public authorities. However, such right of access was limited and only to be granted under certain conditions, for example for the purpose of investigating criminal allegations.

Nonetheless, in theory, the aggregate volume of the information collected allowed very accurate conclusions regarding the private life of persons whose data was retained, such as habits of daily life, preferred locations and activities and social relationships.

IS THERE A DIFFERENCE BETWEEN EU DATA RETENTION RULES AND THE ACTIVITIES OF THE NSA?

It appears that the main difference is that while in the case of European data retention where access through the public authorities took place only in a second step on the basis of certain conditions being fulfilled, the activities of the U.S. authorities focus(ed) from the outset on the collection of data for direct access by public authorities. Further, data collected for purposes of European data retention was collected by private companies and encompassed "EU-domestic" data only. As was made clear from media reports, the NSA itself collects data and (also) focuses on data from foreign countries. In addition, the NSA allegedly saves the content of the communication and also specifically tapped the phone of high-ranking foreign officials, such as German Chancellor Merkel.

Thus, the NSA's data collection program goes far beyond the European data retention according to the Directive.

WHY HAS THE ECJ STRUCK DOWN THE DIRECTIVE?

The ECJ held the Directive to infringe upon the fundamental rights of respect of privacy and protection of personal data. The Court has deemed the obligation to retain data to be a "particularly serious interference" with the mentioned fundamental rights. The data collected enables the drawing of very accurate conclusions on citizens' habits of daily life. Among citizens, the data retention may result in the feeling "that their private life is the object of permanent supervision" because they are not given information on the retention itself and in particular on how the information retained will be used.

THE DATA WAS TO BE KEPT AVAILABLE ON THEIR SERVERS FOR A "SECOND STEP," THE ACCESS BY PUBLIC AUTHORITIES. HOWEVER, SUCH RIGHT OF ACCESS WAS LIMITED AND ONLY TO BE GRANTED UNDER CERTAIN CONDITIONS, FOR EXAMPLE FOR THE PURPOSE OF INVESTIGATING CRIMINAL ALLEGATIONS.

REGARDING THE OBJECTIVE TO FIGHT SERIOUS CRIME AND TERRORISM

The ECJ admitted on the one hand that fighting serious crime, in particular organized crime and terrorism, is of utmost importance for warranting public safety and that its effectiveness can to a high degree depend on the use of up-to-date investigation techniques. However, such objective serving the common well-being, can, fundamental as it may be, in itself not justify the need for a retention policy – as was provided for by the Directive – serving to fight crime.

Protecting the fundamental right of privacy requires in any case constant decision practice of courts to the effect that exceptions of protection of personal data and its limits are restricted to the absolute minimum necessary. The Directive, however, covered comprehensively all persons using electronic communication services, irrespective of whether such persons were involved in serious crime or not. Furthermore, the Directive did not provide for any exceptions for persons with "privileged" communication, as e.g. physicians or lawyers.

The ECJ took this up and argued that the Directive was too far-reaching targeting also people not even remotely connected to crime and in particular had not provided for any exceptions, so that it covered also persons whose communications are subject to professional secrecy according to national laws.

This general failure to define restrictions and exceptions resulted in the fact that in issuing the Directive EU legislation exceeded the admissible limits which it was to comply with in order to ensure the principle of proportionality.

IS THERE A POSSIBILITY FOR A NEW EU DIRECTIVE ON DATA RETENTION TO BE ISSUED?

It may be the end of European data retention regulations for the time being, but not necessarily forever as the ECJ did not declare data retention per se to be inadmissible and rejected only the directive as it was. If future EU legislation took into account the legal prerequisites set forth in the decision, the European legislator would be free, assuming respective political willingness, to issue a new regulation on data retention. However, as current public opinion stands, such new directive will likely not be on the immediate to-do list of European legislators.

Rainer Kaspar, a graduate of University of Michigan Law School, advises private and corporate clients, private equity firms and financial institutions in a wide range of matters. He particularly focuses on cross-border M&A, Financing and Capital Markets transactions. Rainer is a regular lecturer at seminars and conferences, including thoses sponsored by the IBA and AIJA and speaks German, English and French.

Hermann Hansmann, a graduate of University of Vienna, works in the field of public law, where he regularly advises clients regarding questions of environmental and facility law. He further focuses on Life Sciences. Among his other areas of activity are Data Protection/IT, Energy, PPP, Environment and Public Procurements. He speaks German and English.