[DE] Federal Constitutional Court Finds Data Retention Unconstitutional

IRIS 2010-4:1/12

Sebastian Schweda
Institute of European Media Law (EMR), Saarbrücken/Brussels

In a decision of 2 March 2010 on the implementation of the Data Retention Directive 2006/24/EC, the *Bundesverfassungsgericht* (Federal Constitutional Court - BVerfG) drew a temporary line under the debate on the constitutionality of the German implementing act.

The judges considered that the provisions of Art. 113a(1) and 113b(1) of the *Telekommunikationsgesetz* (Telecommunications Act - TKG) and Art. 100g of the *Strafprozessordnung* (Code of Criminal Procedure - StPO) infringed the privacy of telecommunications enshrined in Art. 10(1) of the *Grundgesetz* (Basic Law - GG). They declared the provisions invalid and ordered the immediate deletion of retained data. In so doing, the court imposed the severest available sanction against an unconstitutional legislative act.

The constitutional judges did not consider data retention without occasion, as described in the Directive, to be "absolutely incompatible" with Art. 10 GG and therefore did not have to comment on the awkward question of whether the Directive should apply with precedence over German constitutional law. However, under the principle of proportionality, it was necessary to take appropriate account of the particular extent of the intrusion on basic rights. Furthermore, such extensive levels of data retention should remain the exception. It should not lead, together with other files, to a record being kept of everything a citizen ever did. When considering new data retention obligations or entitlements, the legislature should therefore "show greater restraint in view of all the various data collections that already exist". The court also thought that the scope for further data retention without occasion at EU level was considerably reduced.

In concrete terms, the constitutional judges considered in particular that the provisions on data security, data use, transparency and legal protection were not sufficiently "sophisticated and well defined". For example, there were no specific security provisions taking into account the particularly serious intrusion on basic rights, but rather merely a reference to the care generally needed in the telecommunications sector. In principle, separate storage of data, sophisticated encryption, secure access procedures using the four-eyes principle, for example, and audit-proof recording were all necessary.

Concerning the use of data, the judges criticised the lack of an exhaustive list of criminal offences that would justify the retrieval of data for prosecution purposes. The act had only required a general suspicion that an offence of substantial weight had been committed. In addition, it allowed retained data to be retrieved for all offences committed "by means of telecommunications", regardless of the crime. The court considered this rule to be too broad and lacking in exceptional character.

In terms of warding off danger, the court ruled that there should at least be actual evidence of concrete danger to the life, limb or freedom of a person, to the existence or security of the Federal Republic or of a *Land*, or a need to ward off a common danger. The purposes laid down in Art. 113b TKG did not meet this requirement, since they were not sufficiently concrete. They created an open data pool that the police and intelligence services could access on the grounds of insufficiently defined objectives. The resulting loss of the connection between storage and the purpose of storage was incompatible with the Constitution.

For a narrow group of telecommunications connections that rely on particular confidentiality, such as anonymous telephone helplines, the transmission of data should also be prohibited.

Finally, the judges thought that transparency rules were insufficient to counteract the "diffuse sense of threat" created by data storage and to enable citizens to exercise their rights. In criminal prosecution, the use of data should and could normally be open. Where this was impossible, without frustrating the purpose of retrieval, as was generally the case for warding off danger, the person concerned should be informed subsequently. Exceptions to this required a judicial ruling. However, there was no provision for this in Art. 100g StPO.

Less stringent standards applied only to the indirect use of data to identify the owners of IP addresses, since the authority requesting the information did not itself retrieve the data, while the telecommunications company only used the data to identify the owner. An exhaustive list of criminal offences was therefore unnecessary in this regard. However, such information should not be obtained "at random", but only "on the basis of a sufficient initial suspicion or of a concrete danger on the basis of facts relating to the individual case".

Under the Directive, the legislature is now obliged to revise the implementing regulations. However, the day before the ruling was published, the Commission announced that it was reviewing the whole Directive and did not rule out a complete lifting of data retention obligations.

Urteil des BVerfG, Az. 1 BvR 256/08 vom 2. März 2010

http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.

html

Ruling of the Federal Constitutional Court, case no. 1 BvR 256/08 of 2 March 2010