B 4

The Constitutional Court decision of Germany regarding data retention (BVerfG, 1 BvR 256/08 of 2.March2010, para. 1-315)

The Constitutional Court of Germany decided that data retention for a period of six months for the prosecution of crime and warding off danger is not unconstitutional as such, although it interferes strongly with constitutional rights (particularly with Article 10.1 of the German Basic law (GG) which guarantees the secrecy of telecommunications).

Significant to justification of data retention and compatibility with the secrecy of telecommunications is – in addition to the fact, that the storage of communication data does not extend to the contents of the communications itself (such as in electronic eavesdropping cases were the content of the communication is fundamental) - the design of the provision. It can be described as a two-level procedure (zweistufiges Konzept) data retention and data access).

1. First Level: Data retention

First of all, the data is not directly retained by the state. Instead, economic operators are obliged to retain the data. The data is spread across a variety of economic operators and is not available to the state as a whole (this actually makes it difficult to trace a profile of individuals).

2. Second Level: Data Access

The access to retained data by public authorities - in a second step - occurs as soon as a suspicion arises (on occasional basis) and according to legally defined criteria.

Thus, this two-level procedure (data retention and data access) and its design are key elements of the judgment of the Constitutional Court. Only the design of the provisions access and the further use of the retained data (purpose limitation) will ensure that the retention of data is not for indefinite or not yet definable purposes[1].

[1] "Die Ausgestaltung der zum Abruf und zur weitern Verwendung der gespeicherten Daten ermächtigenden Bestimmungen kann dabei sicherstellen, dass die Speicherung nicht zu unbestimmten oder noch nicht bestimmbaren Zwecken erfolgt", BVerfG, 1 BvR 256/08 of 2.3.2010, para. 214.

Keeping this in mind, the provisions are not structured in a manner adapted to the principle of proportionality. The challenged provisions guarantee neither **adequate data security** nor an **adequate restriction of the purposes of use of the data**. Nor do they satisfy the constitutional requirements of **transparency** and **legal protection**. Articles 113a, 113b of the Telecommunications Act (TKG) and Article 100g of the Code of Criminal Procedure (StPO), insofar as the latter permits the retrieval of the data to be stored under Article 113a TKG, are therefore incompatible with the German Constitution and the rights of privacy, ensuring the "security and integrity" of communications by post and telephone which is laid down in Article 10.1 of the Basic Law.

The German case could have been tricky for the Data Retention Directive, but the German Constitutional Court upheld the EU directive, saying the problem lay instead with how the German Parliament chose to interpret it.

1. Data Security:

General requirements:
Data security is of great importance for the proportionality of the challenged provisions. There is a need for legislation which provides for a particularly high degree of security, whose essential provisions are at all events well-defined and legally binding. In this connection the legislature is free to entrust a regulatory agency with the technicalities of putting the prescribed standard into concrete terms. In this process, however, the legislature must ensure that the decision as to the nature and degree of the protective precautions to be taken does not ultimately lie without supervision in the hands of the respective telecommunications providers.
(BVerfG, 1 BvR 256/08 of 2 March 2010, para. 221-225)

In particular regarding the German law (Article 113a.10 TKG)

The necessary guarantee of a particularly high standard of data security is missing. The Act essentially refers only to the *care generally needed in the field of telecommunications* (Article 113a.10 TKG) and in doing so qualifies the security requirements in a way that remains undefined by introducing general considerations of economic adequacy in the individual case (Article 109. 2 sentence 4 TKG)[2]. Here, putting the measures in more specific terms is left to

[2] Die "im Bereich der Telekommunikation erforderliche Sorgfalt" ist weder in der Gesetzesbegründung noch in der Literatur hinreichend konkretisiert. In der Gesetzesbegründung steht lediglich, dass der "Verpflichtete die die zu speichernden Verkehrsdaten mit der Sorgfalt zu behandeln hat, die beim

the individual telecommunications service providers, which in turn have to offer the services subject to the conditions of competition and cost pressure. In this respect, the persons with a duty of storage are neither required in a manner that can be enforced to use the instruments suggested by the experts in the present proceedings to guarantee data security (separate storage, asymmetric encryption, the four-eyes principle in conjunction with advanced authentication procedures for access to the keys, audit-proof recording of access and deletion), nor is a comparable level of security otherwise guaranteed. Nor is there a balanced system of sanctions that attributes no less weight to violations of data security than to violations of the duties of storage themselves.
(BVerfG, 1 BvR 256/08 of 2 March 2010, para. 271-275)

2. Direct use of data

General requirements

A use of the data comes into consideration only for paramount tasks of the protection of legal interests (überragend wichtige Rechtsgüter).

The court differentiates the requirements for direct use of data for criminal proceedings and the direct use of data to ward off danger and for the tasks of the intelligence services.

In both cases however, the court judges that as a product of the principle of proportionality, it **is also constitutionally required** that there should be a fundamental prohibition of transmission of data, at least for a narrowly defined group of telecommunications connections which rely on particular confidentiality. These might include, for example, connections to persons, authorities and organisations in the social or ecclesiastical fields which offer advice in situations of emotional or social need, completely or predominantly by telephone, to callers who normally remain anonymous, where these organisations themselves or their staffs are subject to other obligations of confidentiality in this respect.[3]

Umgang mit vom Fernmeldegeheimnis geschützten Daten erforderlich ist" (BT-Drs. 16/5846,72). In der Literatur hingegen bedeutet dies eine Bekräftigung des einfachgesetzlichen Schutzes des Fernmeldegeheimnisses auf § 88 TKG. Weiterhin wird auf – bezüglich des erforderlichen Sicherheitsniveaus ebenfalls sehr offen gehaltenen – Vorschriften des § 109 TKG und des § 9 BDSG mit Anlage verwiesen. Beide Regelungen erklären Maßnahmen nur dann für erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Die besonders hohe Schutzbedürftigkeit der Vorratsdaten und das hohe Schadenspotential beim Abhandenkommen der Daten werden damit weder in der Gesetzesbegründung noch im Gesetz selbst deutlich gemacht.

[3] BVerfG, 1 BvR 256/08 of 2.3.2010, para. 238; the court refers here to Article 99.2 TKG. This issue is also raised by the European Federation of Journalists who claim that they will need a protection of theirs sources, because they fear that their resources will not contact them anymore.

(BVerfG, 1 BvR 256/08 of 2 March 2010, para. 226-238)

a. Direct use of data for criminal proceedings

General requirements

For the prosecution of crimes, there must at least be the suspicion of a serious criminal offence (schwere Straftat) , based on specific facts, that is serious even in an individual case. Together with the obligation to store data, the legislature must provide an exhaustive list of the criminal offences that are to apply here.
(BVerfG, 1 BvR 256/08 of 2 March 2010, para. 228-229)

In particular regarding the German law (Article 113b no. 1 TKG, Article 100 g StPO)

Article 100g.1 sentence 1 no. 1 StPO does not ensure that in general and also in the individual case only serious criminal offences may be the occasion for collecting the relevant data, but – independently of an exhaustive list – merely generally accepts criminal offences of substantial weight as sufficient. Article 100g.1 sentence 1 no. 2, sentence 2 StPO satisfies the constitutional standards even less, in that it accepts every criminal offence committed by means of telecommunications, regardless of its seriousness, as the possible trigger for data retrieval, depending on a general assessment in the course of a review of proportionality. This provision makes the data stored under Article 113a TKG usable with regard to virtually all criminal offences. As a result, in view of the increasing importance of telecommunications in everyday life, the use of these data loses its exceptional character. Here, the legislature no longer confines itself to the use of data to prosecute serious criminal offences, but goes far beyond this, and thus far beyond the objective of data storage specified by EU law.

Nor does Article 100g StPO comply with the constitutional requirements, in that it permits data retrieval not merely for individual cases to be sustained by a judge, but as a general rule even without the knowledge of the person affected (Article 100g.1 sentence 1 StPO).

In contrast, the judicial control of data retrieval and data use and the provisions for the duties of notification are essentially guaranteed in a manner that satisfies the constitutional requirements. Under Article 100g.2 sentence 1, Article 100b.1 sentence 1 StPO, the

collection of the data stored under Article 113a TKG requires a judicial order. In addition, under Article 101 StPO there are differentiated duties of notification and the possibility subsequently to arrange a judicial review of the lawfulness of the measure. It is not apparent that these provisions do not, as a whole, guarantee effective legal protection. However, the lack of judicial monitoring of a failure to inform under Article 101.4 StPO is constitutionally objectionable.
(BVerfG, 1 BvR 256/08 of 2 March 2010, para. 277-284)

b. Direct use of data to ward off danger and for the tasks of the intelligence services

General requirements

For warding off danger, it follows from the principle of proportionality that a retrieval of the telecommunications traffic data stored by way of precaution may only be permitted if there is a sufficiently evidenced concrete danger to the life, limb or freedom of a person, to the existence or the security of the Federal Government or of a *Land* (state) or to ward off a common danger. These requirements apply in the same way to the use of the data by the intelligence services, since this is also a form of prevention of danger. In fact, this also means that in many cases the intelligence services will probably not be able to use the data. However, this results from the nature of their tasks in advance intelligence and does not create a constitutionally acceptable occasion to relax the requirements for an encroachment of this kind that arises from the principle of proportionality.
(BVerfG, 1 BvR 256/08 of 2 March 2010, para. 230-231)

In particular regarding the German law (Article 113b Nos. 2, 3 TKG)

The very structure of Article 113b sentence 1 nos. 2 and 3 TKG does not satisfy the requirements of sufficient limitation of the purposes of use. In this provision, the Federal legislature contents itself with sketching in a merely general manner the fields of duty for which data retrieval in accordance with later legislation, in particular legislation of the *Länder*, is to be possible. By all means, it does not satisfy its responsibility for the constitutionally required limitation of the purposes of use. Instead, by giving the service providers a duty of precautionary storage of all telecommunications traffic data, at the same time combined with the release of these data to be used by the police and the intelligence services as part of virtually all their tasks, the Federal legislature creates a data pool open to diverse and unlimited uses to which – restricted only by broad objectives – the data can be accessed, in each case on the basis of decisions of the Federal and *Länder* legislatures. The supply of

such a data pool with an open purpose removes the necessary connection between storage and purpose of storage and is incompatible with the constitution.

The regulation on data processing of the data stored under Article 113a TKG is also disproportionate in that no protection of confidential relations is provided for the transmission. At least for a narrowly defined group of telecommunications connections which rely on particular confidentiality, such a protection is fundamentally required. [4]
(BVerfG, 1 BvR 256/08 of 2 March 2010, para. 285-287)

c. Indirect use of the data for information of the service providers

Although, there are no objections to the fact that Article 113b sentence 1 half-sentence 2 TKG permits information independently of a list of criminal offences or legal interests. However, constitutional compatibility is raised that such information is also made possible for the general prosecution of administrative offences (Ordnungswidrigkeiten), without further limitation. In addition, there are no duties of notification following the provision of such information.
(BVerfG, 1 BvR 256/08 of 2 March 2010, para. 288-291)

3. Transparency

The legislature must pass effective transparency provisions to counteract that an individual may establish a feeling of permanent control and diffuse threat.

As the matter of principle data retention and use of personal data must be open. However, the usage of data without the knowledge of the person affected may fulfil constitutional requirements, only if the purpose of the investigation would otherwise be hindered. The legislature may in principle assume that this is the case for warding off danger and carrying out the duties of the intelligence services.
In contrast, in criminal prosecution data may be retained and used openly (in most cases investigative measures are used openly and with the knowledge of the accused individual, see e.g. Article 102, 103, 106 StPO). There may only be a provision for secret use of the data here if such use is in the individual case necessary and a judicial order is supplied.

[4] This is the argumentation previously described and raised by the European Federation of Journalist.

In cases where data usage occurs secretly, the legislature must provide for a duty of subsequent information of the person affected of the data access. Exceptions to this require judicial scrutiny.
(BVerfG, 1 BvR 256/08 of 2 March 2010, para. 239-245)

4. Legal protection and sanctions

Data access and usage of retained data require the monitoring of an independent body, thus require a judicial authorization. A direct access by the state to the data is therefore avoided.
(BVerfG, 1 BvR 256/08 of 2 March2010, para. 247-250)

Persons, who were affected of data access and usage and did not have the opportunity to defend themselves against it beforehand [e.g. in cases of warding off danger], must have the opportunity of subsequent judicial control. (BVerfG, 1 BvR 256/08 of 2 March 2010, para. 251)

As a principle of proportionality effective sanctions are obligatory in cases of violation of fundamental rights (e.g. serious breaches of the secrecy of telecommunications in the case were retained data was used unauthorized). This emphasizes the duty of the state to enable individuals to develop their personality and to protect them against third-party threats to the right of personality. However, there is a marked scope for the design and the legislature may also take into account that the already existing law may already consider this (e.g. the exclusion of evidence which was acquired in a manner that breaches a persons constitutional rights – "fruit of the poisonous tree doctrine"). (BVerfG, 1 BvR 256/08 of 2 March 2010, para. 252-253)

5. Retention Period

The court found that a six month period is legitimate. Despite the remarkable width, such a measure is effective and time-limited. The content of the telecommunication data is excluded. The retention period is time-limited. Considering the scope and the significance of the retained data the period of the six months lies in the upper limit of what is justifiable under the principle of proportionality. After the expiry of the retention period of six months the individual can rely on that the retained data will be deleted und cannot be reconstructed from anybody, unless there was an exceptional reason for accessing such data. (BVerfG, 1 BvR 256/08 of 2 March 2010, para. 215)

7. Quick-Freeze

Of particular interest is the decision of the Constitutional Court, that the legislator may judge a six month data retention of telecommunication traffic data as necessary. Less restrictive measures, which also enable a wide-ranging clarification of criminal offences, are not apparent. A comparable effective clarification possibility is particularly not seen in the so called "Quick-Freeze Model", where in place of a general and without suspicion based retention of telecommunications data a preservation per-incident and only from the time suspicion arises is ordered. Such a procedure, which can only capture data from the time a preservation order is issued if the data is still available, is not as effective as a continuous retention, which ensures the existence of a complete data set for the past six months"[5].

8. Requirements for IP Addresses

Less stringent constitutional standards apply to an indirect use of retained data, in form of official rights to be informed by the service providers regarding the owners' particular IP addresses which are already known.

Particularly of importance is that authorities neither get access to the retained data nor any information of the retained data. Instead, authorities only identify the subscriber (name and address) of a particular known IP address, which is determined by the service providers through using retained data (formally this is comparable to a request of a telephone number).

A systematic investigation over a long period of time, creating personality profiles and track people's movements on the basis of such information is not possible.

Since for such information only a small section of the retained data, which is determined in advance, is used, the retention of this particular data is not a serious encroachment in itself. It could therefore be ordered under far less strict requirements.

---

[5] BVerfG, 1 BvR 256/08 of 2 March 2010, para. 208 ""Der Gesetzgeber darf eine sechsmonatige Speicherung der Telekommunikationsverkehrsdaten auch als erforderlich beurteilen. Weniger einschneidende Mittel, die ebenso weitreichende Aufklärungsmaßnahmen ermöglichen, sind nicht ersichtlich. Eine vergleichbar effektive Aufklärungsmöglichkeit liegt insbesondere nicht im sogenannten Quick-Freezing-Verfahren, bei dem an die Stelle der anlasslos-generellen Speicherung der Telekommunikationsdaten eine Speicherung nur im Einzelfall und erst zu dem Zeitpunkt angeordnet wird, zu dem dazu etwa wegen eines bestimmten Tatverdachts konkreter Anlass besteht. Ein solches Verfahren, das Daten aus der Zeit vor der Anordnung ihrer Speicherung nur erfassen kann, soweit sie noch vorhanden sind, ist nicht ebenso wirksam wie eine kontinuierliche Speicherung, die das Vorhandensein eines vollständigen Datenbestandes für die letzten sechs Monate gewährleistet. "

The identification of IP addresses is still of considerable weight, bearing in mind that with the officials' right to be informed, the legislator is interfering with the communication conditions of the internet and restricting the anonymity of such environment (in that case a direct line between a request of a telephone number cannot be drawn).

The legislator may allow such requests to identify IP addresses regardless of a specific list of criminal offences or protected rights for the prosecution of crime, for warding off danger or for the performance of duties of the intelligence services on the basis of the special legislative authorization to encroach.

However, it must be ensured that indiscriminate investigation is not possible and permitted. Instead, a sufficiently evidenced initial suspicion or a concrete danger on the basis on specific facts in the individual case is required.
For such information, a judicial order is not necessary; however, the legislature must provide for a duty of subsequent information of the person affected of the data access. The rules of transparency are to be obeyed.
Such information may also not be admitted generally and without restriction to the prevention or prosecution of any administrative offences. The abolition of anonymity in the internet needs at least a breach of legally protected interest, which the legal system placed special emphasis to. This does not completely preclude such information for the prevention or prosecution of administrative offences. But they must be administrative offences that are particularly serious – even in an individual case – and they must be expressly named by the legislature.
(BVerfG, 1 BvR 256/08 of 2 March 2010, para. 254-263)