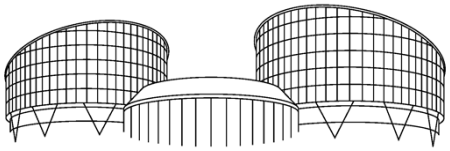

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FIFTH SECTION

CASE OF BREYER v. GERMANY

(Application no. 50001/12)

JUDGMENT

Art 8 • Respect for private life • Legal obligation on service providers to store personal data of users of prepaid mobile telephone SIM cards and make them available to authorities upon request • Interference concerning limited data set • Data retrieval by authorities accompanied by adequate safeguards • Impugned storage proportionate to legitimate aims of protecting national security and fighting crime

STRASBOURG

30 January 2020

FINAL

07/09/2020

This judgment has become final under Article 44 § 2 of the Convention. It may be subject to editorial revision.

In the case of Breyer v. Germany,

The European Court of Human Rights (Fifth Section), sitting as a Chamber composed of:

Yonko Grozev, *President,*
Angelika Nußberger,
Síofra O'Leary,
Carlo Ranzoni,
Mārtiņš Mits,
Lətif Hüseynov,
Lado Chanturia, *judges*,
and Claudia Westerdiek, *Section Registrar*,

Having deliberated in private on 3 December 2019,

Delivers the following judgment, which was adopted on that date:

PROCEDURE

1. The case originated in an application (no. 50001/12) against the Federal Republic of Germany lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by two German nationals, Mr Patrick Breyer and Mr Jonas Breyer ("the applicants"), on 27 July 2012.

2. The German Government ("the Government") were represented by their Agents, Mr H.-J. Behrens and Ms K. Behr of the Federal Ministry of Justice and Consumer Protection.

3. The applicants complained under Articles 8 and 10 that, as users of prepaid mobile phone SIM cards, certain personal data had been stored by their respective service providers owing to the legal obligation provided by section 111 of the Telecommunications Act.

4. On 21 March 2016 the Government were given notice of the application.

5. Written submissions were received from Privacy International and ARTICLE 19, which had been granted leave by the Vice-President to intervene as third parties (Article 36 § 2 of the Convention and Rule 44 § 2 of the Rules of Court).

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

A. Background to the case

6. The applicants were born in 1977 and 1982 respectively and live in Wald-Michelbach. Both applicants were involved in a civil-liberties union which campaigned against the general retention of telecommunications data. In that context both applicants organised public protests and published articles criticising State surveillance. The first applicant was also a member of the Parliament of Schleswig-Holstein.

7. In June 2004 a legal obligation for telecommunications providers to store personal details of all their customers, even of customers where such details were not necessary for billing purposes or other contractual reasons (prepaid ("pay-as-you-go") mobile telephone SIM cards), was introduced via amendments to the Telecommunications Act (*Telekommunikationsgesetz*). Until these amendments came into force, telecommunications service providers had been entitled solely to collect and store the data necessary for their contractual relationship. Where prepaid mobile telephone SIM cards were concerned, no such data had been considered necessary. These amendments were made in the framework of a fundamental revision of the Telecommunications Act which was felt necessary after the adoption of five EU Directives on 7 March and 12 July 2002 which had to be transposed into German Law before July and October 2003.

8. Both applicants use prepaid mobile phone SIM cards and had to register under section 111 of the Telecommunications Act (see paragraph 27 below) certain personal details with their respective service providers when activating those SIM cards.

B. Proceedings before the Federal Constitutional Court

9. On 13 July 2005 the applicants lodged a constitutional complaint against, amongst other provisions, sections 111, 112 and 113 of the Telecommunications Act. Section 111 of this Act introduced the obligation to collect and store the telephone numbers, the name, address and date of birth of an allocation holder and the effective date of the contract (see paragraphs 27-28 below). Sections 112 and 113 of the Telecommunications Act contained an automated and a manual procedure for accessing the data stored under section 111 (see paragraphs 29 and 31 below). The applicants argued that the above-mentioned sections violated their right to privacy of correspondence, post and telecommunications as well as their right to

informational self-determination (*Recht auf informationelle Selbstbestimmung* – see paragraph 25 below).

10. Section 111 of the Telecommunications Act was amended by an Act of 21 December 2007 by which other identifiers of an allocation were included under the obligation to store subscriber data and the data to be stored were expanded to include the respective device number, in cases in which a mobile-communication end device was made available together with the mobile-communication allocation.

11. The applicants extended their pending constitutional complaint to include the amended version of the Telecommunications Act. Consequently, the Federal Constitutional Court considered in its judgment the Telecommunications Act as in force on 1 January 2008.

C. Decision of the Federal Constitutional Court (no. 1 BvR 1299/05)

12. On 24 January 2012 the Federal Constitutional Court decided, in so far as relevant for the present case, that sections 111 and 112 of the Telecommunications Act were compatible with the Basic Law (*Grundgesetz*), that section 113(1), sentence 1, was compatible with the Basic Law when interpreted in conformity with it, and that sections 112 and 113 required independent enabling legislation for the retrieval of data by the authorities listed or referred to therein (see paragraphs 29 and 31 below). Concerning the parts of the applicants' constitutional complaint that are not at issue in the present proceedings, the Federal Constitutional Court held that the manual information procedure set out in section 113(1) could not be used for the assignment of dynamic IP addresses and that the security authorities could only request information on access codes under section 113(1) if the statutory requirements for their use were satisfied.

13. It also noted that according to the federal government, the automated retrieval procedure under section 112 of the Telecommunications Act was of primary importance. Experience had shown that the number of manual retrievals carried out under section 113 of the Telecommunications Act was between 3% and 5% of the number of automated requests made under section 112 of the Telecommunications Act.

14. As regards the relevant parts of the applicants' constitutional complaint, the Federal Constitutional Court first held that the provisions being challenged interfered with the right to informational self-determination. It further stated (as translated into English on the Federal Constitutional Court's website; references to the court's jurisprudence have been omitted in the quotes below) as follows:

> "122. a) The right to informational self-determination takes account of endangerments and violations of personality which arise in the conditions of modern data processing from information-related measures. The free development of personality presupposes the protection of the individual against unrestricted

collection, storage, use and transmission of the individual's personal data. This protection is therefore covered by the fundamental right of Article 2(1) in conjunction with Article 1(1) of the Basic Law. In this respect, the fundamental right guarantees the authority of the individual in principle himself or herself to decide on the disclosure and use of his or her personal data. The guarantee of the fundamental right takes effect in particular when the development of personality is endangered by government authorities using and combining personal information in a manner which persons affected can neither fully appreciate nor control. The extent of protection of the right to informational self-determination is not restricted to information which by its very nature is sensitive and for this reason alone is constitutionally protected. In view of the possibilities of processing and combining, there is no item of personal data which is in itself, that is, regardless of the context of its use, insignificant. In particular, the protection of informational self-determination also includes personal information on the procedure by which telecommunications services are provided.

123. Provisions which give authority for government authorities to deal with personal data as a rule create a number of encroachments which build on each other. In this respect, a distinction must in particular be made between the collection, storage and use of data. In legislating for data exchange for the purpose of the performance of government duties, however, a distinction must also be made between data transfer by the party supplying the information and data retrieval by the agency seeking the information. A data exchange takes place through the encroachments of retrieval and transfer, which correspond to each other and each of which requires an independent legal basis. Figuratively speaking, the legislature must open not only the door for the transmission of data, but also the door for their retrieval. It is only both legal bases together, which must operate together like a double door, which give authority to exchange personal data. This does not exclude – subject to the system of competencies and the requirements of clear drafting – the possibility of both legal bases being contained in one provision.

124. b) The challenged provisions encroach upon the complainants' fundamental right to informational self-determination. Firstly, there are encroachments upon the duty of collection and storage of [section 111 of the Telecommunications Act]. There are independent further encroachments upon fundamental rights by the duty of service providers laid down in [section 112(1) of the Telecommunications Act] to make the data available as customer databases which can be accessed in an automated procedure and by the authority of the Federal Network Agency to retrieve these data and to transmit them to particular authorities (see [section 112(4) of the Telecommunications Act]). Accordingly, [section 113(1), sentences 1 and 2, of the Telecommunications Act] create independent encroachments upon fundamental rights by imposing on the telecommunications service providers a duty to provide information on demand with regard to the data stored by themselves.

125. Finally, [sections 112 and 113 of the Telecommunications Act] are subject to prior retrieval of the data by the authorities entitled to retrieve, in the form of a request ([sections 112(1), 112(2) and 112(4) of the Telecommunications Act]) or a demand ([section 113(1) of the Telecommunications Act]); this constitutes an independent encroachment which must be distinguished from the foregoing. But under the legislature's legislative concept, this also requires a further legal basis, which must be contained in federal or *Land* legislation, depending on the area involved. The provisions of [sections 112 and 113 of the Telecommunications Act] – corresponding to the distinction between collection and transmission in the legislative typology of the data protection Acts – are to be understood solely as the legal basis for the

transmission. They presuppose that the authorities entitled to receive information have independent powers of collection ..."

15. In connection with section 111 of the Telecommunications Act the Federal Constitutional Court held that the obligation to maintain a database for subscriber information pursued the legitimate aim of, in particular, criminal prosecution. Even though the database constituted a precautionary collection and storage of a great range of data and criminal offenders would still be able to circumvent the provision by using telecommunications services anonymously, under false names or with mobile-telephone cards acquired from third parties, the interference with the right to informational self-determination was ultimately justified owing to the relatively restricted nature of the information stored.

16. Concerning proportionality, the Federal Constitutional Court stated, *inter alia*:

"136. [Section 111 of the Telecommunications Act] does not violate the requirements of proportionality in the narrow sense. Even if the provision orders a precautionary collection and storage, without occasion, of a great range of telecommunications data, in view of the relatively restricted information content of the collected data this is an encroachment of limited weight.

137. However, the encroachment is non-trivial. It has weight in so far as [section 111 of the Telecommunications Act] makes it possible to attribute telecommunications numbers and subscribers almost completely for all telecommunications services and for this purpose individualising data such as address, date of birth and date when the contract commences are recorded and kept available by the government. The data form a general basis for information and fulfil the function of a telecommunications number register. As a rule, they make it possible to obtain all the telecommunication numbers of any person; conversely, virtually every telecommunications event for which a telecommunications number is determined may also be attributed to a connection and thus to a subscriber. As data which relate to the fundamental elements of telecommunications events they are therefore associated with particularly protected information relationships whose confidentiality is essential for a free order. In addition, the corresponding data are collected and stored without cause by way of precaution in order to make them available for the performance of government duties.

138. Nevertheless, the encroachment constituted by this is not of very great weight. In particular, the fact that the data are collected by way of precaution does not give the procedure a very great weight. For even if [section 111 of the Telecommunications Act] has a great range, the encroachment is restricted in substance to narrowly restricted data which in themselves give no evidence as to the specific activities of individuals and whose use the legislature has restricted to purposes defined in more detail. In such cases, even a precautionary storage is not automatically a particularly serious encroachment for the mere reason that it is carried out without occasion. Admittedly, the precautionary storage of data must always remain an exception to the rule and needs to be justified. But it is not excluded from the outset that precautionary data collections may be justified as the basis of the performance of a variety of government duties, such as are currently familiar in the form of the register of residents or, in the field of motor vehicles, in the form of the Central Vehicle Register ... and the Central Register of Driving Licences ...

139. The data covered by [section 111 of the Telecommunications Act] have limited probative value. They merely make it possible for telecommunications numbers to be individually attributed to the respective subscribers and thus to those numbers' potential (and typical) users. These data contain no more detailed private information. In a fundamentally different way than in the case of precautionary storage of all telecommunications traffic data, neither do these data as such contain highly personal information, nor is it possible to use them to create personality profiles or track users' movements. ...

140. Nor does a particular weight of the encroachment result from the fact that the data of [section 111 of the Telecommunications Act], taken in context, permit individual telecommunications events known to the authorities to be attributed and thus in certain circumstances make it possible to obtain individualised knowledge of their circumstances or their content. For in this way all that is made possible from the outset is the investigation of individual events where required by a specific case. In these cases, the authority already knows the circumstances or the content of the telecommunications event which is to be individualised with the data of [section 111 of the Telecommunications Act], whether because the authority has found them by investigation within its own competence – for example on the basis of § 100g of the Code of Criminal Procedure ... – involving encroachment upon the secrecy of telecommunications, whether because it has learnt of them through its own observations or from third-party information without such an encroachment. In the same way, conversely, no particular weight of the encroachment results from the fact that a retrieval of telecommunications numbers may be followed by further measures which in certain circumstances may entail serious encroachments, including encroachments upon the secrecy of telecommunications. For such further encroachments are only permissible under independent legal bases, which must take account of the weight of the encroachment in question.

141. The possibility of attribution of the data collected in [section 111 of the Telecommunications Act] serves the effective performance of the duties of the authorities defined in more detail in the provisions on use. It is constitutionally justified by the fact that the State may have a legitimate interest in successfully investigating particular telecommunications events if occasion arises, and this interest in the performance of particular tasks may have considerable weight, in individual cases even pre-eminent weight. It may not be cited in opposition to this that direct communication without means of telecommunications has no comparable encroachments. For the situation in that case is different. Because direct communication does not resort to technical means of communication which make it possible, without public observation, to interact over any distance in real time, it has no comparable basis, nor is there a comparable necessity for such a register. The traditional powers of investigation, for example the examination of witnesses or the seizure of documents, are more useful for clarification here than they are with regard to communication by means of electronic services. However, it is correct that even the possibilities of the modern means of telecommunications provide no justification for registering, if possible, all activities of citizens by way of precaution and making them basically reconstructible in this way. But there is no question of this when a register of telecommunications numbers is established, even when account is taken of the interaction with other available data."

17. With regard to section 112 of the Telecommunications Act, the Federal Constitutional Court clarified (paragraph 144) that this provision

"governs the use of the data stored under [section 111 of the Telecommunications Act] in the form of an automated information procedure in which the Federal Network Agency [*Bundesnetzagentur*] is to transmit the data on request to particular authorities named in [section 112(2) of the Telecommunications Act]. The provision is the legal basis only for the duty to make the data available as customer databases, for access to and transmission of these data, but not also for the retrieval in the form of a request from the authorities entitled to receive information."

However, according to the court, a general entitlement to collect data could be sufficient for a request by the entitled authorities. In this connection the court used the analogy of a double door (see paragraph 123, cited in paragraph 14 above), stating that, while section 112 of the Telecommunications Act opened the door for transmission, it did not open the door for data collection by the specialised authorities.

18. Nonetheless, the Federal Constitutional Court held that – for several reasons – the interference provided for by section 112 of the Telecommunications Act was considerably weighty:

"156. However, the provision acquires a considerable weight of encroachment from the fact that [section 111 of the Telecommunications Act] very much simplifies data retrievals. The procedure, which is centrally organised and automated, permits an access which largely removes practical difficulties of data collection and makes the data of the persons affected available without delay or attrition in the form of requirements of review. In addition, the information is given without telecommunications enterprises or other third parties becoming aware of this. Admittedly, the fact that the issuing of information is not noticed by the telecommunications enterprise ensures discretion for the persons whose data are involved; but at the same time, this means that the encroachments lack the effects of restraint and control which are entailed by observation by third parties. In addition, a legal review by the Federal Network Agency, which transmits the data, is only made if there is a particular occasion for this (see [section 112(4), sentence 2, of the Telecommunications Act]). Since the retrieving authority does not have to give reasons for its request, however, such an occasion will scarcely ever arise.

157. Weight also attaches to the fact that the legislature has drafted the purposes of the data very broadly. The data may generally be transmitted to the authorities named in [section 112(2) of the Telecommunications Act] for the performance of their statutory duties. This is restricted only for the law enforcement authorities under [section 112(2), no. 2, of the Telecommunications Act], and under [section 112(2), nos. 3 and 7, of that Act] for the customs authorities named there. But it is important in this connection that data may be issued to the former, under [section 112 of the Telecommunications Act], only for purposes of warding off danger, which excludes mere risk precaution. In connection with the respective duties of the authorities entitled to retrieve, the information duties of the Federal Network Agency are also not very restricted. In particular, there are no strict encroachment thresholds in the statute; instead, the duty of information is opened in full to the respective competence of the authorities. However, the fact that information may only be given in so far as it is necessary for the performance of the duty does create an objectively limiting factor. This ensures that retrievals are not casually permitted for mere guidance in advance but only when information actually needed for the performance of duties cannot be obtained more easily but equally effectively in another way.

...

163. However, [section 112 of the Telecommunications Act] does not in fact restrict information to retrievals which are legitimised by specific legal bases relating to the automated information procedure, but also accepts requests which are based on simple powers of data collection. As a result, there is no requirement on the non-constitutional level for the entitled authorities to be expressly specified over and above [section 112(2) of the Telecommunications Act] and for further conditions for data retrieval which are to be observed. ...”

19. The Federal Constitutional Court nevertheless concluded that section 112 of the Telecommunications Act was proportionate:

“155. [Section 112 of the Telecommunications Act] satisfies the requirements of the principle of proportionality. The provision serves to increase the effectiveness of the performance of their duties by the authorities named in [section 112(2) of the Telecommunications Act] and it is suitable and necessary for this. It is also proportionate in the narrow sense.

...

158. Despite the fact that the weight of the encroachment is considerable, the provision is proportionate. The authorities entitled to retrieve are at least limited in number. The purposes for which they are given information under [section 112(2) of the Telecommunications Act] are central duties relating to the guarantee of security. In view of the increasing importance of electronic means of communication and the concomitant changes of human communication behaviour in all areas of life, the authorities here depend to a great extent on a possibility which is as uncomplicated as possible of being able to attribute telecommunications numbers individually. In this respect, it is a decision of the legislature which is constitutionally unobjectionable if it permits the transmission of these data in order to investigate criminal offences and dangers, to observe developments which endanger the Constitution in order for the government and the public to be informed or to give assistance in emergencies. Because such investigations must often be carried out rapidly and without the knowledge of those affected, an automated information procedure is of particular importance for them. Increasing the effectiveness of the work of the courts is also a concern whose weight is supported by such a provision.

159. The limited probative value of the data is of central importance for the weighing of interests: They provide information solely on the attribution of individual telecommunications numbers to their subscriber. Even if, in specific collection contexts, sensitive information may result from them, the information content of this information as such remains limited and in addition depends on further investigations whose lawfulness is to be evaluated under different provisions.

...

163. ... Since the subject here is the transmission of data by an authority and the substantive conditions for this, including those with regard to the persons whose data are involved, are laid down definitively and with sufficient clarity [in section 112 of the Telecommunications Act], then, taking account of the limited weight of encroachment of the provision, this is compatible with the principle of proportionality and corresponds to the structure of the provisions on the automated retrieval of vehicle and vehicle owner data from the vehicle register ... and the provision on data transmission in the law relating to the registration of residents ... . Admittedly, this does not change the responsibility of the legislature – and in this connection, where applicable, of the *Länder* – for the constitutional formulation of the data collection provisions, which are not themselves the subject of the present proceedings. ...”

In addition, the court emphasised the responsibility of the public authorities to apply these provisions in such a way that specific account was taken of the requirements of section 112(1) and (2) of the Telecommunications Act and in particular of the requirement that collection had to be necessary even in an individual case, and of the further requirements of the principle of proportionality.

20. In respect of section 113 of the Telecommunications Act, the Constitutional Court held that the provision could only be understood as a release provision and that an additional legal basis for the retrieval of data by the authorities was required. The court also noted that there was no limitation regarding the requesting authority – except in relation to the authorities' duties – and that the purposes for data retrieval were stated in broad terms. It concluded, nonetheless, that, in view of the information from the data in question, which in itself was limited, and their great importance for an effective performance of duties, the reach of this provision was constitutionally unobjectionable.

21. The Federal Constitutional Court stated, *inter alia*:

> "176. However, [section 113(1), sentence 1, of the Telecommunications Act] opens the manual information procedure very wide. It permits information for the purpose of warding off dangers, prosecuting criminal offences or regulatory offences and performing intelligence duties. In this connection, the provision is also given no specific thresholds of encroachment which define its scope in more detail. Instead, it always permits information in the individual case if this is necessary to perform the above duties.
>
> 177. However, in view of the information content of the data in question, which in itself is limited, and their great importance for an effective performance of duties, the reach of this provision is constitutionally unobjectionable. In this connection, account must be taken of the fact that it by no means permits information to be given indiscriminately. On the contrary, there is a restrictive effect in the fact that information under [section 113(1), sentence 1, of the Telecommunications Act is] called for in the individual case and must be necessary. In relation to warding off danger, which the legislature has expressly not defined as including risk precaution, a prudent interpretation reveals that a 'concrete danger' within the meaning of the 'general clauses' [*Generalklauseln*] of police law is a requirement for such information. Admittedly, this threshold is low and also admits the suspicion of dangers. Equally, it does not in advance restrict information to persons endangering public security within the meaning of general police and regulatory law. However, this does not relieve it from restriction to such an extent as to be disproportionate in view of its limited weight of encroachment. In particular it does not enable information as a general means for lawful administrative enforcement, but in the individual case it requires the duty in question to have a security-law character. It is true that in regard to the intelligence services, which in general act in advance, irrespective of concrete dangers, there is no comparable threshold of encroachment. But this is justified by the restricted duties of the intelligence services, which are not directly aimed at police measures, but only at a duty to provide reports to the politically responsible State bodies or to the public. Apart from this, it follows here too from the requirement of necessity in the individual case that information under [section 113(1), sentence 1, of the Telecommunications Act] must be required in order

to successfully investigate a particular action or group which requires observation by the security authorities. In so far as information relates to the prosecution of criminal offences and regulatory offences, the requirement of necessity in an individual case means that there must at least be an initial suspicion.

178. Taken together, these thresholds are not high, but they are constitutionally acceptable. In this connection, it must be taken into account in comparison to [section 112 of the Telecommunications Act] that a manual information procedure entails certain procedural efforts on the part of the retrieving authority, which is likely to encourage the authority to obtain the information only where it is sufficiently needed."

22. Regarding legal remedies against information requests under sections 112 and 113 of the Telecommunications Act, the Federal Constitutional Court held:

"186. ... Nor are there objections to the fact that in view of the slightness of the encroachment no specific proceedings of legal redress are intended against information under [sections 112 and 113 of the Telecommunications Act]. Legal redress in this connection may be sought under general rules – in particular together with legal redress proceedings against the final decisions of the authorities.

187. The requirements of the principle of proportionality do not give rise to a blanket requirement for the persons affected by the information to be notified of the information under [sections 112 and 113 of the Telecommunications Act], ..."

23. In its decision the Federal Constitutional Court established that 26.6 million data sets – either subscriber identity or telephone number – had been queried in 2008 under section 112 of the Telecommunications Act. That figure did not differentiate between data sets relating to pay-as-you-go mobile-telephone users and other customers.

II. RELEVANT DOMESTIC LAW AND PRACTICE

A. The Basic Law

24. The provisions of the Basic Law, in so far as relevant for the present case, read:

Article 1

"1. Human dignity shall be inviolable. To respect and protect it shall be the duty of all State authority. ..."

Article 2

"1. Every person shall have the right to free development of his personality in so far as he does not violate the rights of others or offend against the constitutional order or the moral law. ..."

Article 10

"1. The privacy of correspondence, post and telecommunications shall be inviolable.

2. Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a *Land*, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature."

25. In its judgment of 15 December 1983 (nos. 1 BvR 209, 269, 362, 420, 440, 484/83) the Federal Constitutional Court established the right to informational self-determination and held:

"In the context of modern data processing, the protection of the individual against unlimited collection, storage, use and disclosure of his or her personal data is encompassed by the right to protection of personality rights under Article 2 § 1 in conjunction with Article 1 of the Basic Law. This basic right warrants in this respect the capacity of the individual to determine in principle the disclosure and use of his or her personal data."

26. In its judgment of 2 March 2010 (nos. 1 BvR 256, 586, 263/08) the Federal Constitutional Court decided upon the constitutionality of provisions transposing EU Directive 2006/24/EC (see paragraphs 49-50 below) into German law (sections 113a and 113b of the Telecommunications Act and Article 100g of the Code of Criminal Procedure), which obliged service providers to store for a limited time (six months) all traffic data of telephone services and allowed the use of such data in the context of criminal prosecutions. The court declared section 113a of the Telecommunications Act (obligation to store) unconstitutional and void, owing to a violation of the right to protection of the secrecy of telecommunications. It held that a duty of storage to the extent provided was not automatically unconstitutional at the outset. However, it was not structured in a manner adapted to the principle of proportionality. The challenged provisions guaranteed neither adequate data security nor an adequate restriction of the purposes of use of the data. Nor did they in every respect satisfy the constitutional requirements of transparency and legal protection.

B. Telecommunications Act

27. Section 111 of the Telecommunications Act obliges service providers to collect and store certain personal data of their customers. It thereby creates the basis for information requests under sections 112 and 113 of the Telecommunications Act. It read, at the relevant time and in so far as relevant, as follows:

"(1) Any person commercially providing or assisting in providing telecommunications services and in so doing allocating telephone numbers or

providing telecommunications connections for telephone numbers allocated by other parties or other identifiers of the respective allocation, is, for the information procedures under sections 112 and 113, to collect, prior to activation, and store without undue delay:

1. The telephone numbers and other identifiers of the respective allocation;

2. The name and address of the allocation holder;

3. The date of birth in the case of natural persons;

4. In the case of fixed lines, additionally the address for the line;

5. In cases in which a mobile-communication end device is made available together with the mobile-communication allocation, also the device number of the device in question, as well as;

6. The effective date of the contract.

Even if such data are not necessary for operational purposes; where known, the date of termination of the contract is likewise to be stored. Sentence 1 also applies where the data are not included in directories of subscribers. ... A person with obligations under sentence 1 or sentence 3 receiving notice of any changes is to correct the data without undue delay; in this connection the person with obligations under sentence 1 is subsequently to collect and store data not yet recorded if collecting the data is possible with no special effort. The manner in which data for the information-retrieval procedure provided for under section 113 are stored is optional.

(2) Where the service provider in accordance with subsection (1), sentence 1 or sentence 3, operates in conjunction with a sales partner, such a partner shall collect data according to subsection (1), sentences 1 and 3, under the pre-requisites set out therein and shall transmit to the service provider, without undue delay, these and other data collected under section 95; subsection (1), sentence 2, applies accordingly. Sentence 1 also applies to data relating to changes, inasmuch as the sales partner receives notice of them in the course of normal business transactions.

(3) Data within the meaning of subsection (1), sentence 1 or sentence 3, need not be collected subsequently for contractual relationships existing on the date of entry into force of this provision, save in the cases referred to in subsection (1), sentence 4.

(4) The data are to be erased upon expiry of the calendar year following the year in which the contractual relationship ended.

..."

28. In July 2016 section 111 of the Telecommunications Act was amended and an obligation for service providers to verify prior to collection the personal data of the mobile-telephone user was included. Presentation of an identity card, a passport or other official identity document is required when the data are being registered initially. The amendment had been considered necessary to further restrict the possibilities available for circumventing the obligations laid down in section 111 of the Telecommunications Act. According to the preparatory work of the amendment (Publication of the Federal Parliament (*Bundestagsdrucksache*) no. 18/8702, p. 22), a considerable amount of false data had been found in the telecommunications providers' databases, which had the character of a

mass phenomenon. Requests of the relevant authorities pursuant to sections 112 and 113 of the Telecommunications Act had therefore in many procedures not resulted in useful information being provided. A constitutional complaint challenging the compatibility of this amendment with the Basic Law is currently pending before the Federal Constitutional Court (no. 1 BvR 1713/17).

29. Section 112 of the Telecommunications Act sets out an automated procedure for the data stored under section 111 of the Telecommunications Act. In accordance with this procedure, providers of telecommunications services must supply the data in such a way that they can be retrieved by the Federal Network Agency without the knowledge of the providers. Moreover, the possibility of data retrieval using incomplete search data or a search with a similarity function must be provided. The relevant parts of section 112 of the Telecommunications Act read at the relevant time:

> "(1) Any person providing publicly available telecommunications services shall store, without undue delay, data collected under section 111(1), sentences 1, 3 and 4, and subsection (2) in customer data files .... The obligated person shall ensure that:
>
> 1. the Federal Network Agency is enabled, at all times, to retrieve data from customer data files by way of automation within Germany;
>
> 2. data can be retrieved using incomplete search data or searches made by means of a similarity function.
>
> The obligated person and his agent are to ensure by technical and organisational measures that no retrievals can come to their notice. The Federal Network Agency may retrieve data from customer databases only to the extent that knowledge of the data is necessary:
>
> 1. in order to prosecute administrative offences under the present Act or under the Unfair Competition Act [*Gesetz gegen den unlauteren Wettbewerb*];
>
> 2. in order to process requests for information lodged by the bodies set out in subsection (2).
>
> The requesting body shall verify without undue delay to what extent it needs the data transmitted in response to its request and shall erase any data it does not need without undue delay; this shall also apply to the Federal Network Agency regarding the retrieval of data in accordance with sentence 7, no. 1.
>
> (2) Information from the customer data files according to subsection (1) shall be provided to:
>
> 1. the courts and criminal prosecution authorities;
>
> 2. Federal and *Land* law-enforcement authorities for purposes of averting danger;
>
> 3. the Customs Criminal Investigations Office [*Zollkriminalamt*] and customs investigation offices [*Zollfahndungsämter*] for criminal proceedings and the Customs Criminal Investigations Office for the preparation and execution of measures under section 23a of the Customs Investigation Service Act [*Zollfahndungsdienstgesetz*];
>
> 4. Federal and *Land* offices for the protection of the Constitution, the Federal Armed Forces Counter-Intelligence Office, and the Federal Intelligence Service;

5. the emergency service centres under section 108 and the service centre for the maritime mobile emergency number '124 124';

6. the Federal Financial Supervisory Authority; and

7. the authorities of the customs administration for the purposes listed in section 2(1) of the Undeclared Work Act [*Schwarzarbeitsbekämpfungsgesetz*] via central enquiries offices

as stipulated in subsection (4), at all times, as far as such information is needed to discharge their legal functions and the requests are submitted to the Federal Network Agency by means of automated procedures.

...

(4) At the request of the authorities referred to in subsection (2), the Federal Network Agency is to retrieve and transmit to the requesting authority the relevant data sets from the customer data files in accordance with subsection (1). It shall examine the admissibility of the transmission only where there is special reason to do so. Responsibility for such admissibility lies with:

1. the Federal Network Agency, in the cases governed by subsection (1), sentence 7, no. 1; and

2. the bodies set out in subsection (2), in the cases of subsection (1), sentence 7, no. 2.

For purposes of data-protection supervision by the competent body, the Federal Network Agency shall record, for each retrieval, the time, the data used in the process of retrieval, the data retrieved, information clearly identifying the person retrieving the data, as well as the requesting authority, its reference number, and information clearly identifying the person requesting the data. Use for any other purposes of data recorded is not permitted. Data recorded are to be erased after a period of one year.

..."

30. In June 2017 a regulation was issued concerning the automatic retrieval procedure under section 112 of the Telecommunications Act. This subscriber data information regulation (*Kundendatenauskunftsverordnung*) describes in more detail the possibilities of requesting information based on the address, name or telephone number of subscribers and outlines the required information to be provided for the requested search. In addition, it regulates searches based on incomplete data and searches made by means of a similarity function. The regulation was accompanied by a technical directive, setting the technical standards for the searches and for communication between the Federal Network Agency, the requesting authorities and the telecommunications providers.

31. Section 113 of the Telecommunications Act provides for a manual procedure for requesting data stored pursuant to section 111 of the Telecommunications Act. In contrast to the automated information procedure, this provides for a duty of the service providers themselves to supply information to the entitled authorities. In the same way as in the automated information procedure, confidentiality regarding information requests in respect of the persons to whom the data relate must be preserved.

Section 113 does not contain an exhaustive list of the authorities entitled to receive information thereunder. Information requests are permissible in so far as they are necessary to prosecute criminal and regulatory offences, to avert danger (*Gefahrenabwehr*) and to perform intelligence tasks. Section 113 of the Telecommunications Act read, in so far as relevant, at the relevant time:

> "(1) Any person commercially providing or assisting in providing telecommunications services may use, subject to the stipulations of subsection (2), the data collected under sections 95 and 111 in accordance with this provision of the Law in order to fulfil its obligations to provide information to the bodies listed in subsection 3. ...
>
> (2) The information may be provided only inasmuch as one of the bodies set out in paragraph 3 has requested that this be done, in text form, in an individual case in order to prosecute criminal or administrative offences, in order to avert danger to public safety or order, and in order to discharge the legal functions of the bodies set out in subsection (3), no. 3, citing a provision of the law that allows it to so collect the data referenced in subsection (1); no data pursuant to subsection (1) may be transmitted to any other public or non-public bodies. In the case of imminent danger, the information may be provided also if the request is made in a form other than text form. In such an event, the request is to be confirmed subsequently in text form; this shall be done without undue delay. Responsibility for the admissibility of the request for information lies with the bodies set out in subsection (3).
>
> (3) The following are 'bodies' in the sense of subsection (1):
>
> 1. The authorities responsible for prosecuting criminal or administrative offences;
>
> 2. The authorities responsible for preventing threats to public security or to public order;
>
> 3. Federal and *Land* offices for the protection of the Constitution, the Federal Armed Forces Counter-Intelligence Office, and the Federal Intelligence Service.
>
> (4) A person commercially providing or assisting in providing telecommunications services is to transmit the data to be provided pursuant to a request completely and without undue delay. The parties obligated to provide information are to keep confidential requests for information and the provision of information both *vis-à-vis* the party/parties affected and *vis-à-vis* third parties.
>
> ..."

C. Legal basis for automated information requests under section 112 of the Telecommunications Act

32. Information requests in the context of criminal investigations by the public prosecutor's office and the police under the automated procedure under section 112 of the Telecommunications Act are regulated in the Code of Criminal Procedure (*Strafprozessordnung*). The applicable Articles read, at the relevant time and in so far as relevant, as follows:

Article 160

"1. As soon as the public prosecutor's office obtains knowledge of a suspected criminal offence either through a criminal complaint or by other means it shall investigate the facts to decide whether public charges are to be brought.

2. The public prosecutor's office shall ascertain not only incriminating but also exonerating circumstances, and shall ensure that evidence, the loss of which is to be feared, is taken.

3. The investigations of the public prosecutor's office shall extend also to the circumstances which are important for the determination of the legal consequences of the act. For this purpose it may avail itself of the service of the court assistance agency."

Article 161 § 1

"For the purpose indicated in Article 160 § 1 to § 3 [of the CCP], the public prosecutor's office shall be entitled to request information from all authorities and to initiate investigations of any kind, either itself or through the authorities and officials in the police force provided there are no other statutory provisions specifically regulating their powers. The authorities and officials in the police force shall be obliged to comply with such a request or order of the public prosecutor's office and shall be entitled, in such cases, to request information from all authorities."

Article 163 § 1

"The authorities and officials in the police force shall investigate criminal offences and shall take all measures that may not be deferred, in order to prevent concealment of facts. To this end they shall be entitled to request, and in exigent circumstances to demand, information from all authorities, as well as to conduct investigations of any kind in so far as there are no other statutory provisions specifically regulating their powers.

..."

33. For the prevention of crime the Federal Office for Criminal Investigation (*Bundeskriminalamt*) and the Federal Police (*Bundespolizei*) may request information under the automated procedure under section 112 of the Telecommunications Act in accordance with the following provisions which read at the relevant time:

Section 2 of the Federal Office for Criminal Investigation Act (*Bundeskriminalamtgesetz*)

"(1) As the central office for the information and intelligence system of the police, the Federal Office of Criminal Investigation supports police forces at *Land* and federal level in the prevention and investigation of crimes of cross-*Land*, international or considerable importance

(2) The Federal Office for Criminal Investigation shall for the performance of this task:

1. collect and analyse all, for this purpose, necessary, data;

..."

Section 7 of the Federal Office for Criminal Investigation Act

"(1) The Federal Office for Criminal Investigation may store, change or use personal data, in so far as required by its respective task as central office.

(2) The Federal Office for Criminal Investigation may, in so far as required for the performance of its task as central office under section 2(2), no. 1, collect data via requests for information or enquiries at public and non-public entities for the supplementation of existing information or other analytic purposes. ..."

Section 21 of the Federal Police Act (*Bundespolizeigesetz*)

"(1) The Federal Police may, unless this chapter states otherwise, collect personal data in so far as required for the performance of its tasks.

(2) For the prevention of criminal acts the collection of personal data is permitted, in so far as facts justify the presumption that:

1. an individual will commit a serious criminal act in the meaning of section 12(1) and that the information is required for the prevention of said criminal act; or

2. an individual is or will be in contact with an individual as described in no. 1 in a way that it can be expected that the measure will lead to the prevention of a criminal act as described in no. 1 and that the prevention in another way would be impossible or severely hampered."

34. Provisions similar to section 21 of the Federal Police Act exist for the police forces of the *Länder*. In addition these police forces are also permitted to collect personal information in so far as necessary for averting danger and the protection of the rights of others.

35. Under section 7 and 27 of the German Customs Investigation Service Act, the Customs Criminal Investigations Office and the Customs Investigation Offices are authorised to collect personal information in so far as required for the performance of their tasks. In addition the customs authorities may collect information under Article 163 of the Code of Criminal Procedure (see paragraph 32 above) when investigating undeclared work.

36. The Federal and *Land* offices for the protection of the Constitution, may request the information stored pursuant to section 111 of the Telecommunications Act in so far as necessary for the performance of their tasks and not prohibited by the Federal Data Protection Act.

37. The Military Counter-Intelligence Office may, under section 4 of the Military Counter-Intelligence Office Act, collect the information required for its tasks, except for the assessment of the security situation of the offices and facilities under the administration of the Ministry of Defence, of allied forces or of international military headquarters.

38. Under section 2(1) of the Federal Intelligence Service Act, the Federal Intelligence Service may request information stored pursuant to section 111 of the Telecommunications Act, in so far as necessary and not prohibited by the Federal Data Protection Act:

– for the protection of its personnel, facilities and sources against security-endangering activities and secret-service activities;
– for vetting future or current personnel;
– for the verification of incoming information, necessary for the performance of its tasks.

D. Legal basis for manual information requests under section 113 of the Telecommunications Act

39. Owing to criticism by the Federal Constitutional Court of section 113(1) of the Telecommunications Act (see paragraphs 12 and 20-21 above) several new provisions regulating retrieval of data by authorities under the manual procedure under section 113 were introduced in June 2013, after this application had been lodged.

40. Information requests by the public prosecutor's office and the police were subsequently regulated in Article 100j of the Code of Criminal Procedure, which in so far as relevant, reads:

> "1. In so far as necessary to establish the facts or to determine the whereabouts of an accused person, information on data collected pursuant to sections 95 and 111 of the Telecommunications Act may be requested from any person providing or collaborating in the provision of telecommunications services on a commercial basis (section 113(1), sentence 1, of the Telecommunications Act).
>
> ...
>
> 5. On the basis of a request for information under subsection (1) or (2), any person providing or collaborating in the provision of telecommunications services on a commercial basis shall transmit without delay the data required for the provision of the information. ..."

Similar provisions were created for the Federal Police, the Federal Office of Criminal Investigation and the Customs Investigation Service.

41. The Federal Office for the Protection of the Constitution is permitted to request the data collected pursuant to section 111 of the Telecommunications Act from service providers under section 8d of the Federal Act on the Protection of the Constitution (*Bundesverfassungsschutzgesetz*), which reads in so far as relevant:

> "In so far as necessary for the performance of its tasks the Federal Office for the Protection of the Constitution may request from any person providing or collaborating in the provision of telecommunications services on a commercial basis information on data collected pursuant to sections 95 and 111 of the Telecommunications Act (section 113(1), sentence 1, of the Telecommunications Act). ..."

Similar provisions were introduced for the offices for the protection of the Constitution of the *Länder*. Moreover, the legal basis for manual information requests by the Military Counter-Intelligence Office and the Federal Intelligence Service refer to section 8d of the Federal Act on the Protection of the Constitution.

E. Judicial review of investigative measures

42. Under Article 98 § 2 of the Code of Criminal Procedure, a person affected by the seizure of an object in the absence of court involvement may apply for a court decision at any time.

43. In accordance with the well-established case-law of the Federal Court of Justice (see, for example, case no. 5 ARs (VS) 1/97, 5 August 1998), an analogous application of Article 98 § 2 of the Code of Criminal Procedure offers the possibility of judicial review of any completed investigative measure by a public prosecutor if the measure constituted a serious interference with the person's fundamental rights.

F. Data protection law

44. The relevant parts of the Federal Data Protection Act (*Bundesdatenschutzgesetz*), as in force until 24 May 2018, read as follows:

Section 1 – Purpose and scope

"(1) The purpose of this Act is to protect individuals against infringements of their right to privacy as the result of the handling of their personal data.

(2) This Act shall apply to the collection, processing and use of personal data by

1. public bodies of the Federation,

2. public bodies of the *Länder*, where data protection is not covered by *Land* legislation and where the *Länder*

(a) execute federal law, or

(b) act as judicial bodies and administrative matters are not involved,

...

(3) Where other federal laws apply to personal data and their publication, they shall take precedence over the provisions of this Act. The obligation to abide by legal obligations of secrecy or professional or special official secrecy not based on law shall remain unaffected."

Section 2 – Public and private bodies

"(1) 'Public bodies of the Federation' shall mean the authorities, judicial bodies and other public-law institutions of the Federation, of the direct federal corporations, institutions and foundations under public law, as well as their associations irrespective of their legal forms. ..."

Section 3a – Data reduction and data economy

"Personal data shall be collected, processed and used, and data-processing systems shall be chosen and organised in accordance with the aim of collecting, processing and using as little personal data as possible. In particular, personal data shall be rendered anonymous or aliased as allowed by the purpose for which they are collected

and/or further processed, and in so far as the effort required is not disproportionate to the desired purpose of protection."

Section 4 – Lawfulness of data collection, processing and use

"(1) The collection, processing and use of personal data shall be lawful only if permitted or ordered by this Act or other law, or if the data subject has given consent.

(2) Personal data shall be collected from the data subject. They may be collected without the data subject's participation only if

1. allowed or required by law, or

2. (a) the data must be collected from other persons or bodies on account of the nature of the administrative task to be performed or the commercial purpose, or

(b) collecting the data from the data subject would require disproportionate effort and there are no indications that overriding legitimate interests of the data subject would be adversely affected."

Section 13 – Data collection

"(1) Collecting personal data shall be lawful when knowledge of such data is necessary for the controller to perform its tasks.

(1a) If personal data are collected from a private body rather than from the data subject, this body shall be informed of the legal provision requiring the supply of information or that such supply is voluntary."

Section 19 – Access to data

"(1) Upon request, data subjects shall be given information on

1. recorded data relating to them, including information relating to the source of the data,

2. the recipients or categories of recipients to which the data are transferred, and

3. the purpose of recording the data.

The request should specify the type of personal data on which information is to be given. If the personal data are recorded neither in automated format nor in non-automated filing systems, this information shall be provided only if the data subject provides information enabling the data to be located and if the effort required is not disproportionate to the data subject's interest in the information. The controller shall exercise due discretion in determining the procedure for providing such information and in particular the form in which it is provided.

(2) Subsection 1 shall not apply to personal data recorded only because they may not be erased owing to legal, statutory or contractual provisions on retention, or only for purposes of monitoring data protection or safeguarding data, where provision of the information would require a disproportionate effort.

(3) If the provision of information relates to the transfer of personal data to authorities for the protection of the constitution, to the Federal Intelligence Service, the Military Counterintelligence Service and, as far as the security of the Federation is concerned, other agencies of the Federal Ministry of Defence, such provision shall be lawful only with the consent of these bodies.

(4) Information shall not be provided if

1. the information would endanger the orderly performance of tasks for which the controller is responsible,

2. the information would threaten public security or order or otherwise be detrimental to the Federation or a *Land*, or

3. the data or the fact of their recording, in particular on account of the overriding legitimate interests of a third party, must be kept secret by law or because of the nature of the data, and therefore the data subject's interest in obtaining information shall not take precedence.

(5) It is not necessary to provide reasons for refusing to provide information if stating the actual and legal grounds for refusal would threaten the purpose of refusing to provide the information. In this case, data subjects shall be informed of the possibility of contacting the Federal Commissioner for Data Protection and Freedom of Information.

(6) If no information is provided to the data subject, at the data subject's request this information shall be supplied to the Federal Commissioner for Data Protection and Freedom of Information unless the relevant supreme federal authority finds in the individual case that doing so would endanger the security of the Federation or a *Land*. The information provided by the Federal Commissioner to the data subject may not provide any indication of the knowledge available to the controller without its consent.

(7) Information shall be provided free of charge."

Section 19a – Notification

"(1) If data are collected without the data subject's knowledge, he or she shall be notified of such recording, the identity of the controller and the purposes of collection, processing or use. The data subject shall also be notified of recipients or categories of recipients except where he or she must expect transfer to such recipients. If a transfer is planned, notification shall be provided no later than the first transfer.

(2) Notification shall not be required if

1. the data subject already has this information,

2. notifying the data subject would involve a disproportionate effort, or

3. recording or transferring of personal data is expressly laid down by law.

The controller shall specify in writing the conditions under which notification shall not be provided in accordance with nos. 2 or 3.

(3) Section 19(2) to (4) shall apply accordingly."

Section 21 – Appeals to the Federal Commissioner for Data Protection and Freedom of Information

"Anyone who believes that his or her rights have been infringed through the collection, processing or use of his or her personal data by public bodies of the Federation may appeal to the Federal Commissioner for Data Protection and Freedom of Information. This shall apply to the collection, processing or use of personal data by federal courts only where they are active in administrative matters."

Section 24 – Monitoring by the Federal Commissioner for Data Protection and Freedom of Information

"(1) The Federal Commissioner for Data Protection and Freedom of Information shall monitor compliance by the public bodies of the Federation with the provisions of this Act and other data protection provisions.

(2) Monitoring by the Federal Commissioner shall also extend to

1. personal data obtained by public bodies of the Federation concerning the contents of and specific circumstances relating to postal communications and telecommunications, and

2. personal data subject to professional or special official secrecy, especially tax secrecy under Article 30 of the German Fiscal Code. ..."

45. Similar provisions existed in *Länder*. In addition the *Länder* have their own data protection commissioner monitoring the compliance of *Länder* authorities with the respective data protection acts.

III. EUROPEAN UNION LAW AND PRACTICE

A. Charter of Fundamental Rights of the European Union

46. Articles 7 and 8 of the Charter provide as follows:

Article 7 – Respect for private and family life

"Everyone has the right to respect for his or her private and family life, home and communications."

Article 8 – Protection of personal data

"1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which have been collected concerning him or her, and the right to have them rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

B. EU secondary legislation relating to data protection

47. The relevant recitals of the Privacy and Electronic Communications Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector) state as follows:

"(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the

European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.

...

(11) Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms."

48. The Directive further provides, in so far as relevant:

Article 1 – Scope and aim

"1. This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law."

Article 15 – Application of certain provisions of Directive 95/46/EC

"1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with

the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union."

49. On 15 March 2006 the Data Retention Directive (Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC) was adopted. It provided, in so far as relevant:

Article 1 – Subject matter and scope

"1. This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network."

Article 3 § 1 – Obligation to retain data

"By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned."

50. In essence, the Directive established an obligation for providers of publicly available electronic communication services or of public communications networks to retain all traffic and location data for periods of from six months to two years. It aimed at ensuring that the data were available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each member State in its national law. The retention obligation entailed, *inter alia*, data necessary to trace and identify the source and destination of a communication, meaning the telephone number and the name and address of the subscriber or registered user (Article 5 § 1 (a) and (b)).

C. Relevant case-law of the Court of Justice of the European Union

51. In a judgment adopted on 8 April 2014 in *Digital Rights Ireland* and *Seitlinger and Others* (joined cases C-293/12 and C-594/12, EU:C:2014:238) the Court of Justice of the European Union (CJEU) declared the Data Retention Directive invalid (see paragraphs 49-50 above).

52. The CJEU further developed its *Digital Rights* case-law in *Tele2 Sverige* and *Tom Watson and Others* (judgment of 21 December 2016, joined cases C-203/15 and C-698/15, EU:C:2016:970). The court stated, *inter alia* (references to further CJEU judgments have been omitted in the quote below):

> "103. ... while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight.
>
> 104. In that regard, it must be observed, first, that the effect of such legislation, in the light of its characteristic features as described in paragraph 97 of the present judgment, is that the retention of traffic and location data is the rule, whereas the system put in place by Directive 2002/58 requires the retention of data to be the exception.
>
> 105. Second, national legislation such as that at issue in the main proceedings, which covers, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as all traffic data, provides for no differentiation, limitation or exception according to the objective pursued. It is comprehensive in that it affects all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences. Further, it does not provide for any exception, and consequently it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.
>
> 106. Such legislation does not require there to be any relationship between the data which must be retained and a threat to public security. In particular, it is not restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime.
>
> 107. National legislation such as that at issue in the main proceedings therefore exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.
>
> 108. However, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.
>
> 109. In order to satisfy the requirements set out in the preceding paragraph of the present judgment, that national legislation must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing

minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary.

110. Second, as regards the substantive conditions which must be satisfied by national legislation that authorises, in the context of fighting crime, the retention, as a preventive measure, of traffic and location data, if it is to be ensured that data retention is limited to what is strictly necessary, it must be observed that, while those conditions may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected.

111. As regard the setting of limits on such a measure with respect to the public and the situations that may potentially be affected, the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security."

53. Subsequent to the latter judgment, national courts in several EU member States have sought preliminary rulings from the CJEU seeking to clarify the scope and effects of the *Tele2 Sverige* judgment. Two of those cases are still pending (see *Privacy International*, C-623/17, and *Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX*, C-520/18).

54. In a third case, *Ministerio Fiscal* (judgment of 2 October 2018, C-207/16, EU:C:2018:788), the CJEU was asked whether Article 15 § 1 of the Data Retention Directive, read in the light of Articles 7 and 8 of the Charter of Fundamental Rights, must be interpreted as meaning that public authorities' access to data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone, such as the surnames, forenames and, if need be, addresses of the owners of the SIM cards, entails interference with their fundamental rights, enshrined in those Articles of the Charter, which is sufficiently serious to entail that access being limited, in the area of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime and, if so, by reference to which criteria the seriousness of the offence at issue must be assessed.

55. In its judgment of 2 October 2018, the CJEU held as follows (references to further CJEU judgments have been omitted in the quote below):

"51. As to the existence of an interference with those fundamental rights, it should be borne in mind ... that the access of public authorities to such data constitutes an interference with the fundamental right to respect for private life, enshrined in

Article 7 of the Charter, even in the absence of circumstances which would allow that interference to be defined as 'serious', without it being relevant that the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way. Such access also constitutes interference with the fundamental right to the protection of personal data guaranteed in Article 8 of the Charter, as it constitutes processing of personal data.

...

56. In accordance with the principle of proportionality, serious interference can be justified, in areas of prevention, investigation, detection and prosecution of criminal offences, only by the objective of fighting crime which must also be defined as 'serious'.

57. By contrast, when the interference that such access entails is not serious, that access is capable of being justified by the objective of preventing, investigating, detecting and prosecuting 'criminal offences' generally.

58. It should therefore, first of all, be determined whether, in the present case, in the light of the facts of the case, the interference with fundamental rights enshrined in Articles 7 and 8 of the Charter that police access to the data in question in the main proceedings would entail must be regarded as 'serious'.

59. In that regard, the sole purpose of the request at issue in the main proceedings, by which the police seeks, for the purposes of a criminal investigation, a court authorisation to access personal data retained by providers of electronic communications services, is to identify the owners of SIM cards activated over a period of 12 days with the IMEI code of the stolen mobile telephone. ... that request seeks access to only the telephone numbers corresponding to those SIM cards and to the data relating to the identity of the owners of those cards, such as their surnames, forenames and, if need be, addresses. By contrast, those data do not concern ... the communications carried out with the stolen mobile telephone or its location.

60. It is therefore apparent that the data concerned by the request for access at issue in the main proceedings only enables the SIM card or cards activated with the stolen mobile telephone to be linked, during a specific period, with the identity of the owners of those SIM cards. Without those data being cross-referenced with the data pertaining to the communications with those SIM cards and the location data, those data do not make it possible to ascertain the date, time, duration and recipients of the communications made with the SIM card or cards in question, nor the locations where those communications took place or the frequency of those communications with specific people during a given period. Those data do not therefore allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned.

61. In those circumstances, access to only the data referred to in the request at issue in the main proceedings cannot be defined as 'serious' interference with the fundamental rights of the persons whose data is concerned."

IV. INTERNATIONAL LAW AND PRACTICE

56. The United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, recommended in his Report to the Human Rights Council on the use of

encryption and anonymity to exercise the rights to freedom of opinion and expression in the digital age (A/HRC/29/32, 22 May 2015, § 60):

> "States should not restrict encryption and anonymity, which facilitate and often enable the rights to freedom of opinion and expression. Blanket prohibitions fail to be necessary and proportionate. ... States should refrain from making the identification of users a condition for access to digital communications and online services and requiring SIM card registration for mobile-telephone users."

57. The Council of Europe Convention of 1981 for the Protection of Individuals with Regard to Automatic Processing of Personal Data ("the Data Protection Convention"), which was ratified by all Council of Europe member States and came into force in respect of Germany on 1 October 1985, formulates a number of core principles for the collection and processing of personal data. The purpose of the Convention is, according to Article 1, to secure respect for every individual's rights and fundamental freedoms, and in particular his or her right to privacy, with regard to the automatic processing of personal data relating to him or her. The Convention includes the following basic principles:

Article 2 – Definitions

"For the purposes of this Convention:

a 'personal data' means any information relating to an identified or identifiable individual ('data subject');

b 'automated data file' means any set of data undergoing automatic processing;

c 'automatic processing' includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination;

..."

Article 5 – Quality of data

"Personal data undergoing automatic processing shall be:

a obtained and processed fairly and lawfully;

b stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

c adequate, relevant and not excessive in relation to the purposes for which they are stored;

d accurate and, where necessary, kept up to date;

e preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."

Article 7 – Data security

"Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination."

Article 8 – Additional safeguards for the data subject

"Any person shall be enabled:

a to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

b to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

c to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention;

d to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this Article is not complied with."

Article 9 – Exceptions and restrictions

"No exception to the provisions of Articles 5, 6 and 8 of this Convention shall be allowed except within the limits defined in this Article.

Derogation from the provisions of Articles 5, 6 and 8 of this Convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

b protecting the data subject or the rights and freedoms of others.

Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects."

The Data Protection Convention is currently being updated to, *inter alia*, better address challenges resulting from the use of new information and communication technologies. A Protocol amending the Data Protection Convention was opened for signature by the Contracting States to that Convention on 10 October 2018 and was signed by Germany on the same day.

V. COMPARATIVE LAW

58. From a comparative-law report on thirty-four Council of Europe member States' practices as to the retention of subscriber information of

prepaid SIM card customers, it appears that fifteen States require telecommunications providers to store such data and that none of the States surveyed currently permits its authorities to maintain their own database of personal data of telecommunications subscribers. Moreover, there is variation as regards the length of time such data may be stored, the purposes for which they may be used, and the procedural requirements that must be met in order to access them. In particular, a majority of the States prescribe in law a list of specific authorities who are permitted to access subscriber information and limit the acceptable purposes to the investigation of crimes or for the prevention of threats to public order. Furthermore, in most States, procedural requirements for accessing stored subscriber information include an order by a court or a public prosecutor, typically if the subscriber data are to be used mainly for criminal investigative purposes. Lastly, only a minority of States require that customers be notified where their personal data have been accessed.

THE LAW

ALLEGED VIOLATION OF ARTICLES 8 AND 10 OF THE CONVENTION

59. The applicants complained that, as users of prepaid mobile phone SIM cards, certain personal data had been stored by their respective telecommunications service providers owing to the legal obligation provided in section 111 of the Telecommunications Act. They relied on their right to respect for private life and correspondence as provided in Article 8 of the Convention and their freedom of expression as provided in Article 10 of the Convention which read, in so far as relevant to the present case, as follows:

Article 8

"1. Everyone has the right to respect for his private ... life ... and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or ..., for the prevention of disorder or crime ..."

Article 10

"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. ...

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security ... or public safety, for the prevention of disorder or crime ...”

A. Scope of the application and the Court’s assessment

1. The Convention rights to be assessed

60. At the outset the Court notes that the applicants relied on Article 8 (right to respect for private life and correspondence) and Article 10 (right to anonymous communication as an aspect of freedom of expression). However, it also observes that before the Court the applicants merely challenged the compatibility of section 111 of the Telecommunications Act with the Convention. They did not explicitly complain about sections 112 or 113 of that Act, which had also been the subject of their complaint before the Federal Constitutional Court, or about any further measures concerning surveillance or interception of telephone communications. This does not mean, however, that those other provisions of the Telecommunications Act will not prove relevant when assessing the proportionality of the interference complained of and how it operates in practice (see paragraphs 97-101 below).

61. Section 111 of the Telecommunications Act only concerns the storage of subscriber data, namely the telephone number, name and address, date of birth, and date of the contract. This provision does not extend to traffic data, location data or data which reveal the content of communications. Moreover, the applicants have not alleged that their communications have been intercepted or that their telecommunications have been subjected to any other surveillance measure. The interference complained of relates to the storage of the data set described above and the potential for national authorities to access that data set in certain defined circumstances. Therefore, while the Court is mindful of the circumstances of the data storage at issue and its proximity to telephone communications and the right to correspondence, it considers that the key aspect of the applicants’ complaint is the storage of their personal data and not any particular interference with their correspondence or with their freedom of expression.

62. The Court is therefore not called upon in the present case to decide whether and to what extent Article 10 of the Convention may be considered to guarantee a right for users of telecommunications services to anonymity (see, regarding the interest of Internet users in not disclosing their identity, *Delfi AS v. Estonia* [GC], no. 64569/09, § 147, 16 June 2015) and how this right would have to be balanced against other imperatives (see, *mutatis mutandis*, *K.U. v. Finland*, no. 2872/02, § 49, 2 December 2008).

63. In sum, the Court finds it appropriate to examine the applicants' complaints solely under the right to respect for private life as provided in Article 8 of the Convention.

2. Temporal scope of the assessment

64. The Court notes that the applicants' subscriber data have been temporarily stored by the telecommunications provider since the registration of their SIM cards. It also notes that section 111 of the Telecommunications Act was amended in 2007 and 2016. It observes, however, that in its judgment of 24 January 2012, the Federal Constitutional Court examined the Telecommunications Act as in force on 1 January 2008 and that proceedings concerning the subsequent amendment to the Telecommunications Act of 2016 are still pending before the Federal Constitutional Court (see paragraphs 11 and 28 above). The Court will therefore examine the relevant provisions as in force on 1 January 2008.

B. Admissibility

65. The Court notes that the complaint is not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention. It further notes that it is not inadmissible on any other grounds. It must therefore be declared admissible.

C. Merits

1. The parties' submissions

(a) The applicants

66. The applicants argued that the obligation to store their personal data under section 111 of the Telecommunications Act interfered with their right to privacy, as it had forced them to disclose their personal data, which had subsequently been stored. This interference was not justified, in particular since it was disproportionate and not necessary in a democratic society. Firstly, the provision was not a suitable instrument, as the identification process could easily be circumvented by submitting false names or using stolen, second-hand or foreign SIM cards. It was also not necessary as the identification of mobile-telephone users suspected of a criminal offence could easily be accomplished by other investigatory measures. Consequently, the amendment of section 111 of the Telecommunications Act had not led to a reduction in crime.

67. According to the applicants, the interference was very serious as it constituted mass pre-emptive storage of personal data of everyone who used telecommunications. The provision did not include any prerequisites for

storage, but was generally applicable to all mobile-telephone users. The vast majority of affected people were innocent and did not present any danger or risk for public safety or national security. In that regard the applicants submitted that, according to the Federal Network Agency, the number of queried data sets under the automated procedure of section 112 of the Telecommunications Act had risen from 26.62 million in 2008 to 34.83 million in 2015. Moreover, the provision also did not differentiate between "normal" communication and communication that was particularly protected by the Convention, such as between a lawyer and his or her client or a doctor and his or her patient. Furthermore, data storage increased the risk of misuse and data leaks and thereby the risk of identity fraud.

(b) The Government

68. The Government conceded that section 111 of the Telecommunications Act had constituted an interference with the applicants' right to private life. It had obliged their service providers to store their personal data. The Government emphasised that no so-called traffic data – meaning data originating in the course of a communication process – had been stored, only the subscriber information listed above (see paragraph 61 above). Moreover, section 111 had to be read in conjunction with sections 112 and 113 of the Telecommunications Act and the further limiting provisions regulating the access to the stored data, as the authorities retrieving subscriber data needed to have a statutory basis for doing so.

69. This limited interference had pursued the legitimate aims of public safety, prevention of disorder or crime and the protection of the rights and freedoms of others and had been a suitable instrument to do so, as it had provided security agencies with the possibility to correlate mobile-telephone numbers of prepaid SIM cards to specific individuals. This possibility would contribute to effective law enforcement and serve to avert danger. The possibility of circumventing the provision had been further restricted by the amendment of 2016 (see paragraph 28 above).

70. The provision at issue also complied with the requirements for protection of personal data as established by the Court in *S. and Marper v. the United Kingdom* ([GC], nos. 30562/04 and 30566/04, § 103, ECHR 2008). It limited the amount of data to that which was absolutely necessary for identification. The time-period for data storage was clearly defined and limited to a maximum term not exceeding the term necessitated by the purpose being pursued. Furthermore, sections 112 and 113 of the Telecommunications Act in conjunction with the specific provisions for retrieval constituted effective safeguards against abuse.

71. It had also to be taken into account that the margin of appreciation afforded to member States was relatively broad, not only because the German authorities had to strike a balance between various competing rights and obligations protected by the Convention (they referred to *Evans v. the*

United Kingdom [GC], no. 6339/05, § 77, 10 April 2007), but also because there was no European consensus as regards the obligation to store subscriber data when acquiring prepaid mobile telephone SIM cards. In sum, the storage of a very minimal set of data, protected by several procedural safeguards, was proportionate in the crucial interests of public safety and prevention of disorder and crime.

(c) The third-party interveners

72. The third-party interveners, Privacy International and ARTICLE 19, outlined the significance of anonymity and anonymous speech for a democratic society and citizens' rights of privacy and freedom of expression. This fundamental role had increasingly been recognised by national courts and international organisations, such as the United Nations and the Council of Europe. In addition the Court itself had confirmed the importance of anonymity in *Delfi AS v. Estonia* (cited above, §§ 147-48). Moreover, they pointed to the fact that there had been a growing recognition by courts in Europe that blanket, indiscriminate retention of identifying information and traffic data had been disproportionate to the undoubtedly important fight against serious crime. This had also been confirmed by the CJEU in its judgment in *Digital Rights Ireland* and *Seitlinger and Others* (see paragraph 51 above).

2. The Court's assessment

(a) General principles

73. The Court reiterates that private life is a broad term not susceptible to exhaustive definition. Article 8 protects, *inter alia*, the right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life" (see *Uzun v. Germany*, no. 35623/05, § 43, 2 September 2010).

74. In the context of personal data, the Court has pointed out that the term "private life" must not be interpreted restrictively. It has found that the broad interpretation corresponds with that of the Data Protection Convention, the purpose of which is "to secure in the territory of each Party for every individual ... respect for his rights und fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such personal data being defined as "any information relating to an identified or identifiable individual" (Article 2) (see *Amann v. Switzerland* [GC], no. 27798/95, § 65, 16 February 2000).

75. It further follows from the Court's well-established case-law that where there has been a compilation of data on a particular individual, the

processing or use of personal data or publication of the material concerned in a manner or degree beyond that normally foreseeable, private-life considerations arise. Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged (see *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], no. 931/13, §§ 136-37, 27 June 2017, with further references).

76. The Court notes that while it has already examined a wide range of interferences with the right to private life under Article 8 of the Convention as a result of the storage, processing and use of personal data – for example, the use of surveillance via GPS in criminal investigations (see *Uzun*, cited above, and *Ben Faiza v. France*, no. 31446/12, 8 February 2018), the disclosure of identifying information to law-enforcement authorities by telecommunication providers (see *K.U. v. Finland*, cited above, and *Benedik v. Slovenia*, no. 62357/14, 24 April 2018), the indefinite retention of fingerprints, cell samples and DNA profiles after criminal proceedings (see *S. and Marper*, cited above), the so-called metering or collection of usage or traffic data (see *Malone v. the United Kingdom*, 2 August 1984, Series A no. 82, and *Copland v. the United Kingdom*, no. 62617/00, 3 April 2007) or the inclusion of sex offenders in an automated national judicial database subsequent to a conviction for rape (see *B.B. v. France*, no. 5335/06, 17 December 2009; *Gardel v. France*, no. 16428/05, ECHR 2009; and *M.B. v. France*, no. 22115/06, 17 December 2009) – none of the previous cases have concerned the storage of a data set like that in the present case.

77. An obligation, similar to that in section 111 of the Telecommunications Act, to create databases storing information (first name, patronymic and family name, home address and passport number for natural persons) about all subscribers and providing law-enforcement agencies remote access to the databases was admittedly part of the system of secret surveillance which the Court considered in the case of *Roman Zakharov v. Russia* ([GC], no. 47143/06, §§ 132-33 and 269-70, ECHR 2015). However, given the further possibilities available to the Russian authorities to intercept telecommunications, the mere obligation to store subscriber information and provide remote access to this database was not decisive for the Court in finding a violation of Article 8 in that case.

78. In its judgment in *S. and Marper* (cited above, § 103) the Court held as follows:

> "The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article .... The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such

> data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored (see Article 5 of the Data Protection Convention ... [in paragraph 47 above]). The domestic law must also afford adequate guarantees that retained personal data were efficiently protected from misuse and abuse (see notably Article 7 of the Data Protection Convention [in paragraph 47 above]) ...."

79. The Court has acknowledged that, when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this margin is subject to European supervision embracing both legislation and decisions applying it (see *Roman Zakharov*, cited above, § 232; *Liblik and Others v. Estonia*, nos. 173/15 and 5 others, § 131, 28 May 2019; and *Szabó and Vissy v. Hungary*, no. 37138/14, § 57, 12 January 2016).

80. The breadth of the margin of appreciation varies and depends on a number of factors, including the nature of the Convention right in issue, its importance for the individual, the nature of the interference and the object pursued by the interference. The margin will tend to be narrower where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights. Where, however, there is no consensus within the member States of the Council of Europe, either as to the relative importance of the interest at stake or as to how best to protect it, the margin will be wider (see *S. and Marper*, cited above, § 102).

(b) Application of the above principles to the present case

(i) Existence of an interference

81. It is not contested by the parties that the obligation for service providers to store personal data in accordance with section 111 of the Telecommunications Act interfered with the applicants' right to respect for their private life, since their personal data were stored. In this connection the Court reiterates that the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 of the Convention (see *Leander v. Sweden*, 26 March 1987, § 48, Series A no. 116). It furthermore takes note of the Federal Constitutional Court's finding that the extent of protection of the right to informational self-determination under domestic law was not restricted to information which by its very nature was sensitive and that, in view of the possibilities of processing and combining, there is no item of personal data which is in itself – that is, regardless of the context of its use – insignificant (see

paragraph 122 of the Federal Constitutional Court's judgment cited in paragraph 14 above).

(ii) Justification for the interference

82. The Court reiterates that an interference with an applicant's right to respect for his or her private life breaches Article 8 unless it is "in accordance with the law", pursues one or more of the legitimate aims referred to in paragraph 2 and is, in addition, "necessary in a democratic society" to achieve those aims (see *M.N. and Others v. San Marino*, no. 28005/12, § 71, 7 July 2015, with further references).

(α) "In accordance with the law"

83. According to the Court's established case-law, the requirement that an interference be "in accordance with the law" does not only mean that the measure in question should have some basis in domestic law, but also that the law should be accessible to the person concerned and foreseeable as to its effects. In the context of, *inter alia*, storage of personal information it is essential to have clear, detailed rules governing minimum safeguards concerning among other things duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction (see *S. and Marper*, cited above, § 99, with further references)

84. The Court finds that the storage of the applicants' personal data, when acquiring mobile telephone SIM cards, took place on the basis of section 111 of the Telecommunications Act, which was, in so far as the amount of stored data is concerned, sufficiently clear and foreseeable. In addition, the duration of the storage was clearly regulated and the technical side of the storage was, at least after the issuance of the respective regulation and technical directive, clearly laid out.

85. In so far as safeguards, access of third parties and further use of the stored data are concerned, section 111 of the Telecommunications Act has to be read in conjunction with its sections 112 and 113 and, according to the "double door" analogy used by the Federal Constitutional Court (see paragraph 123 of the Federal Constitutional Court's judgment cited in paragraph 14 above), in conjunction with the relevant legal basis for individual information requests. The Court considers, however, that the question of foreseeability and whether sufficient detail is contained in these provisions are in the present case closely related to the broader issues of whether the interference was necessary in a democratic society and proportionate. It will therefore assess them further when it comes to those issues (see paragraphs 88-110 below).

(β) Legitimate aim

86. Having regard to the context of the data storage at issue and in particular to the purposes of information requests and the authorities entitled to make them under sections 112 and 113 of the Telecommunications Act, the Court accepts the Government's argument that the interference pursued the legitimate aims of public safety, prevention of disorder or crime and the protection of the rights and freedoms of others.

87. In this connection the Court notes the Federal Constitutional Court's explanation in its judgment that access to the information stored is for "the purpose of warding off dangers, prosecuting criminal offences or regulatory offences and performing intelligence duties" (see paragraph 176 of the Federal Constitutional Court's judgment cited in paragraph 21 above). These purposes are further emphasised in the Telecommunications Act, which states that information requests are permissible in so far as they are necessary to prosecute criminal and regulatory offences, to avert danger and to perform intelligence tasks (see paragraph 31 above).

(γ) "Necessary in a democratic society"

88. An interference will be considered "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and if it is proportionate to the legitimate aim pursued. The Court finds that the fight against crime, and in particular against organised crime and terrorism, which is one of the challenges faced by today's European societies, upholding public safety and the protection of citizens constitute "pressing social needs" (compare, *mutatis mutandis*, *Szabó and Vissy*, cited above, § 68, and *Ramda v. France*, no. 78477/11, § 96, 19 December 2017). It also recognises that modern means of telecommunications and changes in communication behaviour require that investigative tools for law enforcement and national security agencies be adapted (see *S. and Marper*, cited above, § 105).

89. The Court observes that the Government argued that the possibility of correlating mobile-telephone numbers of prepaid SIM cards to specific individuals was necessary for effective law enforcement and to avert danger. The applicants, however, contested the effectiveness of section 111 of the Telecommunications Act, since there was no empirical evidence that mandatory registration had led to a reduction in crime. Moreover, they argued that the identification process could easily be circumvented by submitting false names or using stolen, second-hand or foreign SIM cards.

90. The Court acknowledges that pre-registration of mobile-telephone subscribers strongly simplifies and accelerates investigation by law-enforcement agencies and can thereby contribute to effective law enforcement and prevention of disorder or crime. Moreover, it considers that the existence of possibilities of circumventing legal obligations cannot be a reason to call into question the overall utility and effectiveness of a

legal provision. Lastly, the Court reiterates that in a national security context, national authorities enjoy a certain margin of appreciation when choosing the means for achieving a legitimate aim and notes that according to the comparative-law report, there is no consensus between the member States as regards the retention of subscriber information of prepaid SIM card customers (see paragraph 58 above). Having regard to that margin of appreciation, the Court accepts that the obligation to store subscriber information under section 111 of the Telecommunications Act was, in general, a suitable response to changes in communication behaviour and in the means of telecommunications.

91. The question, however, remains whether the interference was proportionate and struck a fair balance between the competing public and private interests.

92. At the outset the Court has to establish the level of interference with the applicants' right to private life. In that regard the Court agrees with the Federal Constitutional Court (see paragraphs 138-39 of the Federal Constitutional Court's judgment cited in paragraph 15 above) that only a limited data set was stored. These data did not include any highly personal information or allow the creation of personality profiles or the tracking of the movements of mobile-telephone subscribers. Moreover, no data concerning individual communication events were stored. The level of interference therefore has to be clearly distinguished from the Court's previous cases that concerned, for example, "metering" (see *Malone* and *Copland*, both cited above), geolocation (see *Uzun* and *Ben Faiza*, both cited above), or the storage of health or other sensitive data (see, for example, *S. and Marper*, cited above, and *M.M. v. the United Kingdom*, no. 24029/07, 13 November 2012). Moreover, the case has to be distinguished from cases in which the registration in a particular database led to frequent checks or further collection of private information (see *Dimitrov-Kazakov v. Bulgaria*, no. 11379/03, 10 February 2011, and *Shimovolos v. Russia*, no. 30194/09, 21 June 2011).

93. Lastly, in so far as the applicants argued that the interference was severe, because section 111 of the Telecommunications Act created a register of all users of mobile SIM cards, and in that sense was comparable to the data retention at issue in *Digital Rights Ireland* and *Seitlinger and Others*, as well as *Tele2 Sverige* and *Tom Watson and Others* (see paragraphs 51-52 above), the Court notes that the Directive at issue in those cases applied to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user.

94. Indeed, the data at issue in the present case bear greater resemblance to those at issue in a different preliminary reference, *Ministerio fiscal* (see paragraph 54 above). As the CJEU stated in that case, the data in question "do not make it possible to ascertain the date, time, duration and recipients

of the communications made with the SIM card or cards in question, nor the locations where those communications took place or the frequency of those communications with specific people during a given period. Those data do not therefore allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned". The CJEU therefore concluded that the access to the data at issue could not be defined as a serious interference with the fundamental rights of the persons whose data were concerned (see paragraph 55 above).

95. In sum, the Court concludes that the interference was, while not trivial, of a rather limited nature.

96. As regards safeguards, the Court observes that the applicants have not alleged that the data storage at issue was subject to any technical insecurities. Moreover, the duration of the storage is limited to the expiry of the calendar year following the year in which the contractual relationship ended (section 111(4) of the Telecommunications Act – see paragraph 27 above). This duration of storage does not appear inappropriate, given that investigations into criminal offences may take some time and extend beyond the end of the contractual relationship. Moreover, the stored data appear to be limited to the information necessary to clearly identify the relevant subscriber.

97. The Court further observes that even though the applicants have only complained about the storage of their personal information under section 111 of the Telecommunications Act, both parties accepted that the data storage had to be assessed in conjunction with sections 112 and 113 of that Act. The Government argued that these sections, in conjunction with other specific provisions for data retrieval, limited access to and use of the data and constituted effective safeguards against abuse. The applicants, however, submitted that each further investigative measure into a person's conduct – connected to mobile communication – had been based on the information stored under section 111 of the Telecommunications Act and that therefore the possibilities of subsequent use of their personal data had to be taken into account when assessing the proportionality of the provision in relation to data storage. The Court agrees with the parties that, in the present case, it cannot consider the proportionality of the interference without closely assessing the future possible access to and use of the data stored. Therefore, it finds it of relevance to consider the legal basis for information requests and the safeguards available (see, *mutatis mutandis*, *S. and Marper*, cited above, §§ 67 and 103, with further references).

98. Regarding section 112 of the Telecommunications Act, the Court agrees with the Federal Constitutional Court (see paragraph 156 of the Federal Constitutional Court's judgment cited in paragraph 18 above) that this provision has very much simplified data retrieval for the authorities. The centralised and automated procedure permits a form of access which largely removes practical difficulties of data collection and makes the data

available to the authorities at all times without delay. However, the fact that the authorities which can request access are specifically listed in section 112 of the Telecommunications Act constitutes a limiting factor. Even though the list appears broad, all authorities mentioned therein are concerned with law enforcement or the protection of national security.

99. As regards section 113 of the Telecommunications Act, the Court first notes that the information retrieval is not simplified to the same extent as under section 112, since the authorities have to submit a written request for the information sought. A further difference between sections 112 and 113 of the Telecommunications Act is that the authorities entitled to request access pursuant to the latter provision are identified with reference to the tasks they perform but are not explicitly enumerated. While the Court considers this description by task less specific and more open to interpretation, the wording of the provision is nonetheless detailed enough to clearly foresee which authorities are empowered to request information. In that regard the Court also notes that the Federal Constitutional Court concluded that the limited tasks of the intelligence services justified their wide-ranging legal powers to request information on a pre-emptive basis (see paragraph 177 of the Federal Constitutional Court's judgment cited in paragraph 21 above).

100. Concerning both provisions, the Court observes that the stored data are further protected against excessive or improper information requests by the fact that the requesting authority requires an additional legal basis to retrieve the data. As explained by the Federal Constitutional Court through its "double door" analogy (see paragraph 123 of the Federal Constitutional Court's judgment cited in paragraph 14 above), sections 112 and 113 of the Telecommunications Act only allow the Federal Network Agency or the respective service provider to release the data. However, a further legal provision is required to allow the specified authorities to request the information. Moreover, the retrieval is limited to necessary data and this necessity requirement is safeguarded by a general obligation for the respective authorities retrieving the information to erase, without undue delay, any data they do not need. The Federal Constitutional Court pointed out that the requirement of "necessity" meant in the context of the prosecution of offences that there had to be at least an initial suspicion (see paragraph 177 of the Federal Constitutional Court's judgment cited in paragraph 21 above). The Court accepts that there are sufficient limitations on the power to request information and that the requirement of "necessity" is not only inherent in the specific legal provisions that are the subject of this complaint but also to German and European data protection law.

101. In view of these elements, the Court can accept the Federal Constitutional Court's conclusion that the thresholds provided in section 113 of the Telecommunications Act were still acceptable in the light of constitutional law, taking into account also that the obligation to submit a

written request for information was likely to encourage the authority to obtain the information only where it was sufficiently needed (see paragraph 178 of the Federal Constitutional Court's judgment cited in paragraph 21 above). In this connection the Court also notes that, in practice, manual retrievals did indeed seem to have been made in a limited number of cases compared to the automated requests under section 112 of the Telecommunications Act (see paragraph 13 above).

102. Lastly, the Court will consider the available possibilities of review and supervision of information requests under sections 112 and 113 of the Telecommunications Act. In *Klass and Others v. Germany* (6 September 1978, § 55, Series A no. 28) the Court held that a review of interferences with the right to respect for private life under Article 8 of the Convention – in that case interferences which took the form of secret surveillance measures – might come into play at three different stages: when the interference was first ordered, while it was being carried out, or after it had been terminated. In cases where the review was effected without the individual's knowledge during the first two stages, it was essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding the individual's rights. On a more general note the Court stated (ibid.):

> "... the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded. One of the fundamental principles of a democratic society is the rule of law, which is expressly referred to in the Preamble to the Convention ... The rule of law implies, *inter alia*, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure."

103. It subsequently relied on these principles, in particular the possibility of effective control and review, concerning different interferences with the right to respect for private life under Article 8 of the Convention (see, for example: storing of sensitive personal data in security files, *Rotaru v. Romania* [GC], no. 28341/95, § 59, ECHR 2000-V; seizure of bank documents, *M.N. and Others*, cited above, §§ 73 and 78; decision to override lawyer's privilege against disclosure of her bank statements in criminal proceedings, *Brito Ferrinho Bexiga Villa-Nova v. Portugal*, no. 69436/10, § 55, 1 December 2015; telephone tapping, *Lambert v. France*, 24 August 1998, § 31, *Reports of Judgments and Decisions* 1998-V; a system of secret surveillance of mobile-phone communications, *Roman Zakharov*, cited above, § 233; and strategic monitoring of communication, *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 117, ECHR 2006-XI). The Court observes, however, that all these cases concerned individualised and more serious and intrusive interferences with the right to respect for private life that cannot be compared to the question

of access to data in the present case. In sum, it considers that the level of review and supervision has to be considered an important, but not decisive, element in the proportionality assessment of the collection and storage of such a limited data set.

104. Turning to the facts of the present case, the Court notes that in principle, subsection 2 of section 113 of the Telecommunications Act clarifies that the responsibility for the legality of the information request lies with the retrieving agency and that the telecommunications providers have no competence to review the admissibility of any request, as long as the information is requested in written form and a legal basis is referred to. Under section 112 of the Telecommunications Act, however, the Federal Network Agency is competent to examine the admissibility of the transmission when there is a special reason to do so.

105. In addition, each retrieval and the relevant information regarding the retrieval (time, data used in the process, the data retrieved, information clearly identifying the person retrieving the data, requesting authority, its reference number, information clearly identifying the person requesting the data) are recorded for the purpose of data protection supervision. This supervision is conducted by the independent Federal and *Länder* data protection authorities. The latter are not only competent to monitor compliance with data protection regulations of all authorities involved but they can also be appealed to by anyone who believes that his or her rights have been infringed through the collection, processing or use of his or her personal data by public bodies.

106. Lastly, the Court notes that the Federal Constitutional Court held that legal redress against information retrieval could be sought under general rules (see paragraph 186 of the Federal Constitutional Court's judgment cited in paragraph 22 above) – in particular, together with legal redress proceedings against the final decisions of the authorities.

107. The Court considers that the possibility of supervision by the competent data protection authorities ensures the availability of a review by an independent authority. Moreover, since anyone who believes that his or her rights have been infringed can lodge an appeal, the lack of notification and confidentiality of the retrieval procedure does not raise an issue under the Convention.

108. Lastly, the Court acknowledges that – as there is no consensus among the member States concerning collection and storage of limited subscriber information (see paragraph 58 above) – member States have a certain margin of appreciation in choosing the means for achieving the legitimate aims of protecting national security and fighting crime, which Germany did not overstep in the present case.

109. Having regard to the above, the Court concludes that the storage of the applicants' personal data by their respective service providers pursuant to section 111 of the Telecommunications Act (in its version examined by

the Federal Constitutional Court – see paragraph 64 above) was proportionate and therefore "necessary in a democratic society".

110. There has accordingly been no violation of Article 8 of the Convention.

FOR THESE REASONS, THE COURT

1. *Declares*, unanimously, the application admissible;

2. *Holds*, by six votes to one, that there has been no violation of Article 8 of the Convention.

Done in English, and notified in writing on 30 January 2020, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Claudia Westerdiek	Yonko Grozev
Registrar	President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the separate opinion of Judge Ranzoni is annexed to this judgment.

Y.G.
C.W.

DISSENTING OPINION OF JUDGE RANZONI

I. Introduction

1. I voted for finding a violation of Article 8 of the Convention in the present case because I cannot agree with the assessment of some of the relevant facts by the majority or their interpretation and application of the Court's general principles.

2. The main question in the present case, to my mind, is the following: what are the requirements under Article 8 – in particular concerning safeguards – with regard to storage of personal data which are qualified as being of limited weight but may easily be retrieved in huge amounts by a broad range of authorities?

3. At the outset, it should be borne in mind and emphasised that the present case is not confined to measures concerning the fight against terrorism or other similar serious crimes, and nor is it limited to issues of national security. The legislation which the Court is called upon to examine also allows storage of data for other less serious purposes, and provides access to such data for different authorities. These include not only courts and criminal prosecution authorities, but also other authorities such as customs investigation services, emergency services, customs administration services concerning undeclared work, the financial supervisory authority and several intelligence agencies.

II. Level of interference

4. My first issue with the findings of the majority concerns the level of interference. The majority concluded that the interference, that is to say the storage of the applicants' personal data, was "while not trivial, of a rather limited nature" (see paragraph 95 of the judgment). In my view, the majority overlooked several relevant facts when assessing the level of this interference.

5. I agree with the majority and the German Federal Constitutional Court ("the Constitutional Court") that no sensitive information was stored. However, the majority overlooked the fact that the data serves as the key to (sensitive) telecommunications data and enables a person to be linked up to a phone number or a phone number to be connected to a person. It thus facilitates the identification of the parties to every telephone call or message exchange and the attribution of possibly sensitive information to an identifiable person. This capability was the purpose of the provision in question. Nevertheless, the majority unfortunately did not take this aspect into account. This is all the more regrettable as the Court had previously dealt with this possibility of identifying the persons behind communications. In *Benedik v. Slovenia* (no. 62357/14, 24 April 2018) the

Court considered the possibilities of identifying an internet user by obtaining the subscriber information associated with a dynamic IP address, and emphasised the significance of the particular context in which the subscriber information was sought. It held (ibid., § 109):

> "... Therefore what would appear to be peripheral information sought by the police, namely the name and address of a subscriber, must in situations such as the present one be treated as inextricably connected to the relevant pre-existing content revealing data ... To hold otherwise would be to deny the necessary protection to information which might reveal a good deal about the online activity of an individual, including sensitive details of his or her interests, beliefs and intimate lifestyle."

6. However, the majority did not take this aspect into account when assessing the level of interference.

7. Nor did the majority consider that the present case, and, in particular, the comprehensiveness of the data storage, are comparable to the cases of *Digital Rights Ireland* and *Seitlinger and Others* and *Tele2 Sverige* and *Tom Watson and Others*, decided by the Court of Justice of the European Union (CJEU) (see paragraphs 51-52 of the judgment). The applicants argued that the data storage at issue was comparable to the one decided by the CJEU, given that it was comprehensive in that it affected all persons using mobile-communication services, even though there was no evidence to suggest that their conduct might have a link to criminal or other offences. The majority dismissed this argument. However, to my mind, the present case in that regard is actually comparable to the cases decided by the CJEU. The aim of section 111 of the Telecommunications Act was to establish a comprehensive register of all users of mobile communications. This is shown *inter alia* by the fact that after having established that incorrect information was stored, the provision was amended and users had to provide proof of their identity. The purpose of the provision was indeed a comprehensive storage of subscriber data, which legislation is assessed *in abstracto* in the present case.

8. Had the majority accepted that section 111 of the Telecommunications Act was aimed at establishing a comprehensive register of all mobile users, it also could have considered the societal consequences of such a register. The Court had previously acknowledged that anonymity had long been a means of avoiding reprisals or unwanted attention and was, as such, capable of promoting the free flow of ideas and information in an important manner (see *Delfi AS v. Estonia* [GC], no. 64569/09, § 147, ECHR 2015). This is consistent, for example, with the opinion of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (see paragraph 56). However, the majority did not discuss this aspect of the interference.

9. In short, to my mind, the majority did not adequately assess the level of interference and, by neglecting certain relevant aspects, concluded that

the interference was limited. This, however, had severe consequences for the examination of the case, because in the subsequent parts the majority overemphasised the limited nature of the interference and consequently also unduly lowered the level of the required safeguards.

III. Proportionality

10. I further disagree with certain aspects of the majority's proportionality assessment.

11. The focus of such an assessment lies in striking a fair balance between the competing public and private interests by examining, on the one hand, the storage of the specific personal data, and on the other hand, the relevant safeguards, in order to limit the measure to what is strictly necessary, to prevent the personal data from being used in a way inconsistent with the guaranties of Article 8, and thus to protect the personal data from misuse and abuse. The outcome of this balancing exercise will depend *inter alia* on the weight to be given to the personal data in issue. The less weight one attaches to this kind of data, the fewer are the safeguards required.

12. This is also the logic behind the CJEU *Ministerio Fiscal* case (see paragraphs 54-55 of the judgment): the less serious the interference, the more readily it can be justified in areas of prevention, investigation, detection and prosecution of criminal offences. The majority alluded to that preliminary reference and its conclusion "that the access to data at issue could not be defined as a serious interference" (see paragraph 94).

13. However, when comparing that case with the present case, some major differences need to be emphasised. The CJEU accepted the interference as justified "in the circumstances" of its case. That case concerned the SIM cards of one stolen mobile telephone that was linked during a period of 12 days with the identity of owners of those SIM cards. The request sought access only to the telephone numbers corresponding to those SIM cards and to the data relating to the identity of the owners of those cards. Only in these circumstances the Luxembourg Court held that access to that specific data could not be defined as "serious" interference.

14. The present case, however, is quite different. First, it does not directly concern access to data, but rather the storage of data. Secondly, it does not relate to a specific criminal investigation with concrete investigative measures to be examined. Thirdly, it is – in contrast to *Ministerio Fiscal* – neither about very specific data (SIM cards from one telephone) nor a limited duration (12 days), but rather about the data sets of millions of people stored for a much longer period. Fourthly, access to data in the present case is not limited for the purpose of combating criminal offences, whether serious crimes or not. Rather, the Telecommunications Act also allows data access for regulatory offences and other general

purposes pursued by customs investigation services, emergency services, customs administration services in relation to undeclared work, the financial supervisory authority and several intelligence services – the latter acting irrespective of concrete dangers (see paragraphs 176-177 of the Constitutional Court's decision). By contrast, most of the member States included in the Court's comparative-law report limit the acceptable purposes to the investigation of crimes or the prevention of threats to public order (see paragraph 58 of the judgment).

15. The Chamber majority in the present case considered "that the stored data is further protected against excessive or abusive information requests by the fact that the requesting authority requires an additional legal basis to retrieve the data" (see paragraph 100 of the judgment). While it is true that the Constitutional Court confirmed that an additional legal basis was required for data retrieval by the relevant authorities, it also conceded that general powers of data collection were sufficient (see paragraph 163 of the Constitutional Court's decision). If one considers the legal provisions in question, which are listed in the judgment (see paragraphs 32-38 of the judgment), it is apparent that most authorities are generally entitled to collect data in performing their legal tasks and duties. Consequently, there is no clear threshold limiting data collection to the investigation of serious crimes or specific serious threats to national security. In that regard, it should also be noted that the Court has already considered the "general clause" for investigative measures under Article 161 of the Code of Criminal Procedure ("CCP) as one of the additional legal bases which, according to the majority, protects mobile subscribers against excessive or abusive information requests. In *Sommer v. Germany* (no. 73607/13, § 58, 27 April 2017) the Court concluded that the threshold for interferences was relatively low and that the provision did not provide particular safeguards.

16. The number of affected persons, which is already high owing to the breadth of the legal regulations, is further increased by the technical design of the database and the query possibilities. Information requests do not need to be limited to specific telephone numbers or names. Section 112(1) of the Telecommunications Act enables the authorities to search on the basis of incomplete data, by means of a similarity function. Therefore, the retrieved data may concern a large number of persons for whom there is no evidence whatsoever to suggest that their conduct might have even an indirect or remote link to criminal or regulatory offences, other than having a similar name or telephone number. Nonetheless, these persons might still be subjected to further investigative measures based on data retrieval under section 112 of the Telecommunications Act.

17. When information is requested and the database is searched, the name/number is compared to every mobile user in the database. Consequently, the personal data of every user is processed, albeit in a limited manner. Depending on the precision of the search criteria, the search

provides a list of all subscribers who meet the criteria. Taking into account the similarity function and incomplete searches, this result list can still encompass data relating to a very large number of people. In order to further reduce the list – and ultimately identify the relevant number or person – the authorities have then to implement additional investigative measures. Therefore, those persons may be subjected to further interferences based on data retrieval under section 112 of the Telecommunications Act, even though they have given no reason for being investigated apart from having a similar name or telephone number. It is important to point out that around 35 million data sets were consulted in 2015 under the automated procedure (see paragraph 67 of the judgment), each data set corresponding to an individual.

18. One of my main disagreements with the majority, however, lies in the assessment of safeguards and whether the existing ones, if any, are sufficient in order to effectively prevent the misuse and abuse of personal data (*S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 103, ECHR 2008, referred to by the majority in paragraph 78). This is, as I see it, the crux of the case.

19. The outcome of the assessment depends *inter alia* on the meaning of "effective" safeguards. In particular, does domestic or international legislation entail, in itself, a sufficient safeguard? The answer should be "no", because legislation only constitutes the legal basis determining the lawfulness of the interference: it does not, in addition and in itself, constitute an effective safeguard. In my understanding of the requirement of effective safeguards, they should protect the individual from the application of national law by domestic authorities in an arbitrary manner and from abuse of legal powers. Such protection must go beyond legal rules, in particular when those rules and legal powers are couched in broad terms, as conceded in this case by the Constitutional Court, and when the rules and powers allow data retrieval in a highly simplified and automated manner. In this regard, I would once again refer to the total of some 35 million data sets which were consulted under the automated procedure in 2015.

20. In support of assertion that sufficient safeguards were in place, the majority relied on the double-door comparison made by the Constitutional Court (see paragraphs 17, 85 and 100 of the judgment). However, as seen above, the legal provisions for data retrieval are very general and broad. While they may suffice as legal keys for the double door, there is no subsequent mechanism to control the information passing through. The double-door can be easily opened by those keys, but there is nobody waiting on the other side of the door to check which items pass the door and are subsequently used.

21. Furthermore, the majority argue that not only was the retrieval safeguarded by legal provisions, but it was also limited to necessary data, a requirement itself safeguarded by a general obligation to erase data that is

not needed (see paragraph 100). What does that mean and what do the safeguards actually consist of? In my view, to put it simple, they consist of general provisions for data retrieval which, according to the majority, are "protected" by a general necessity requirement, which is "safeguarded" by a further general obligation. I fail to see any real protection against possible misuse and abuse. Consequently, in the circumstances of the present case, the double-door concept does not provide such an efficient safeguard.

22. Retrievals of personal data do not require an order by a judicial or otherwise independent authority. While the Federal Network Agency ought – at least for requests under section 112 of the Telecommunications Act – to examine the admissibility of the transmission when there is a special reason for doing so, the Constitutional Court itself has rightly pointed out that since the retrieving authority does not have to give reasons for its request, such an eventuality will hardly ever arise (see paragraph 18 of the judgment). Therefore, this agency is not able to act as an efficient safeguard. For information retrievals under section 113 of the Telecommunications Act, paragraph 2 of that section makes clear that the responsibility for the legality of the information request lies with the retrieving agency and that the telecommunications providers have no competence to review admissibility, as long as the information is requested in written form and a legal basis is invoked. In sum, the retrieving authority is competent to issue an information request and at the same time also to examine the admissibility of its request. In other words, the retrieving authority is its own safeguard. However, effective review and supervision of retrieval requests, whether submitted under section 112 or 113 of the Telecommunications Act, by a judicial or otherwise independent authority, are lacking.

23. The Court has previously accepted that a retrospective review of interference can be sufficient in the context of security operations. However, information requests under the automated procedure occur without the knowledge of the telecommunications provider or of the relevant subscriber, and there is no obligation to notify a mobile-telephone subscriber of the fact that his or her personal details have been retrieved. A similar situation exists for manual information requests under section 113 of the Telecommunications Act, since paragraph 4 of that provision requires telecommunications providers to ensure the confidentiality of the request for information and of the information provided in support of it (see paragraph 31 of the judgment). Consequently, the victim of the interference has no knowledge and cannot seek a review of the information retrieval.

24. The majority accepted this consequence by relying *inter alia* on the Constitutional Court's argument that redress can be sought together with legal redress proceedings against final decisions of the authorities (see paragraph 105). However, this only applies to information requests that have led to further telecommunications surveillance or other investigative

measures. Even in this case, only the further investigative measure can be challenged, but not the information retrieval and storage itself. Moreover, this form of review is only available to a very limited number of victim categories. The vast majority of them are left without any possibility of review.

25. In this connection, the Chamber judgment eventually refers to the supervision conducted by the data protection authorities (see paragraph 107). Notwithstanding the important work done by these authorities, it appears unrealistic for them to review some 35 million data sets consulted by a wide range of different authorities. Given the personnel available to these data protection authorities and their broad range of tasks, this constitutes neither an adequate form of review nor an effective safeguard.

IV. Conclusion

26. My assessment of domestic legislation and practice in the present case leads me to conclude that the available safeguards are not at all sufficient to effectively prevent the misuse and abuse of vast amounts of personal data, to which I attach considerably more weight than my colleagues in the Chamber have done. I take the view, therefore, that the interference in the applicant's Article 8 rights was not proportionate to the legitimate aims pursued, in particular because the domestic legislation was not confined to measures against terrorism or other serious crimes or to issues of national security, but in fact went far beyond that. The interference did not correspond to a "pressing social need" and, consequently, was not necessary in a democratic society.

27. This led me to vote for finding a violation of Article 8 of the Convention.