## NJ 2020/431

Dommering, E.J.

**Publication date**
2020
**Document Version**
Final published version
**Published in**
Nederlandse Jurisprudentie

**NJ 2020/431**

**EUROPEES HOF VOOR DE RECHTEN VAN DE MENS**
30 januari 2020, nr. 50001/12
(Y. Grozev, A. Nußberger, S. O'Leary, C. Ranzoni, M. Mits, L. Hüseynov, L. Chanturia)
m.nt. E.J. Dommering

Art. 8 EVRM

NJB 2020/1054
RAV 2020/31
ECLI:CE:ECHR:2020:0130JUD005000112

**Recht op eerbiediging privéleven. Wettelijke verplichting voor telecomproviders om bij prepaid simkaarten persoonsgegevens op te slaan en op verzoek te delen met autoriteiten. Geen schending art. 8 EVRM.**

*Klagers, civil rights-activisten Patrick en Jonas Breyer, hebben een klacht ingediend bij het Duitse Bundesverfassungsgericht, omdat zij als prepaid simkaarthouders identificatiegegevens hebben moeten registreren (naam, adres en geboortedatum). Telecomproviders zijn op grond van art. 111 van de Duitse Telecommunicatiewet hiertoe verplicht. Verzoekers vinden dat deze wettelijke verplichting een schending oplevert van onder meer het recht op privacy (art. 8 EVRM) en het recht op vrijheid van meningsuiting (art. 10 EVRM). Het Bundesverfassungsgericht stelt hen in het ongelijk, waarop zij een procedure bij het Straatsburgse Hof zijn gestart.*

*EHRM: Omdat de klacht primair ziet op het opslaan van gegevens, wordt de zaak alleen onder art. 8 EVRM behandeld. Aan het begrip 'privéleven' moet een ruime reikwijdte worden gegeven. Geïnterpreteerd en uit eerdere jurisprudentie van het Hof blijkt dat een dataverzameling binnen het bereik van art. 8 kan vallen. Art. 8 EVRM bevat een recht op informationele zelfbestemming en individuen kunnen een beroep doen op het recht op privacy wanneer data worden verzameld, verwerkt en verspreid, ook al zijn die data op zichzelf neutraal van aard. Dit betekent dat de plicht tot opslaan van persoonsgegevens in de zin van art. 111 van de Duitse Telecommunicatiewet, een inmenging vormt in het recht op privacy, beschermd door art. 8 EVRM.*

*Deze inbreuk heeft evenwel een wettelijke basis en dient een legitiem doel, te weten het beschermen van openbare veiligheid, het opsporen van strafbare feiten en de bescherming van de rechten en vrijheden van anderen. Registratie van telefoongebruikers kan bijdragen aan effectieve rechtshandhaving. Aan lidstaten komt een zekere margin of appreciation toe als het gaat om de keuze van maatregelen om de nationale veiligheid te beschermen. De maatregel moet wel proportioneel zijn en er moet sprake zijn van fair balance tussen het individuele belang en het algemeen belang. In dit geval is de inbreuk proportioneel. Bij prepaid-kaarten wordt slechts een beperkt aantal gegevens opgeslagen die bovendien geen uiterst persoonlijke informatie betreffen. Ze zijn beperkt tot gegevens die nodig zijn om de gebruiker te kunnen identificeren en er worden bijvoorbeeld geen data over inhoudelijke communicatie opgeslagen. Bovendien zijn in de artikelen 112 en 113 van de Duitse Telecommunicatiewet waarborgen opgenomen als het gaat om gegevensopslag, een beperkte bewaartermijn (maximaal een jaar na beëindiging contract), de toegang tot en het gebruik van de opgeslagen gegevens en het (onafhankelijke) toezicht daarop en de mogelijkheden om bezwaar te maken tegen een informatieverzoek. Aldus is geen sprake van een schending van art. 8 EVRM.*

Breyer
tegen
Duitsland

**EHRM:**

*The law*

Alleged violation of Article 8 and Article 10 of the Convention

59. The applicants complained that, as users of pre-paid mobile phone SIM cards, certain personal data were stored by their respective telecommunication service providers owing to the legal obligation provided in section 111 of the Telecommunications Act. They invoked 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, so far as relevant in 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. Rights of the Convention to be assessed

60. At the outset the Court notes that the applicants invoked 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 the applicants before the Court 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 (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, date of the contract. This provision does not extend to traffic data, location data or data which reveals 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 just described 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 nor with their freedom of expression.

62. The Court is therefore not called in the present case to decide if and to what extent Article 10 of the Convention maybe be considered as guaranteeing a right for users of telecommunication 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 (*NJ* 2016/457, m.nt. E.J Dommering; *red.*)) and how this right would have to be balanced against others imperatives (see, *mutatis mutandis, K.U. v. Finland*, no. 2872/02, § 49, 2 December 2008 (*NJ* 2009/470, m.nt. E.A. Alkema; *red.*)).

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 has been temporarily stored by the telecommunication 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 later amendment to the Telecommunications Act of 2016 are still pending before the Federal Constitutional Court (see paragraphs 11 and 28 above). The Court therefore will 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 forced them to disclose their personal data, which was subsequently 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 could be easily circumvented at that time by submitting false names or using stolen, second-hand or foreign SIM cards. It was also not necessary as the identification of suspected mobile-telephone users could be easily 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 pre-requirements 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

(paragraph 61). 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 pre-paid SIM cards to specific individuals. This possibility would contribute to effective law enforcement and serve to avert danger. The possibilities to circumvent 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 (*NJ* 2009/410, m.nt. E.A. Alkema; *red.*)). 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 (reference 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 pre-paid 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 the judgment in *Delfi AS v. Estonia* (cited above, §§ 147-48 (*NJ* 2016/457, m.nt. E.J. Dommering; *red.*)). 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* (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' (*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 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 (*NJ* 2018/67, m.nt. E.J. Dommering; *red.*)).

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 — see, for example, the use of surveillance via GPS in criminal investigations (*Uzun v. Germany*, no. 35623/05, 2 September 2010, or *Ben Faiza v. France*, no. 31446/12, 8 February 2018), the disclosure of identifying information to law enforcement authorities by telecommunication providers (*K.U. v. Finland*, no. 2872/02, 2 December 2008 (*NJ* 2009/470, m.nt. E.A. Alkema; *red.*) or *Benedik v. Slovenia*, no. 62357/14, 24 April 2018), the indefinite retention of fingerprints, cell samples and DNA profiles after criminal

proceedings (*S. and Marper*, cited above (*NJ* 2009/410, m.nt. E.A. Alkema; *red.*)), the so-called metering or collection of usage or traffic data (*Malone v. the United Kingdom*, no. 8691/79, 2 August 1984 (*NJ* 1988/534, m.nt. J.V. van Dijk; *red.*); *Copland v. the United Kingdom*, no. 62617/00, 3 April 2007 (*NJ* 2007/617, m.nt. E.J. Dommering; *red.*)) or the inclusion of sex offenders in an automated national judicial database subsequent to a conviction for rape (*B.B. v. France*, no. 5335/06, *Gardel v. France*, no. 16428/05 and *M.B. v. France*, no. 22115/06, all 17 December 2009) — none of the previous cases have concerned the storage of such a data set as in the present case.

77. An obligation, similar to 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 indeed 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, 4 December 2015 (*NJ* 2017/185, m.nt. E.J. Dommering; *red.*)). However, given the further possibilities of 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 *S. and Marper* (cited above, § 103 (*NJ* 2009/410, m.nt. E.A. Alkema; *red.*)) the Court has held the following:

> '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 (…), paragraph 47 above). The domestic law must also afford adequate guarantees that retained personal data are efficiently protected from misuse and abuse (see Article 7 of the Data Protection Convention — 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 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 (*Roman Zakharov*, cited above, § 232 (*NJ* 2017/185, m.nt. E.J. Dommering; *red.*); *Liblik and others v. Estonia*, nos. 173/15 and others, § 131, 28 May 2019; *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 (*NJ* 2009/410, m.nt. E.A. Alkema; *red.*)).

(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 respect 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 (*Leander v. Sweden*, 26 March 1987, § 48, Series A no. 116). It takes furthermore 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 14 above (§ 122)).

(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 accessi-

ble 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 amongst 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 (*NJ* 2009/410, m.nt. E.A. Alkema; *red.*)).

84. The Court finds that the storage of the applicants' personal data, when acquiring mobile-telephone SIM cards, was 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 outlined.

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 concept' explained by the Federal Constitutional Court (see paragraph 14 above (§ 123)), in conjunction with the relevant legal basis for individual information requests. The Court considers, however, that the question of foreseeability and sufficient detail of 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 further assess them 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 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 explanation of the Federal Constitutional Court's 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 21 above (§ 176)). These purposes are further emphasized 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; *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 are adapted (*S. and Marper*, cited above, § 105 (*NJ* 2009/410, m.nt. E.A. Alkema; *red.*)).

89. The Court observes that the Government argued that the possibility to correlate mobile-telephone numbers of pre-paid 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 had been no empirical evidence that mandatory registration had led to a reduction in crime. Moreover, they argued that identification could be easily 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 to circumvent 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 pre-paid 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 paragraph 15 above (§§ 138 and 139)) that only a limited data set was stored. This 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 was sto-

red. 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 (*NJ* 1988/534, m.nt. J.V. van Dijk en *NJ* 2007/617, m.nt. E.J. Dommering; *red.*)), geolocating (*Uzun* and *Ben Faiza*, both cited above), or the storage of health or other sensitive data (see, for example, *S. and Marper*, cited above (*NJ* 2009/410, m.nt. E.A. Alkema; *red.*), *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; *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 and 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 that at issue in a different preliminary reference, *Ministerio fiscal* (paragraph 54 above). As the CJEU stated in the latter 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 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 ended. Moreover, the stored data appears limited to the necessary information 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, 103, with further references (*NJ* 2009/410, m.nt. E.A. Alkema; *red.*)).

98. Regarding section 112 of the Telecommunications Act the Court agrees with the Federal Constitutional Court (see paragraph 18 above (§ 156)) 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 nonetheless is 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 21 above (§ 177)).

100. Concerning both provisions, the Court observes 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. As explained by the Federal Constitutional Court through its double door comparison (see paragraph 14 above (§ 123)), 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 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 any data they do not need without undue delay. The Federal Constitutional Court had pointed out that the requirement of 'necessity' meant in the context of prosecution of offences that there had to be at least an initial suspicion (see paragraph 21 above (§ 177)). The Court accepts that there are sufficient limitations to the power to request information and that the requirement of 'necessity' is not only inherent in the specific legal provisions 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 also into account 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 21 above (§ 178)). In this respect the Court also notes that, in practice, manual retrievals seemed indeed 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 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 is first ordered, while it is being carried out, or after it has been terminated. In case the review is effected without the individual's knowledge during the first two stages, it is 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 para. 2 (art. 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 v. San Marino*, cited above, §§ 73, 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 (*NJ* 2017/185, m.nt. E.J. Dommering; *red.*); strategic monitoring of communication — *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 117, 29 June 2006). 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 transferred to the access of data in the present case. In sum it considers that the level of review and supervision has to be considered as 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 under section 113 of the Telecommunications Act its paragraph 2 clarifies that the responsibility for the legality of the information request lies with the retrieving agency and that the telecommunication 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 invoked. 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 indepen-

dent Federal and *Länder* data protection authorities. The latter are not only competent to monitor compliance with data protection regulation 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 may be sought under general rules (paragraph 22 above (§ 186)) — 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 review by an independent authority. Moreover, since anyone, who believes 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 had 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 FCC — see paragraph 64) 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.

**Noot**

1. In deze uit Duitsland afkomstige zaak staat centraal de uitleg die het Bundesverfassungsgericht (hierna: BVerfG) aan de Duitse telecommunicatiewetgeving heeft gegeven met betrekking tot de opslag van persoonlijke communicatiegegevens. Het gaat om het opslaan van persoonsgegevens op Simkaarten. De zaak vertoont daarom verwantschap met de uitspraak van het HvJ EU in de Spaanse zaak *Ministerio Fiscal* (HvJ EU 2 oktober 2018, *NJ* 2020/232, m.nt. E.J. Dommering), die het EHRM ook onder het relevante recht vermeldt.

2. De klagers zijn Duitse civil rights-activisten die over deze kwestie een klacht wegens schending van de Duitse Grondwet hadden ingediend bij het BVerfG. De feiten zijn als volgt: in 2004 werd ter implementatie van EG-richtlijnen de Telecommunicatiewet aangepast en de mogelijkheid om persoonsgegevens op Simkaarten op te slaan verruimd. Tot dan toe ging het alleen om gegevens die nodig waren voor het afrekenen van het gebruik van de mobiele telefoon en voor andere contractuele doeleinden. Bij prepaid mobiele telefoons was dat niet nodig, maar de wetswijziging maakte mogelijk dat het nu wel mocht. De twee klagers, gebruikers van prepaid mobiele telefoons, verzetten zich dat zij door die registratie als gebruiker hun anonimiteit moesten prijsgeven.

3. In zijn beslissing opent het BVerfG met een klaroenstoot, die in de Engelse vertaling in de beslissing van het EHRM als volgt klinkt:

> "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."

Dit is de modernisering van zijn eerste uitspraak over dit zelfbeschikkingsrecht in de jaren tachtig van de vorige eeuw (BVerfG 15 december 1983, *Neue Juristische Wochenschrift* 1984, p. 419):

> "Iedereen die er niet zeker van kan zijn dat gegevens over maatschappelijk afwijkend gedrag voor langere tijd worden geregistreerd en kunnen worden gebruikt op een manier waarvan hij niets weet, zal proberen om dat gedrag niet te vertonen. Dat is in strijd met de elementaire functie van zelfbeschikking in een democratische samenleving waarin de burgers de mogelijkheid moeten hebben om deel te nemen aan het maatschappelijke en politieke leven zonder

risico te lopen op een voor hem ondoorzichtige manier te worden geregistreerd."

4. Maar dan zet toch een fijnmazige vioolpartij van geoorloofde en noodzakelijke beperkingen in. Je moet om te beginnen kijken of de inmenging gerechtvaardigd is en dat vindt het Hof omdat het aanleggen van een databank voor het bestrijden van criminaliteit waarin anoniem of onder een valse naam bellen een grote rol speelt, gerechtvaardigd is. Dan volgt een beoordeling van de proportionaliteit van de inbreuk. Op zichzelf is het registreren van de gebruikers van de prepaid mobiele telefoons een flinke inbreuk op het zelfbeschikkingsrecht maar de mate van inbreuk die het verzamelen oplevert is, in het licht van de al of niet daarop volgende beperkingen in de verwerkingen, proportioneel en daardoor geoorloofd. Het BVerfG:

"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 (...) 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."

5. Het BVerfG voegt hier een nauwgezette proportionaliteitstoetsing aan toe waarin het de heimelijke waarneming in real life vergelijkt met die in cyberspace en laat zien dat die in cyberspace minder ver gaat als je de verzameling van gegevens beperkt tot de registratie van een identiteit zonder verdere verwerking:

"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."*

6. Deze aanpak neemt het EHRM over en het wijst daarom de klacht (met één dissenting opinion) af. Het zet iets bescheidener en ook casuïstischer in dan het BVerfG in de overwegingen 74 e.v.:

"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,[1] 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).

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 form or manner that their Article 8 rights may be engaged."

Volgt een overweging 76 met alle gevallen waarin het Hof de verzameling en opslag van persoonsgegevens een inbreuk op artikel 8 EVRM heeft bevon-

1 [Het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, *Trb.* 1988, 7, *red.*].

den. Het stelt vast dat het in de zaak *Roman Zakharov* (EHRM 4 december 2015, appl. 47143/06, *NJ* 2017/185, m.nt. E.J. Dommering, overwegingen 132-33 en 269-70) om de beoordeling van de proportionaliteit van de opslag ging. Maar een kernbeslissing blijft de zaak *S. en Marper* (EHRM 4 december 2008, appl. 30562/04 en 30566/04) in het bijzonder de overweging in die beslissing, die het ook in dit arrest citeert:

> "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 (...), paragraph 47 above). The domestic law must also afford adequate guarantees that retained personal data are efficiently protected from misuse and abuse (see Article 7 of the Data Protection Convention — paragraph 47 above) (...)."

7. Het Hof pakt het ongeveer op dezelfde manier aan als het BVerfG. In overweging 90 gaat het mee met het argument dat er een legitiem doel is:

> "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 to circumvent 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 pre-paid 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."

8. Evenals de Duitse rechters stelt het vast dat de onderhavige registratie op zichzelf nauwelijks een privacy-inbreuk is:

> "This 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 was 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), geolocating (Uzun and Ben Faiza, both cited above), or the storage of health or other sensitive data (see, for example, S. and Marper, cited above, 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; Shimovolos v. Russia, no. 30194/09, 21 June 2011)."

9. In zijn conclusie dat de inbreuk proportioneel is, refereert het Hof uitdrukkelijk aan de aan het begin van deze noot geciteerde beslissing van het HvJ EU in *Ministerio Fiscal:*

> "Indeed the data at issue in the present case bear greater resemblance to that at issue in a different preliminary reference, Ministerio fiscal. As the CJEU stated in the latter 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 data at issue could not be defined as a serious interference with the fundamental rights of the persons whose data were concerned."

In de overwegingen 96-98 noemt het verder als relevante omstandigheden: de noodzaak van registratie voor beveiligingsdoeleinden, de termijn van opslag gerelateerd aan de tijd die redelijkerwijs nodig is voor onderzoek, de gereguleerde toegankelijkheid. Dat laatste vindt het Hof heel belangrijk. In overweging 97 stelt het:

> "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".

10. Het Hof vindt dat de waarborgen in de Duitse regeling voldoende zijn, maar het vraagt in overweging 102 aparte aandacht voor de rechtsbescherming waarin het de stand van de opvattingen van het Hof hierover samenvat:

> "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 review of interferences with the right to respect for private life under Article 8 of the Convention — in that case interfe-

rences which took the form of secret surveillance measures — might come into play at three different stages: *when the interference is first ordered, while it is being carried out, or after it has been terminated. In case the review is effected without the individual's knowledge during the first two stages, it is 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 para. 2 (art. 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.'"

Maar als het om een lichte niet geïndividualiseerde inbreuk gaat is dat toch weer niet doorslaggevend (r.o. 103, 106 -108):

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

(.. 106):

"Lastly, the Court notes that the Federal Constitutional Court held that legal redress against information retrieval may be sought *under general rules* — 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 review by an independent authority. Moreover, since anyone, who believes 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 — Member States had 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."

11. Het belang van de beslissing is vierledig. 1. Zowel het HvJ EU als het EHRM erkent dat bij de huidige stand van de informatietechnologie in het belang van de organisatie van de samenleving en bescherming van de veiligheid van de samenleving en de burgers grootschalige opslag van persoonsgegevens onvermijdelijk is. 2. Je moet bij de beoordeling van de mate van inbreuk die het verzamelen en opslaan van persoonsgegevens oplevert in aanmerking nemen wat zij precies omtrent het privéleven onthullen. Vroeger maakten wij een onderscheid tussen persoonsgegevens en 'gevoelige gegevens' (zoals bijvoorbeeld levensovertuiging), nu moet je binnen de persoonsgegevens een onderscheid maken tussen gegevens die alleen naar de identiteit van de persoon verwijzen en die welke het persoonlijke leven kunnen ontsluiten (gedragsgegevens). Helemaal nieuw is dat niet, omdat NAW-gegevens altijd een lichter regiem van bescherming hebben gekend. 3. Van belang is welke waarborgen er zijn in het verwerkingstraject: het doel van de verzameling, de duur van de opslag (de redelijke tijd die nodig is om die in stand te houden), de toegankelijkheid voor functionarissen en derden, de methode van verwerking. 4. Er is een integrale beoordeling nodig van de (individueel of collectief, vooraf, tijdens, achteraf) rechtsbescherming tegen verkeerd gebruik in relatie tot de aard van de opslag. Dat hoeft niet per se een rechterlijke instantie te zijn, als de instantie maar onafhankelijk is en effectief. Het hele traject van toezicht moet in aanmerking worden genomen.

E.J. Dommering