NJ 2020/192

Dommering, E.J.

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

NJ 2020/192

EUROPEES HOF VOOR DE RECHTEN VAN DE MENS
24 januari 2019, nr. 43514/15
(L.-A. Sicilianos, A. Pejchal, K. Turković, A. Harutyunyan, P. Koskelo, T. Eicke, G. Felici)
m.nt. E.J. Dommering

Art. 8 EVRM

NJB 2019/587
ECLI:CE:ECHR:2019:0124JUD004351415

Recht op eerbiediging voor privéleven. Opslag van persoonsgegevens van vredesactivist in extremisme-databank politie. Belangenafweging. Databank dient legitiem doel, maar voortdurend bewaren gegevens in casu disproportioneel. Schending art. 8 EVRM.

De in 1925 geboren Brit John Oldroyd Catt is gedurende een groot deel van zijn leven vredesactivist geweest. Hij heeft regelmatig deelgenomen aan verschillende demonstraties, onder andere aan acties van de organisatie Smash EDO tegen de activiteiten van een Amerikaans wapenbedrijf in het Verenigd Koninkrijk. Hij is in dat kader door de politie aangehouden, maar dit heeft nooit tot een strafrechtelijke veroordeling geleid. Op zijn verzoek heeft de politie hem in 2010 inzage gegeven in informatie die over hem was opgeslagen in een politie-databank over 'binnenlands extremisme' (domestic extremism). Deze ingevoerde gegevens betroffen Catt's naam, zijn aanwezigheid bij een evenement, geboortedatum, adres en soms een beschrijving van zijn uiterlijk. Catt heeft hierop de Association of Chief Police Officers (ACPO) verzocht de gegevens over hem te vernietigen. ACPO heeft dit verzoek afgewezen. In de procedures die hierop volgden en waarbij duidelijk werd dat er nog meer gegevens van hem waren opgeslagen dan destijds door de politie gemeld, heeft uiteindelijk de Supreme Court Catt op 4 maart 2015 in het ongelijk gesteld.

EHRM: de noodzaak om de gegevens te verzamelen is komen vast te staan. De databank van de politie diende in het onderhavige geval een legitiem doel, te weten het voorkomen van wanordelijkheden en strafbare feiten en de bescherming van de rechten en vrijheden van anderen. Het verzamelen van de gegevens over klager was gerechtvaardigd, omdat over de activiteiten van Smash EDO bekend was dat deze gewelddadig waren. Hoewel klager zelf nooit gewelddadig is geweest, heeft hij zich wel meerdere malen openlijk met Smash EDO geïdentificeerd.

Het voortdurend bewaren van de gegevens was evenwel disproportioneel. Klager, zo heeft de Britse regering erkend, vormde alleen al vanwege zijn hoge leeftijd geen dreiging voor wie dan ook. Dit terwijl gegevens in het geding zijn waaruit politieke opvattingen blijken, die effect kunnen hebben op de vrijheid van meningsuiting en het demonstratierecht en die daarom een hoger beschermingsniveau toe komen. De procedure om deze gegevens te verwijderen boden onvoldoende waarborgen. Zo was er te weinig duidelijkheid over een tijdslimiet met betrekking tot de bewaartermijn, zijn bij een herbeoordeling niet alle relevante overwegingen betrokken en bleken de nationale autoriteiten gaandeweg de procedure meer gegevens te hebben bewaard dan zij aanvankelijk hadden aangegeven.

Volgt: Schending art. 8 EVRM.

Catt
tegen
Verenigd Koninkrijk

EHRM:

The law

I. Alleged violation of Article 8 of the Convention

72. The applicant complained that the retention of his data by the police was in violation of his right to privacy as provided in Article 8 of the Convention, which reads as follows:

'1. Everyone has the right to respect for his private and family life, his home 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 the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

A. Admissibility

73. The Government raised two arguments relating to admissibility.

74. The first was that the applicant was no longer a victim to the extent claimed in his application, because nearly all the entries in the database he complained of were deleted in 2012.

75. In this connection, the applicant underlined that his complaint was about the refusal of the police in 2010 to delete the sixty six records mentioning him in their database, which were collected and retained from 2004 onwards. The fact that all but six of those records were deleted in 2012 in the context of a weeding procedure triggered by revelations about undercover police work in unrelated domestic proceedings was not relevant.

76. The Court notes that the applicant's data was first collected and retained in 2005 (see paragraph 9, above). Since then, the police have continually retained his personal data on the database in one form or another. He has therefore had victim status from a Convention perspective since 2005. This conclusion is not affected by the fact that some of the applicant's personal data was deleted in 2012.

77. The second argument made by the Government was that the applicant had at his disposal a range of judicial remedies which he could have used to secure the deletion of his personal data.
78. The Court recalls that under its established case-law, when a remedy has been pursued, use of another remedy which has essentially the same objective is not required (see, *inter alia, Micallef v. Malta* [GC], no. 17056/06, § 58, ECHR 2009 (*NJ* 2010/180, m.nt. E.A. Alkema; *red.*) and *Kozacıoğlu v. Turkey* [GC], no. 2334/03, § 40, 19 February 2009 (*RvdW* 2007/1079; *red.*)).
79. In light of the above, the Court notes that the application 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.

B. Merits
1. The parties' submissions
80. The applicant complained that the systematic collection and retention of information about him in a searchable database amounted to an interference with his right to privacy under Article 8. He argued that this interference was not justified because the database on which the data were held did not provide sufficient safeguards and so was not in accordance with the law. In particular he argued that the scope of the database may be adjusted arbitrarily by the police; data is retained for excessively long periods on the basis that the database as a whole may be useful; data is subject to automated and manual processing. He did not make arguments based on data protection legislation but submitted that the retention is unjustified given that the data retained related to his involvement in proper and lawful political protest activity and has never been useful for any police functions. The retention of such data is likely to have a chilling effect.
81. The applicant also argued that as records relating to him were found on the database after the Supreme Court's decision, the Supreme Court had made its decision on an incomplete factual basis. Recalling his assertion that the database had inadequate safeguards, the applicant argued that the fact records are not properly disclosed even in the context of proceedings before the Supreme Court indicates that the database is not in accordance with the law. He also alleged that there is no real system of oversight or independent review, emphasising that making a 'subject access request' under the DPA will only be effective if all relevant data is disclosed by the police when they receive such a request. The applicant also asserted that the margin of appreciation to be afforded in light of the decisions of the domestic courts is reduced, given that those courts did not have all the relevant information before them.
82. The Government accepted that the collection and retention of information about the applicant constituted an interference with his right to respect for private life. However, relying on the findings of the Supreme Court, they contended that the interference was very limited.
83. They also relied on the findings of the Supreme Court that the interference was in accordance with the law, being subject to the Data Protection Act 1998, and a statutory Code of Practice and Guidance.
84. As to the necessity of storing the applicant's information, the Government underlined that the differences of view between the Court of Appeal and the Supreme Court reflect opinions properly open to both courts on the evidence. With reference to the extensive amount of judicial scrutiny on this point at the domestic level, they contended that the question of whether it was necessary to retain the applicant's data falls within the state's margin of appreciation.
85. In relation to the disclosure of additional reports concerning the applicant after the domestic proceedings, the Government stated that these do not have any particular impact on the standing of the domestic judgments and that the applicant should make use of domestic remedies to bring a challenge concerning those disclosures, for example by way of judicial review.

2. The submissions of third party interveners
(a) The Equality and Human Rights Commission
86. The Equality and Human Rights Commission (EHRC) submitted remarks concerning the Extremism Database, which it characterised as a computerised and searchable police database which stores large quantities of intelligence about lawful public protests and those attending such protests. According to the EHRC, the database is not established under any legislation, has no statutory foundation, nor does any published policy refer to its creation, purposes or function.
87. The intervention recalls relevant standards and guidance set out in various international instruments including the Article 17 of the International Covenant on Civil and Political Rights and the Council of Europe's Committee of Ministers' Recommendation R(87) Regulating the use of personal data in the police sector. Drawing on the case law of this Court and the Court of Justice of the European Union, it goes on to set out what it considers to be the core minimum principles required to satisfy the requirement that a legal regime is 'in accordance with the law' in the context of the police database at issue in this case. Those are:
(i) the creation of police powers must be published and accessible to the public;
(ii) clear and publicly accessible safeguards are required to ensure that the interference does not

occur in an arbitrary, inappropriate or unnecessary manner;
(iii) there must be clear and accessible criteria enabling individuals, whose personal data is stored, to secure its deletion, including by way of independent review;
(iv) information relating to those not suspected of criminal activity must be removed.
88. The EHRC then concluded that the minimum safeguards are not present in relation to the Extremism Database. They also highlighted the danger of a chilling effect on legitimate political protests where the Extremism Database contains information about political activities.

(b) Privacy International
89. Privacy International is an NGO based in the United Kingdom and concerned with unlawful use of surveillance.
90. Privacy International criticised the Supreme Court's characterisation of the interference with the applicant's right to privacy as minor because it relates to activities that occurred in public, underlining that the collection of such information should be seen in its context. Privacy International argued that with rapid technological development, this approach would allow the monitoring of large amounts of information which is to some extent public, such as information from social media, facial recognition technology, body worn cameras, CCTV and automatic number plate recognition technology. It criticised the absence of legislation governing the collection and use of data obtained from such sources.
91. Privacy International concluded that the retention of such data is an infringement of privacy rights and also the right to freedom of expression, again underlining that such an infringement cannot be characterised as minor.

3. The Court's assessment
(a) Interference
92. In light of the conclusion of the Supreme Court, the Government conceded that the collection and retention of the applicant's personal data interfered with his Article 8 rights. However, they argued that the infringement in the applicant's rights was limited.
93. The Court recalls that it is well established in its case-law that the mere storing of information amounts to an interference with the applicants' right to respect for private life as secured by Article 8 § 1 of the Convention (see *S. and Marper*, cited above, § 67 and *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, § 73, ECHR 2006-VII with further references (*NJ* 2009/449, m.nt. E.J. Dommering; *red.*)). The Court considers that the question of the alleged 'limited' nature of the interference in the applicant's rights is more appropriately addressed in the context of whether the interference was necessary in a democratic society (see paragraphs 109-128, below).

(b) Justification
(i) In accordance with the law
94. As the Court has recalled the expression 'in accordance with the law' not only requires the impugned measure to have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the person concerned and foreseeable as to its effects. For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope and discretion conferred on the competent authorities and the manner of its exercise (see, among other authorities, *M.M. v. the United Kingdom*, no. 24029/07, § 193, 13 November 2012 with further references).
95. The Court has also observed that there are various crucial stages at which data protection issues under Article 8 of the Convention may arise, including during collection, storage, use and communication of data (*M.M.*, cited above, § 195).

(α) Collection of data
96. Turning to the question of the collection of data, the Court notes that in the present case the collection of data was undertaken on the basis of general police powers in the common law, with reference to a working definition of 'domestic extremism'. That definition varied between bodies in the police, and its ambiguity has been criticised by HMIC [Her Majesty's Inspectorate of Constabulary, een overheidsdienst die toezicht houdt op de politie, *red.*] (…).
97. In light of the general nature of the police powers and the variety of definitions of the term 'domestic extremism', the Court considers that there was significant ambiguity over the criteria being used by the police to govern the collection of the data in question. It notes that perhaps as a result, the database in issue appears to have been assembled on a somewhat ad hoc basis. The Court therefore agrees with the applicant that from the information available it is difficult to determine the exact scope and content of the data being collected and compiled to form the database.
98. However, the Government have argued that the creation of the database does not need to be statutory. The Court considers that this assertion is supported by Principle 3.1. of the Committee of Ministers' Resolution (74) 29 on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector (…) which states that such databanks must have been provided for by law, or by special regulation or have been made public in a statement or document, in accordance with the legal system of each member state. In this connection the Court notes that the 'management' of data was regulated by legislation and a code of practice (see… paragraph 99) whilst the general police powers which permitted the collection of data were provided for in the common law. The Supreme Court referred to a HMIC report from 2003

(…), and contemporaneous news reporting to support its conclusion that the collection of the applicant's data was foreseeable. The Court notes that the existence of a specific database was not clearly acknowledged until the domestic proceedings in this case, although it accepts that from the information publicly available it was possible to deduce that the police were likely to be maintaining such a database.

99. It is of concern that the collection of data for the purposes of the database did not have a clearer and more coherent legal base. However, the framework governing the collection of the applicant's data cannot be viewed in isolation from the provisions governing retention and use of the applicant's personal data. Accordingly, before coming to a conclusion under this head the Court turns to examine those provisions, which impose certain legal protections against arbitrariness.

(β) Retention and use of data

100. The Court has recently examined the provisions governing the retention of the data in the present case in *M.M.*, cited above. Those provisions were the Data Protection Act and the 2005 Code of Practice on the Management of Police Information. In the present case, those rules on retention of data stated that there was a presumption in favour of retention where data is not excessive, is necessary for a policing purpose, and is up to date. After the initial decision to retain, data must be retained for a minimum of six years. After that point it should be reviewed, and may be deleted. There is no fixed point in time identified for when reviews must take place, or when the data must be deleted. The police retain a general discretion to retain data if it is necessary to do so.

101. In *M.M.*, cited above, the Court found a violation of Article 8 on the basis that the retention and disclosure of personal data was not in accordance with the law. It observed that the indiscriminate and open-ended collection of criminal record data was unlikely to comply with the requirements of Article 8 in the absence of clear and detailed statutory regulations clarifying the safeguards applicable and setting out the rules governing, inter alia, the circumstances in which data can be collected, the duration of their storage, the use to which they can be put and the circumstances in which they may be destroyed. It also noted the absence of any mechanism for independent review of a decision to retain or disclose data (see *M.M.*, cited above, §§ 199– 206).

102. However, whilst the provisions on retention of data in this case bear some similarity to those in *M.M.*, other elements are not the same.

103. In the first instance, the Court notes that *M.M.* concerned the retention of criminal record data which the Court identified as not only personal but also sensitive, with 'potentially devastating consequences' if disclosed. Moreover, the complaint in *M.M.* did not relate to police intelligence gathering but focussed on the disclosure regime for criminal records, and the Court criticised the absence of a statutory framework governing the (in some cases obligatory) communication of such data by the police to prospective employers in Northern Ireland at the time (see *M.M.*, cited above, § 203).

104. Against this background, the Court also notes that in contrast to the applicant in *M.M.*, the applicant in the present case had the possibility to make a request for the review and deletion of his data which he exercised (see *a contrario M.M.*, cited above, § 206).

(γ) Conclusion

105. The Court has concerns about the ambiguity of the legal basis for the collection of the applicant's personal data. In particular the Court notes the loosely defined notion of 'domestic extremism' and the fact that applicant's data could potentially be retained indefinitely. However, the data retained would not be disclosed to third parties; and the applicant had the possibility to apply for the deletion of his data.

106. In this connection, the Court recalls that the question of whether the collection, retention and use of the applicant's personal data was in accordance with the law is closely related to the broader issue of whether the interference was necessary in a democratic society (*S. and Marper,* cited above, § 99, ECHR 2008).

107. Therefore, in view of its analysis in paragraphs 109–128 below, the Court does not find it necessary to decide whether the interference was 'in accordance with the law', within the meaning of Article 8 § 2 of the Convention.

(ii) Legitimate aim

108. There has been no significant dispute about whether the creation and maintenance of the database by the police pursues a legitimate aim. The Court equally considers that it does so, that aim being the prevention of disorder or crime and safeguarding the rights and freedoms of others.

(iii) Necessary in a democratic society

109. The Court has set out on many occasions the elements to be taken into account when considering whether an interference in an applicant's Article 8 rights was necessary and therefore justified. "It will be necessary in a democratic society if it answers to a 'pressing social need', if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are relevant and sufficient". A margin of appreciation must be left to the competent national authorities in this assessment (see *S. and Marper*, cited above, § 101–102).

110. Dealing with the latter element first, the Court notes the Government argued that the domestic courts had closely examined the issues in light of Article 8. Those courts differed in their conclusions but this indicated that the point was one

upon which a correct application of the principles under Article 8 could nonetheless result in a different result. With reference to the extensive amount of judicial scrutiny at the domestic level, they contended that the question of whether it was necessary to retain the applicant's data falls within the state's margin of appreciation and it was therefore not for this Court to decide.

111. In this respect, the Court recalls that in Article 8 cases it has generally understood the margin of appreciation to mean that, where the independent and impartial domestic courts have carefully examined the facts, applying the relevant human rights standards consistently with the Convention and its case-law, and adequately balanced the applicant's personal interests against the more general public interest in the case, it is not for it to substitute its own assessment of the merits (including, in particular, its own assessment of the factual details of proportionality) for that of the competent national authorities, unless there are shown to be compelling reasons for doing so (see *McDonald v. the United Kingdom*, no. 4241/12, § 57, 20 May 2014).

112. However, the Court considers in the present case there are reasons for doing so. In the first place it considers significant that personal data revealing political opinion falls among the special categories of sensitive data attracting a heightened level of protection (see paragraphs 58–60 and 67–70 above and *S. and Marper*, cited above, § 76). It notes that at the domestic level this element of the complaint was characterised as one of data protection law and was not a particular focus of the litigation. Having concluded that retention of the applicant's data was not justified under Article 8, the Court of Appeal did not consider that examining the specific principles of data protection would add anything to their analysis (see § 65). The applicant did not pursue specific data protection arguments before the Supreme Court, which therefore only referred to data protection law generally in the context of lawfulness. However, the Court considers that the nature of the applicant's complaint meant that the sensitive nature of the data in question was a central feature of the case both before the domestic courts as well as before this Court (see paragraph 80 above).

113. The Court also notes that notwithstanding its well established case-law (see paragraph 93, above) the High Court considered that the collection and retention of the applicant's data was not an interference under Article 8. This question was resolved by the Court of Appeal and Supreme Court who found that it was an interference and gave detailed and comprehensive judgments referring extensively to Strasbourg jurisprudence. However the Government maintained arguments that the retention was not systematic and the nature of the interference was limited. The applicant argued that a decisive ruling was necessary. The Court agrees that some clarification of these elements appears to be called for.

114. The Court also recalls the importance of examining compliance with the principles of Article 8 where the powers vested in the state are obscure, creating a risk of arbitrariness especially where the technology available is continually becoming more sophisticated (see *Roman Zakharov v. Russia* [GC], no. 47143/06, § 229, ECHR 2015 (*NJ* 2017/185, m.nt. E.J. Dommering; *red.*), and *Szabó and Vissy v. Hungary*, no. 37138/14, § 68, 12 January 2016). Unlike the present case, those cases dealt with covert surveillance. However, the Court considers it should be guided by this approach especially where it has already highlighted concerns relating to the ambiguity of the state's powers in this domain (see paragraph 105 above).

115. Finally, the Court takes into account the manner and timing of the disclosure and the fact that there was more personal data held on the applicant than revealed at the time of the domestic proceedings (…). This has an impact on its evaluation of the available safeguards (see paragraph 122 below).

116. Therefore, the Court turns to the other elements to be examined, beginning with the question of whether there was a 'pressing social need' to collect and retain the applicant's personal data. In doing so, it recalls that the question for it to examine is not whether there was a 'pressing social need' for the police to establish and maintain such a database. To the extent that the Court examines this issue from a more general aspect, it has done so in its conclusion that the creation of the database pursued a legitimate aim (see paragraph 108 above). At this stage, the Court is examining whether the collection and retention of the applicant's personal data may be regarded as justified under the Convention (see mutatis mutandis, *S. and Marper,* cited above, § 106).

117. As to whether there was a pressing need to collect the personal data about the applicant, the Court accepts that there was. It agrees with the Supreme Court that it is in the nature of intelligence gathering that the police will first need to collect the data, before evaluating its value (…). In this respect, the Court again recalls that the personal data in question was overtly obtained.

118. The Court also agrees with the domestic courts that the police had an obvious role to monitor protests of Smash EDO where the activities of that group were known to be violent and potentially criminal. Therefore, even if the applicant himself was not suspected of being directly involved in that group's criminal activities, it was justifiable for the police to collect his personal data. He had after all decided to repeatedly and publicly align himself with the activities of a violent protest group.

119. As to whether there was a pressing need to retain the applicant's data, the Court considers there was not. It shares the domestic courts' concern that there is a need for caution before overriding the

judgment of the police about what information is likely to assist them in their task (…). In this respect, the Court underlines that its conclusion does not call into question the fact that there may have been a pressing need for the police to retain the applicant's personal data for a period of time after it was collected. However, in the absence of any rules setting a definitive maximum time limit on the retention of such data the applicant was entirely reliant on the diligent application of the highly flexible safeguards in the MOPI to ensure the proportionate retention of his data. Where the state chooses to put in place such a system, the necessity of the effective procedural safeguards becomes decisive (see mutatis mutandis *S.M.M. v. the United Kingdom*, no. 77450/12, § 84, 22 June 2017). Those safeguards must enable the deletion of any such data, once its continued retention becomes disproportionate.

120. In this connection, the Court observes that as the applicant's personal data could potentially be retained indefinitely the only time limit that he could be certain of was that the data would held for a minimum of six years, at which point it would be subject to a scheduled review. In the present case, it is not clear that these six year reviews or any later reviews were conducted in any meaningful way. Certainly, they did not directly result in the deletion of any of the applicant's personal data.

121. The Court notes that the circumstances of the case contrast with the approach set out in principle 4 of the Committee of Ministers' Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis the electronic data banks in the public sector, which states that rules should be laid down to specify maximum time-limits beyond which certain categories of information may not be used or kept, other than in some exceptional situations (…).

122. Also, whilst the applicant could and did request the disclosure and destruction of his data, this safeguard appears to have been of limited impact given the refusal to delete his data or to provide any explanation for its continued retention — including the later disclosure without explanation of the retention of additional data (…). So far as the Court is aware, at least some of the applicant's personal data concerning his involvement in non-violent protest was collected over six years ago and remains in the domestic extremism database (…) despite the fact that the police concluded, and the domestic courts affirmed that the applicant was not considered a danger to anyone (…).

123. Moreover, the absence of effective safeguards was of particular concern in the present case, as personal data revealing political opinions attracts a heightened level of protection (see paragraph 112 above). Engaging in peaceful protest has specific protection under Article 11 of the Convention, which also contains special protection for trade unions, whose events the applicant attended (see paragraph 10, above). In this connection it notes that in the National Coordinator's statement, the definition of 'domestic extremism' refers to collection of data on groups and individuals who act 'outside the democratic process'. Therefore, the police do not appear to have respected their own definition (fluid as it may have been (see paragraph 105)) in retaining data on the applicant's association with peaceful, political events: such events are a vital part of the democratic process (see *Gorzelik and Others v. Poland* [GC], no. 44158/98, § 92, ECHR 2004-I (*NJ* 2005/420, m.nt. E.A. Alkema; *red.*)). The Court has already highlighted the danger of an ambiguous approach to the scope of data collection in the present case (see paragraph 97 above). Accordingly, it considers that the decisions to retain the applicant's personal data did not take into account the heightened level of protection it attracted as data revealing a political opinion, and that in the circumstances its retention must have had a 'chilling effect'.

124. Moreover, principle 2 on the collection of data in Recommendation R (87) 15 (see paragraph 65 above) states that the collection of data on individuals solely on the basis that they belong to particular movements or organisations which are not proscribed by law should be prohibited unless absolutely necessary or for the purposes of a particular inquiry (see mutatis mutandis *Segerstedt-Wiberg and Others*, cited above, § 79). The Court considers that the retention of the applicant's data in particular concerning peaceful protest has neither been shown to be absolutely necessary, nor for the purposes of a particular inquiry.

125. The Court also underlines that it makes these findings about the applicant in light also of his age, which Principle 7 of Recommendation R (87) 15 identifies as a particular consideration in this context (…).

126. The Government have argued that it would be too burdensome to review the database and delete all the entries relating to the applicant, because the database is not fully automated. However, the Court notes that the MoPI [Management of Police Information, *red.*] guidance provides for the data to be reviewed after six years and deleted. Whilst this does not appear to have happened in the present case it nonetheless shows that review and deletion of records was intended to be a real possibility. In this connection the Court also recalls that in 2012 following the HMIC report, a significant number of personal data records were deleted, clearly indicating that review and deletion of records is possible (see paragraph 13, above). The Court also notes the MoPI guidance stipulates the importance of ensuring that information is easy to access and use (…).

127. Accordingly, the Court is not convinced that deletion of the data would be so burdensome as to render it unreasonable. In general terms the Court would add that it would be entirely contrary to the need to protect private life under Article 8 if the Government could create a database in such a

manner that the data in it could not be easily reviewed or edited, and then use this development as a justification to refuse to remove information from that database.
128. The foregoing considerations are sufficient to enable the Court to conclude that there has been a violation of Article 8 of the Convention.

II. Application of Article 41 of the Convention
(Enz., *red.*)

For these reasons, the Court, unanimously,
1. *Declares* the application admissible;
2. *Holds* that there has been a violation of Article 8 of the Convention;
3. *Holds*
(a) that the respondent State is to pay the applicant, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, the following amounts, to be converted into the currency of the respondent State at the rate applicable at the date of settlement:
(i) € 27,000 (Twenty-seven thousand euros), plus any tax that may be chargeable to the applicant, in respect of costs and expenses;
(b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amount at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;
4. *Dismisses* the remainder of the applicant's claim for just satisfaction.

Concurring opinion of Judge Koskelo joined by Judge Felici
A. Approach to the case
1. I agree with the outcome of this case, namely that there has been a violation of the applicant's rights under Article 8 of the Convention. The majority in the Chamber have reached this conclusion following an analysis as to whether the impugned interference was 'necessary' within the meaning of Article 8 § 2 of the Convention. I do not have any major objections to the essence of that analysis as such. The misgivings I have are in relation to the preceding analysis of whether the interference with the applicant's rights under Article 8 was 'in accordance with the law'. On this point, the majority do identify a number of concerns but consider that it is not necessary in the present case to reach any firm conclusion as to whether the requirement of lawfulness has been met. Regrettably, I find the approach adopted in this respect lacking in firmness as well as in consistency with existing case-law.
2. According to the Court's well-established case-law, the phrase 'in accordance with the law' in Article 8 § 2 of the Convention requires not only that the impugned measure must have a basis in domestic law but that it must also be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention and is inherent in the object and purpose of Article 8. Thus, the requirement of lawfulness also refers to the quality of the law in question. This entails that the law should be adequately accessible and foreseeable as to its effects, that is to say formulated with sufficient precision to enable any individual — if need be with appropriate advice — to regulate his conduct (see, for instance, *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 95, ECHR 2008 (*NJ* 2009/410, m.nt. E.A. Alkema; *red.*)).
3. For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and, accordingly, indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise. The level of precision required of the domestic law — which cannot provide for every eventuality — depends to a considerable degree on the context and content of the law in question, such as the field it is designed to cover (ibid. § 96).
4. In the field of data protection, the Court has considered it essential for the applicable law to provide clear, detailed rules governing the scope and application of the relevant measures as well as sufficient guarantees against the risk of abuse and arbitrariness at each stage of the processing of personal data (see *M.M. v. the United Kingdom*, no. 24029/07, § 195, 13 November 2012, and *Surikov v. Ukraine*, no. 42788/06, § 74, 26 January 2017; both with further references). These are indeed crucial requirements.
5. In a context such as the present one, namely the processing by the police of personal data, including sensitive data, for the purposes of managing threats to public order, particular vigilance is called for when assessing the requirements of the quality of the law governing such processing. While the collection and further processing of personal data are an indispensable part of the functions of law enforcement authorities, there are, at the same time, significant inherent risks of abuse involved with a view to the exercise and protection of the rights and freedoms of individuals whose data are being processed. A sufficiently rigorous approach when assessing the quality of the law is therefore necessary. This is all the more so in the light of the developments referred to in my separate opinion in *Big Brother Watch and Others v. the United Kingdom* (nos. 58170/13, 62322/14, 24960/15, 13 September 2018, not yet final; paragraph 15 of that opinion), namely the degradation of respect for democratic standards and the rule of law, of which there is increasing evidence in a number of States. Again, without any suggestion that the present respondent State were a case in point in this regard, the Convention standards must nevertheless be considered in the light of the dangers deriving from such

developments vis-à-vis the protection of our common human rights and fundamental freedoms.

6. With this in mind, I consider that the crux of the legal issues raised by the present complaint relate to deficiencies in the quality of the law rather than (merely) the issue of necessity. As will be addressed more specifically below, the domestic legal framework, on an extremely vague and unspecific basis, has allowed for the processing of sensitive personal data without effective safeguards. The crucial importance of the quality of the law in a context such as the present one can be highlighted, most simply, by noting that that the general principles of data protection law — such as those requiring that the processing must be necessary for the purpose of the processing, and that the data to be processed must be adequate, relevant and not excessive in relation to that purpose — become diluted, possibly to the extent of practical irrelevance, where the purpose itself is left without any meaningful definition or limitation.

B. Analysis

7. In the present case, the processing of personal data has its basis in common law, under which the police have the power to obtain and store information 'for policing purposes', including for the maintenance of public order and the prevention and detection of crime (see paragraph 34 of the present judgment). Thus, there is no underlying statutory basis, and the basis in non-statutory law is about as vague as it can get. For the particular database in question, no further legal basis exists.

8. Regarding the purpose of the database, it has been said that 'the records are held to help UK policing manage a future risk of crime' (see paragraph 14 of the present judgment). According to the Government's submissions to the Court, the information is kept 'for policing purposes' and 'includes information relating to extremism but also relating to public disorder that does not involve extremism'. All of this remains, well, extremely vague and obscure. As regards the Code of Practice issued by the Secretary of State (see paragraph 40 of the present judgment), the definition of 'police purposes' given therein finishes with a general reference to the performance of 'any duty or responsibility of the police', and therefore fails to provide any further specificity.

9. Thus, clear rules governing the scope of the measures are lacking. The accessibility and foreseeability of the norms are therefore clearly deficient. As mentioned above, these features in themselves also dilute the relevance and effectiveness of the safeguards against abuse and arbitrariness deriving from the general data protection principles applicable by virtue of the Data Protection Act.

10. In this context, it is worth reiterating that the Court has held that it is not only essential to have clear, detailed rules governing the scope of measures, but also governing safeguards relating to the storage, use, duration of retention, access, as well as procedures for preserving the integrity and confidentiality of data and for their destruction. The Court has stressed that as there are various crucial stages at which data protection issues under Article 8 of the Convention may arise — namely during collection, storage, use and communication of data — what must be in place for each stage are appropriate and adequate safeguards which reflect the principles elaborated in applicable data protection instruments and which prevent arbitrary and disproportionate interference with Article 8 rights (see *M.M.*, cited above, § 195, and *Surikov*, cited above, § 74).

11. In the present case, the Government have stressed that the information was kept for policing purposes and had been neither intended for disclosure, nor disclosed, to any third party. The majority in the Chamber also put weight on this argument (see paragraph 103 of the judgment). The Government have also emphasised in line with the domestic Supreme Court that the information had not been obtained by covert means.

12. Neither of these points, however, is sufficient to make any crucial difference in the present context and circumstances. While it is true that secret surveillance or covert intelligence-gathering, or the accessibility of personal data, and of sensitive personal data in particular, to third parties must, for obvious reasons, entail heightened requirements for the quality of the law, both in terms of the specificity of the legal framework and the robust nature of the requisite safeguards, this cannot mean that the absence of such features could justify a lax approach to those requirements, especially where the processing of sensitive data is concerned. In view of established European principles regarding the processing of personal data, the fact that the processing may be limited to the 'internal' functions of public authorities, without data being made available to 'external' third parties, or that the data do not originate from covert operations, are not decisive distinctions in terms of the required elements of protection. Nor do the facts that the data were collected in relation to events in public places, or that they comprised primary facts which were 'in the public domain', such as a person's name and address, make any decisive or fundamental difference. It is well known that the need for protection of personal data often depends, quite essentially, on elements such as the context, combination, use and accessibility of such data (from the Court's case-law, see, for instance, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], no. 931/13, §§ 134–137, ECHR 2017).

13. With these remarks, I would like to stress that the interpretation of relevant Convention standards should not evolve on the basis of criteria, or distinctions, that would give rise to unwarranted divergences in the approaches between data protection as conceived under Article 8 and as conceived under specific instruments of international law in this field. As the Court has stated in other contexts,

the Convention should be interpreted in harmony with the general principles of international law, and the Court should aim at a combined and harmonious application of relevant international instruments (see, for instance, *X v. Latvia* [GC], no. 27853/09, §§ 92–94, ECHR 2013 (*NJ* 2015/329, m.nt. Th.M. de Boer; *red.*)).

C. Conclusion

14. The present case is, in my view, essentially an individual manifestation of the consequences arising from shortcomings in the underlying legal framework. The applicant, who had never been charged with any crime, nor accused of any violence, nor suspected of being directly involved in criminal activities undertaken by the group Smash EDO, and who had been assessed as not being a threat (see paragraphs 31 and 119 of the present judgment) ended up having personal data relating to his participation in demonstrations and trade union events, and thus to his peaceful exercise of the rights protected under Articles 10–11 of the Convention, kept on police records in a searchable database for an indefinite period. Even the existence of the database in question was not clearly acknowledged until the domestic proceedings in this case (see paragraph 98 of the present judgment). A subsequent review of matters relating to undercover police operations, prompted by allegations made by whistleblowers, also led to a review of the database on overtly obtained intelligence (see paragraph 13 of the judgment), resulting in the deletion of part of the data originally retained concerning the applicant. As pointed out by the applicant in his submissions, a system that must rely on whistleblowers, litigation and press disclosure to ensure proper conduct is not adequate in terms of protections against abuse or arbitrariness.

15. For the reasons set out above, I consider that it would have been appropriate for the Chamber to focus its analysis more thoroughly and consistently on the assessment of the 'quality of the law' aspect of the case, because that is where the crux of the case lies, instead of leaving that issue open and resolving the case on the basis of the assessment of 'necessity'. In my view, the quality of the relevant legal framework was not adequate in a context such as the present one, and therefore the interference was not 'in accordance with the law' within the meaning of Article 8 § 2. This finding is sufficient to conclude that there has been a violation of Article 8.

Noot

1. In deze zaak gaat het opnieuw over de grootschalige verzameling en opslag van persoonsgegevens. Het Hof heeft zich er in de laatste jaren al dikwijls over uitgelaten, in de private sfeer als het ging om de werkplek of supermarkt, in de overheidssfeer als het ging om politie- en veiligheidsdiensten. De feiten zijn als volgt. John Catt is een Engelse vredesactivist die regelmatig demonstraties en protesten bezoekt, zo ook in 2005 van de groep 'Smash EDO' die verschillende malen demonstreerde tegen de vestiging van een Amerikaanse wapenfabriek EDO MBM Technology in Brighton. Er waren behalve veel demonstranten ook veel politieagenten op de been. Naar aanleiding van het treffen tussen politie en demonstranten is Catt twee keer gearresteerd, maar tot een strafrechtelijke veroordeling leidde dat niet. Vijf jaar later doet Catt onder de Britse wet persoonsgegevensbescherming (implementatie van Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens) een verzoek om inzage welke persoonsgegevens over hem bij de politie worden bewaard. De politie bleek 66 vermeldingen met zijn naam naar aanleiding van 'incidenten' in 2005 en 2009 in documenten te bewaren. Daaronder bevonden zich de Smash EDO incidenten, maar ook andere demonstraties. De documenten bevonden zich in de door de politie opgetuigde databank die binnen het corps bekend stond als de 'extremism database'. Catt stapte naar de rechter en vroeg verwijdering.

2. Het Hof bouwt voort op een reeks arresten (gemakshalve verwijs ik naar hoofdstuk VIII van *De Europese informatierechtsorde*, Amsterdam: DeLex 2019). Het noemt in deze beslissing in het bijzonder twee precedenten in Britse zaken. Het eerste daarvan is *S. and Marper/UK*, appl. 30562/04 en 30566/04, EHRM 4 december 2008 (Grand Chamber), *NJ* 2009, 410, m.nt. E.A.A. (Het ging om onbeperkte opslag van vingerafdrukken en DNA-profielen van verdachten. In 2020 oordeelde het EHRM overigens dat de regels omtrent deze opslag zonder tijdslimiet in de UK, die in deze beslissing waren veroordeeld, nog steeds — nu uitgebreid tot die van foto's — de toets der kritiek niet konden doorstaan: zie het arrest *Gaughran/UK*, appl. 45245/15, EHRM 13 februari 2020). Het tweede precedent is de zaak *M.M./UK* 24029/07, EHRM 13 november 2012, (politieregisters). Daarnaast grijpt het terug op een oudere beslissing over de Zweedse veiligheidsdienst, waarin het oordeelde over grootschalige verzameling en opslag van persoonsgegevens, de zaak *Segerstedt*, appl. 62332/00, EHRM 6 juni 2006, *NJ* 2009, 449, m.nt. E.J.D. Verder zijn het Verdrag voor dataprotectie en een aantal resoluties van de Raad van Ministers, geciteerd in de overwegingen 58-66 (hierboven niet weergegeven), van belang.

3. In de procedure hebben twee organisaties die voor grondrechten opkomen geïntervenieerd: de Equality and Human Rights Commission (EHRC) en een Engelse NGO, Privacy International.

4. De politie voerde als verweer aan dat de database werd aangehouden om de 'future risk of crime' te managen en dat de databank uit haar aard vertrouwelijk was en bleef omdat dat nu eenmaal de kern is van 'intelligence' informatie. De term 'extremisme' werd verduidelijkt als: 'binnenlands ex-

tremisme', een term die door de politie werd gebruikt om een activiteit van individuen of groepen aan te duiden 'who carry out criminal acts of direct action to further their protest campaigns, outside the democratic process'. De Engelse appelrechter was niet onder de indruk van dit argument. Veelzeggend is deze overweging: "It is striking that [the National Coordinator] does not say that the information held on Mr Catt over many years has in fact been of any assistance to the police at all."

5. Bij de Supreme Court ging het echter (met één dissenting opinion) de andere kant op. Het is de moeite de gedachtegang van de meerderheid, bij monde van de Lord die de opinion heeft geschreven, te volgen. De eerste stap is dat de SC heen stapt over de tamelijk vage inhoud van de wettelijke regeling waar de retentie op was gebaseerd. Overweging 25:

> "Lord Sumption considered the applicant's argument that the Code of Practice and the Guidance did not enable him to know precisely what data would be obtained and stored or for how long to be unrealistic. Sumption explained that the infinite variety of situations in which issues of compliance might arise and the inevitable element of judgment involved in assessing them made complete codification impossible."

Bij de beoordeling van de proportionaliteit neemt het Hof in aanmerking dat het handelen in het openbaar betreft. Overweging 26:

> "(…) Rather, it was information about the overt activities in public places of individuals whose main object in attending the events in question was to draw public attention to their support for a cause. Although the collation of the information in the form in which it appeared in police records was not publicly available, the primary facts recorded were and always had been in the public domain; no intrusive procedures had been used to discover and record them."

Dat zou dus betekenen dat je bij je politieke handelen in het openbaar 'vogelvrij' bent, omdat dit altijd mag worden geregistreerd. Maar interessant is ook dat het SC ongebreideld verzamelen van gegevens gerechtvaardigd achtte op grond van een argument dat inlichtingendiensten vaak hanteren. Overweging 27:

> "He also underlined some basic facts about intelligence-gathering commenting:
> '… Most intelligence is necessarily acquired in the first instance indiscriminately. Its value can only be judged in hindsight, as subsequent analysis for particular purposes discloses a relevant pattern… The most that can be done is to assess whether the value of the material is proportionate to the gravity of the threat to the public…'."

De laatste stap in de redenering is dat het worden opgenomen in een bestand is toegestaan als dit niet 'stigmatiserend' is. Overweging 28:

> "It did not imply that all those mentioned as participating in events such as Smash EDO protests were being characterised as extremists. (…) It was not used for political purposes or for any kind of victimisation of dissidents and was not available to potential employers."

Die overweging staat op gespannen voet met de overwegingen 25, 26 en 27 dat niet voorzien kan worden in welke variëteit van gevallen het verzamelde materiaal bruikbaar is voor een databank met dit doel, en dat het patroon van handelen alleen in 'hindsight' kan worden beoordeeld. Daardoor kun je immers alsnog een 'verdachte' worden. Bij terugkijken van de databank Binnenlands Extremisme kan een opsporingsambtenaar een eureka ervaring hebben: "Aha daar zagen we hem ook al als demonstrant in dat type demonstratie rondlopen!"

6. De argumentatie van de Supreme Court sneuvelt in Straatsburg. Het EHRM is unaniem in zijn oordeel dat artikel 8 is geschonden, maar verschilt in de argumentatie. De meerderheid vindt dat de opslag in de databank niet aan het noodzakelijkheidscriterium voldeed omdat de opslag, mede gelet op de gevoelige (politieke) aard van de gegevens te onbepaald (in tijdsduur) was. Het acht andere aspecten van de opslag nog net wel door de beugel kunnen. De concurring opinion van de Finse rechter Pauliine Koskelo (gesteund door rechter Gilberto Felici uit San Marino) vindt de hele Engelse regeling niet 'in accordance with the law', een vraag die de meerderheid uit de weg gaat. Ik acht dit een belangwekkende opinie waarop ik hierna inga.

7. In zijn normale beslisboom onderzoekt het Hof eerst of de nationaal opgelegde beperking die heeft geleid tot de vermeende verdragsschennis bij wet zijn voorzien, maar het wijkt daar soms vanaf door over te stappen naar de noodzakelijkheidstest. Ik heb mij er in noten in de NJ wel eens mee beziggehouden (zie mijn noten bij EHRM 18 december 2015, de zaak *Yildrim/Turkije*, *NJ* 2014/320 en EHRM 1 december 2015, de zaak *Cengiz/Turkije*, *NJ* 2016/377). Bij de toetsing van de wetgeving over de controle op veiligheidsdiensten stoot het Hof meestal meteen door naar de noodzakelijkheidstest (zie de zaken *Roman Zakharov/Rusland*, *Szabó en Vissy/Zweden*, *Rättsiva/Zweden* en *Big Brother Watch/VK*, besproken in Hoofdstuk VII.4 van *De Europese informatierechtsorde*). Dit leidt tot een concrete toetsing die meer ruimte laat aan de 'margin of appreciation' van lidstaten in veiligheidskwesties, maar wel casuïstisch is. We zien dat ook in dit geval.

8. In r.o. 99 overweegt het Hof dat het een voorwerp van zorg is dat het opzetten van een databank tegen 'binnenlands extremisme' een duidelijke wettelijke grondslag ontbeert, maar dat dat moet worden beoordeeld tegen de achtergrond van de vraag hoe effectief de rechtsbescherming is. In het vervolg van de beslissing grijpt het Hof terug op de zaak *M.M./VK*, waarin ook politieregisters aan de orde waren die volgens het Hof de toets der kritiek niet konden doorstaan. Het onderzoekt overeenkomst en verschil om het dan in overweging 105 over een andere boeg te gooien:

> "The Court has concerns about the ambiguity of the legal basis for the collection of the applicant's personal data. In particular the Court notes the

loosely defined notion of 'domestic extremism' and the fact that applicant's data could potentially be retained indefinitely. However, the data retained would not be disclosed to third parties; and the applicant had the possibility to apply for the deletion of his data. In this connection, the Court recalls that the question of whether the collection, retention and use of the applicant's personal data was in accordance with the law is closely related to the broader issue of whether the interference was necessary in a democratic society."

9. Dat gezegd hebbende gaat het Hof op het noodzakelijkheidstraject verder, waarbij het begint de 'margin of appreciation' te erkennen van de UK autoriteiten en Engelse rechters waarvan de laatsten ook nogal in de weer geweest waren met de juiste toepassing van artikel 8 EVRM. Maar dat is in dit geval toch niet doorslaggevend. Het Hof somt de basis voor zijn (toch) ingrijpen op: het zijn gevoelige gegevens (bij demonstraties worden politieke overtuigingen uitgedragen), de bevoegdheden van de overheidsorganen zijn 'obscure, creating a risk of arbitrariness especially where the technology available is continually becoming more sophisticated' (onder verwijzing naar de recente beslissingen over veiligheidsdiensten, zie hoofdstuk VIII.3 van *De Europese informatierechtsorde*, Amsterdam: DeLex 2019), de concrete omstandigheden van het geval (hoeveel gegevens werden er wanneer opgeslagen). Tenslotte accepteert het wel de noodzaak om een dergelijke databank op te zetten en persoonsgegevens te verzamelen, ook zonder duidelijke wettelijke basis, maar niet dat de tijdsduur van die opslag niet is beperkt en dat overigens precieze regels voor het gebruik ontbreken. Het valt daarvoor terug op de Resolution (74) 29 en Aanbeveling R (87) 15 van de Raad van Ministers van de Raad van Europa. Het draait daarbij vooral ook om de politiek gevoelige gegevens: "Moreover, principle 2 on the collection of data in Recommendation R (87) 15 (…) states that the collection of data on individuals solely on the basis that they belong to particular movements or organisations which are not proscribed by law should be prohibited unless absolutely necessary or for the purposes of a particular inquiry (see mutatis mutandis Segerstedt-Wiberg and Others, cited above, § 79). The Court considers that the retention of the applicant's data in particular concerning peaceful protest has neither been shown to be absolutely necessary, nor for the purposes of a particular inquiry."

10. De aanpak van de concurring opinion die de kwaliteit van de wettelijke basis toetst voor dit soort verzamelingen geeft meer houvast. Deze formuleert de kern van de eis die aan een wettelijke regeling van deze soort in een democratie moet worden gesteld:

"In a context such as the present one, namely the processing by the police of personal data, including sensitive data, for the purposes of managing threats to public order, particular vigilance is called for when assessing the requirements of the quality of the law governing such processing. While the collection and further processing of personal data are an indispensable part of the functions of law enforcement authorities, there are, at the same time, significant inherent risks of abuse involved with a view to the exercise and protection of the rights and freedoms of individuals whose data are being processed. A sufficiently rigorous approach when assessing the quality of the law is therefore necessary."

11. Het Hof noemt bij het relevante recht wel het EU-recht maar betrekt dat niet in zijn overwegingen. Relevant zijn, dunkt mij, de beslissingen van het HvJ EU van 21 december 2016 in de zaken C-203/15 en C-698/15, *NJ* 2017/186, m.nt. E.J. Dommering, waarin ook vrij zware eisen aan het aanleggen van grootschalige verzamelingen worden gesteld, met name op het punt van de doelomschrijving die 'gericht' moet zijn.

12. De slotsom is dat aan het aanleggen van een databasis met 'gevoelige' persoonsgegevens (politieke en levensbeschouwelijke opvattingen) voor opsporings- of veiligheidsdoeleinden op zich is toegestaan, maar dat daaraan hoge eisen moeten worden gesteld omtrent doelstelling, noodzaak, tijdsduur, (her)gebruik en procedurele waarborgen. Het verdient aanbeveling dat nauwkeurig in een wettelijke regeling vast te leggen.

E.J. Dommering