122

Gebruik gezichtsherkenning vormt inbreuk op art. 8 en art. 10 EVRM

Europees Hof voor de Rechten van de Mens
7 juli 2023, 11519/20,
ECLI:CE:ECHR:2023:0704JUD001151920
(Pastor Vilanova, Schukking, Grozev, Serghides, Roosma, Zünd, Arnardóttir)
Noot mr. dr. T. Mulder

Gezichtsherkenningstechnologie. Demonstrant. Rusland. Biometrische gegevens.

[EVRM art. 8, 10, 11, 35]

Verzoeker is veroordeeld wegens het nalaten te melden van zijn voornemen een solo-demonstratie te houden. De Russische politie heeft tijdens het onderzoek gezichtsherkenningstechnologie gebruikt die was geïnstalleerd op openbare beveiligingscamera's. Verzoeker voert aan dat Rusland hiermee inbreuk maakt op art. 10 en 11 EVRM.
Het Hof herhaalt als eerste dat de bescherming van art. 10 EVRM niet beperkt is tot gesproken of geschreven woorden. Non-verbale uitdrukkingsmiddelen of gedragingen dienen hier ook onder te vallen. Dit kan slechts beperkt worden indien het is voorgeschreven bij wet. De arrestatie en veroordeling vormen een inmenging op verzoekers recht op vrijheid van meningsuiting.
Volgens de Russische nationale wetgeving, dienen demonstraties waarbij gebruik wordt gemaakt van 'snel te (de)monteren objecten' van tevoren te worden gemeld. Rusland stelt hierbij dat de beperking op art. 10 EVRM rechtsgeldig is voorgeschreven. Het Hof oordeelt echter dat hieraan niet is voldaan. De nationale bepaling betreffende 'snel te (de)monteren objecten' bevat immers geen concrete criteria welke soort objecten onder dit begrip kunnen vallen. Tevens acht het Hof dat de inmenging niet noodzakelijk in een democratische samenleving. Het is immers niet vastgesteld dat verzoekers handelingen ernstige verstoring van het dagelijkse leven, of gevaar voor de openbare orde of de veiligheid van het vervoer met zich heeft meegebracht. Er zijn onvoldoende relevante redenen aangevoerd om de inmenging op verzoekers recht op meningsuiting te rechtvaardigen.
Verzoeker voert aan dat Rusland inbreuk maakt op art. 8 EVRM, door de persoonsgegevensverwerking in het kader van administratieve strafprocedures, waaronder het gebruik van gezichtsherkenningstechnologie. Rusland voert aan dat voor de verwerking een wettelijke basis bestond. Het Hof bevestigt het betoog van verzoeker, en neemt inbreuk op art. 8 EVRM aan. De inbreuk kan niet worden gerechtvaardigd, aangezien niet wordt voldaan aan de voorwaarden waaronder een inbreuk is toegestaan. De inbreuk is niet voorzien bij wet en niet noodzakelijk in een democratische samenleving. Hoewel het Hof aanneemt dat de tegen verzoeker genomen maatregelen een wettelijke basis hadden in nationale wetgeving, concludeert het Hof dat de wetgeving kwalitatief niet toereikend is. De nationale wetgeving staat verwerking van biometrische persoonsgegevens toe in verband met rechtsbedeling, waaronder persoonsgegevensverwerking met behulp van gezichtsherkenningstechnologie. Wat betreft de noodzaak van de maatregel in een democratische samenleving, concludeert het Hof dat verzoeker slechts is vervolgd voor een lichte overtreding, zonder laakbare handelingen met ernstige gevolgen. Zijn handelen heeft niet geleid tot enig gevaar voor de openbare orde of veiligheid.
Tevens overweegt het Hof dat toestaan van het gebruik van een zeer ingrijpende maatregel als gezichtsherkenningstechnologie een 'chilling effect' kan hebben op het recht op de vrijheid van meningsuiting. Er is geen dwingende maatschappelijke behoefte tot het gebruik van de gezichtsherkenningstechnologie zoals dit is gebeurd. Het Hof concludeert dat het gebruik van zeer ingrijpende gezichtsherkenningstechnologie onverenigbaar is met de idealen en waarden van een democratische samenleving. De verwerking van verzoekers persoonsgegevens in casu is dan ook niet noodzakelijk in een democratische samenleving.

Glukhin
tegen
Rusland.

Introduction

1. The case concerns the applicant's administrative conviction for his failure to notify the authorities of his intention to hold a solo demonstration

using a "quickly (de)assembled object". During the investigation the police used facial recognition technology to process the applicant's personal data.

The facts
(...; *red.*)

Relevant legal framework

I. Procedure for the conduct of public events
(...; *red.*)

II. Operational-Search Activities
(...; *red.*)

III. Collection of evidence in administrative-offence proceedings
(...; *red.*)

IV. Police powers
(...; *red.*)

V. Processing of personal data
(...; *red.*)

VI. Video surveillance in the Moscow underground
(...; *red.*)

Relevant international material

I. United Nations
(...; *red.*)

II. Council of Europe
(...; *red.*)

III. European Union
(...; *red.*)

IV. Other relevant material
(...; *red.*)

The law

I. Jurisdiction and correspondence with the respondent Government
41. The Court observes that the facts giving rise to the alleged violations of the Convention occurred prior to 16 September 2022, the date on which the Russian Federation ceased to be a Party to the Convention. The Court therefore decides that it has jurisdiction to examine the present application (see *Fedotova and Others v. Russia* [GC], nos. 40792/10 and 2 others, §§ 68-73, 17 January 2023).
42. In view of the Court's continuing jurisdiction under Article 58 of the Convention, Articles 38, 41 and 46 in particular, as well as the corresponding provisions of the Rules of Court, continue to be applicable after 16 September 2022. The respondent Government's abstention from further participation in the proceedings does not release them from the duty to cooperate with the Court and does not prevent the Court from continuing with the examination of applications where it retains jurisdiction (see *Ukraine and the Netherlands v. Russia* ((dec.) [GC], nos. 8019/16 and 2 others, §§ 435-39, 30 November 2022, and *Svetova and Others v. Russia*, no. 54714/17, §§ 29-31, 24 January 2023). The Court may draw such inferences as it deems appropriate from a party's failure or refusal to participate effectively in the proceedings (Rule 44C of the Rules of Court).
43. The Court observes that it continues to use the electronic secured Government website as the means of communication with the authorities of the Russian Federation (see the Practice Direction on secured electronic filing by Governments, issued by the President of the Court in accordance with Rule 32 of the Rules of Court on 22 September 2008 and amended on 29 September 2014 and 5 July 2018) and in order to respect the adversarial nature of the proceedings before it. The site remains secure and accessible to the authorities of the respondent State.

II. Exhaustion of domestic remedies
44. Relying on *Chigirinova v. Russia* ((dec.), no. 28448/16, 13 December 2016), the Government submitted that the applicant had not exhausted domestic remedies because he had not lodged a cassation appeal with the Supreme Court.
45. The Court notes that *Chigirinova* (cited above) concerned proceedings under the Code of Administrative Procedure, while the present case concerns proceedings under the Code of Administrative Offences ("the CAO"). The review/cassation appeal procedure provided for in the CAO is not an effective remedy which needs to be exhausted (see *Smadikov v. Russia* (dec.), no. 10810/15, § 49, 31 January 2017, and *Ecodefence and Others v. Russia*, nos. 9988/13 and 60 others, § 75, 14 June 2022).

46. The Government's non-exhaustion objection must therefore be dismissed.

III. Alleged violation of Article 10 of the Convention

47. The applicant complained that the administrative-offence proceedings against him had breached his rights under Articles 10 and 11 of the Convention. The Court will examine this complaint under Article 10 of the Convention, taking into account the general principles established in the context of Article 11 (see *Novikova and Others v. Russia*, nos. 25501/07 and 4 others, § 91, 26 April 2016). Article 10 of the Convention reads as follows:

"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. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

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, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

A. Admissibility

48. The Court notes that this complaint is neither manifestly ill-founded nor inadmissible on any other grounds listed in Article 35 of the Convention. It must therefore be declared admissible.

B. Merits

49. The applicant submitted that his conviction for failure to submit a prior notification for his solo demonstration had been unlawful. The cardboard figure of Mr Kotov had been made up of one piece of cardboard and could not therefore be considered a "quickly (de)assembled object"; as such, he had not been required to notify the authorities of his solo demonstration. In any event, the applicable legal provisions did not meet the "quality of law" requirement. Furthermore, the domestic authorities had showed zero tolerance towards his peaceful solo demonstration. His arrest several days after the demonstration had not been justified by any pressing social need. The domestic authorities had not made any assessment of the risks posed by the solo demonstration or verified whether it had been necessary to arrest and convict him.

50. The Government submitted that the domestic law required prior notification of public events. The applicant had been lawfully convicted for failure to respect that requirement. His escorting to the police station and his arrest had also been lawful.

51. The Court reiterates that the protection of Article 10 is not limited to the spoken or written word, for ideas and opinions are also capable of being communicated by non-verbal means of expression or through a person's conduct (see *Karuyev v. Russia*, no. 4161/13, § 18, 18 January 2022). Given the nature and the context of the applicant's conduct, the Court considers that through his actions he sought to express his opinion on a matter of public interest, in respect of which there is little scope for restrictions under Article 10 § 2.

52. The applicant's escorting to the police station, administrative arrest and conviction for an administrative offence constituted an interference with his right to freedom of expression (see *Novikova and Others*, cited above § 106).

53. The relevant general principles were summarised in *Novikova and Others* (cited above, §§ 190-201) and *Kudrevičius and Others v. Lithuania* ([GC], no. 37553/05, §§ 108-10, 150-51 and 155, ECHR 2015).

54. As regards the "prescribed by law" criterion, the provision on "quickly (de)assembled objects" contained no criteria allowing a person to foresee what kind of objects could be covered by that provision. Having regard to the nature of the applicant's solo demonstration, and in the absence of either further clarifications concerning the scope and manner of application of the relevant provisions by higher Russian courts or any detailed analysis by the domestic courts in the applicant's specific case, the Court finds that there is reason to doubt that the manner of application of the impugned legal provisions was sufficiently foreseeable to meet the quality requirement in the case at hand (see *Navalnyy v. Russia* [GC], nos. 29580/12 and 4 others, § 118, 15 November 2018).

55. However, even assuming that the interference was in accordance with the law and pursued the legitimate aims of "the prevention of disorder" and "the protection of the rights of others", it was not "necessary in a democratic society" for the following reason.
56. The applicant's solo demonstration was carried out in an indisputably peaceful and non-disruptive manner. The offence of which he was convicted consisted merely of a failure to notify the authorities of his solo demonstration and included no further incriminating element concerning any reprehensible act, such as the obstruction of traffic, damage to property or acts of violence (contrast *Kudrevičius and Others*, cited above, §§ 164-75). It was not established that the applicant's actions caused any major disruption to ordinary life and other activities to a degree exceeding that which was normal or inevitable in the circumstances. Nor was it claimed that his actions had presented any danger to public order or transport safety. However, the authorities did not show the requisite degree of tolerance towards the applicant's peaceful solo demonstration. They did not take the above relevant elements into account and did not assess whether the applicant's use of a cardboard figure holding a banner had constituted an expression of his views. The only relevant consideration was the need to punish unlawful conduct. This is not a sufficient consideration in this context, in terms of Article 10 of the Convention, in the absence of any aggravating elements (see *Novikova and Others*, cited above, § 199). Thus, the courts failed to adduce "relevant or sufficient reasons" to justify the interference with the applicant's right to freedom of expression.
57. There has accordingly been a violation of Article 10 of the Convention.

IV. Alleged violation of Article 8 of the Convention
58. The applicant complained that the processing of his personal data in the framework of administrative offence proceedings, including the use of facial recognition technology, had breached his right to respect for his private life. He relied on 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
59. The Court notes that this complaint is neither manifestly ill-founded nor inadmissible on any other grounds listed in Article 35 of the Convention. It must therefore be declared admissible.

B. Merits

1. The parties' submissions
60. The applicant submitted that he had been filmed by CCTV cameras installed in the Moscow underground, identified by facial recognition technology and subsequently convicted of an administrative offence on the basis of evidence thereby obtained. There had been no judicial decision authorising the collection, storage and use of video-footage of him. The Police Act and Decree no. 410, which had served as the legal basis for the interference, did not meet the "quality of law" requirement. They were too vague and did not provide either for a prior judicial authorisation or for any subsequent judicial control.
61. The applicant further submitted that the interference with his right to respect for his private life had not pursued any legitimate aim and had not been "necessary in a democratic society". His private life had been interfered with for the sole reason that he had held a peaceful solo demonstration.
62. The Government submitted that the applicant had committed an administrative offence and that all the measures taken against him by the police had been lawful and justified. His name was not included in any list of wanted persons. The measures taken against the applicant had had a legal basis (see summary of the legislation referred to in paragraphs 33-34 above).
63. The third-party intervener Article 19 submitted that facial recognition technology was to be used with the utmost caution and was to be attended by adequate legal safeguards. They argued that biometric mass surveillance, in particular

with the use of facial recognition technology, represented one of the greatest threats to fundamental rights in the digital age. It threatened the right to privacy and anonymity and had a strong chilling effect on the rights to freedom of expression and assembly. The awareness of being watched and tracked might discourage people from exercising their right to protest and from freely expressing their opinion in public spaces.

2. The Court's assessment

(a) Existence of an interference

(i) General principles

64. The Court reiterates that the concept of "private life" is a broad term not susceptible to exhaustive definition. It can embrace multiple aspects of the person's physical and social identity. It is not limited to an "inner circle" in which the individual may live his or her own personal life without outside interference, but also encompasses the right to lead a "private social life", that is, the possibility of establishing and developing relationships with others and the outside world. It does not exclude activities taking place in a public context. There is thus a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life" (see *López Ribalda and Others v. Spain* [GC], nos. 1874/13 and 8567/13, §§ 87-88, 17 October 2019).

65. The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding. However, in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained (see *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 67, ECHR 2008).

66. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor in this assessment. As to the monitoring of an individual's actions using photographic or video devices, the Convention institutions have taken the view that the monitoring of the actions and movements of an individual in a public place using a camera which did not record the visual data does not constitute in itself a form of interference with private life. Private-life considerations may arise, however, once any systematic or permanent record of such personal data comes into existence, particularly pictures of an identified person. A person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right of each person to the protection of his or her image is thus one of the essential components of personal development and presupposes the right to control the use of that image. While in most cases the right to control such use involves the possibility for an individual to refuse publication of his or her image, it also covers the individual's right to object to the recording, conservation and reproduction of the image by another person (see *López Ribalda and Others*, cited above, § 89, with further references).

67. The Court has previously found that the collection and storing of data by the authorities on particular individuals constituted an interference with those persons' private lives, even if that data concerned exclusively the person's public activities (see *Amann v. Switzerland* [GC], no. 27798/95, §§ 65-67, ECHR 2000-II, and *Rotaru v. Romania* [GC], no. 28341/95, §§ 43-44, ECHR 2000-V), such as participation in anti-government demonstrations (see *Association "21 December 1989" and Others v. Romania*, nos. 33810/07 and 18817/08, § 170, 24 May 2011, and *Catt v. the United Kingdom*, no. 43514/15, § 93, 24 January 2019). It has also found that the following instances of collection of data in a public place constituted an interference with the persons' private lives: the recording of a questioning in a public area of a police station (see *P.G. and J.H. v. the United Kingdom*, no. 44787/98, §§ 56-60, ECHR 2001-IX); recording by CCTV cameras in a public place and the subsequent disclosure of the video-footage to the media (see *Peck v. the United Kingdom*, no. 44647/98, §§ 57-63, ECHR 2003-I); recording of video-footage at a police station and its subsequent use in criminal proceedings (see *Perry v. the United Kingdom*, no. 63737/00, §§ 36-43, ECHR 2003-IX (extracts); the collection,

through a GPS device attached to a person's car, and storage of data concerning that person's whereabouts and movements in the public sphere (see *Uzun v. Germany*, no. 35623/05, §§ 51-53, ECHR 2010 (extracts), and *Ben Faiza v. France*, no. 31446/12, §§ 53-55, 8 February 2018); the registration of a person's name in a police database which automatically collected and processed information about that person's movements, by train or air (see *Shimovolos v. Russia*, no. 30194/09, § 66, 21 June 2011); and video surveillance of university amphitheatres at a public university (see *Antović and Mirković v. Montenegro*, no. 70838/13, §§ 40-45 and 55, 28 November 2017).

(ii) Application to the present case

68. In the present case, during routine monitoring of the Internet the police discovered photographs and a video of the applicant holding a solo demonstration published on a public Telegram channel. They made screenshots of the Telegram channel, stored them and allegedly applied facial recognition technology to them to identify the applicant. Having identified the location on the video as one of the stations of the Moscow underground, the police also collected video-recordings from CCTV surveillance cameras installed at that station as well as at two other stations through which the applicant had transited. They made screenshots of those video-recordings and stored them. They also allegedly used the live facial recognition CCTV cameras installed in the Moscow underground to locate and arrest the applicant several days later with the aim of charging him with an administrative offence. The screenshots of the Telegram channel and of the video-recordings from the CCTV surveillance cameras were subsequently used in evidence in the administrative-offence proceedings against the applicant (see paragraphs 7-15 above).

69. The Government have not contested that the factual circumstances as described above amounted to an "interference" with the applicant's right to respect for his private life under Article 8 of the Convention. In particular, despite the Court's specific question on the issue, they did not comment on the applicant's allegations that the facial recognition technology had been used, first, to identify him from the photographs and the video published on Telegram and, secondly, to locate and arrest him while he was travelling on the Moscow underground. The Court is mindful of the difficulty the applicant faced in proving his allegations. Indeed, the domestic legislation available to the Court does not require the police to make a record of their use of facial recognition technology or to give the person concerned access to any such record, either automatically or upon request (see paragraph 40 above, describing the practice of using facial recognition technology without making any official record).

70. As regards the applicant's identification from the photographs and the video published on Telegram, the Court notes that although the photographs and the video in question did not contain any information permitting the identification of the applicant, he was identified within less than two days. The police report (see paragraph 11 above) did not explain which operational-search measures had been taken to identify him. The applicant's attempt to challenge the lawfulness of such measures failed, as the courts summarily dismissed his complaints (see paragraphs 16-17 above). In such circumstances it was not unreasonable for the applicant to assume that facial recognition technology had been used in his case. The Government did not explicitly deny this or provide any clarifications as to the measures used to identify the applicant. Lastly, the Court takes note of public information available regarding numerous cases involving the use of facial recognition technology to identify participants of protest events in Russia (see paragraph 40 above).

71. Furthermore, according to the applicant, the police acknowledged the use of the live facial recognition CCTV cameras to arrest him while he was travelling in the Moscow underground (see paragraph 12 above). The Government's reference to the applicable legal basis, including the decree providing for the installation of CCTV cameras in the Moscow underground ensuring detection and identification of target persons by video-surveillance systems, can be interpreted as an implicit acknowledgment that live facial recognition technology was used in the present case (see paragraph 33 above).

72. Against this background, and taking into account the difficulty for the applicant to prove his allegations because the domestic law did not provide for an official record or notification of the use of facial recognition technology, the absence of any other explanation for the rapid identification of the applicant, and the implicit acknowledgment by the Government of the use of live facial

recognition technology, the Court accepts in the particular circumstances of the case that facial recognition technology was used. The Court has previously found that the storage of photographs by the police, coupled with a possibility of applying facial recognition techniques to them, constituted an interference with the right to private life (see *Gaughran v. the United Kingdom*, no. 45245/15, §§ 69-70, 13 February 2020).
73. The Court concludes that the processing of the applicant's personal data in the framework of the administrative offence proceedings against him, including the use of facial recognition technology – first, to identify him from the photographs and the video published on Telegram and, secondly, to locate and arrest him later while he was travelling on the Moscow underground – amounted to an interference with his right to respect for his private life within the meaning of Article 8 § 1 of the Convention.

(b) Justification for the interference

(i) General principles
74. The Court reiterates that any interference can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one or more of the legitimate aims to which paragraph 2 of Article 8 refers and is necessary in a democratic society in order to achieve any such aim (see *Roman Zakharov v. Russia* [GC], no. 47143/06, § 227, ECHR 2015).
75. 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 (see *S. and Marper*, cited above, § 103), and especially where the technology available is continually becoming more sophisticated (see *Catt*, cited above, § 114; *Gaughran*, cited above, § 86; and *Uzun*, cited above, § 61). The protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests (see *S. and Marper*, cited above, § 112).
76. Personal data revealing political opinions, such as information about participation in peaceful protests, fall in the special categories of sensitive data attracting a heightened level of protection (see *Catt*, cited above, §§ 112 and 123).
77. In the context of the collection and processing of personal data, it is therefore essential to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness (see *S. and Marper*, cited above, § 99, and *P.N. v. Germany*, no. 74440/17, § 62, 11 June 2020).

(ii) Application to the present case
78. The Court considers that in the present case the questions of lawfulness and of the existence of a legitimate aim cannot be dissociated from the question of whether the interference was "necessary in a democratic society" (see *S. and Marper*, cited above, § 99; *Nemtsov v. Russia*, no. 1774/11, § 75, 31 July 2014; and *Elvira Dmitriyeva v. Russia*, nos. 60921/17 and 7202/18, § 77, 30 April 2019). It will therefore examine them together below.
79. According to the domestic authorities and the Government, the measures taken against the applicant had a legal basis in the CAO, the OSAA, the Police Act and Decree no. 410.
80. The Court would begin by noting that operational-search activities could be performed only in connection with an offence classified as "criminal" under the domestic law (see paragraph 24 above). The OSAA could not therefore serve as the legal basis for the measures taken in the present case, which concerned an administrative offence.
81. Both the CAO and the Police Act gave powers to the police to investigate administrative offences and to collect evidence, including evidence containing personal data (see paragraphs 26-29 above). Decree no. 410 provided for the installation of live facial recognition CCTV cameras in the Moscow underground which were accessible to the police (see paragraphs 33-34 above). The Court therefore accepts that the measures taken

against the applicant had a legal basis in the domestic law.
82. In so far as the applicant alleged that the domestic law did not meet the "quality of law" requirement, the Court considers that it is essential in the context of implementing facial recognition technology to have detailed rules governing the scope and application of measures as well as strong safeguards against the risk of abuse and arbitrariness. The need for safeguards will be all the greater where the use of live facial recognition technology is concerned.
83. The Court has strong doubts that the domestic legal provisions meet the "quality of law" requirement. It notes, in particular, that the domestic law permits the processing of biometric personal data "in connection with the administration of justice" (see paragraph 31 above). This legal provision is widely formulated. Taking into account that the Government did not refer to any authoritative interpretation of that provision by the Supreme or Constitutional Courts or submit any examples of its restrictive interpretation and application in administrative and judicial practice, it appears that it allows processing of biometric personal data – including with the aid of facial recognition technology – in connection with any judicial proceedings. The domestic law does not contain any limitations on the nature of situations which may give rise to the use of facial recognition technology, the intended purposes, the categories of people who may be targeted, or on processing of sensitive personal data. Furthermore, the Government did not refer to any procedural safeguards accompanying the use of facial recognition technology in Russia, such as the authorisation procedures, the procedures to be followed for examining, using and storing the data obtained, supervisory control mechanisms and available remedies.
84. The Court will further proceed on the assumption that the contested measures pursued the legitimate aim of the prevention of crime.
85. The Court finds it to be beyond dispute 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, depends to a great extent on the use of modern scientific techniques of investigation and identification. However, while it recognises the importance of such techniques in the detection and investigation of crime, the Court must delimit the scope of its examination. The question is not whether the processing of biometric personal data by facial recognition technology may in general be regarded as justified under the Convention. The only issue to be considered by the Court is whether the processing of the applicant's personal data was justified under Article 8 § 2 of the Convention in the present case (compare *S. and Marper*, cited above, §§ 105-06).
86. In determining whether the processing of the applicant's personal data was "necessary in a democratic society", the Court will first assess the level of the actual interference with the right to respect for private life (see *P.N. v. Germany*, cited above, §§ 73 and 84). It notes that the police collected and stored the applicant's digital images and used them to extract and process the applicant's biometric personal data with the aid of facial recognition technology: first, to identify him from the photographs and the video published on Telegram and, secondly, to locate and arrest him while he was travelling on the Moscow underground. The Court considers these measures to be particularly intrusive, especially in so far as live facial recognition technology is concerned (see paragraph 37 above). A high level of justification is therefore required in order for them to be considered "necessary in a democratic society", with the highest level of justification required for the use of live facial recognition technology. Moreover, the personal data processed contained information about the applicant's participation in a peaceful protest and therefore revealed his political opinion. They accordingly fell in the special categories of sensitive data attracting a heightened level of protection (see paragraph 76 above).
87. In the assessment of the "necessity in a democratic society" of the processing of personal data in the context of investigations, the nature and gravity of the offences in question is one of the elements to be taken into account (see, *mutatis mutandis*, *P.N. v. Germany*, cited above, § 72). The domestic law permits the processing of biometric personal data in connection with the investigation and prosecution of any offence, irrespective of its nature and gravity.
88. The Court observes that the applicant was prosecuted for a minor offence consisting of holding a solo demonstration without a prior notification – an offence classified as administrative rather than criminal under the domestic law. He was never accused of committing any reprehensi-

ble acts during his demonstration, such as the obstruction of traffic, damage to property or acts of violence. It was never claimed that his actions presented any danger to public order or transport safety. The Court has already found that the administrative-offence proceedings against the applicant breached his right to freedom of expression (see paragraph 57 above). It considers that the use of highly intrusive facial recognition technology to identify and arrest participants of peaceful protest actions could have a chilling effect in regard of the rights to freedom of expression and assembly.

89. In such circumstances, the use of facial recognition technology to identify the applicant from the photographs and the video published on Telegram – and *a fortiori* the use of live facial recognition technology to locate and arrest him while he was travelling on the Moscow underground – did not correspond to a "pressing social need".

90. In the light of all the above considerations the Court concludes that the use of highly intrusive facial recognition technology in the context of the applicant exercising his Convention right to freedom of expression is incompatible with the ideals and values of a democratic society governed by the rule of law, which the Convention was designed to maintain and promote. The processing of the applicant's personal data using facial recognition technology in the framework of administrative offence proceedings – first, to identify him from the photographs and the video published on Telegram and, secondly, to locate and arrest him while he was travelling on the Moscow underground – cannot be regarded as "necessary in a democratic society".

91. There has accordingly been a violation of Article 8 of the Convention.

V. Alleged violation of Article 6 of the Convention

92. The applicant complained under Article 6 of the Convention that the administrative-offence proceedings against him had been unfair because there had been no prosecuting party. Having regard to the facts of the case, the submissions of the parties and its findings under Articles 8 and 10, the Court considers that there is no need to give a separate ruling on the admissibility and the merits of the complaint under Article 6 (see *Centre for Legal Resources on behalf of Valentin Câmpeanu v. Romania* [GC], no. 47848/08, § 156, ECHR 2014).

VI. Application of Article 41 of the Convention

93. Article 41 of the Convention provides:

"If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

A. Damage

94. The applicant claimed 15,000 euros (EUR) in respect of non-pecuniary damage.

95. The Government submitted that the claim was excessive.

96. The Court awards the applicant EUR 9,800 in respect of non-pecuniary damage, plus any tax that may be chargeable.

B. Costs and expenses

97. Relying on legal-fee agreements and time sheets submitted by his lawyers, the applicant claimed EUR 6,400 in respect of the legal fees incurred before the domestic courts and before the Court.

98. The Government submitted that the applicant's claim in respect of legal fees should be rejected since contingency fee agreements were unenforceable.

99. According to the Court's case-law, an applicant is entitled to the reimbursement of costs and expenses only in so far as it has been shown that these were actually and necessarily incurred and are reasonable as to quantum. The Court notes that the legal-fee agreements signed by the applicant are not based on contingency. Regard being had to the documents in its possession and the above criteria, the Court considers it reasonable to award the sum of EUR 6,400 covering costs under all heads, plus any tax that may be chargeable to the applicant.

For these reasons, the Court, unanimously,

1. *Holds* that it has jurisdiction to deal with the applicant's complaints, as they relate to facts that took place before 16 September 2022;
2. *Declares* the complaints concerning the alleged violations of the rights to respect for private life and to freedom of expression admissible;
3. *Holds* that there has been a violation of Article 8 of the Convention;
4. *Holds* that there has been a violation of Article 10 of the Convention;

5. *Holds* that there is no need to examine separately the complaint under Article 6 of the Convention;
6. *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) EUR 9,800 (nine thousand eight hundred euros), plus any tax that may be chargeable, in respect of non-pecuniary damage;
(ii) EUR 6,400 (six thousand four hundred 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 amounts at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;
7. *Dismisses* the remainder of the applicant's claim for just satisfaction.

NOOT

In steeds meer landen maken gemeentes gebruik van cameratoezicht in de openbare ruimtes om bijvoorbeeld de openbare orde te kunnen handhaven of om te ondersteunen bij het opsporen van criminaliteit. Uit het arrest blijkt dat dit in Moskou niet anders is. In mei 2017 bleken er 3.500 *Closed Circuit Television (CCTV)-camera's* geïnstalleerd te zijn in Moskou. Hiervan werden vier maanden later 3.000 camera's voorzien van live gezichtsherkenning, waaronder in 2018 de camera's in de metro van Moskou. Het aantal camera's in Moskou met live gezichtsherkenning is vervolgens in snel tempo uitgebreid naar 175.000 in september 2020 en meer dan 220.000 in 2022 (par. 5). Daarmee kan dit arrest ook relevant zijn voor overheden in andere landen die gebruik willen maken van gezichtsherkenningssoftware in openbare ruimtes. Daarbij is het wel van belang te benoemen dat het voorstel voor de nieuwe AI-Verordening binnen de EU het inzetten van slimme en realtime biometrische systemen voor identificatie op afstand in openbare ruimte al dan niet met het oog op rechtshandhaving in principe verbiedt of aan strenge voorwaarden onderwerpt (art. 5 lid 1 sub d en art. 6 lid 2 jo. bijlage III AI-Verordening, COM(2021) 206 final (2021/0106(COD)). Hoewel de huidige tekst nog niet definitief is, worden er op dit gebied geen wijzigingen, en zeker geen versoepelingen, verwacht. Het is de bedoeling dat er voor het eind van 2023 een definitief akkoord zal worden bereikt over de definitieve tekst van de AI-Verordening.
Hoewel Rusland sinds 16 september 2022 geen partij meer is bij het Europees Verdrag voor de Rechten van de Mens (EVRM), vonden de feiten die relevant zijn voor deze zaak plaats voor die datum, namelijk van augustus t/m oktober 2019, en om die reden acht het Europees Hof voor de Rechten van de Mens (EHRM) zich in deze zaak bevoegd (zie ook: EHRM 17 januari 2023, 40792/1 (*Fedotova/Russia*)).
De zaak draait zowel om de schending van art. 10 EVRM als om de schending van art. 8 EVRM, waarbij de laatste schending het meest interessant is. Dat er volgens het EHRM sprake is van een schending van art. 10 EVRM, de vrijheid van meningsuiting, is niet heel verrassend. De verzoeker wilde in zijn eentje vreedzaam demonstreren met een van karton gemaakt protestbord. Hij was in de overtuiging dat hij deze demonstratie niet vooraf hoefde aan te kondigen bij de autoriteiten. Volgens de Russische autoriteiten moest hij deze demonstratie echter wel vooraf aankondigen en om die reden is hij een aantal dagen na zijn vreedzame solodemonstratie gearresteerd.
Het EHRM herhaalt in deze zaak nogmaals dat de bescherming van art. 10 EVRM niet beperkt is tot het gesproken of geschreven woord, maar dat meningen en ideeën ook geuit kunnen worden via non-verbale communicatiemiddelen of zelfs via het gedrag van een persoon. Het EHRM is van mening dat de verzoeker zijn mening wilde uiten over een kwestie van publiek belang. Art. 10 lid 2 EVRM biedt in dat geval weinig ruimte voor beperkingen van de vrijheid van meningsuiting. Het gaat om de bekende drietrapsraket, de beperking moet:
– bij wet zijn voorzien, en;
– een legitiem doel dienen, en;
– noodzakelijk zijn in een democratische samenleving.
Van het in Rusland wettelijke voorgeschreven vereiste dat demonstraties met 'snel te (de)monteren objecten' vooraf moeten worden aange-

meld, betwijfelt het EHRM ten zeerste of het voorzienbaar genoeg is. Het EHRM verwijst hierbij naar een eerdere zaak (EHRM 15 november 2018, 29580/12 (*Navalnyy/Rusland*)) waarin de twijfel reeds was uitgesproken of dit soort brede begrippen voldoende voorzienbaar zijn voor burgers. Is het, met andere woorden voldoende voorzienbaar voor de burger wat er onder het betreffende begrip valt en wat niet.
Het EHRM laat het echter niet bij schending van deze vorm van voorzienbaarheid voor de burger, maar geeft aan dat zelfs als deze schending voldoende voorzienbaar zou zijn voor burgers en als er ook sprake zou zijn van legitieme doelen, in dit geval 'het voorkomen van wanorde' en 'de bescherming van de rechten van anderen', het ingrijpen nog steeds niet noodzakelijk was in een democratische samenleving. Dit omdat de solodemonstratie op een vreedzame en niet-verstorende manier werd uitgevoerd.
De veroordeling ziet alleen op het verzuim de autoriteiten op de hoogte te stellen van zijn solodemonstratie en bevat verder geen enkel belastend element, zoals bijvoorbeeld verkeersbelemmering of schade aan eigendommen. Daarmee hebben de autoriteiten in de ogen van het EHRM niet de vereiste mate van tolerantie tegenover de demonstratie getoond. Ze hebben niet op een 'relevante manier aangevoerd dat er voldoende redenen waren om de inmenging op het recht van vrijheid van meningsuiting' te beperken en hebben daarmee art. 10 EVRM overtreden (par. 56 en 57).
Het EHRM geeft ook nog mee dat de inzet van (live) gezichtsherkenningstechnologie om deelnemers van vreedzame protestacties te identificeren een afschrikwekkend effect kunnen hebben op het recht op vrijheid van meningsuiting. Daarmee legt het EHRM de lat voor de inzet van (live) gezichtsherkenningstechnologie in dergelijke situaties heel erg hoog.
Tot zover de schending van art. 10 EVRM. De schending van art. 8 EVRM ziet op een ontwikkeling waar we steeds meer over horen: de inzet van live gezichtsherkenning gekoppeld aan de diverse CCTV-camera's in steden als Moskou.
Het EHRM begint met te herhalen dat het begrip 'privéleven' een breed begrip is dat niet vatbaar is voor een uitputtende definitie (par. 64). Het 'recht op een privéleven' kan ook activiteiten omvatten die plaatsvinden in het openbaar. Alleen al het opslaan van persoonlijke gegevens leidt tot een inmenging in het privéleven van een persoon. Al sinds 2008 weten we dat voor de vraag of er sprake is van een schending van art. 8 EVRM het EHRM rekening houdt met:
– de specifieke context waarin de betrokken informatie is vastgelegd en bewaard;
– de aard van de gegevens;
– de wijze waarop deze documenten worden gebruikt en verwerkt, en;
– de resultaten die kunnen worden verkregen;
(EHRM 4 december 2008, 30562/04 en 30566/04 (*S. en Marper/Groot-Brittannië*)).
Zodra er sprake is van een systematische of permanente registratie van persoonlijke gegevens, zeker indien het gaat over afbeeldingen, heeft dit grote impact op het privéleven van personen. De afbeelding van een persoon maakt het immers mogelijk om een persoon te onderscheiden van een ander persoon, aldus het EHRM (par. 66).
Daarnaast heeft het EHRM al eerder aangegeven dat het verzamelen en opslaan van persoonsgegeven door de overheid leidt tot een schending van hun privéleven, ook als die gegevens alleen zien op iemands publieke activiteiten zoals de deelname aan anti-overheidsdemonstraties (zie ook recent: EHRM 24 januari 2019, 43514/15 (*Catt/Groot-Brittannië*)).
In deze zaak hebben de Russische autoriteiten geen antwoord gegeven op de beweringen van verzoeker dat gezichtsherkenningstechnologie is gebruikt om hem (1) te identificeren aan de hand van foto's en video's die waren gepubliceerd op Telegram en (2) te lokaliseren en te arresteren terwijl hij met de metro reisde in Moskou. Dit ondanks een specifieke vraag hierover van het EHRM aan de Russische autoriteiten. Uit de weigering van de Russische autoriteiten om deze vraag te beantwoorden, het feit dat dat de Russische autoriteiten niet uitdrukkelijk hebben ontkend dat gebruik is gemaakt van gezichtsherkenningstechnologie en uit de feiten van de zaak leidt het EHRM af dat het niet onredelijk is dat verzoeker in dit geval heeft aangenomen dat er gebruik is gemaakt van gezichtsherkenningstechnologie. Het EHRM gaat zelfs nog een stap verder door de verwijzing van de Russische overheid naar de van toepassing zijnde rechtsgrondslag, inclusief het besluit van het voorzien in de installatie van CCTV-camera's in de metro van Moskou, te interpreteren als een impliciete erkenning van live gezichtsherkenningstechnologie (par. 71).

Het EHRM beoordeelt vervolgens de drie vereisten uit art. 8 lid 2 EVRM, bij wet voorzien, een legitiem doel dienen en noodzakelijk in een democratische samenleving, tezamen. Dit aangezien deze drie vereisten in deze zaak niet los van elkaar kunnen worden gezien (par. 78).
Ondanks dat hier sprake was van een administratiefrechtelijke overtreding, die daarmee buiten het strafrecht valt, is het EHRM van mening dat er voldoende rechtsgrond is in het nationale Russische recht om live gezichtsherkenningstechnologie in te zetten. De aanwezigheid van regels op zich is echter niet voldoende. Bij het inzetten van gezichtsherkenningstechnologie acht het EHRM het van essentieel belang dat er gedetailleerde regels zijn die zien op de reikwijdte en toepassing van deze maatregelen, aangevuld met waarborgen die zien op het tegengaan van het risico op misbruik en willekeur. En waar het gaat om live gezichtsherkenningstechnologie is de behoefte aan waarborgen nog groter.
Het EHRM is vrij duidelijk over de vraag waaraan wet- en regelgeving, die voorziet in de inzet van (live) gezichtsherkenningstechnologie, moet voldoen en erkent dat moderne technologie zoals (live) gezichtsherkenningstechnologie van groot belang kan zijn in de strijd tegen (de georganiseerde) misdaad en terrorisme. Daarom benadrukt het EHRM dat het alleen beoordeelt of de wet- en regelgeving in deze specifieke zaak aan onderstaande vereisten, die voortvloeien uit art. 8 lid 2 EVRM, voldeed. De opsomming geeft daarmee een handvat voor toekomstige wet- en regelgeving ten aanzien van (live) gezichtsherkenningstechnologie. De wet- en regelgeving moet duidelijk zijn over (par. 83):
– voor welke doelen gezichtsherkenningstechnologie mag worden ingezet, en voor welke doelen niet;
– welke categorieën van personen het doelwit kunnen zijn van gezichtsherkenningstechnologie;
– welke gevoelige persoonsgegevens (mogen) worden verwerkt;
– de procedurele waarborgen, zoals autorisatieprocedures, het opslaan van de gegevens, en de toezichthoudende controle mechanismen.
De Russische wet- en regelgeving voldeed niet aan bovenstaande. Bovendien werden in deze zaak bijzondere persoonsgegevens verwerkt, aangezien het ging om een protest dat de politieke mening van de verzoeker onthulde, wat de eisen alleen maar strenger maakt.

Over de vraag of de verwerking noodzakelijk was in een democratische samenleving oordeelt het EHRM kort en krachtig. Het ging hier om een vreedzame solodemonstratie zonder dat dit vooraf werd gemeld. Dit kan in het nationale Russische recht eerder worden geclassificeerd als een administratiefrechtelijke overtreding dan als een strafrechtelijk overtreding. De Russische autoriteiten hebben verzoeker niet beschuldigd van andere laakbare handelingen zoals het belemmeren van het verkeer of het gebruik van geweld. Er was, met andere woorden, geen sprake van een dringende maatschappelijke behoefte om een dergelijk zwaarwegend middel in te zetten tegen verzoeker.
Er was in deze zaak wet- en regelgeving aanwezig die zag op een beperking van zowel art. 8 als van art. 10 EVRM. De kwaliteit van deze wet- en regelgeving voldeed echter niet en kon daardoor niet gebruikt worden om art. 8 en art. 10 EVRM daadwerkelijk te beperken. Het EHRM geeft mede om die reden een aantal handvatten waar wet- en regelgeving die ziet op (live) gezichtsherkenningstechnologie aan behoort te voldoen.
Verder overweegt het EHRM dat het opsporen van demonstranten via gezichtsherkenningstechnologie een afschrikwekkend effect kan hebben op het recht van vrijheid van meningsuiting. Daarmee zal de inzet van dit soort technologie in het geval van demonstraties, zeker als het gaat om vreedzame demonstraties, aan een hoge vereisten moeten voldoen voordat het gezien wordt als 'noodzakelijk in een democratische samenleving'.

mr. dr. T. Mulder
Lector Hanzehogeschool Groningen.