dirittifondamentali.it

La Corte Edu sull'utilizzo di tecnologie di riconoscimento facciale
(CEDU, sez. VIII, sent. 4 luglio 2023, ric. n. 11519/20)

La Corte Edu si è pronunciata sul ricorso presentato da un cittadino russo al quale era stata inflitta una condanna amministrativa per avere omesso di notificare alle autorità la sua personale e singolare intenzione di tenere una manifestazione solitaria utilizzando una figura di cartone a grandezza naturale di un attivista politico con uno striscione, denunciando altresì l'impiego di tecniche di riconoscimento facciale da parte della polizia durante le indagini; nel caso di specie, infatti, le autorità di polizia avevano memorizzato alcune immagini del manifestante tratte dal canale Telegram e, con l'ausilio delle telecamere di sorveglianza installate in una delle stazioni della metropolitana di Mosca, avevano successivamente proceduto al riconoscimento e all'arresto del ricorrente.

In primo luogo, la Corte ha ricordato che la registrazione sistematica o permanente dei dati personali di un individuo può costituire un'ingerenza nella vita privata di quest'ultimo, soprattutto se ad essere ripresa sia l'immagine di una persona che appunto costituisce uno degli attributi principali della sua personalità.

A tale riguardo, la Corte ribadisce che qualsiasi interferenza può essere giustificata ai sensi dell'articolo 8 § 2 della Convenzione solo se è conforme alla legge, persegue uno o più degli scopi legittimi a cui si riferisce la disposizione convenzionale ed è necessaria in una società democratica al fine di raggiungere tali scopi; il rispetto di tali requisiti si rende tanto più necessario quando si tratta di proteggere dati personali sensibili (come quelli relativi a opinioni politiche) sottoposti a trattamento automatizzato, nell'ambito del quale è essenziale disporre di norme chiare e dettagliate che disciplinino la portata e l'applicazione delle misure, nonchè alcune garanzie minime riguardanti la durata, la conservazione, l'utilizzo e l'accesso ai dati da parte dei terzi così come le procedure per preservare l'integrità e la riservatezza dei dati e per la loro distruzione, fornendo così garanzie sufficienti contro il rischio di qualsiasi abuso e arbitrarietà.

Nel caso di specie, la Corte obietta da un lato che l'ordinamento giuridico russo non contenga alcuna limitazione effettiva, sostanziale e procedurale, circa l'utilizzo di tecnologie di riconoscimento facciale e, dall'altro, che l'applicazione di simili tecnologie nei confronti del ricorrente, perseguito soltanto per un illecito amministrativo e neppure penale, non potesse essere considerata "necessaria in una società democratica", riscontrandosi per tutti questi motivi una violazione dell'art. 8 della Convenzione.

***

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

THIRD SECTION

CASE OF XXX v. RUSSIA

(Application no. 11519/20)

JUDGMENT

STRASBOURG

4 July 2023

This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention. It may be subject to editorial revision.

In the case of XXX v. Russia,

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

Pere Pastor Vilanova, *President*,

Jolien Schukking,

Yonko Grozev,

Georgios A. Serghides,

Peeter Roosma,

Andreas Zünd,

Oddný Mjöll Arnardóttir, *judges*,

and Milan Blaško, *Section Registrar*,

Having regard to:

the application (no. 11519/20) against the Russian Federation lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a Russian national, Mr XXX ("the applicant"), on 31 January 2020;

the decision to give notice to the Russian Government ("the Government") of the complaints concerning Article 6 § 1 and Articles 8 and 10 of the Convention, and to declare inadmissible the remainder of the application;

the observations submitted by the respondent Government and the observations in reply submitted by the applicant;

the comments submitted by Article 19, which was granted leave to intervene by the President of the Section;

the respondent Government's failure to submit observations in reply to the third-party observations and the lack of any communication from the respondent Government since March 2022;

the decision of the President of the Section to appoint one of the sitting judges of the Court to act as an *ad hoc* judge, applying by analogy Rule 29 § 2 of the Rules of the Court (see, for an explanation of the background for this, *Kutayev v. Russia*, no. 17912/15, §§ 5-8, 24 January 2023);

Having deliberated in private on 23 May and 13 June 2023,
Delivers the following judgment, which was adopted on the last-mentioned date:

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

2. The applicant was born in XXX and lives in XXX. He was represented by Mr N. Zboroshenko and Ms A. Rossius, lawyers practising in Moscow.
3. The Government were initially represented by Mr A. Fedorov, former Representative of the Russian Federation to the European Court of Human Rights, and later by his successor in that office, Mr M. Vinogradov.
4. The facts of the case may be summarised as follows.
5. In May 2017, the official website of the mayor of Moscow reported that more than 3,500 CCTV cameras had been installed in Moscow. In September of the same year, more than 3,000 CCTV cameras were equipped with a live facial recognition system. In the spring of 2018, facial recognition CCTV cameras were installed in the Moscow underground. According to the mayor of Moscow, a live facial recognition system was tested in 2019. By 1 September 2020, all CCTV cameras in Moscow – there were about 175,000 by then and more than 220,000 in 2022 – were equipped with live facial recognition technology.
6. On 12 August 2019 a political activist, Mr XXX, was arrested and charged with a repeated breach of the rules on "public events" under Article 212.1 of the Russian Criminal Code. Mr XXX's detention and the criminal proceedings against him attracted a great deal of media and public attention and caused a public outcry.
7. On 23 August 2019 the applicant travelled by Moscow underground with a life-size cardboard figure of Mr XXX holding a banner stating: "You must be f**king kidding me. I'm XXX. I'm facing up to five years [in prison] under [Article] 212.1 for peaceful protests."
8. It appears from a police report dated 24 August 2019 that "monitoring of the Internet" by the anti-extremism unit of the Moscow underground police ("the police anti-extremism unit") had revealed a photograph of a man standing at an underground station with a human figure holding a banner.
9. The police anti-extremism unit then took screenshots of a public Telegram channel containing photographs and a video of the applicant holding the cardboard figure of Mr XXX at an underground station and inside an underground train. The text written on the banner mentioned in paragraph 7 was clearly readable in the screenshots. The screenshots were printed out and stored by the police anti-extremism unit "in accordance with Chapter 26 of the Code of Administrative Offences" ("the CAO"; see paragraphs 26-27 below).

10. It follows from another police report dated 24 August 2019 that the police anti-extremism unit obtained video-recordings from CCTV cameras installed at Chistye Prudy and Sretenskiy Bulvar underground stations. The police anti-extremism unit watched those recordings on 27 August 2019, took screenshots of the applicant's image, printed them out and stored them in the case file.
11. It follows from a police report dated 26 August 2019 that the police anti-extremism unit conducted "operational-search activities" to identify the man in the photographs and the video published on Telegram, successfully identified him as the applicant and established his home address.
12. According to the applicant, at about 10 a.m. on 30 August 2019 the police anti-extremism unit went to his home while he was not there. At about 11 a.m. on the same day, he was arrested at an underground station. The police allegedly told him that he had been identified by the facial recognition CCTV cameras installed in the Moscow underground.
13. The applicant was then taken to a police station where he was charged with the administrative offence of breaching the established procedure for the conduct of public events under Article 20.2 § 5 of the CAO. The charges stated that on 23 August 2019 the applicant had held a solo demonstration at the Chistye Prudy underground station and on the underground train using a "quickly (de)assembled object" and should therefore have submitted a prior notification to the local authorities.
14. In a letter of 2 September 2019, the acting head of the police anti-extremism unit requested the head of the Moscow underground security to provide copies of video-recordings of 23 August 2019 from 8.15 to 8.35 p.m. from twenty-two CCTV cameras installed at Okruzhnaya underground station. He relied on sections 6-3, 7-2(1) and 15-1 of the Operational-Search Activities Act (see paragraphs 22-23 and 25 below) and section 13-1(4) of the Police Act (see paragraph 29 below). He further stated that the request was being made in the framework of an inquiry being conducted with the aim of combating extremism during approved mass public events in Moscow. The police anti-extremism unit watched those recordings on 5 September 2019, took screenshots of the applicant's image, printed them out and stored them in the case file.
15. On 23 September 2019 the Meshchanskiy District Court of Moscow convicted the applicant as charged. The court noted that the applicant had made oral submissions and had pleaded not guilty. It then relied, among others, on the screenshots of the Telegram channel and the screenshots of video-recordings from the surveillance cameras in the underground in support of its finding that the applicant had held a solo demonstration using a "quickly (de)assembled object". Contrary to the applicant's argument, the cardboard figure of Mr XXX could be considered a "quickly (de)assembled object" because it had a prop. The court sentenced the applicant to a fine of 20,000 Russian roubles ((RUB), about 283 euros).
16. The applicant appealed. He complained, in particular, that the operational-search activities performed to identify him had been unlawful because the Operational-Search Activities Act did not permit performing such activities to investigate administrative offences. The evidence thereby obtained was therefore inadmissible. He also complained about the absence of a prosecuting party, claiming that that situation had breached the principle of impartiality. Lastly, he submitted that his conviction for a peaceful solo demonstration had breached his right to freedom of expression. It

had never been claimed that the demonstration had created any risk to public order or to the life or health of others.

17. On 30 October 2019 the Moscow City Court upheld the conviction on appeal. The applicant attended the hearing and made oral submissions. The court found that the peaceful nature of the demonstration was irrelevant because the applicant had been convicted for a breach of the established procedure for the conduct of public events, namely for failure to submit a prior notification. His escorting to the police station and administrative arrest had been lawful. The offence had been discovered and the evidence had been collected by the police in accordance with the Police Act.

RELEVANT LEGAL FRAMEWORK

I. PROCEDURE FOR THE CONDUCT OF PUBLIC EVENTS

18. The Public Events Act (no. FZ-54 of 19 June 2004) provides that no notification is required for solo demonstrations, except where the demonstrator intends to use a "quickly (de)assembled object" (*"быстровозводимая сборно-разборная конструкция"*) (section 7(1.1)). Notification of a solo demonstration involving such an object obstructing passers-by or traffic must be lodged three to four days in advance (section 7(1)).

19. It is forbidden to hold a public event if no notification was submitted within the time-limits established by the Act (section 5(5)).

20. Article 20.2 § 5 of the Code of Administrative Offences ("the CAO") provides that a breach by a participant of the established procedure for the conduct of public events which has not caused damage to anyone's health or property is punishable by a fine of RUB 10,000 to 20,000 or up to forty hours of community service.

II. OPERATIONAL-SEARCH ACTIVITIES

21. The Operational-Search Activities Act (no. 144-FZ of 12 August 1995 – "the OSAA") provides that the aims of operational-search activities are (a) the detection, prevention, suppression and investigation of criminal offences and the identification of persons conspiring to commit, committing, or having committed a criminal offence; (b) the tracing of fugitives from justice and missing persons; (c) obtaining information about events or activities endangering the national, military, economic or ecological security of the Russian Federation; and (d) obtaining information about property subject to confiscation (section 2 of the OSAA).

22. Audio and video-recording, photography, filming and other technical means may be used during operational-search activities, provided that they are not harmful to the life or health of those involved or to the environment (section 6-3 of the OSAA).

23. Operational-search activities may be conducted following receipt of information that an offence has been committed, is being committed or is being plotted, or about persons conspiring to commit, committing or having committed an offence if there are insufficient grounds for opening a criminal case (section 7-2(1) of the OSAA).

24. In its Ruling no. 86-O of 14 July 1998, the Constitutional Court held that section 7-2(1) of the OSAA should be read in conjunction with section 2 of the OSAA. The term "offence" mentioned in section 7-2(1) should therefore be interpreted as meaning a "criminal offence". If it became clear during operational-search activities that the investigated offence was not classified as criminal, operational-search activities had to immediately be stopped.

25. Agencies performing operational-search activities may seize documents, objects, materials and communications (section 15-1 of the OSAA).

III. COLLECTION OF EVIDENCE IN ADMINISTRATIVE-OFFENCE PROCEEDINGS

26. Chapter 26 of the CAO provides that documents, photographs, audio and video-recordings, databases, and other forms of data can be used in evidence in administrative-offence cases if they contain information that is relevant to the case. The person in charge of the case, be it a judge or another official, must take all the necessary steps to safeguard the evidence until the case is finished and then make a decision about its fate (Article 26.7).

27. The judge or other official in charge of an administrative-offence case may request any information necessary to resolve the case. This information must be submitted within three days of receiving the request. If the information cannot be provided, the organisation must notify the requesting judge or other official in writing within three days (Article 26.10).

IV. POLICE POWERS

28. The Police Act (no. 3-FZ of 07 February 2011) provides that the police must take measures to detect, supress and investigate administrative offences within their competence (section 12-1(11)). They must also take measures to prevent, discover and supress extremist activities (section 12-1(16)).

29. When investigating criminal or administrative offences or examining registered complaints about criminal or administrative offences or accidents, the police are entitled to make reasoned requests for, and to obtain free of charge, information, documents or copies thereof or other necessary data, including personal data, from State and municipal authorities, public associations, organisations, officials and citizens, except for information for which federal law sets up a special access procedure (section 13-1(4)).

V. PROCESSING OF PERSONAL DATA

30. The Personal Data Protection Act (no. 152-FZ of 27 July 2006, as in force at the material time) provided that personal data could be processed, among others, in connection with a person's involvement in administrative judicial proceedings, and also if personal data had been made publicly available by the subject of those data (section 6(1)(3) and (10)).

31. Biometric personal data was defined as information that reveals a person's physiological and biological characteristics that can be used to identify that person. It could only be processed with the written consent of the individual concerned, unless otherwise provided for in the section in question (section 11(1)). Biometric personal data could be processed without the data subject's consent, among others, in connection with the administration of justice, and in cases provided for by the legislation concerning defence, security, counterterrorism, transport security, anti-corruption and operational-search activities (section 11(2)).

32. Processing of special categories of personal data revealing race, nationality, political opinions, religious or philosophical beliefs, health status, or intimate life was generally prohibited, except when authorised by the section in question (section 10(1)). Special categories of personal data could be processed, among others, if personal data had been made publicly available by the subject of those data; in connection with the administration of justice; and in cases provided for by the legislation concerning defence, security, counterterrorism, transport safety, anti-corruption,

operational-search activities and civil and criminal judicial enforcement (section 10(2)(2), (6) and (7)).

VI. VIDEO SURVEILLANCE IN THE MOSCOW UNDERGROUND

33. Governmental Decree no. 410 of 5 April 2017 on requirements for transport security, in force at the material time, provided for a requirement for technical equipment to be installed in underground stations depending on their security profile. In particular, the underground stations in the first (highest security) category had to be equipped with transport security systems ensuring:

– identification of target persons and vehicles by video-surveillance systems on checkpoints at the boundaries of the security zone and its subzones and on parts of the underground essential for its functioning;

– detection and identification of target events by video-surveillance systems at any time and place inside the underground, including in unlimited access subzones, subzones with ticket access and on parts of the underground essential for its functioning;

– detection of target persons and vehicles by video-surveillance systems at any time and place in the "for staff only" subzones of the underground;

– detection of target persons and vehicles by video-surveillance systems at a specific time and place on the perimeter of the security zone;

– real-time transmission of data;

– storage of data on electronic devices for at least thirty days;

– real-time detection of an offender trying to access the underground outside the checkpoints on the perimeter of the security zone and on parts of the underground essential for its functioning;

– registration and real-time transmission of data about staff and passengers crossing the boundaries of the subzones with ticket access, "for staff only" subzones and accessing parts of the underground essential for its functioning (Article 6 § 1).

34. Competent agencies of the Federal Security Service, the police and the Federal Transport Supervision Service were to have access to the data obtained by the transport security systems (Article § 5 (10)).

RELEVANT INTERNATIONAL MATERIAL

I. UNITED NATIONS

35. The relevant parts of the report of the United Nations High Commissioner for Human Rights of 24 June 2020 entitled "Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests" (UN Doc. A/HRC/44/24) read as follows (footnotes omitted):

"33. The use of facial recognition technology to identify persons in the context of assemblies has considerable adverse effects on the rights to privacy, freedom of expression and peaceful assembly, if effective safeguards are not in place. A person's image constitutes one of the key attributes of her or his personality as it reveals unique characteristics distinguishing her or him from other persons. Recording, analysing and retaining someone's facial images without her or his consent constitute interferences with a person's right to privacy. By deploying facial recognition technology at assemblies, these interferences occur on a mass and indiscriminate scale, as this requires the

collection and processing of facial images of all persons captured by the camera equipped with or connected to a facial recognition technology system.

34. Assemblies traditionally have allowed participants a certain level of protection against being singled out or identified. This protection was already considerably weakened by many States that routinely made audiovisual recordings of assembly participants. The rise of facial recognition technology has led to a paradigm shift in comparison with practices of audiovisual recordings, as it dramatically increases the capacity to identify all or many participants in an assembly in an automated fashion. This is particularly problematic if live facial recognition technology is deployed, permitting real-time identification as well as targeted surveillance and tracking of participants. Faulty live identification may also lead to undue interventions in peaceful assemblies by security forces. The negative effects of the use of facial recognition technology on the right of peaceful assembly can be far-reaching, as United Nations human rights experts have pointed out. Many people feel discouraged from demonstrating in public places and freely expressing their views when they fear that they could be identified and suffer negative consequences.

35. Audiovisual recording and facial recognition techniques should only be used when such measures meet the three-part test of legality, necessity and proportionality. The possibility that recourse to facial recognition technology during peaceful protests could ever meet the test of necessity and proportionality, given its intrusiveness and serious chilling effects, has been questioned. Authorities should generally refrain from recording assembly participants. As required by the need to show proportionality, exceptions should only be considered when there are concrete indications that serious criminal offences are actually taking place or that there is cause to suspect imminent and serious criminal behaviour, such as violence or the use of firearms. Existing recordings should only be used for the identification of assembly participants who are suspects of serious crimes.

36. While the use of facial recognition technology in the context of peaceful assemblies is discouraged, governments that still deploy this technology should ensure that they do so on a clear legal basis, including a robust, human rights-compliant regulatory framework. In addition, the authorities that continue to use audiovisual recording and facial recognition techniques should put in place a regulatory framework that contains provisions effectively protecting personal data, including with regards to facial images and the data derived from them. Measures should provide for the immediate deletion of all data, except for the specific segments that may be necessary for the conduct of criminal investigations and the prosecution of violent crimes. All persons concerned should have the right to access and to request the rectification and expungement of such information that is stored without a legitimate purpose and a legal basis, except when this would frustrate criminal investigations or prosecutions for which these data are needed.

37. Furthermore, any use of audiovisual recording and facial recognition technology must be subject to robust and well-resourced oversight mechanisms. While part of the oversight can be carried out by independent and impartial data protection authorities, States should consider additional measures, including the involvement of an independent body, preferably of a judicial nature, in charge of authorizing the use of facial recognition technology measures in an assembly context. In any case, any use of recording and facial recognition technology should be open to judicial challenge. In all circumstances, the authorities should be transparent about the use of

recording and facial recognition technology and always notify members of the public when they are, or may be, recorded and/or when their images may be processed in a facial recognition system.

...

53. In this context, the High Commissioner recommends that States:

...

(h) Never use facial recognition technology to identify those peacefully participating in an assembly;

(i) Refrain from recording footage of assembly participants, unless there are concrete indications that participants are engaging in, or will engage in, serious criminal activity, and such recording is provided by law, with the necessary robust safeguards;"

II. COUNCIL OF EUROPE

36. Recommendation No. R (87) 15 of the Committee of Ministers regulating the use of personal data in the police sector (adopted on 17 September 1987) states, *inter alia*:

"Principle 2 – Collection of data

2.1. The collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation.

...

2.4. The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry."

37. The Guidelines on Facial Recognition (2021) by the Consultative Committee of the Convention for the protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) provide as follows (footnotes omitted):

"Facial recognition is the automatic processing of digital images containing individuals' faces for identification or verification of those individuals by using face templates.

The sensitivity of information of a biometric nature was recognised explicitly with the inclusion of data uniquely identifying a person under the special categories of data in Article 6 of the modernised Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (hereinafter 'Convention 108+').

The context of the processing of images is relevant to the determination of the sensitive nature of the data, as not all processing of images involves the processing of sensitive data. Images shall only be covered by the definition of biometric data when they are processed through a specific technical means which permits the unique identification or authentication of an individual.

These guidelines cover uses of facial recognition technologies, including live facial recognition technologies. ...

Integrating facial recognition technologies into existing surveillance systems poses a serious risk to the rights to privacy and protection of personal data, as well as to other fundamental rights, since use of these technologies does not always require the awareness or co-operation of the individuals

whose biometric data are processed in this way. This is the case, for instance, with the possibility to access digital images of individuals on the internet.

In order to prevent such infringements, the parties to Convention 108+ shall ensure that the development and use of facial recognition respect the rights to privacy and personal data protection, thereby strengthening human rights and fundamental freedoms by implementing the principles enshrined in the Convention in the specific context of facial recognition technologies.

...

Lawfulness

As provided for by Article 6 of Convention 108+, the processing of special categories of data, such as biometric data, shall only be authorised if such processing relies on an appropriate legal basis, and if complementary and appropriate safeguards are enshrined in domestic law. These safeguards shall be adapted to the risks involved and to the interests, rights and freedoms to be protected.

In some legislation, the prohibition of such processing is a rule and its implementation is allowed only by way of exception, in certain specific cases (for example, with the explicit consent of individuals, to protect their vital interests or when the processing is necessary for reasons of overriding public interest), and subject to safeguards that are appropriate to the risks involved.

The necessity for the use of facial recognition technologies has to be assessed together with the proportionality to the purpose and the impact on the rights of the data subjects.

The different cases of use should be categorised and a legal framework applicable to the processing of biometric data through facial recognition should be in place. This legal framework should address, for each different use, in particular:

- a detailed explanation of the specific use and the intended purpose;
- the minimum reliability and accuracy of the algorithm used;
- the retention duration of the photos used;
- the possibility of auditing these criteria;
- the traceability of the process;
- the safeguards.

Strict limitation of certain uses by law

The level of intrusiveness of facial recognition and related infringement of the rights to privacy and data protection will vary according to the particular use and there will be cases where domestic law will strictly limit or even completely prohibit its use where that decision has been reached through the democratic process.

The use of live facial recognition technologies in uncontrolled environments [the notion of 'uncontrolled environment' covers places freely accessible to individuals, which they can also pass through, including public and quasi-public spaces such as shopping centres, hospitals, or schools], in light of its intrusiveness on the right to privacy and the dignity of individuals, coupled with the risk of an adverse impact on other human rights and fundamental freedoms, should be subject to a democratic debate and the possibility of a moratorium pending a full analysis.

...

Integrating digital images into facial recognition technologies

Legislators and decision makers shall ensure that images available in a digital format cannot be processed to extract biometric templates, or to integrate them into biometric systems, without a specific legal basis for the new processing, when those images were initially captured for other purposes (from social media, for instance).

As extracting biometric templates from digital images involves the processing of sensitive data, it is necessary to ensure the possible legal basis considered below, which varies according to the different sectors and uses.

Specifically, using digital images that were uploaded onto the internet, including social media or online photo management websites, or that were captured by video surveillance cameras, cannot be considered lawful on the sole basis that the personal data were made manifestly available by the data subjects.

...

Use of facial recognition technologies in the public sector

Consent should not, as a rule, be the legal ground used for facial recognition performed by public authorities in view of the imbalance of powers between the data subjects and these authorities. ...

Legislators and decision makers have to lay down specific rules for biometric processing using facial recognition technologies for law enforcement purposes. These rules will ensure that such uses must be strictly necessary and proportionate to these purposes and prescribe the necessary safeguards to be provided.

Law enforcement authorities

Biometric data processing using facial recognition technologies for identification purposes in a controlled or uncontrolled environment should be restricted, in general, to law enforcement purposes. It should be carried out solely by the competent authorities in the area of security.

Laws may provide for different necessity and proportionality tests depending on whether the purpose is verification or identification, taking into account the potential risks to fundamental rights and as long as individuals' images are lawfully collected.

For identification purposes, strict necessity and proportionality shall be observed both in the setting up of the database (watch list) and deployment of (live) facial recognition technologies in an uncontrolled environment.

Laws should provide clear parameters and criteria that law enforcement authorities should adhere to when creating databases (watch lists) for specific, legitimate and explicit law enforcement purposes (for example, suspicion of severe offences or a risk to public security).

Considering the intrusiveness of these technologies, in the deployment phase of the live facial recognition technologies in uncontrolled environments, the law shall ensure that law enforcement authorities demonstrate that a variety of factors, including the place and timing of deployment of these technologies, justify the strict necessity and proportionality of the uses.

..."

III. EUROPEAN UNION

38. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal

offences or the execution of criminal penalties, and on the free movement of such data states, among others:

"Article 10 Processing of special categories of personal data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:

(a) where authorised by Union or Member State law;

(b) to protect the vital interests of the data subject or of another natural person; or

(c) where such processing relates to data which are manifestly made public by the data subject."

39. Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement of 26 April 2023 by the European Data Protection Board provide as follows (footnotes omitted):

"36. The processing of biometric data under all circumstances constitutes a serious interference in itself. This does not depend on the outcome, e.g. a positive matching. The processing constitutes an interference even if the biometric template is immediately deleted after the matching against a police database results in a no-hit ...

43. Article 52(1) of the Charter sets the requirement of a specific legal basis. This legal basis must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which authorities are empowered to resort to any measures of collection of data and secret surveillance. It must indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities so as to ensure individuals the minimum degree of protection as entitled under the rule of law in a democratic society. Moreover, lawfulness requires adequate safeguards to ensure that in particular an individual's right under Article 8 of the Charter is respected. These principles also apply to the processing of personal data for purposes of evaluating, training and further developing of FRT [facial recognition technology] systems.

44. Given that biometric data when processed for the purpose of uniquely identifying a natural person constitute special categories of data listed in Article 10 LED [the Data Protection Law Enforcement Directive, cited in paragraph 38 above], the different applications of FRT in most cases would require a dedicated law precisely describing the application and the conditions for its use. This encompasses in particular the types of crime and, where applicable, the appropriate threshold of severity of these crimes, in order to, among other things, effectively exclude petty crime ...

51. According to the CJEU's settled case-law, derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary. This also implies that there are no less intrusive means available to achieve the purpose. Possible alternatives such as – depending on the given purpose – additional staffing, more frequent policing or additional street lighting have to be carefully identified and assessed. Legislative measures should differentiate and target those persons covered by it in the light of the objective, e.g. fighting serious crime. If it covers all persons in a general manner without such differentiation, limitation or exception, it

intensifies the interference. It also intensifies the interference if the data processing covers a significant part of the population.

52. The protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter. Legislation must lay down clear and precise rules governing the scope and application of the measure in question and impose safeguards so that the persons whose data have been processed have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access or use of that data. The need for such safeguards is all the greater where personal data is subject to automatic processing and where there is a significant risk of unlawful access to the data. Furthermore, internal or external, e.g. judicial, authorisation of the deployment of FRT may also contribute as safeguards, and may prove to be necessary in certain cases of severe interference.

53. The rules laid down have to be adapted to the specific situation, e.g. the quantity of data processed, the nature of the data and the risk of unlawful access to the data. This calls for rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality.

54. With regard to the relationship between the controller and the processor it should not be permitted for the processors to have regard only to economic considerations when determining the level of security which they apply to personal data; this could endanger a sufficient high level of protection.

55. An act of law has to lay down substantive and procedural conditions and objective criteria by which to determine the limits of competent authorities' access to data and their subsequent use. For the purposes of prevention, detection or criminal prosecutions, the offences concerned would have to be considered sufficiently serious to justify the extent and seriousness of these interferences with the fundamental rights enshrined for example in Articles 7 and 8 of the Charter.

56. The data has to be processed in a way that ensures the applicability and effect of the EU data protection rules; in particular those provided by Article 8 of the Charter, which states that the compliance with the requirements of protection and security shall be subject to control by an independent authority. The geographical place where the processing takes place may in such a situation be relevant.

57. With regard to the different steps of processing of personal data, a distinction should be made between the categories of data on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned. The determination of the conditions of the processing, for example, the determination of the retention period, must be based on objective criteria in order to ensure that the interference is limited to what is strictly necessary.

58. Based on each situation, the assessment of necessity and proportionality has to identify and consider all implications that fall within the scope of other fundamental rights, such as human dignity under Article 1 of the Charter, freedom of thought, conscience and religion under Article 10 of the Charter, freedom of expression under Article 11 of the Charter as well as freedom of assembly and association under Article 12 of the Charter.

59. Furthermore, it has to be considered as a matter of severity, that if the data is systematically processed without the knowledge of the data subjects, it is likely to generate a general conception

of constant surveillance. This may lead to chilling effects in regard of some or all of the fundamental rights concerned ...

73. Processing can only be regarded as "strictly necessary" if the interference to the protection of personal data and its restrictions is limited to what is absolutely necessary. The addition of the term "strictly" means that the legislator intended the processing of special categories of data to only take place under conditions even stricter than the conditions for necessity. This requirement should be interpreted as being indispensable. It restricts the margin of appreciation permitted to the law enforcement authority in the necessity test to an absolute minimum. In accordance with the settled case-law of the CJEU, the condition of "strict necessity" is also closely linked to the requirement of objective criteria in order to define the circumstances and conditions under which processing can be undertaken, thus excluding any processing of a general or systematic nature ...

104. The use of facial recognition technologies is intrinsically linked to processing of significant amounts of personal data, including special categories of data. The face and, more generally, biometric data are permanently and irrevocably linked to a person's identity. Therefore, the use of facial recognition has direct or indirect impact on a number of fundamental rights and freedoms enshrined in the EU Charter of Fundamental Rights that may go beyond privacy and data protection, such as human dignity, freedom of movement, freedom of assembly, and others. This is particularly relevant in the area of law enforcement and criminal justice.

105. The EDPB understands the need for law enforcement authorities to benefit from the best possible tools to quickly identify the perpetrators of terrorist acts and other serious crimes. However, such tools should be used in strict compliance with the applicable legal framework and only in cases when they satisfy the requirements of necessity and proportionality, as laid down in Article 52(1) of the Charter. Moreover, while modern technologies may be part of the solution, they are by no means a 'silver bullet'.

106. There are certain use cases of facial recognition technologies, which pose unacceptably high risks to individuals and society ('red lines'). For these reasons the EDPB and the EDPS have called for their general ban.

107. In particular, remote biometric identification of individuals in publicly accessible spaces poses a high risk of intrusion into individuals' private lives and does not have a place in a democratic society, as by its nature, it entails mass surveillance. In the same vein, the EDPB considers AI-supported facial recognition systems categorising individuals based on their biometrics into clusters according to ethnicity, gender, as well as political or sexual orientation as not compatible with the Charter. Furthermore, the EDPB is convinced that the use of facial recognition or similar technologies, to infer emotions of a natural person is highly undesirable and should be prohibited, possibly with few duly justified exceptions. In addition, the EDPB considers that processing of personal data in a law enforcement context that would rely on a database populated by collection of personal data on a mass-scale and in an indiscriminate way, e.g. by "scraping" photographs and facial pictures accessible online, in particular those made available via social networks, would, as such, not meet the strict necessity requirement provided for by Union law."

IV. OTHER RELEVANT MATERIAL

40. The relevant parts of the report of 17 January 2022 by OVD-Info, an independent human rights media project, entitled "How the Russian state uses cameras against protesters" read as follows:

"Detentions of protesters after the end of the event, or, as we call them, 'post factum detentions', have taken place before 2021. In 2018, OVD-Info counted 219 such cases in 39 regions of Russia; they were mostly isolated in nature: one or two people were detained in connection with one event, in exceptional cases the number of detainees reached ten. They began to be widely used in 2020 ...

We believe that the increase in the number of post factum detentions is based on the development of technologies for monitoring social networks and facial recognition ...

Our report is devoted to the use of facial recognition systems to restrict freedom of assembly. Although our research focuses on Moscow, according to our data, the geography of this phenomenon goes far beyond the capital ...

The use of facial recognition technology is evidenced, first of all, by the large-scale post factum detentions and the prosecution of non-public figures, as well as the words of police officers ...

Although the use of a facial recognition system to identify protesters was widely covered in the media after the January 2021 protests, the technology is rarely mentioned in official documents ...

The paucity of direct evidence of the use of facial recognition technology in police reports, case files and court rulings may indicate that the police and courts prefer not to officially document this information. Nevertheless, in some documents there are indirect signs of the use of technology ...

People whom the police suspected of participating in the protest events were detained right at the workplace, removed from university classes, one person was taken right from a lesson at school. There were cases of detentions in cafes, on the street, in the subway, on the train platform and on the train ...

Detentions on platforms, in cafes and in rented apartments may indicate the use of movement tracking systems around the city against the persecuted participants of the protests. Records from an CCTV at residential entrances can be used for this search ...

If a report on an offense against a person was issued post factum, and not after a person being detained at an event, this often means that their identity was not established on the spot ... Therefore, law enforcement officers need to explain the process behind a comparison of identity between the person captured on the video and the person they are trying to hold liable because of participation in an unauthorised event.

Having studied the available materials, OVD-Info has come to the conclusion that there are two main ways for the police to do this:

1. an indication that the identification of persons occurred during 'operational-search activities';
2. a police officer's report in which they state that they 'identified' a specific citizen on photos and videos, without further explanation.

In none of these cases does the police 'on paper' admit that facial recognition technology was used in any way to determine a person's identity. It is possible that law enforcement officers prefer not to document the use of facial recognition precisely because it is in the 'gray zone' of Russian legislation ...

At the same time, in such cases there are no references to investigative activities, and there are also no answers to the question of how exactly it was possible to identify a particular person ...

To identify the protesters, recordings from surveillance cameras ..., recordings made on the ground by law enforcement officers, photos and videos from the Internet (Telegram channels, chats, personal pages on social networks, YouTube) have been used.

There are cases when cameras – for example, installed in the entrances of residential buildings or in the subway – were also used to determine the location of a person to hold him administratively responsible.

For identification, the police use databases with photos from documents (internal and external passports, social cards) and from social networks ...

Prosecution for participation in protests, delayed in time, is associated with additional difficulties and large negative consequences compared to detention during an event. Among other things, with a serious invasion of privacy and influence on other areas of human life.

The practice of post factum detentions has a clear punitive orientation and has an intimidating and marginalising effect on potential participants of assemblies. Taking into account the fact that the statute of limitations of the most common 'rally' Article 20.2 of the Code of Administrative Offences has been increased to a year, protest participants remain waiting for a possible detention for a long time. There are already known cases when a report was issued more than six months after the event. Finally, post factum administrative liability gives law enforcement agencies the opportunity to manipulate the times of court hearings, creating the basis for the use of accusations of 'repeated' and 'multiple' violations (Part 8 of Article 20.2 of the Code of Administrative Offences and Article 212.1 of the Criminal Code), which are fraught with severe sanctions ...

In some cases, the courts approve the use of facial recognition in the cases of demonstrators under the pretext of protecting public interests. Meanwhile, the lack of mass usage of this technology for many other types of offenses (such as crossing the road in the wrong place or stowaway) indicates that the main goal is not to protect public interests, but to persecute political opponents of the authorities.

A number of issues related to the creation and functioning of the infrastructure necessary for the use of a facial recognition system to limit protests (street photography and video recording, storage of the received data, the formation of databases of photographs with personal identification), access of police officers to databases, protection of personal data are insufficiently regulated. In combination with the lack of transparency of usage and the lack of public control, it is possible to turn this technology into an instrument of politically motivated persecution."

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 XXX 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 reprehensible 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.
   Done in English, and notified in writing on 4 July 2023, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

   Milan Blaško Registrar
   Pere Pastor Vilanova President