In the European Court of Human Rights

Application No. 11519/20

BETWEEN:

Nikolay Sergeyevich GLUKHIN

Applicant

v.

Russia

Respondent Government

THIRD-PARTY INTERVENTION

ARTICLE 19: Global Campaign for Free Expression

Submitted on 10 June 2022

INTRODUCTION

1. This third-party intervention is submitted on behalf of ARTICLE 19: Global Campaign for Free Expression (ARTICLE 19, or the Intervener). The Intervener welcomes the opportunity to intervene as a third-party in this case, by the leave of the President of the Court, which was granted on 22 September 2021 and extension on 20 May 2022, pursuant to Rule 44 (3) of the Rules of Court. This submission does not address the facts or merits of the applicant's case.

2. The Intervener believes that this case provides the Court with the opportunity to rule for the first time on the compatibility of government usage of facial recognition (FR) technology with the rights under the Convention, in particular the right to personal and family life (Article 8), the right to freedom of expression (Article 10) and the right to freedom of peaceful assembly (Article 11). The case raises fundamental questions on the scope of use of biometric mass surveillance and its application to suppress socio-political protest and freedom of expression. In these submissions, the Intervener addresses the following:
   (i) International and comparative standards on the use of biometric technologies, namely those pertaining to the right to private and family life, the right to freedom of expression and the right to peaceful assembly; and

   (ii) Overall challenges biometric and facial recognition (FR) technologies pose to human rights based on international and comparative national standards and what guarantees should be applied in the development and deployment of biometric technologies based on comparative and international standards.

SUBMISSION

i. International and comparative standards on the use of biometric technologies

Standards in relation to the right to private and family life

3. There is an important set of international standards applicable to biometric technologies in relation to the right to private and family life, including data protection. The UN High Commissioner for Human Rights in his report on the right to privacy in the digital age highlighted the concerns over the use of biometric data, its potential to be "gravely abused" and States embarking on biometrics-based projects without "adequate legal and procedural safeguards in place." [1] The report recommends that States, *inter alia*, "*[e]nsure that data-intensive systems, including those involving the collection and retention of biometric data, are only deployed when States can demonstrate that they are necessary and proportionate to achieve a legitimate aim."*[2]

4. In Europe, the Council of Europe Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (the Convention 108+) provides that biometric data uniquely identifying a person shall only be allowed where appropriate safeguards are enshrined in law, complementing those of the Convention 108.[3]

---

[1] UN High Commissioner for Human Rights, The right to privacy in the digital age, A/HRC/39/29, 3 August 2018, para 14.
[2] *Ibid*., para 61 c).
[3] Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 January 1981, ETS 108.

5. The same principles are enshrined in the European Union by the General Data Protection Regulation (GDPR) which prohibits the processing of biometric data for the purpose of uniquely identifying a natural person allowing very limited exceptions.[4] In addition, the GDPR treats biometric data used for identification purposes as "special category data" meaning it is considered more sensitive and in need of more protection. The same approach is adopted in the Standards for Personal Data Protection for Ibero-American States.[5]

6. The importance of ensuring strong safeguards to prevent unlawful collection, processing and use of biometric data has been stressed in the European Union by the Fundamental Rights Agency (FRA) with particular reference to the collection of personal data including fingerprints of asylum and visa applicants, as well as migrants in an irregular situation.[6] A number of States in different areas of the world have also established the protection of these rights and privacy safeguards in their national legislation.[7]

7. Moreover, standards have been developed to ensure data subjects have a right to be informed and give consent to the collection and use of their personal data, which leads to a variety of information obligations by the controller. The controller can be either private or public and the data subjects have a right to know whether their personal information has been processed, the categories of data, for what purposes and the use, and how long they have been stored. This right has been incorporated in General Comment 16 as part of the Right to Privacy[8], by the European Court of Human Rights (ECHR) as part of Article 8 on the Right to Private and Family Life[9] and in Article 15 of the GDPR.[10]

8. In 2020, the European Data Protection Board (EDPB) adopted specific Guidelines[11] to examine how the GDPR applies in relation to the processing of personal data by video devices. The Guidelines highlight how the intensive use of video devices has massive implications for data protection, it affects citizens' behaviour, the risks related to the possible malfunctioning of these devices and the biases they may produce.

9. International human rights bodies have also moved towards recognising a right to anonymity as an important aspect of the right to privacy. This has implications for biometric technologies used to identify individuals, whether this being in their homes or in public spaces. Hence, state interference with anonymity should be subject to the

[4] Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 9.
[5] Ibero-American Data Protection Network (RIPD), Data Protection Standards of the Ibero-American States, Articles 2.1(d) and 29.4.
[6] FRA, Opinions Biometrics, 2019.
[7] See e.g. the Illinois State Biometric Information Privacy Act, which recognised that "an overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information;" Illinois Compiled Statutes 740 ILCS 14/1 Biometric Information Privacy Act, Sec 5 (d).
[8] HR Committee, General Comment No. 16 (Article 17 ICCPR), 8 April 1988, para 10; in which the HR Committee noted that the right is necessary in order to ensure respect of the right to privacy.
[9] *C.f.* European Court, *Gaskin v. the United Kingdom*, 7 July 1989, Series A no. 160, para 49; *M.G. v. the United Kingdom*, App. No. 39393/98, 24 September 2002, para 27; *Odièvre v. France* [GC], App. No. 42326/98, ECHR 2003III), paras 41-47; *Guerra and Others v. Italy*, App. No. 14967/89, 19 February 1998.
[10] GDPR, *op.cit*.
[11] EDPB Guidelines 3/2019 on processing of personal data through video devices adopted on 29 January 2020.

three-part test of legality, necessity, and proportionality, as is any other interference with the right to privacy.[12]

10. Specific standards have been developed with regards to facial recognition technologies (FR technologies). The Guidelines on FR technologies adopted by the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108) in January 2021 provide recommendations for governments, companies and FR developers to ensure that the development of this technology does not adversely affect human rights. They call for prohibitions on the use of particularly intrusive FR technologies such as the use of live FR in "uncontrolled environments" whose notion covers places freely accessible to individuals which they can also pass through, including public and quasi-public spaces like shopping centres, hospitals or schools, the "affect recognition" that can arguably detect personality traits, inner feelings, mental health and workers' engagement or the use of FR technologies for the sole purpose of determining a person's skin colour, religious or other beliefs, sex, racial or ethnic origin.[13] These uses should be strictly limited or even completely prohibited.[14]

Standards in relation to the right to freedom of expression

11. UN human rights mandates have warned about the impact of biometrics systems on freedom of expression. In 2019, the UN Special Rapporteur on Freedom of Expression raised concerns about the impact of biometric systems on human rights defenders, journalists, politicians and UN investigators, and called for an immediate moratorium on the sale, transfer and use of surveillance technology until human rights-compliant regulatory frameworks are in place.[15]

12. In relation to FR technologies, in October 2021 the EU Parliament passed a resolution calling for a ban on the use of FR technology in public spaces.[16] In particular, the resolution cites the failure of the artificial intelligence used in FR technology to identify minority groups

13. In June 2021, the EDPB and the European Data Protection Supervisor (EDPS) have called for a ban on the use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination. Similarly, the EDPB and EDPS recommend a ban on AI systems using biometrics to categorise individuals into clusters based on ethnicity, gender, political or sexual orientation, or other grounds on which discrimination is prohibited under Article 21 of the EU Charter of Fundamental Rights.[17]

---

[12] Special Rapporteur on freedom of expression, Report on encryption, anonymity, and the human rights framework, A/HRC/29/32, 22 May 2015.

[13] Council of Europe, Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), Guidelines on facial recognition (2021)

[14] *Ibid*. p. 8

[15] OHCHR, UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools, 25 June 2019.

[16] EU Parliament, Use of artificial intelligence by the police: MEPs oppose mass surveillance, Resolution adopted on 6th October 2021.

[17] EPDB & EDPS, Statement released on 21 June 2021, "Call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination."

Standards in relation to the right to peaceful assembly

14. In 2019, the UN Special Rapporteur on Freedom of Association and Assembly declared in his Report that "*[t]he use of surveillance techniques for the indiscriminate and untargeted surveillance of those exercising their right to peaceful assembly and association, in both physical and digital spaces, should be prohibited*." [18]

15. With regards to the right to protest, in 2018, the UN Special Rapporteur on the Right to Privacy has criticised the use of FR technology during a peaceful demonstration as a violation of the right to privacy and for having the potential of discouraging people from exercising the fundamental right to free association.[19]

16. In the same vein, in 2020, the UN Human Rights Council adopted a resolution specifically condemning the use of FR technology in the context of peaceful protests, since these technologies create a chilling effect on the exercise of the right to protest by enhancing governments' abilities to identify, monitor, harass, intimidate, and prosecute protesters.[20] The Council called on States to refrain from using FR technology to monitor individuals involved in peaceful protests.

Comparative standards on the use and deployment of biometric and FR technologies

17. National parliaments, bodies and courts in the EU have issued important decisions in relation to biometric and FR technologies in which they addressed the compatibility of the use and deployment of these technologies with the right to privacy. For instance, the Swedish Data Protection Authority fined a municipality for checking school attendance through FR technology. Despite the consent being obtained from the parents, the authority considered there were other less intrusive means to check attendance such as signing a paper.[21] Similarly, in France, an administrative court in Marseille ruled that the system adopted in two high schools to monitor the entrance to the school with FR technology was unlawful.[22] One of the arguments made was that no impact assessment had occurred before the system was put in place. The Court also considered that it violated Article 8 of the ECHR. In 2020, the Dutch Data Protection Authority issued a fine for the unlawful processing of employees' biometric data as it had been used to monitor their attendance and time registration on the grounds that the processing was disproportionate and did not qualify under any exceptions under the GDPR.[23]

18. In December 2021, the Italian Parliament introduced a moratorium on the development and deployment of FR surveillance systems in public spaces both by public and private actors until they can ensure the full protection of freedom of expression and full compliance with fundamental rights. The moratorium will last until December 2023 unless a new law on biometric surveillance is passed. This followed an earlier opinion of the Data Protection Authority that warned about FR surveillance systems in public spaces constituting mass surveillance and amounting to a violation of fundamental rights

[18] Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, A/HRC/41/41 17 May 2019, para 57.
[19] Biometric Update, Biometric Update, UN privacy rapporteur criticizes accuracy and proportionality of Wales police use of facial recognition, 3 July 2018.
[20] See UN Human Rights Council, Resolution on the promotion and protection of human rights in the context of peaceful protests, A/HRC/44/L.11, 2020.
[21] EDPB, Facial recognition in school renders Sweden's first GDPR fine, 22 August 2019.
[22] France, Tribunal Administratif de Marseille, Decision 1901249, 27 February 2020.
[23] Dutch Supervisory Authority Fines Company for Processing Biometric Data of Employees, Inside Privacy, 1 May 2020.

including the right to personal and family life as enshrined in Article 8 ECHR if specific rules were not adopted to ensure they are strictly proportionate to the aim pursued and necessary.[24]

19. Additionally, in the United Kingdom, a variety of public bodies delivered decisions in relation to FR technologies. In 2019, the Information Commissioner's Office (ICO) dealt with the lack of consent of the data subjects with regards to the instalment and use of a FR technology system at King's Cross Station in London where passers-by were filmed without being informed. The police using the FR technology system allegedly shared "watchlists" with the company deploying it to carry out identification operations against the people on file. The ICO called on the government to adopt a binding code of practice on the subject while reminding the police that they must assess more carefully and justify any use made of these technologies in public spaces.[25] Furthermore, in August 2020, the UK Court of Appeal ruled that the FR technology system used by the police to scan faces in public spaces to identify individuals violates personal freedoms, invades privacy, and is discriminatory. The applicant argued that South Wales Police caused him "distress'' by scanning his face as he shopped in 2017 and as he attended a peaceful anti-arms protest in 2018. The appeals judges ruled that the way the system was being used during tests was unlawful and that authorities should take greater care in how they deploy it.[26] Adopting an approach similar to the one of the Court and the ICO, in February 2020, the Scottish Parliament, following an inquiry into Police Scotland's proposed use of FR technology surveillance, stated that there was "no justification" for police to use live FR technology surveillance and that it would be a "radical departure" from policing by consent.[27]

20. Outside Europe, in 2021 the Court of Justice of Sao Paolo blocked the use of FR on subway stations and ordered the concessionary of the Sao Paulo metro not to capture personal data of commuters through cameras or other devices without their explicit consent.[28] The judge stated that the company behind the technology had not presented sufficient information about what they would be doing with the collected data and that the justification provided for the deployment of the technology, i.e. to serve public agencies, was "no more than conjecture".[29] The decision has been appealed and until the appeal judgment will be delivered the system is still in place and operating.

21. In the United States, several States are discussing bills that deal with biometric technologies, such as California,[30] Kentucky,[31] Maine,[32] Maryland,[33] Massachusetts,[34]

---

[24] Italy Garante Privacy, Parere sul sistema Sari Real Time - 25 March 2021 [9575877].
[25] UK Information Commissioner's Office, ICO investigation into how the police use facial recognition technology in public places, 31 October 2019; E. Denham, Information Commissioner, Blog: Live facial recognition technology – police forces need to slow down and justify its use.
[26] UK court says face recognition violates human rights, TechXplore, 11 August 2020.
[27] Facial recognition: "No justification" for Police Scotland to use technology, BBC, 11 February 2020.
[28] Privacy win for 350,000 people in Sao Paulo: court blocks facial recognition cameras in metro, 12 May 2020, AccessNow.
[29] Brazil: Civil society blocks facial recognition tech on São Paulo Metro, ARTICLE 19, 9 May 2022 (Judgement in Portuguese accessible here); São Paulo subway ordered to suspend use of facial recognition, ZDNet, 23 March 2022
[30] California, Senate Bill No. 1189 Introduced by Senator Wieckowski on 17 February 2022.
[31] Kentucky, House Bill 626 introduced by State Representative Josh Bray on 28 February 2022.
[32] Maine, House Bill 1945 introduced by Margaret O'Neil on 26 January 2022.
[33] Maryland, House Bill 259 introduced by State delegate Sara Love on 13 January 2022.
[34] Massachussetts, Senate Bill 2687 presented by Joint Committee on Advanced Information Technology, the Internet, and Cybersecurity on 14 February 2022.

Missouri[35] and New York[36]. All these laws set specific privacy obligations and rules for the collection, use and processing of biometric data. These bills follow the initiatives of Illinois,[37] Texas[38] and Washington[39] where biometric laws have been passed earlier.

ii. Overall challenges biometric and in particular FR technologies pose to human rights and what constitutes adequate and sufficient safeguards against abuse

22. There are a number of challenges to human rights posed by the misuse and abuse of biometric technologies that ARTICLE 19 would like to flag to this Court:

    a) **Lack of specific legal basis**: This technology is often deployed without a legal basis, in the absence of any specific legislative framework or any adequate safeguard for human rights and without previous public consultation. Data protection legislation is often used to provide protection against the unlawful collection and processing of biometric data. However, it might not be sufficient to cope with all relevant problems for the protection of other rights. In addition, these frameworks provide for exceptions when it comes to the processing of personal data for law enforcement purposes, which are often shaped in vague and broad terms, without sufficient guarantees for the protection of individuals' data.

    b) **Data collection, storage and retention**: The development and deployment of biometric technologies imply the collection and generation of large amounts of sensitive personal data. Biometric data are a special category of personal data which, because of their capacity to reveal intimate information about a person (fingerprints, eye scans, racial or ethnic origin, sex and so on), require additional safeguards and enhanced protection. Datasets are often built through problematic methods of collection and hold biases that reflect existing patterns of societal stereotyping.[40]Equally problematic is the diffuse practice of indiscriminate retention of biometric data that does not meet the necessity and proportionality test.[41] Furthermore, these massive databases can easily be re-purposed by state or private actors for purposes other than which they were originally intended. This raises the issue of 'mission creep,' or the potential to expand the application of such technologies to collect data and/or execute functions that were not originally approved.[42]

---

[35] Missouri, House Bill 2716 introduced by State Representative Doug Clemens on 16 February 2022.
[36] New York, Assembly Bill A27 introduced by Member Aileen Gunther and other 25 legislators introduced in January 2021 but discussed in January 2022.
[37] Illinois, Biometric Information Privacy Act (BIPA), 740 ILCS 14/.
[38] Texas, Business and Commerce Code, Title 11. Personal Identity Information, Subtitle A. Identifying Information, Chapter 503. Biometric Identifiers.
[39] Washington, Chapter 19.375 RCW, Biometric Identifiers.
[40] An EU-wide asylum fingerprint database, the European Asylum Dactyloscopy Database (EURODAC) is meant to store fingerprints of all people who cross a European border. However, concerns were raised, when it was announced that the information in the database would be made available to law enforcement authorities and Europol in their terrorism investigations. The repurposing of the database for terrorism purposes rather than for immigration further stereotypes and stigmatises an already vulnerable population: asylum seekers, who are already fleeing persecution, are being immediately associated with terrorist acts; see Statewatch and PICUM, Data protection, Immigration Enforcement and fundamental Rights: What's the EU's Regulations on Interoperability Mean for People with Irregular Status.
[41] *S. and Marper v. the UK*, *op.cit*., para 103.
[42] The EU-wide example of bulk metadata collection shows how States collect information for a particular use (e.g. finding terrorists) but over time increase the scope to include non-violent crimes such as burglaries.

c) **Necessity and proportionality**: Even when a legitimate purpose for the use of biometrics is identified, its deployment does not always meet a narrowly constructed test of necessity and proportionality: the technology has to be absolutely necessary to achieve the scope and there should be no other less invasive means to do so. If this test is not passed, the use of the technology should not be allowed, irrespective of its availability or allure.[43]

d) **Lack of remedies in cases of human rights violations**: Neither public nor private actors dealing with biometric technologies have put in place effective remedies in case of violations of human rights. For instance, if the use of biometric technology leads to a discriminatory result, it is not clear how such a situation will be addressed. Equally, if the police use biometric technology to track individuals engaging in political, religious, or other categories of protected expression, it is not clear what would be the remedy at disposal for those individuals. In any case, a precondition to the right of an effective remedy is that people are aware that their biometric data is being processed or that a decision concerning them has been taken based on the use of biometric technologies. This is not the case in a vast majority of situations.

23. With regards in particular to the ability of individuals to exercise their right to freedom of expression, the use of biometric technologies poses the following challenges:

a) **Chilling effect of mass surveillance:** Studies show that the awareness of being watched and tracked might lead people not to join public assemblies or not participate in social and cultural life, and not to freely express their thoughts, conscience and religious beliefs in public spaces.[44]

b) **Impact on the right to freedom of expression of specific categories of individuals:** journalists could be discouraged in conducting investigations or establishing contacts with their sources of information if they know that they could be monitored/spied upon and identified by biometric technologies in public or private spaces.[45] The fear of being tracked and watched can have a strong chilling effect on them; this, in turn prevents quality journalism and investigative reporting, frustrating the role that media play in our societies. Activists and political opponents might have similar fears and thus the same incentives for self-censorship. For example, they can be dissuaded from exercising their right to protest if, as a consequence of the use of biometric technologies by the State, they will be attributed specific classifications, such as 'habitual protestors' or similar.[46] Moreover, biometric technologies directly impede the way in which NGOs operate with regards to the protection of their sources as well as their "watchdog" function.[47]

---

[43] The Administrative Tribunal of Marseille, 27 February 2020, req. n. 1901249.

[44] See e.g. FRA 2020 report, *op.cit*., p. 20; or London Policing Ethics Panel, Final Report on Live Facial Recognition, May 2019.

[45] Surveillance and Human Rights, *op. cit*., p. 26.

[46] See e.g. The Indian Express, Delhi Police film protests, run its images through face recognition software to screen crowd, 28 December 2019; India Today, Amit Shah on Delhi riots probe: 1100 people identified using face recognition tech, 300 came from UP, 11 March 2020.

[47] C.f. European Court, Szabó and Vissy v Hungary, App nos. 37138/14, 12 January 2016, para 38. See also Human Rights Watch & Pen International, With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy, July 2014; and CNIL, 2019 report, op.cit. (the CNIL noted that constant surveillance and facial recognition in public spaces can make seemingly normal attitudes and behaviours appear suspect, such as wearing sunglasses, having one's hood up, or staring at the ground or a phone).

24. Many concerns about the deployment and use of **facial recognition** are similar to those listed earlier for other biometric technologies. However, due to its specific features, FR technologies raise specific challenges. ARTICLE 19 would like to express some key concerns in relation to the use of FR technologies:

    a) **Consent**: FR technologies do not need contact, nor an active behaviour from the target. For this reason, actors using FR can easily subject targets to FR without their knowledge or consent.[48]

    b) **Accuracy**: FR is based on statistical estimation of correspondence between the compared elements; therefore, it is intrinsically fallible. Numerous studies demonstrate that FR fails in terms of accuracy, particularly for underrepresented or historically disadvantaged groups.[49]

    c) **Little to no oversight**: Apart from a few exceptions, law enforcement agencies have little to no oversight of the use of FR technology in various countries. In most places, there is nothing explicitly preventing authorities from using FR technology on live camera feeds, turning passers-by into unknowing participants of a virtual police line-up; and there are no rules about the retention of data collected through the use of FR technology.

    d) **Lack of necessity and proportionality**: Many use-cases of FR technologies have already been considered as failing the necessity and proportionality test. Among others, the use in schools, with the purpose of controlling students' access has been condemned by data protection authorities and courts alike.[50]

25. FR technologies have serious repercussions on the right to freedom of expression, which adds to those listed with regards to biometric technologies in general, namely:

    a) **Right to remain anonymous**: The use of FR technologies, and especially live FR technologies, in public spaces is an evident challenge to anonymity. It limits the

[48] In early 2019, the Serbia Minister of Interior and the Director of Police announced the placement of 1000 cameras on 800 locations in Belgrade. The public was informed that these surveillance cameras will have facial and license plate recognition software. Three civil society organisations in the country published a detailed analysis of the Ministry of Interior's DPIA on the use of smart video surveillance, which concluded that it did not meet the formal or material conditions required by the Law on Personal Data Protection in Serbia. The Serbian data protection authority confirmed the findings. For more information, see, e.g. EDRigram, Serbia: Unlawful facial recognition video surveillance in Belgrade, 4 December 2019.

[49] See e.g. the National Institute of Standards and Technology, NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software, 19 December 2019; D. Leslie, Understanding bias in facial recognition technologies, The Alan Turing Institute, 2020; A. Najibi, Racial Discrimination in Face Recognition, 24 October 2020.

[50] In 2019, CNIL, the French data protection authority condemned the use of face recognition technology aimed to smooth and control children's access to school on the grounds that the same objective can be achieved by means which are less invasive of children's fundamental rights; see CNIL, op.cit. Several NGOs also denounced the implementation of this facial recognition technology in schools; see, e.g. La Quadrature du Net, the League of Human Rights, CGT Educ'Action des Alpes-Maritimes and the Federation of Parents' Councils of Public Schools in the Alpes-Maritimes, Facial Recognition in High Schools: A recourse to block biometric surveillance, 19 February 2019. See also Administrative Court of Marseille, 9th ch., Judgment of 27 February 2020. Incidentally, the French magistrate, involved in a relevant case in Marseille, stated during the hearing that "the Region is using a hammer to hit an ant" which perfectly visualises the lack of proportionality between the measure implemented (FR system) and the objective to be achieved (controlling students' access). In a similar vein, students, from various schools across US cities, have protested against the use of facial recognition and in some cases, this has led to the school management abandoning the plan to deploy the technology. See e.g. The Guardian, Ban this technology': students protest US universities' use of facial recognition, 3 March 2020.

possibility of anonymous movement and anonymous use of services, and more generally the possibility to remain unnoticed. Protection of public space for the exercise of fundamental rights and freedoms, in particular the right to freedom of expression, is crucial. If deployed extensively, for example on surveillance videos or police-worn cameras, FR technology can significantly redefine the nature of public space;[51] its use will not pass the test of necessity and proportionality. Indiscriminate and untargeted use of FR technologies which leads to mass surveillance in public spaces should never be allowed.[52]

b) **Right to protest**: Using FR technologies during protests may discourage people from taking part, having clear negative implications vis-à-vis the effective functioning of participatory democracy.[53] Even if applied to police violence in protests, FR technologies may still affect those protesters who do not engage in violence or bystanders. In other words, the deployment of FR technologies may generate a chilling effect whereby individuals alter their behaviour and refrain from exercising their rights to protest. People might thus be discouraged from meeting individuals or organisations, attending meetings, or taking part in certain demonstrations. Likewise, live FR technologies in public spaces can be used to target journalists, posing a chilling effect on individuals' and society's access to information on protests.

c) **Religious freedom**: The use of FR technologies could interfere with people's religious freedom.[54] This can happen, for example, if people are obliged to uncover their faces in public spaces contrary to their religious traditions, and if they are subject to fines or other negative consequences in case they do not.

26. In light of the challenges to the use of biometric and FR technologies in public spaces by State actors described above, ARTICLE 19 considers guarantees should be put in the place for the development and deployment of such technologies. These guarantees are:

a) When a legitimate purpose for the use of biometric technology is identified, its development and deployment must meet a narrowly constructed test of necessity and proportionality;

b) Biometric data should be collected, processed and retained for a legitimate purpose only and they shall not be re-purposed without the individuals' consent;

c) Protection against security breaches should be ensured and individuals should be able to ask for redress when they suffer harm from such a breach. A data security

[51] Civil society around the world started to raise its voice about the impact of FR surveillance on anonymity and about its chilling effect on freedom of expression. For example, in Australia, the deputy director of the New South Wales Council for Civil Liberties, in the context of the NSW parliamentary enquiry about the deployment of facial images matching systems said that "this brings with it a real threat to anonymity. But the more concerning dimension is the attendant chilling effect on freedoms of political discussion, the right to protest and the right to dissent. We think these potential implications should be of concern to us all;" see The Guardian, Facial image matching system risks 'chilling effect' on freedoms, rights groups say', 7 November 2018.

[52] See e.g. E. Denham, Information Commissioner, Blog: Live facial recognition technology – police forces need to slow down and justify its use.

[53] By way of example, the Home Ministry in India, on February 2020, arrested 1100 people who participated in peaceful protests, identifying them with the use of face recognition. See India Today, Amit Shah on Delhi riots probe: 1100 people identified using face recognition tech, 300 came from UP, *op. cit.*

[54] Religious freedom is guaranteed by Article 18 UDHR and given effect by the provisions of Article 18 ICCPR, as well as other regional and national instruments.

infrastructure should exist and be sufficiently developed to protect individuals' biometric data from security risks;

d) Effective remedies should exist in case of violations of human rights, in particular when the police use biometric technologies to track individuals engaging in political, religious or other categories of protected expression;

e) Accuracy shall be ensured through data quality and comprehensiveness of the training databases. This ensures that systems are developed without bias, including racial bias, and they do not over or under-represent certain characteristics.

CONCLUSIONS

27. The use and deployment of biometric technologies, and in particular FR technologies, represent one of the greatest threats to fundamental rights in the digital age. They constitute a threat to the right to privacy and anonymity and have at least a strong "chilling effect" on the rights to freedom of expression and on the right to freedom of assembly and association. Therefore, the Intervener suggests that the Court should carefully consider the implications of government use of these technologies on individuals' human rights, particularly in the absence of sufficient safeguards in the national legal framework.

Barbora Bukovska
Senior Director for Law and Policy
ARTICLE 19