European Journal of Risk Regulation (2025), 1–28
doi:10.1017/err.2025.26

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

The Use of Facial Recognition Technologies in the Context of Peaceful Protest: The Risk of Mass Surveillance Practices and the Implications for the Protection of Human Rights

Giulia Gabrielli

Department of International, Legal, Historical and Political Studies, University of Milan, Milan, Italy
Email: giulia.gabrielli@unimi.it

Abstract

The increasing use of Artificial Intelligence (AI)-based surveillance technologies such as facial recognition for national and public security purposes in the area of law enforcement raises serious concerns regarding the potential risks of abuse and arbitrariness it might entail, in the absence of adequate safeguards. At an international level, the impact of biometric identification systems on the protection and promotion of human rights and fundamental freedoms has been consistently emphasised by international organisations, human rights monitoring mechanisms and the civil society, particularly with regards to the risk of mass surveillance possibly resulting in the infringement upon the right of privacy and freedom of assembly. This contribution will assess the international human rights and standards applicable to the use of these technologies for national security purposes especially in the context of peaceful protest by assessing the position of the European Court of Human Rights in *Glukhin v Russia* (11519/20) and recent regulatory attempts.

Keywords: European Court of Human Rights; facial-recognition technologies; international human rights law

I. Introduction

The deployment of facial recognition technology (FRT) is experiencing an exponential and seemingly unrestrainable growth in private and public life. Technological developments and increased availability of training data have facilitated the spread and deployment of biometric systems enabling the authentication and the automatic identification of individuals for a variety of purposes.[1] By virtue of their potential benefits and (either actual or perceived) efficiency, FRT applications are diverse and rapidly expanding: in retail settings, they are deployed to identify known shoplifters or recognise regular

[1] Unlike identification and authentication, which are designed to compare different features of a person for the purpose of determining who they are or who they are claiming to be, categorisation allows to extract some features from the face image of an individual to deduce certain characteristics, including their age, gender or ethnic origin, or in some cases even emotions, personality traits or potential behaviours. Categorisation and emotion recognition are outside the scope of this paper. For an analysis of the variety of technologies and different purposes of biometric systems, see European Union Agency for Fundamental Rights (FRA), *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement* (Luxembourg, Publications Office of the European Union 2020) pp 2, 7–8. On a discussion on biometric applications, see also Art 29 Working Party, "Opinion 3/2012 on developments in biometric technologies" (27 April 2012) 00720/12/EN, WP193.

customers; in the workplace or at school, they assist in monitoring attendance and obtaining access to dedicated services; during or in the aftermath of natural disasters or armed conflicts, they are a useful tool to identify victims whose documents have been lost or destroyed, or to reveal the identity of potential war criminals.[2]

These technologies have become extremely attractive for States as well, as they facilitate the scrutiny and monitoring of the public sphere at relatively small costs. The increased accuracy and availability of face recognition software has profoundly shaped State surveillance, by enhancing law enforcement authorities' ability to detect criminal activities, identify potential suspects and control borders. By extracting and processing the biometric data from a video or picture, these technologies allow the automatic identification of a person, based on their face. Aside from the potential benefits in terms of national security and public order often used to justify such use of FRT, a worrying trend is represented by the extensive use of biometric identification systems during peaceful protest to recognise, pre-emptively arrest, or even detain those participating. Notably, governments worldwide, whether democratic or authoritarian, have increasingly taken advantage of FRT-enabled tools to systematically detect, monitor and identify large crowds, dissident activities, protest movements and protesters alike, often in absence of a regulatory framework and oversight mechanisms.[3] Recent instances of FRT-enabled tools in concert with a variety of other surveillance measures have been used to tackle and monitor peaceful protests in India, Hong Kong, Chile, Russia, the United States, the United Kingdom, and others, often in name of public order and security.[4]

In the public debate, FRT expansion has inevitably sparked opposed views, ranging from enthusiasm for the opportunities that this technology offers, to concerns about the potential for an increased authoritarian control. Indeed, due to their social, political and legal importance, FRT have been in recent years under close scrutiny, especially due to their inherent implications for the protection of human rights and fundamental freedoms, including the right to privacy and freedoms of expression and assembly. Whilst the risks linked to police use of biometric identification during peaceful protest have been stressed by the civil society and academia, who have firmly warned about the challenges of enhanced surveillance practices facilitated by FRT for the protection of human rights and our democratic societies as a whole, and advocated for a total ban, these very concerns have seemingly been set aside and somewhat overlooked in the discussions about its

[2] For an analysis on the uses of FRT in various sectors, see N Selwyn et al., "Facial Recognition Technology: Key Issues and Emerging Concerns" in R Matulionyte and M Zalnieriute (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge, Cambridge University Press 2024) pp 14–17; J Espindola, "Facial Recognition in War Contexts: Mass Surveillance and Mass Atrocity" (2023) 37 (2) Ethics & International Affairs 177.

[3] M Zalnierute, "Power and Protest: Facial Recognition and Public Space Surveillance" in R Matulionyt and M Zalnieriute (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge, Cambridge University Press 2024) pp 96–8.

[4] See, for example, M Borak, "London Police Deploy Facial Recognition During Palestine and Israel Protests" (*BiometricUpdate.com*, 15 January 2024) available at <www.biometricupdate.com/202401/london-police-deploy-facial-recognition-during-palestine-and-israel-protests>; D Loucaides, "The Changing Face of Protest" (*Rest of World*, 27 March 2024) available at <https://restofworld.org/2024/facial-recognition-government-protest-surveillance/>; B Gonzalez, "Are Indian Police Using Facial Recognition to Identify Protesting Farmers?" (*BiometricUpdate.com*, 4 March 2024) available at <www.biometricupdate.com/202403/are-indian-police-using-facial-recognition-to-identify-protesting-farmers>; P Mozur, "In Hong Kong Protests, Faces Become Weapons" (*New York Times*, 26 June 2019) available at <www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html>; A Ulmer, Z Siddiqui, "India's Use of Facial Recognition Tech During Protests Causes Stir" (*Reuters*, 17 February 2020) available at <www.reuters.com/article/world/indias-use-of-facial-recognition-tech-during-protests-causes-stir-idUSKBN20B0ZP/> (last accessed 25 September 2024).

regulation.[5] Recent regulatory attempts appear to have focused on limiting their use and establishing safeguards, rather than questioning the compatibility of these technologies with human rights and democratic values *per se*, especially in the – unfortunately, not too rare – event FRT are deployed as a tool to suppress dissent. A recent notable example of this trend is embodied by the Artificial Intelligence Act (AI Act) adopted within the European Union (EU),[6] the first comprehensive instrument attempting to regulate the use of AI, including biometric identification systems. As is well known, the final adopted version of the AI Act does not include an outright ban on the use of FRT by law enforcement in publicly available spaces.

In the broader discussion on the compatibility of FRT with international human rights law (IHLR), significant relevance has been attributed to the position of the European Court of Human Rights (ECtHR), which was called upon deciding whether the use of FRT in the context of peaceful protest was compatible with the European Convention on Human Rights (ECHR). On 4 July 2023, in *Glukhin v Russia*, the Court indeed found that the use of highly intrusive facial recognition technology to identify, locate and arrest a peaceful protester had breached his right to a private life and freedom of expression.[7] Although the judgment was soon welcomed as "groundbreaking"[8] – it was the first time that an international court had ruled on the compatibility with human rights of the processing of biometric data collected with the aid of FRT[9] – the decision has not been exempt from criticism, especially regarding its limited ambition.

In lack of comprehensive available information about the modalities and extent of their use by law enforcement and resulting fundamental rights implications,[10] together with general poor knowledge about how this technology works,[11] further study on the use of biometric identification systems, especially in the context of peaceful protest, is deemed necessary. This contribution seeks to discuss the IHRL standards applicable to the use of FRT for national security purposes during peaceful demonstrations, especially considering and discussing the recent developments provided by the ECtHR's case-law in *Glukhin v Russia*. To this end, section II describes the risks and concerns of FRT use by law enforcement from a human rights perspective. Section III examines the international human rights law standards applicable to FRT when deployed in the context of peaceful protest, namely with respect to the potential infringements upon freedom of expression, freedom of assembly and the right to a private life. Section IV assesses the ECtHR's

[5] D Murray, "Facial Recognition and the End of Human Rights as We Know Them?" (2024) 42 (2) Netherlands Quarterly of Human Rights 145, 146.

[6] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) OJ L, 2024/1689 (12 July 2024).

[7] *Glukhin v Russia* App no 11519/20 (ECtHR, 4 July 2023); Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR).

[8] Art 19, "European Court of Human Rights: Groundbreaking Ruling on Facial Recognition" (*Art 19*, 4 July 2023) available at <www.article19.org/resources/european-court-of-human-rights-groundbreaking-ruling-on-facial-recognition/> (last accessed 31 July 2024).

[9] M Zalnieriute, "Glukhin v. Russia. App. No. 11519/20. Judgment" (2023) 117 American Journal of International Law 695, 697. In *Gaughran v UK* App no 45245/15 (ECtHR, 13 June 2020), paras 37, 67–70, the ECtHR had found that the UK police's ability to apply facial recognition and facial mapping techniques to the applicant's custody photograph, which was to be taken and retained on a local database indefinitely, amounted to a violation of his right to a private life under Art. 8(1) of the ECHR.

[10] M O'Flaherty, "Facial Recognition Technology and Fundamental Rights" (2020) 6 (2) European Data Protection Law Review 170, 170–1.

[11] Commission Nationale de l'Informatique et des Libertés (CNIL), "Reconnaissance faciale: pour un débat à la hauteur des enjeux" (*CNIL*, 15 November 2019) available at <www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux>.

approach in *Glukhin v Russia* in light of the recent debate around FRT and the protection of human rights and fundamental freedoms. Section V concludes.

II. FRT: risks and concerns from a human rights perspective

FRT is a biometric software application that detects and automatically recognises individuals based on their facial features. As a biometric system,[12] face recognition employs algorithms and machine learning techniques to extract and process a digital representation of distinct facial features from a digital image, either a photograph or a video, referred to as a "sample." This digital representation is used to create a biometric template that is unique for a specific person and can be stored in a database. At a later stage, in a proper recognition phase, such template can be compared to other templates within a given database or watchlist to verify potential matches and possibly determine the identity of a person.[13]

The term FRT usually refers to multiple and distinct technologies relying on different algorithms and data, performing different tasks and involving different levels of potential risks.[14] Authentication or *one-to-one* verification is a commonly used tool that allows to compare two templates to determine whether a person is who they claim to be. In this case, the biometric template of an individual interacting with the system, eg, standing in front of a camera equipped with FRT, is compared with a pre-existing template that was stored beforehand, for example in a passport or identity card, to verify whether they belong to the same person and confirm their identity. This functionality finds extensive applications, for example, in access control at airports' security gates, to unlock electronic devices such as smartphones, to verify school or work attendance or, in general, to access specific services, information systems or buildings.

Conversely, identification or *one-to-many* comparison refers to the process of determining a person's identity – whose image may be taken from social media, photos or videos taken from a smartphone, police officers' body-worn cameras, or footage from closed-circuit television (CCTV) cameras – by comparing their facial template against a database of many (perhaps thousands or millions)[15] others to deduce with some degree of probability the identity of that person. For example, police officers might use it to compare the image of an individual captured by a security camera against a set of known terrorists or criminals to find possible matches.[16] A more complex process involves *many-to-many* facial recognition systems, which is not necessarily aimed at identifying a specific person,

[12] On a definition of biometric technologies, see, among others, Art 29 Working Party, *supra*, note 1, pp 3–4; European Data Protection Board (EDPB), "Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement" (26 April 2023) p 9, available at <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en> (last accessed 26 July 2024); CNIL, *supra*, note 11, pp 3 et sqq.

[13] For a definition of FRT, see I Berle, *Facial Recognition Technology* (Cham, Springer 2020) pp 1–3, 9 et sqq; EDPB Guidelines 05/2022, *supra*, note 12, p 9 et sqq; B Driessen and M Dürmuth, "Achieving Anonymity against Major Face Recognition Algorithms" in B De Decker et al. (eds), *Communications and Multimedia Security* (Heidelberg, Springer Berlin 2013) p 20.

[14] This is why some experts prefer the term "facial recognition technologies," in place of "facial recognition technology." P Dauvergne, *Identified, Tracked, and Profiled* (Cheltenham, Edward Elgar Publishing Ltd 2022) p 4.

[15] The main reference materials used by enforcement authorities are passports or social cards, or national custody images. For example, the UK National Police database contains circa 19 million images. See D Murray, "Police Use of Retrospective Facial Recognition" (2024) 87 (4) Modern Law Review 833, 838, fn. 30; OVD-Info, "How the Russian State Uses Cameras Against Protesters" (OVD-Info, 17 January 2022) available at <https://en.ovdinfo.org/how-authorities-use-cameras-and-facial-recognition-against-protesters#1>.

[16] Identification resulting from the comparison of two biometric templates based on the likelihood that two images belong to the same person, is often referred to as "automated facial recognition" (AFR). For a detailed classification and different functions and FRT applications, see eg, EDPB, "Guidelines 05/2022," *supra*, note 12, pp 8–13.

for example for the purposes of a criminal investigation, but entails the scanning of large crowds to simultaneously verify or identify individuals against a watchlist or database of security risks. This functionality often includes the use of live or quasi live material and is referred to as "real-time FRT" (as opposed to "ex post" or "post-remote" FRT), which might be used by public authorities to monitor public events or mass demonstrations for security or public order purposes.[17]

Whilst verification/authentication is not likely to have significant human rights implications, as it does not normally require biometric data to be stored in a database (yet, they may be stored in passports or identity cards) and usually involves the collaboration of the person whose identity shall be verified,[18] the situation changes when it comes to the possibility that State authorities are able to scan large crowds for the purposes of monitoring and tracking individuals or groups to either identify them. This FRT use has sparked concern among civil liberties groups and privacy advocates, who have warned against governments' augmented surveillance capabilities to the detriment of protest movements worldwide, arguing that these technologies are being deployed to suppress political dissent and undermine democratic participation, all in name of public order and security.[19]

Recent research on empirical data concerning AI and big-data surveillance use in 179 countries has found that, between 2012 and 2022, State authorities were employing public facial recognition systems for surveillance purposes in at least seventy-eight of them.[20] Although not all of these systems involve database matching but also collect aggregated demographic trends or conduct sentiment analysis through crowd scanning, said data show that their adoption is expanding at a fast pace and that their geographical distribution is heterogenous. The phenomenon is not limited to authoritarian systems, as one might believe, but liberal democracies are likewise investing and relying upon increasingly sophisticated automated monitoring capabilities, including "predictive policing, safe cities, facial recognition systems, social media surveillance, and automated border control."[21]

With these data in mind, the risks for human rights and fundamental freedoms associated with mass surveillance, especially when facilitated by new technologies, including FRT, become evident and require close consideration. In a 2020 report focusing on the impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests, the UN High Commissioner for Human Rights warned about the "problematic" practice of routinely recording of assembly participants in combination with FRT deployment, and the resulting human rights implications, including the right to peaceful assembly.[22]

[17] O'Flaherty, *supra*, note 10, p 172.

[18] FRA, *Facial Recognition Technology*, *supra*, note 1, p 7.

[19] Zalnierute, "Power and Protest," *supra*, note 3, p 99.

[20] S Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance* (Oxford University Press 2021) p 225 et sqq.; S Feldstein "AI & Big Data Global Surveillance Index (2022 updated)" (*Mendeley Data V4*, 2022) available at <https://data.mendeley.com/datasets/gjhf5y4xjp/4> (last accessed 28 August 2024).

[21] Predicting policing is a technique that takes advantage of data and algorithms to make predictions about future criminal activity. Through massive data aggregation of past criminal activity and arrests, these systems claim to predict where future crimes will be committed and by whom. In countries where this technique has accelerated, such as the US, serious concerns about the risks of bias and prejudice have been raised. Ibid, p 227.

[22] Human Rights Council (HRC), Report of the United Nations High Commissioner for Human Rights "Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests" (24 June 2020) A/HRC/44/24, paras 30 et sqq. See also HRC, Joint report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on extrajudicial, summary or arbitrary executions on the proper management of assemblies (4 February 2016) A/HRC/31/66, para 76; HRC, Concluding observations on the initial report of Macao, China, adopted by the Committee at its 107th session (29 April 2013) CCPR/C/CHN-MAC/CO/1, para 16.

These concerns become ever more pressing considering the inherent characteristics of facial recognition systems, which, like any other technology, are not exempt from challenges and weaknesses when it comes to their efficiency, reliability and accuracy.[23] In recent years, FRT have benefited from advancements in machine learning and deep learning techniques, facilitated by enhanced computational processing power and increased data storing capacity, which have enabled the development and training of more sophisticated models.[24] Moreover, cheaper and improved camera hardware, the subsequent spread of high-definition cameras in private devices and public places, together with the unprecedented availability of publicly accessible videos and photos on social media platforms, have created a fertile ground for a progressive FRT expansion.[25]

Despite the increase in accuracy and precision of these systems, which led public authorities worldwide to start testing, planning the use of or using FRT, they are still prone to errors.[26] Assessing FRT accuracy, or the likelihood of false positives and negatives produced by the software is challenging, as error rates vary with deployment conditions, the tasks, and the goals. While the software performs better in controlled settings (eg, mugshots), accuracy greatly diminishes in uncontrolled environments, like public places.[27] Even under favourable conditions, higher accuracy does not automatically eliminate risks. The EU Fundamental Rights Agency notes that in busy places like airports, even a low error rate (eg, 0.01%) can result in hundreds of people being wrongly flagged.[28] Moreover, it shall be recalled that algorithms, including face recognition, are probabilistic technologies that do not produce definitive results, but rely on *probabilities* that two face images compared belong to the same person. As a consequence, said probability, or "confidence score," varies with biometric samples' quality, which can be negatively impacted by "[b]lurriness of input images, low resolution of camera, motion, and light," as well as with the quality of training data used.[29]

The issue of *which* training data and dataset are used to "feed" and build the facial recognition algorithms is closely related to a second key issue of concern, that is the intrinsic bias and the risk of discrimination.[30] It has been noted, indeed, that facial recognition systems perform poorly in relation to younger individuals, people of colour,

[23] EDPB, Guidelines 05/2022, *supra*, note 12, pp 12–13.

[24] N Menéndez González, "The Impact of Facial Recognition Technology Empowered by Artificial Intelligence on the Right to Privacy" in D M Bielicki (ed), *Regulating Artificial Intelligence in Industry* (Abingdon, Oxon, Routledge 2022), pp 22–3; D Heaven, "Expression of Doubt: Why Faces Don't Always Tell the Truth About Feelings" (2020) 578 Nature 502–4.

[25] According to Selwyn et al., in addition to the technological advances in AI and camera hardware, an expansion in FRT use and normalisation was fuelled by "a combination of cultural factors, alongside exceptional societal events such as the COVID-19 pandemic, and the wider political economic will to propose and embrace techno-solutions for redressing social issues and to increasingly automate access to various spaces and services". Selwyn et al, *supra*, note 2, p 13.

[26] A/HRC/44/24, *supra*, note 22, para. 31; Berle, *supra*, note 13, p 15 et sqq.

[27] Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), "Guidelines on Facial Recognition" (*Council of Europe*, 2021) available at <https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751>, fn. 10.

[28] FRA, *Facial Recognition Technology*, *supra*, note 1, pp 9–10.

[29] Ibid; EDPB, Guidelines 05/2022, *supra*, note 12, p 13. Image quality has a role in determining the accuracy of FRT, whereas poor image quality may be related to technical factors (eg, poor photography, illumination or posture) and properties related to the demographics, including for instance the age of individuals. P Grother, M Ngan and K Hanaoka, "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects" (National Institute of Standards and Technology, 2019) pp 15–17, available at <https://doi.org/10.6028/NIST.IR.8280>.

[30] For a IHRL perspective of the potential harms caused by algorithmic decision-making, see L McGregor, D Murray and V Ng, "International Human Rights Law as a Framework for Algorithmic Accountability" (2019) 68 International and Comparative Law Quarterly 309.

and women, who are at higher risk of being misidentified.[31] As a result, intersectional analyses on specific facial recognition algorithms have demonstrated how identification of females with darker skin tones recorded higher error rates, also due to the unbalanced composition of datasets.[32] Misidentification can have serious impacts on the civil liberties of subjects, who can be wrongfully flagged, or accused of criminal activity and arrested. Besides, even if the technology may be trained to reduce or minimise bias, for instance by ensuring diversity in databases (eg, age, gender, "race"),[33] biometric identification may be used to profile certain individuals based on their gender, ethnicity/nationality or disability, with the risk of perpetuating and amplifying discrimination against individuals or groups who are already marginalised.[34]

III. FRT and the protection of human rights in the context of peaceful protest: an introductory note on international standards

Digital technologies have played an undeniable positive and transformative role for the exercise of the right of peaceful assembly and related rights. Information and communications technologies (ICTs) have indeed been instrumental in enabling and facilitating the organisation and coordination of protests, in forming networks and raising awareness to generate support for the cause, but also in increasing transparency and accountability for possible abuses and violations.[35] Meanwhile, these same technologies have been used by States, which have been responding to peaceful protests and movements with surveillance activities, forms of censorship, and violent repression. In this context, FRT have been indeed deployed in concert with a variety of tools and measures, which range from interferences with internet and communications, such as internet shutdowns, to preventing or disrupting access to websites or platforms used to plan, organise or mobilise protesters, and filtering protests-related content, as well as other forms of indiscriminate untargeted surveillance. These include hacking of ICTs tools used by organisers and protesters alike, including infiltrating their communication platforms and social media, as well as intercepting and monitoring their mobile phone traffic and track their position.[36] These forms of indiscriminate untargeted surveillance allow real-time identification, targeted surveillance and tracking of participants to protests, with significant implications for the right to privacy, freedom of expression and peaceful assembly.[37]

[31] SH Abdurrahim, S Abdul Samad and A Baseri Huddin, "Review on the Effects of Age, Gender, and Race Demographics on Automatic Face Recognition" (2018) 34 The Visual Computer 1617; BF Klare et al, "Face Recognition Performance: Role of Demographic Information" (2012) 7 (6) EEE Transactions on Information Forensics and Security 1789. On the general topic of AI and gender-based discrimination, see, eg, F Lütz "Artificial Intelligence and Gender-Based Discrimination" in Matulionyte and Zalnieriute, *supra*, note 3.

[32] J Buolamwini and T Gebrut, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" (2018) 81 Proceedings of Machine Learning Research 1.

[33] Abdurrahim et al, *supra*, note 31.

[34] A/HRC/44/24, *supra*, note 22, para. 32. For example, it has been underlined how in the US, in the context of law enforcement's use of FRT, databases are composed of images of individuals arrested, sometimes wrongfully, and this causes minorities to be overrepresented. See H Ruhrmann, "Facing the Future: Human Rights and Facial Recognition Technology Use in Law Enforcement" (*Citris Policy Lab*, May 2019), p 63; AI Act, *supra*, note 6 (recital 32 notes that "[t]echnical inaccuracies of AI systems intended for the remote biometric identification of natural persons can lead to biased results and entail discriminatory effects. Such possible biased results and discriminatory effects are particularly relevant with regard to age, ethnicity, race, sex or disabilities").

[35] A/HRC/44/24, *supra*, note 22, paras 7–15.

[36] Ibid, paras 16 et sqq; I Siatitsa, "Freedom of Assembly Under Attack: General and Indiscriminate Surveillance and Interference with Internet Communications" (2020) 102 International Review of the Red Cross 181, 183.

[37] A/HRC/44/24, *supra*, note 22, paras 24–34.

In recent years, along with various institutional organs within international organisations, including the United Nations (UN), Council of Europe (CoE) and the European Union (EU),[38] several human rights activists, civil society groups and non-governmental organisations have been vocal about the dangers of highly intrusive biometric surveillance in the context of peaceful protest calling for stricter regulatory frameworks, transparency and even an outright ban on their use.[39] Unlike other physical features (eg, fingerprints or iris), indeed, facial features are unique and immutable bodily characteristics that can be seen and registered fairly easily, especially in public places, with enhanced risks for interference with personal autonomy and the shrinking of the civic space.[40] These concerns, together with the risk of errors, doubts about accuracy and potential discrimination inherent to automated facial recognition, as well as the weak position of data subjects, whose biometric data are often acquired and processed without them knowing, have given way to a number of regulation efforts worldwide: nationally, some attempts to limit FRT use by the police are being recorded[41]; internationally, various regulatory and legislative initiatives within international and regional organisations are gaining traction, including within the UN, the CoE, and the EU. In the following section the right to protest will be considered under IHRL in order to discuss FRT's impact on related rights and fundamental freedoms, i.e. the freedoms of expression and assembly and the right to a private life.

1. The protection of the right to protest under international human rights law

Protest is a form of action that is performed individually or collectively with the purpose of expressing ideas, views, or dissenting or opposing against specific policies or

[38] See, for instance, HRC, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression "Surveillance and Human Rights" (28 May 2019) A/HRC/41/35, paras 48–49 (calling for a moratorium on the use and export of targeted surveillance technologies until sufficient measures to prevent abuse are in place); A/HRC/44/24, *supra*, note 22, para. 40; HRC Resolution, "The Promotion and Protection of Human Rights in the Context of Peaceful Protests" (14 July 2022) A/HRC/RES/50/21, para 29 (urging states "to refrain from the arbitrary or unlawful use of biometric identification technologies, including facial recognition, to identify those peacefully participating in an assembly"). At a European level, see CoE, Parliamentary Assembly, "Les opérations de surveillance massive" (14 October 2015) Doc 13911; European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), "Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)" (*EDPB-EDPS*, 18 June 2021) available at <www.edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf> (calling for a general ban on *any* use of AI-based automated recognition of human features in publicly available place, including faces).

[39] See, for instance, "Ban Facial Recognition" available at <www.banfacialrecognition.com/>; European Digital Rights (EDRi) Campaign "Reclaim Your Face" available at <https://reclaimyourface.eu/>; Amnesty International, "Ban Dangerous Facial Recognition Technology That Amplifies Racist Policing" (*Amnesty International*, 26 January 2021) available at <www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/>; Privacy International, "Submission on Article 21 of the International Covenant on Civil and Political Rights" (*Privacy International*, 14 February 2019) available at <https://privacyinternational.org/advocacy/2764/privacy-internationals-submission-un-human-rights-committee-article-21-iccpr>.

[40] EDRi, "Ban Biometric Mass Surveillance: A Set of Fundamental Rights Demands for the European Commission and EU Member States" (*EDRi*, 2020) available at <https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf> (last accessed 29 July 2024).

[41] In the US, some States put a moratorium on FRT in police body cameras, while a number of municipalities are either enacting or considering bans on FRT use by governments and city agencies, including police departments. Max Read, "Why We Should Ban Facial Recognition Technology" (*Intelligencer*, 30 January 2020) available at <https://nymag.com/intelligencer/2020/01/why-we-should-ban-facial-recognition-technology.html>; T Ryan-Mosley, "The Movement to Limit Face Recognition Tech Might Finally Get a Win" (*MIT Technology Review*, 20 July 2023) available at <www.technologyreview.com/2023/07/20/1076539/face-recognition-massachusetts-test-police> (last accessed 30 September 2024).

institutions. As such, it may take many forms, including non-verbal demonstrations, civil disobedience, boycotts or other visual forms of communication. Regardless of how dissent or views are expressed, protests play an essential role both in the consolidation and the very existence of democratic societies, enabling individuals to express their ideas and aspirations in the public domain and to participate in shaping the societies they live in, individually or in solidarity with others. Together with the exercise of related rights, assemblies form the "very foundation of a system of participatory governance based on democracy, human rights, the rule of law and pluralism".[42]

Recent years have witnessed a proliferation of social protest movements in many countries, driven by a number of complex and diverse motives, which find common underlying root causes in structural and institutional discrimination, worsening economic conditions, corruption, inequality, and abuse or denial of human rights.[43] Suffice it to recall, for example, the rise of political and social movements advocating for actions against climate change, such as FridaysForFuture or Extinction Rebellion, or highlighting racism, discrimination and inequality, such Black Lives Matter; and the pro-democracy social upheavals in Hong Kong and Chile between 2019 and 2020.

The significance of protest does not start and end with the opportunity for individuals to mobilise to advance their ideas and goals and possibly influence States' policies,[44] but is instrumental for the promotion and full enjoyment of a broad range of other civil, political, economic, social, and cultural rights. In particular, protest is of fundamental importance for those individuals or groups of individuals who are marginalised or do not conform with the established political and economic system, as it allows them to amplify their voices in the public domain[45] and possibly overcome inequalities, discrimination and exclusion that prevent them from accessing decision making processes.[46]

Despite the prominent role of political and social protest in our societies, international and regional human rights instruments do not *expressly* recognise a "right to protest" per se. However, the right to peaceful protest is generally protected and enabled by a number of associated and intertwined rights, including the freedom of expression, the right of peaceful assembly and the freedom of association.[47] The close inter-relation and interaction between these rights in guaranteeing the right to protest has been emphasised by international human rights courts and monitoring bodies, which have acknowledged how they, as a whole, concur to "make the democratic process possible."[48]

[42] Human Rights Committee (HRCttee), General Comment No. 37 (2020) on the right of peaceful assembly (17 September 2020) CCPR/C/GC/37, para 1. More in detail on the right to protest, see Inter-American Commission on Human Rights (IACHR), Office of the Special Rapporteur for Freedom of Expression, *Protest and Human Rights* (Washington, Organization of American States 2019); Article 19, "The Right to Protest: Principles on the Protection of Human Rights in Protests" (*Background Paper*, December 2016) available at <www.article19.org/resources/the-right-to-protest-principles-on-the-protection-of-human-rights-in-protests/>.

[43] A/HRC/44/24, *supra*, note 22, para 4; IACHR, Annual Report 2005, Volume III, Report of the Office of the Special Rapporteur for Freedom of Expression (27 February 2006) OEA/Ser.L/V/II.124 Doc. 7, p 121.

[44] HRC, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai (21 May 2012) A/HRC/20/27, para 24.

[45] CCPR/C/GC/37, *supra*, note 42, para 2; A/HRC/31/66, *supra*, note 22, para 6.

[46] UN General Assembly (UNGA), Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Clément Nyaletsossi Voule (27 July 2023) A/78/246, para 3.

[47] See, HRC, "Report of the United Nations High Commissioner for Human Rights" (2 December 2013) A/HRC/25/32; European Commission for Democracy Through Law (Venice Commission) and OSCE Office for Democratic Institutions and Human Rights (OSCE/ODHIR), "Joint guidelines on freedom of peaceful assembly (3rd edition)" (15 July 2020) CDL-AD(2019)017rev, para 10; Article 19, "The Right to Protest," *supra*, note 42; IACHR, *Protest and Human Rights*, *supra*, note 42. On the right to protest in general, see also "Protest" in S Marks, A Clapham, *International Human Rights Lexicon* (Oxford University Press 2005) pp 271–86.

[48] *López Lone et al v Honduras* (Preliminary objections, merits, reparations and costs) IACHR Series C No 302 (5 October 2015) para 160.

The freedom to hold opinions and express them is an essential precondition for a person's full development and forms, together with the freedom of opinion, the cornerstone of a free and democratic society.[49] As such, freedom of expression is enshrined in several human rights instruments, whether universal, regional or specialised.[50] Article 19 of the ICCPR and the equivalent guarantees provide that this freedom not only covers the right to hold opinions without interference by public authorities, but also to seek and receive information and to disseminate them in whatever form one deems adequate, including spoken, written and sign language, non-verbal expression and objects of art, and through any medium of choice.[51] The protection from undue restriction extends to more traditional means of transmission and reception of ideas and information, including books, newspapers, television, and radio[52] and to internet-based forms alike.[53]

As regards the content, the ECtHR and IACtHR have both pointed out that the freedom of expression is applicable to information and ideas that are normally perceived as "inoffensive" or "as a matter of indifference," but also extends to satire[54] and expression that offends, shocks or disturbs.[55] Expression may as such cover potentially unlimited content, including political and religious discourse and requires tolerance by the authorities. However, certain limitations to the substantive scope of the provision clauses may be applied, as in case of offensive statements solely intended to insult, or hate speech.[56]

Freedom of expression constitutes the foundation for the enjoyment of other related rights, including freedom of assembly and association.[57] As such, expression in the form of exchange of ideas and social claims is a necessary requirement for the right of citizens to assemble and to demonstrate, and for the free flow of information and opinions.[58] The ECtHR has, in many occasions, reiterated the close interaction between the two rights, stressing that, despite their autonomous and specific scope of application, "[t]he protection of opinions and the freedom to express them is one of the objectives of the freedoms of assembly and association as enshrined in Article 11".[59] In the same vein, the African

[49] *Stoll v Switzerland* (GC) App no 69698/01 (ECtHR, 10 December 2007) para. 101; *Steel and Morris v UK* App no 68416/01 (ECtHR, 15 May 2005) para. 87; HRCttee, General comment No 34 (12 September 2011) CCPR/C/GC/34, para 2.

[50] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR) Art.19; International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) Art. 19; International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976) 993 UNTS 3 (ICESCR) Art. 15(3), Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3 (CRC), Art. 13; Convention on the Rights of Persons with Disabilities (adopted 13 December 2006, entered into force 3 May 2008) 2515 UNTS 3 (CRPD) Art 21; African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) (1982) 21 ILM 58 (African Charter) Art 9; American Convention on Human Rights (adopted 22 November 1969, entered into force 18 July 1978) 1144 UNTS 123 ("Pact of San José"), Art 13; ECHR Art 10.

[51] CCPR/C/GC/34, *supra*, note 49, para 12; *Müller and Others v Switzerland* App no 10737/84 (ECtHR, 24 May 1988).

[52] *Zundel v Canada* Communication no 1341/2005 (4 April 2007); *Société de Conception de Presse et d'Edition et Ponson v France* App no 26935/05 (ECtHR, 5 March 2009).

[53] In particular, the internet has been instrumental in providing for enhanced access to ideas and information, as well as unprecedented possibilities for expressive activities. *Cengiz and Others v Turkey* App nos 48226/10 and 14027/11 (ECtHR, 1 March 2016) paras 49 and 52.

[54] *Ziembiński v Poland* App no 1799/07 (ECtHR, 5 October 2016) paras 44 et sqq.

[55] *Handyside v UK* App no 5493/72 (ECtHR, 7 December 1976) para 49.

[56] *Gaspari v Armenia (no. 2)* App no 67783/13 (ECtHR, 11 October 2023) para 27); W Kälin and J Künzli, *The Law of International Human Rights Protection* (2nd edition, Oxford, Oxford University Press 2019) p 493.

[57] CCPR/C/GC/37, *supra*, note 42, para 4.

[58] IACHR, Report of the Office of the Special Rapporteur, *supra*, note 43, para 5.

[59] *Women On Waves and Others v Portugal* App no 31276/05 (ECtHR, 3 February 2009) para 28 (noting that "la question de la liberté d'expression est en l'espèce difficilement séparable de celle de la liberté de réunion"); *Vogt v Germany* (GC) App no 17851/91 (ECtHR, 26 September 1995) para 64 (noting that "[t]he protection of personal opinions ... is one of the objectives of the freedoms of assembly and association").

Commission found that the freedom of expression can be implicitly infringed when a violation of the right of assembly and association occurs.[60] In its inter-relation with the freedom of expression, the freedom of assembly "secure[s] a forum for public debate and the open expression of protest."[61]

The right to freedom of peaceful assembly and association is recognised by Article 20 of UDHR and is enshrined in various human rights treaties.[62] Article 21 of the ICCPR and equivalent regional guarantees protect the right of individuals to freely and non-violently gather in public or private places for a common expressive purpose. Such freedom protects those who organise and those who take part to the assembly and can be exercised by everyone: citizens and non-citizens alike, foreign nationals, migrants regardless of their legal status, asylum seekers, refugees and stateless persons.[63]

The modalities, time, duration and place of the assembly can be freely chosen,[64] along with the subject matter addressed. As a matter of fact, the protection not only applies to assemblies pursuing relatively uncontroversial goals, but extends to demonstrations that may even annoy or offend persons opposed to the ideas or claims that they are seeking to promote. Unjustifiably interfering with assemblies, no matter how disturbing, offensive, shocking or unacceptable they may appear to the authorities, would still "do a disservice to democracy and often even endanger it."[65] Notwithstanding the freedom to decide how the demonstrations shall be performed, and which aims they pursue, the protection covers assemblies that are *peaceful* in nature. This implies that a protest in which participants engage in violent behaviour, causing death or injury or damage to property, would be excluded from protection. Moreover, the guarantees provided shall not apply to assemblies where participants have violent intentions, incite others to violence, or reject core principles of a democratic society.[66] Mere disturbances, acts disrupting daily activities or civil disobedience, including blocking multiple lanes of a highway to slow down traffic, shall however not be considered violent, even if they are unlawful in domestic law.[67] Nor should the sporadic violent behaviour of a handful of participants be attributed to the organisers or the other peaceful protesters, who hence do not cease to enjoy the protection.[68]

As can be seen, the paramount importance of freedom of expression and right to assembly in ensuring democratic societies based on human rights and pluralism does not automatically entail that these are absolute or overriding.[69] On the contrary, IHRL instruments generally allow States to limit, under certain circumstances and conditions, the enjoyment of certain rights or freedoms.

In principle, States have a negative obligation not to unduly intervene in the exercise of the right of freedom of assembly. The prohibition of "unwarranted interference"

[60] *International PEN, Constitutional Rights Project, Civil Liberties Organisation and Interights (on behalf of Ken Saro-Wiwa Jnr.) v Nigeria* (31 October 1998) 137/94-139/94-154/96-161/97.

[61] *Éva Molnár v Hungary* App no 10346/05 (ECtHR, 7 January 2009) para 42.

[62] ICCPR Arts 21 and 22; CRC Art15; International Convention on the Elimination of All Forms of Racial Discrimination (adopted 21 December 1965, entered into force 4 January 1969) UNGA resolution 2106 (XX) (CERD) Art 5(d)(ix); ACHPR Arts 10 and 11; ECHR Art. 11; IACHR Arts 15 and 16. In addition, the freedom of association is protected in: CRPD Art 29; Convention on the Elimination of All Forms of Discrimination against Women New York (adopted 18 December 1979, entered into force 3 September 1981) 1249 UNTS 13 (CEDAW) Art 7.

[63] *Djavit An v Turkey* App no 20652/92 (ECtHR, 9 July 2003) para 56; CCPR/C/GC/37, *supra*, note 42, para 4.

[64] *Sáska v Hungary* App no 58050/08 (ECtHR, 27 February 2013) paras 21–3.

[65] *Kudrevičius and Others v Lithuania* (GC) App no 37553/05 (ECtHR, 15 October 2015) para 145.

[66] CCPR/C/GC/37 *supra*, note 42, paras 15–20; *Frumkin v Russia* App no 74568/12 (ECtHR, 6 June 2016) para 98.

[67] *Affaire Barraco v France* App no 31684/05 (ECtHR, 5 June 2009) para 47; Venice Commission, OSCE/ODHIR, *supra*, note 47, para 48.

[68] *Frumkin v Russia*, *supra*, note 65, para 99; *Annenkov and Others v Russia* App no 31475/10 (ECtHR, 25 July 2017) pp 122–9.

[69] Marks, Clapham, *supra*, note 47, p 273.

materialises in the duty to refrain from imposing measures aimed at in any way banning, restricting, blocking, dispersing or disrupting peaceful protests without sufficient justifications, and from punishing participants, absent legitimate causes.[70] Interferences may take the form of conditional authorisations, a total ban on protests, preventive arrests to ensure non-participation, dispersing assemblies by using force, and – after demonstrations – arresting, detaining or imposing charges against participants.[71]

Second, States do have a positive obligation to facilitate and safeguard peaceful assemblies. This obligation requires that States "promote an enabling environment for the exercise of the right of peaceful assembly without discrimination, and put in place a legal and institutional framework within which the right can be exercised effectively."[72] In this regard, States are bound to implement preventive safety measures to guarantee the safety of the protest, for instance providing first-aid services,[73] and to adopt adequate measures to protect participants against violent acts, including from possible counterdemonstrations. These shall be in principle allowed, as long as they do not "extend to inhibiting the exercise of the right to demonstrate."[74]

Notwithstanding the above, States do enjoy a certain leeway in restricting the exercise of these rights in order either to protect the rights and freedoms of other subjects, for instance minimising the disruption to traffic, or to safeguard certain public interests.[75] Restrictions to the freedom of assembly and expression are considered legitimate if they comply with certain conditions of a procedural and substantial nature. These shall be provided by law and be necessary either for respect of the rights of others (and their reputation, as regards expression), and the protection of national security, public safety or public order (*ordre public*), or of public health or morals.[76] Articles 10 and 11 ECHR impose similar conditions, by requiring that the restrictions to which freedom of expression and of assembly and association may be subjected to "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 rights and freedom of others," including their reputation, as regards expression.[77]

The ECtHR has clarified in many occasions that the expression "prescribed by law" not only demands that any limitation to the rights have some legal basis in the domestic system, but also makes reference to the *quality* of the law in question, which "should be accessible to the persons concerned and formulated with sufficient precision to enable them – if need be, with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the

[70] CCPR/C/GC/37 *supra*, note 42, para 23; Venice Commission, OSCE/ODHIR, *supra*, note 47, p 12.

[71] See, for example, *Berladir and Others v Russia* App no 34202/06 (ECtHR, 19 November 201) paras 47–51 (on conditional authorisation); *Schwabe and M.G. v Germany* App nos 8080/08 and 8577/08 (ECtHR, 1 March 2012) para 102 et sqq (on arresting individuals to prevent their participation to demonstration against the G8 summit); *Zakharov and Varzhabetyan v Russia* App nos 35880/14 and 75926/17 (ECtHR, 13 January 2021) paras 88–9 (on the use of force to disperse protests).

[72] CCPR/C/GC/37 supra, note 42, para 24.

[73] *Oya Ataman v Turkey* App no 74552/01 (ECtHR, 5 March 2007) para 39.

[74] *Plattform "Ärzte für das Leben" v Austria* App no 10126/82 (ECtHR, 21 June 1988) para 32–9.

[75] *Oya Ataman v Turkey*, *supra*, note 73, para 39. On restrictions and derogations within the ECHR framework, see M Pedrazzi, "La Convenzione europea sui diritti umani e il suo sistema di controllo" in L Pineschi (ed), *La Tutela Internazionale dei Diritti Umani* (Milano, Giuffrè Editore 2015) pp 286–8. Moreover, the right to protest may as well be qualified by the prohibition of abusive invocation as provided by Art 5(1) ICCPR, which states: "Nothing in the present Covenant may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms recognized herein or at their limitation to a greater extent than is provided for in the present Covenant." An equivalent provision is set forth in Art 17 ECHR.

[76] ICCPR Arts 19(3) and 21.

[77] ECHR Arts 10 and 11.

consequences which a given action may entail."[78] In *Navalnyy v Russia*, for example, the Grand Chamber noted that the Russian domestic legal framework regulating the notification system for public events was of such a broad nature that the foreseeability of its application could be questioned, and that it gave local authorities excessively wide discretion in interfering with the event – including the power to put an end to it – through administrative law-enforcement measures, such as arrest, transfer to a police station and pre-trial detention.[79]

The condition that a restriction shall be "necessary in a democratic society" implies that any limitation to the freedom of expression or interference with a peaceful protest must be "necessary and proportionate in the context of a society based on democracy, the rule of law, political pluralism and human rights, as opposed to being merely reasonable or expedient."[80] Any restriction must not be overbroad in nature, but the authorities shall ensure that limitations to a right are aimed at responding to a "pressing social need" and that they are proportionate to the end pursued.[81] This implies that the authorities shall conduct a value assessment weighing the impact of the measure on the effective exercise of the right against the resulting expected benefit to a specific legitimate ground for interference, for instance public order or prevention of crime.[82] In any case, they should always prefer the least intrusive measures or tools to achieve said aims.[83] Significantly, in the Human Rights Committee's opinion, in evaluating possible restrictions upon the right to assembly in order to pursue certain legitimate goals, "the State party [to the ICCPR] should be guided by the objective of facilitating the right rather than seeking unnecessary or disproportionate limitations to it."[84] Similarly, the ECtHR – whilst recognising that States do enjoy a certain, not unlimited, margin of appreciation in determining which restrictions on the rights and freedoms protected by the ECHR are "necessary in a democratic society"[85] – held that the authorities should demonstrate some degree of tolerance towards peaceful protests, regardless of their lawfulness, to ensure that the protection ensured by Article 11 is not "deprived of all substance."[86]

2. *FRT and peaceful protest: the freedoms of assembly and expression* . . .

After having briefly analysed the scope and content of the right to protest from the perspective of the freedom of assembly and expression, one may wonder how and to what extent the deployment of FRT in the context of peaceful protest may impact or influence the effective enjoyment of these rights. As a matter of fact, the deployment of surveillance activities by law enforcement and States' authorities is not at all a novel issue, especially when it comes to their possible infringement upon fundamental rights and freedoms. International and national jurisprudence and legal doctrine have extensively addressed

[78] *Maestri v Italy* App no 39748/98 (ECtHR, 17 February 2004) para 30.

[79] *Navalny v Russia* App nos 29580/12 and 4 others (ECtHR, 15 November 2018) paras 114–119. See also below, Section IV.

[80] CCPR/C/GC/37 *supra*, note 42, para 40. See also UNGA, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (6 September 2016) A/71/373, paras 18–19.

[81] CCPR/C/GC/34, *supra*, note 49, para 34.

[82] CCPR/C/GC/37 *supra*, note 42, para 40.

[83] Ibid; Venice Commission, OSCE/ODHIR, *supra*, note 47, para 29.

[84] *Marina Statkevich and Oleg Matskevich v Belarus* Communication no 2133/2012 (29 October 2015) para 9.4.

[85] See, for instance, *Coster v UK* (GC) App no 24876/94 (ECtHR, 18 January 2001) para 105 (holding that the authorities are in principle better equipped than the Court itself to evaluate the need of such restricting measures).

[86] *Frumkin v Russia*, *supra*, note 66, para 97.

the compatibility of surveillance measures, including "bulk" and covert surveillance measures that are key instruments to the fight against terrorism, with IHRL.[87]

While surveillance activities by public authorities may and do in fact raise several issues as regards the right to a private life, especially privacy and the protection of personal data, as will be further explored in the following section, the deployment of a variety of surveillance measures, including by FRT, by law enforcement agencies worldwide to track and monitor peaceful protests deeply impacts on the right to protest, and the intertwined freedoms of assembly and expression.[88]

Significantly, assembly surveillance facilitated by FRT, whose main functions and limits were discussed above, may directly or indirectly adversely impact the freedom of assembly and expression. In particular, employing FRT to acquire and process facial images in public places, whether roads, squares, or other uncontrolled environments in the context of peaceful protest, often in concert with other digital tools aimed at the overall monitoring of demonstrators, before, during and after assemblies,[89] carries significant risks for interference.[90] In principle, as discussed, an interference would be admissible if authorities can prove that it was necessary to serve public interests, for example public order or safety, or to protect other participants to the demonstration.[91] The nexus between the measure and the legitimate ground justifying any interference should not however be construed on an abstract aspiration that a certain measure might facilitate a certain aim that is pursued.[92] In the hypothesis of a restriction to the right of assembly that invokes, for example, the protection of "public safety," authorities must establish that the assembly in question "creates a real and significant risk to the safety of persons (to life or security of persons) or a similar risk."[93] In the event that participants' intentions turn violent, inciting others to violence or resorting to violence themselves, thus depriving the assembly of its peaceful character, targeted forms of surveillance may therefore be deemed legitimate. Clément Nyaletsossi Voule, former Special Rapporteur on the rights to freedom of peaceful assembly and of association, exploring the human rights impact of digital-enabled surveillance, especially bulk collection of communications metadata, suggested that "surveillance against individuals exercising their rights of peaceful assembly and association can only be conducted on a targeted basis, where there is a reasonable suspicion that they are engaging in or planning to engage in serious criminal offences, and under the very strictest rules, operating on principles of necessity and proportionality and providing for close judicial

[87] See, *ex multis*, *Big Brother v UK* (GC) App nos 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021); M Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age" (2015) 56 (1) Harvard International Law Journal 81; E Watt, "The Right to Privacy and the Future of Mass Surveillance" (2017) 21 (7) International Journal of Human Rights 773; S Zuboff, *The Age of Surveillance Capitalism* (New York, Public Affairs 2019); A Stiano, "Il Diritto alla privacy alla prova della sorveglianza di massa e dell'*intelligence sharing*: la prospettiva della Corte europea dei Diritti dell'Uomo" (2020) 2 Rivista di diritto internazionale 511.

[88] In literature, it has been noted that little attention has yet been devoted to the distinct implications of these activities on other human rights and fundamental freedoms, apart from privacy. Siatitsa, *supra*, note 36, pp 189–190; C Ashraf, "Artificial Intelligence and the Rights to Assembly and Association" (2020) 5 (2) Journal of Cyber Policy 163, 164 (noting how "[d]iscussion about AI's impact on human rights besides freedom of expression and privacy has been scarce).

[89] See, above, introduction to Section III.

[90] FRA, *Facial Recognition Technology*, *supra*, note 1, p 29.

[91] In *S. and Marper v UK* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008) para 101, the ECtHR, explicitly dealing with surveillance and finding that the retention of fingerprints, cellular samples and DNA profiles by the authorities in criminal proceedings amounted to an interference, held that "[a]n interference will be considered 'necessary in a democratic society' for a legitimate aim if it answers a 'pressing social need' and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are 'relevant and sufficient'."

[92] Siatitsa, *supra*, note 36, p 191.

[93] CCPR/C/GC/37 *supra*, note 42, paras 40 et sqq.

supervision" and hence recommended that "indiscriminate and untargeted surveillance" both online and offline should be outlawed.[94]

In the context of FRT, the requirement of "necessary in a democratic society" shall hence be evaluated assessing the potential benefit for human rights – for example the prevention of crimes or the protection of rights – deriving from an interference with the right to a private life or in light of the chilling effect caused by the restriction invoked on other fundamental freedoms. However, as noted by Murray, "it is not simply a case of 'does the benefit outweigh the harm?'" question, since any interference should meet the constraints of a democratic society.[95] In the words of the ECtHR in *Gorzelik and others v Poland*, "the only necessity capable of justifying an interference with any of the rights enshrined in … Articles [8, 9, 10 and 11 ECHR] is one that may claim to spring from 'democratic society'."[96]

The ritual recording of protests, especially when FRT is deployed, has been associated with the severe risk of causing a chilling effect on the freedoms of assembly and expression, with negative consequences on the individuals' right to the unfettered development of their personality and free political participation in the society.[97] Simply knowing that they are being recorded in public places and that their actions are scrutinised by law enforcement officers may induce people to alter their behaviour and discourage them from participating in demonstrations or freely expressing their views for fear of being identified and facing negative consequences.[98] In light of the crucial importance of the right to protest and the related freedoms, as discussed, such a chilling effect may negatively impact on the society as a whole, whose democratic and pluralist nature could be threatened.

When it comes to FRT deployment in the context of peaceful protest, it is dubious that mass and indiscriminate real-time surveillance and identification of individuals through automated systems simultaneously targeting hundreds or even thousands of unaware individuals simply exercising their right to protest and expressing their views – however controversial or challenging – could ever prove the link needed for invoking one of the legitimate grounds and be considered a justified interference.[99] Even in the event that a protest loses its peaceful character, hence in principle justifying forms of targeted surveillance measures against specific violent individuals, the other (peaceful) participants would not lose their protection under IHRL. In the writer's opinion, the deployment of real-time FRT could hardly be considered proportionate or necessary in terms of the human rights guarantees afforded by the individuals involved, who may be (even wrongly) identified for the mere fact of having expressed their opinions. Moreover, it is also doubtful that acquiring and processing such an amount of personal data could be considered to be the "least invasive option" that authorities have at their disposal to respond to possible threats deriving from (in principle, peaceful) assemblies.[100]

[94] HRC, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association (17 May 2019) A/HRC/41/41, para 57.

[95] Murray, "Police Use of Retrospective Facial Recognition," *supra*, note 15, pp 857–858.

[96] *Gorzelik and Others v Poland* App no 44158/98 (ECtHR, 17 February 2004) para 89.

[97] Murray, "Police use of Retrospective Facial Recognition," *supra*, note 15, pp 843–844. On the practice of arrests facilitated by recording of protesters by the police, see *Gülcü v Turkey* App no 17526/10 (ECtHR, 19 January 2016).

[98] FRA, *Facial recognition technology*, *supra*, note 1, pp 29–30; A/HRC/31/66, *supra*, note 21, para 76; Venice Commission, OSCE/ODIHR, *supra*, note 47, para 172.

[99] Siatitsa, *supra*, note 36, pp 191–2; A/HRC/44/24, *supra*, note 22, paras 33, 35; FRA, *Facial Recognition Technology*, *supra*, note 1, p 34. In assessing the compatibility of AI-enabled biometric identification with EU law, the EDPB and EDPS held that such systems "might present serious proportionality problems, since it might involve the processing of data of an indiscriminate and disproportionate number of data subjects for the identification of only a few individuals (eg, passengers in airports and train stations)" hence require stricter approaches. EDPB/EDPS, *supra*, note 38, paras 30–1.

[100] A/HRC/41/41, *supra*, note 94, para. 56. Among the positive obligations of the State, there is also the presumptive peaceful character of protests.

Aside from the chilling effect produced by surveillance with respect to States' obligation not to unduly interfere with peaceful protest, Siatitsa has noted that indiscriminate surveillance may directly infringe States' positive obligations when it comes to their duties in facilitating assemblies and promoting an enabling environment for the exercise of the right, including by putting in place an institutional framework that safeguards the effective exercise of the right. As a result, deploying surveillance tools, including FRT, absent specific legal frameworks, including transparent domestic legislation and effective safeguards against abuses shall amount to a violation of the positive obligation to facilitate assemblies.[101]

3. . . . *and the right to respect for private life*

Anonymity is a central aspect of protest. Traditionally, when participating to a public demonstration or peaceful gathering, individuals normally reasonably expect that they do enjoy a certain degree of anonymity, or at the very least a little chance of being identified or singled out.[102] As a matter of fact, the protection offered by the right to a private life is not limited to the private sphere of the individual or their inner circle, but equally covers the "private social life," meaning the possibility of establishing and developing relationships also occurring outside of their homes or inner circle.[103] This entails that an action performed in public does not exclude the individual's expectation of privacy.[104]

However, such protection is dramatically reduced by the possibility that audio-visual recordings of assemblies are associated with the automated identification of all or many of the participants to a political or social demonstration or protest.[105] FRT shifts the paradigm on state surveillance, as it considerably impacts on each individual's personal development, which presupposes an ongoing process of discussion, challenge and debate of ideas and views among like-minded communities.[106] In this context, the "shield of privacy" protects individuals from external scrutiny allowing them to develop and exchange ideas, playing the crucial role of "sponsor and guardian to the creative and the subversive."[107]

In light of the fundamental importance of privacy in enabling the realisation of other related rights and fundamental freedoms,[108] its crucial role during peaceful assembly should not be dismissed for the mere fact that protests are normally performed in *public*. A certain degree of privacy is a key element for protest: it facilitates the essential social interactions that foster mobilisation; it enables individuals to separate different aspects of their life without fearing that their political or social views challenge their private or

[101] Siatitsa, *supra*, note 36, p 195.

[102] Venice Commission, OSCE/ODIHR, *supra*, note 47, para 71.

[103] *López Ribalda and Others v Spain* App nos 1874/13 and 8567/13 (ECtHR, 17 October 2019) paras 87–8.

[104] CCPR/C/GC/37 *supra*, note 42, para. 62 (noting that the mere fact that an assembly occurs in a public place does not imply that participants' privacy can be infringed).

[105] A/HRC/44/24, *supra*, note 22, para 34.

[106] Murray, "Police use of Retrospective Facial Recognition," *supra*, note 15, p 845.

[107] T Macklem, *Independence of Mind* (Oxford University Press 2008) p 36; N Richards, "The Dangers of Surveillance" (2013) 126 Harvard Law Review 1934, 1950.

[108] See, for example, HRC, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (17 April 2013) A/HRC/23/40, paras 21–4 (noting how privacy can also be defined as the presumption of having an area of autonomous development, interaction with others and freedoms, a private sphere free from State intervention, and that the right to privacy may be considered "as an essential requirement for the realization of the right to freedom of expression").

professional life; and it allows them to hold and freely express unconventional or unorthodox views without fearing others' judgment or disproval.[109]

Enjoying a right to anonymity during assemblies by participants and organisers shall not be understood as being absolute: individuals participating to political protests or demonstrations know that they are visible and even recognisable by their peers, but not necessarily by the State or third parties. Knowing that they are monitored and possibly identified in an automated fashion may lead them to adopt more mainstream positions, with detrimental effects on the full development of their personalities. Such a negative effect of surveillance may be aggravated with regards to those communities that are at the margin of society or those who challenge the economic or political status quo, who may be pushed to conform to or comply with existing social norms. This may carry negative consequences not only on the fundamental freedoms of opinion, expression and assembly of those involved, but also on the democratic and pluralist character of societies at large.[110]

The right to privacy in the context of FRT use during peaceful assembly is also closely linked to the protection of data of participants and organisers,[111] whose facial digital images are recorded and indefinitely retained for the purposes of identification. As noted by the Venice Commission and OSCE Office for Democratic institutions and human rights, "[t]he taking and retention of digital imagery for purposes of identifying persons engaged in lawful activities, or the retention of data extracted from such images (such as details of an individual's presence at an assembly) in a permanent or systematic record may give rise to violations of the right to privacy."[112] Similarly, the Human Rights Council, in acknowledging the importance of privacy for the realisation of other rights, including the right to freedom of expression and peaceful assembly, has stressed that the "unlawful or arbitrary surveillance and/or interception of communications, and the unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the right to privacy."[113]

In the event of surveillance activities, the ECtHR has clarified that the reasonable expectation of privacy is not a conclusive factor in assessing an interference with Article 8 ECHR. If on the one side it endorsed the view that using a camera to monitor an individual in a public place without recording does not amount to an interference,[114] any systematic or permanent record of personal data, in particular pictures, may conversely cause private life concerns.[115] Hence, any restriction under the scope of Article 8(2) in the event of secret surveillance activities, including on the protection of personal data, must be in "accordance with the law" against the risk of arbitrariness. As technology is becoming more and more sophisticated, the law regulating the use of covert surveillance measures

[109] On the respect of privacy during protests and the notion of "public privacy," see V Aston, "State Surveillance of Protest and the Rights to Privacy and Freedom of Assembly: A Comparison of Judicial and Protester Perspectives" (2017) 8 European Journal of Law and Technology 1, 3–9.

[110] Murray, "Police Use of Retrospective Facial Recognition," *supra*, note 15, pp 845–6.

[111] The right to privacy is protected by various international instruments: UDHR Art 12; ICCPR Art 17; CRC Art 16; CRPD Art 22; ACHR, Art 21; ECHR, Art 8; IACHR, Art 11. The EU Charter of Fundamental Rights provides for two distinct provisions respectively protecting private and family life (Art 7) and personal data (Art 8). Art 8 stipulates that data concerning a person must be processed fairly for specified purposes and on the basis of the consent of the person concerned, or some other legitimate basis laid by law. Moreover, authorities' compliance with said rules shall be subjected to control by an independent authority. For further discussion on the right to privacy and surveillance, see K Humble, "International Law, Surveillance and the Protection of Privacy" (2021) 25 The International Journal of Human Rights 1.

[112] Venice Commission, OSCE/ODIHR, *supra*, note 47, para 172.

[113] HRC, The Right to Privacy in the Digital Age (7 April 2017) A/HRC/RES/34/7, pp 2–3.

[114] *Perry v UK* App no 63737/00 (ECtHR, 17 July 2003) para. 38; *López Ribalda and Others v Spain*, *supra*, note 103, para 89; *Herbecq and the Association "Ligue des Droits de l'Homme" v Belgium*, nos. 32200/96 and 32201/96, Commission decision of 14 January 1998, Decisions and Reports 92-B, p 92.

[115] *López Ribalda and Others v Spain*, *supra*, note 103, para 89.

must meet the requirements of foreseeability and accessibility and must be sufficiently clear to inform citizens about the circumstances and conditions in which the authorities can rely on surveillance measures and the resulting data collection. Further, minimum safeguards relating to the "nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by national law" shall be provided by law against any risks of abuse.[116]

With this in mind, FRT quite clearly poses greater risks than traditional surveillance, providing law enforcement authorities with more sophisticated tools capable of monitoring large numbers of individuals at the same time in an automated fashion, and identifying them.[117] Facial recognition, due to its potential to infringe personal autonomy and the right to privacy not only of individuals, but entire communities, raises important questions about the proportionate and legitimate grounds that may justify its deployment by law enforcement. As put by Smith and Miller, "threats to life on a small scale might not be of sufficient weight to justify substantial infringements of privacy/autonomy, eg, a low level terrorist threat might not justify citizen-wide biometric facial recognition database." Hence, according to the authors, regulation and accountability mechanisms should ensure that access by law enforcement to repositories created for legitimate purposes, for example containing passport photos, could be allowed for detecting serious crimes, but not to identify peaceful protesters.[118]

For example, in *Bridges v South Wales Police*, the first successful legal challenge to police use of FRT at a domestic level, the UK Court of Appeal held that the automated facial recognition by South Wales police forces to identify individuals was unlawful and was not "in accordance with law" under Article 8 ECHR. Between 2017 and 2019, the police had deployed a real-time surveillance system known as "AFR Locate" in various public events against a watchlist of persons of interest, leading to an estimate of 500,000 faces scanned by the software, the large majority of which were not on the watchlist. Despite an applicable legal framework was present, it did not provide clear guidance on *who* could be included in the watchlist and *where* such a system could be deployed. Hence, although it might be deemed necessary for the purposes of crime prevention, the legal basis accorded police officers too wide discretion to meet the standard of "in accordance with the law" requirement provided by Article 8(2) ECHR.[119]

Accordingly, in light of the need of strong safeguards against the risks of abuse and arbitrariness and the potential of high levels of intrusion in the right to privacy of individuals deriving from the automated processing of their facial images, the Guidelines on Facial Recognition by the Consultative Committee of the CoE's Convention for the protection for the protection of individuals with regard to Automated Processing of Personal Data (Convention 108) detailed minimum safeguards and guarantees to be implemented in the processing of sensitive data such as facial biometric data. Such processing must be subjected to the requirements of legality, strict necessity and proportionality to the purpose(s) aimed and the impact on the rights of data subjects. In

[116] *Shimovolos v Russia* App no 30194/09 (ECtHR, 21 June 2011) para 68. For further insights on data protection law within the EU, see G Mobilio, "Your Face Is Not New to Me – Regulating the Surveillance Power of Facial Recognition Technologies" (2023) 12 Internet Policy Review 1.

[117] For a discussion on the challenges facing human rights law in the context of FRT and the concept of "compound human rights harm," see Murray, "Facial Recognition and the End of Human Rights as We Know Them?" *supra*, note 5.

[118] M Smith and S Miller, *Biometric Identification, Law and Ethics* (Cham, Springer 2021) p 32.

[119] *R (on the application of Bridges) v Chief Constable of South Wales Police* ([2020] EWCA Civ 1058). At a national level, other claims were brought against FRT use by the police. See, for instance, *State of New Jersey v Francisco Arteaga* A-3078-21 (2023); *Observatorio de Derecho Informático Argentino O.D.I.A. y otros v GCBA* Actuación Nro: 2453371/2022 (2022).

considering the high intrusiveness on privacy and human dignity of real-time FRT in uncontrolled environments, its use should be, according to the Committee, subjected to a democratic debate and the possibility of a moratorium pending comprehensive analysis.[120]

IV. The scope of the protection under the ECHR in the event of surveillance activities: the ECtHR's approach in *Glukhin v Russia*

In 2020, the ECtHR was for the first time called upon to decide on the compatibility with the ECHR of police use of FRT in the context of peaceful protest, following an application by Russian national Mr Nikolaj Sergeyevich Glukhin. The applicant's complaints before the Court concerned an administrative conviction for failing to notify Russian authorities about his intention to hold a solo demonstration. On 23 August 2019, he travelled in Moscow underground with a life-sized cardboard of a Russian activist, Mr Kostantin Kotov, who had been arrested a few days earlier for peaceful protest, an event that had sparked significant public interest and indignation.[121] After the demonstration, Mr Glukhin was indeed arrested and charged with an administrative offence for having violated the procedure for the conduct of public events as established in domestic law, which required the prior submission of a notification, and was convicted to a fine of 20,000 Russian roubles (about 283 euros).[122] Before the Court, the applicant complained that the operational-search activities performed by the police anti-extremism unit that led to his identification and arrest were not lawful, as they were intended for investigating on criminal offences and activities compromising national security, not to investigate administrative offences. Moreover, considering the peaceful character of his protest, which had not caused any risk for public order nor the life and health of others, the applicant claimed that the conviction had infringed on his right to freedom of expression.[123]

In particular, in the application it was alleged that the anti-extremism unit of the Russian police had employed FRT in at least two ways. By using "post-remote FRT"[124] they were able to identify him using photos and screenshots of a video of his protest taken from a public Telegram channel and video-recordings from the CCTV cameras installed in two Moscow underground stations.[125] After having successfully identified him, they were able to establish his home address. At a later time, since they could not find him at home, they allegedly used "real time FRT"[126] installed in CCTV cameras in the Moscow underground to locate and arrest him while he was transiting in an underground station.[127]

While the applicant could not prove that the police had used the technology – domestic legislation does not require the police to report its use nor to give the person concerned the access to data collected[128]–, the Court found that this was plausible,

[120] Consultative Committee on Convention 108, *supra*, note 27, p 8.

[121] *Glukhin v Russia*, *supra*, note 7, paras. 1, 6–7.

[122] Ibid, paras 13, 15.

[123] Ibid, paras. 16, 21.

[124] "'Post' biometric identification systems ... would be systems enabling capture of biometric data and comparison and identification processes to run after a significant delay, based on pictures or video footage generated by closed circuit television (CCTV) cameras or private devices". T Madiega and H Mildebrath, *Regulating Facial Recognition in the EU – In-depth Analysis* (European Parliament European Parliament, Directorate-General for Parliamentary Research Services, 2021) p 25, available at <https://data.europa.eu/doi/10.2861/140928>.

[125] *Glukhin v Russia*, *supra*, note 7, paras 12–14.

[126] "'Real-time' biometric identification systems would be defined as systems that are able to capture biometric data and run the comparison and identification processes instantaneously (or without a significant delay), based on 'live' or 'near-live' material, such as video footage, generated by a camera or other device." Madiega and Mildebrath, *supra*, note 124, p 25.

[127] *Glukhin v Russia*, *supra*, note 7, para 12.

[128] Ibid, paras 40, 68–9.

considering that between 2017 and 2022 more than 220,000 CCTV cameras equipped with FRT were installed in Moscow, enabling the authorities to identify Mr Glukhin in less than two days.[129]

1. The decision of the Court: FRT and the infringement upon Articles 8 and 10 ECHR

Once it had established its jurisdiction on the case,[130] the ECtHR considered the case under Article 10 (freedom of expression) and Article 8 (right to respect for private and family life) of the ECHR.[131]

With regards to Article 10, the Court noted that the State's prerogative in imposing restrictions related to Mr Glukhin's solo demonstration, given its nature and character, was limited in scope, as his conduct was aimed at expressing his opinions "on a matter of public interest".[132] The subsequent arrest and conviction were to be considered an interference with his right to freedom of expression.[133] In assessing the legitimacy of such interference, the Court found that domestic legislation was not clear nor foreseeable enough with regards to the conduct of public events to meet the "quality of law" requirement.[134] Not only, even assuming that the interference complied with the law and pursued the legitimate goals of preventing disorder and protecting the rights of others, the fact that the applicant's actions did not cause any significant harm to others nor disrupt public order or transport safety, made the restriction unnecessary in a democratic society. As such, Russian authorities "did not show the requisite degree of tolerance" and infringed his right to freedom of expression.[135] In particular, with respect to FRT, the Court found that the use of "highly intrusive facial recognition technology" for the purposes of identifying and arresting a peaceful protester could have a "chilling effect in relation to the rights to freedom of expression and assembly".[136]

In examining the complaint under Article 8, the Court further assessed the processing of the applicant's personal data, including the use of FRT, in the context of administrative offence proceedings, concluding that it amounted to an interference with his right to respect for his private life.[137] Moving to the proportionality test, the Court noted that, while there was a legal basis for this interference in domestic law, the relevant provisions

[129] Ibid, paras 5, 70–2.

[130] The Court established that it had jurisdiction to deal with the case, as the facts giving rise to the alleged violations of the Convention had taken place before 16 September 2022, the date on which Russia ceased to be a Party to the ECHR. Ibid, paras 41–3.

[131] Ibid, para 47. The Court relied on precedent case-law in *Novikova and Others v Russia* App nos 25501/07, 57569/11, 80153/12, 5790/13 and 35015/13 (ECtHR, 12/09/2016), where it deemed appropriate to examine the impugned actions of Russian authorities in relation to applicants' solo demonstrations under the freedom of expression, rather than peaceful assembly, however "taking into account, where appropriate, the general principles it has established in the context of Article 11 of the Convention," para 91.

[132] *Glukhin v Russia*, *supra*, note 7, para 51.

[133] Ibid, para 52.

[134] The Public Event Act (no. FZ-54 of 19 June 2004) regulating public events does not require a prior notification for holding of solo demonstrations, except if a "quickly (de)assembled object" is used. In that case, if the demonstrator fails to submit a notification within three days, they are punishable with a fine or community service, even if no damage to anyone's health or property resulted from their conduct. In the case at hand, the applicant alleged that the cardboard figure of Mr Kotov did not fall in the category of "quickly (de)assembled object". Ibid, paras 15, 18–20; 49–53.

[135] *Glukhin v Russia*, *supra*, note 7, paras 55–7.

[136] Ibid, para 88. See also third-party intervention by NGO Article 19: Global Campaign for Free Expression submitted 10 June 2022, available at <www.article19.org/wp-content/uploads/2022/07/Glukhin-v-Russia-A19-Third-Party-Intervention-10-June-2022.pdf>, esp. paras 23, 25, 27.

[137] *Glukhin v Russia*, *supra*, note 7, para. 73.

governing the processing of biometric personal data were widely formulated and lacked reference to any limitations related to the nature of the situations justifying FRT use, the potential targets, the intended goals, or the processing of sensitive data. This would allow the authorities to use FRT in connection with potentially any judicial proceeding. In addition, the Russian legal system lacked any procedural guarantees for FRT use, including pre-emptive authorisation, procedures regulating data examination, use and storing, let alone supervisory control mechanisms or available remedies for data subjects.[138]

With respect to the legitimate aims pursued by the impugned measure, despite surveillance measures could potentially be justified for crime prevention and terrorism, the applicant's conduct in the context of his solo demonstration gave rise to a minor offence related to failure to notify and did not involve any violence or significant disruption of traffic or public order.[139] More specifically, the Court considered the storing and processing of Mr Glukhin's personal data, particularly live FRT, to identify, locate, and arrest him, as "particularly intrusive." According to the Court, for these measures to be deemed "necessary in a democratic society," a high level of justification is needed, and the "highest" level of justification [is] required for the use of live facial recognition technology." In the case at hand, even stronger guarantees should have been accorded, since the data acquired and processed by the authorities revealed the applicant's political opinion, thus falling within the special categories of sensitive data "attracting heightened level of protection".[140] The Court concluded that the lack of detailed rules governing the use of FRT and of strong safeguards against the risk of abuse and arbitrariness, together with its deployment in a peaceful protest, rendered it disproportionate, as it did not correspond to a "pressing social need" and could not be regarded as "necessary in a democratic society."[141] The Court ruled on the violation of Article 8 by Russian authorities and concluded:

> [T]he use of highly intrusive facial recognition technology in the context of the applicant's 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.[142]

2. *Some considerations on the Court's ruling in light of current debates and trends*

With its landmark ruling,[143] the Court asserted itself amid ongoing debates currently occurring in various fora. However groundbreaking, as it authoritatively addressed some of the main concerns that are at the heart of FRT use in relation with IHRL and that have been raised by a variety of actors, including scholars, policymakers, data protection authorities and NGOs,[144] the ruling contains certain positive aspects, but overlooks some others.

[138] Ibid, paras 81–3.

[139] Ibid, para 85, 88. It must be noted that prior notification of an assembly is not a necessary requirement under IHRL, although it may be instrumental to ensure peaceful and safe assemblies. On the issue, international case-law has held somewhat similar positions. Moreover, according to OSCE/ODHIR and Venice Commission, individual protesters should not be required to notify authorities. See, OSCE/ODHIR Guidelines, *supra*, note 47, para 113; *Skiba v Poland*, Application no. 10659/03 (ECtHR, 7 July 2009); Kälin and Künzli, *supra*, note 56, pp 504–5; *Tatár and Fáber v Hungary* App nos 26005/08 and 26160/08 (ECtHR, 12/09/2012) finding that the imposition of an administrative sanction on two participants of a political performance for failure to notify the authorities could have a chilling effect on public speech and amounted to a violation of Art 10 ECHR.

[140] *Glukhin v Russia*, *supra*, note 7, para. 86; *Catt v UK* App no 43514/15 (ECtHR, 24 January 2019) para, 114.

[141] *Glukhin v Russia*, *supra*, note 7, paras 89–90.

[142] Ibid.

[143] F Palmiotto and N Menéndez González, "Facial Recognition Technology, Democracy and Human Rights" (2023) 50 Computer Law and Security Review 1, 6.

[144] See *supra*, notes 38 and 39.

In particular, the Court emphasised a key issue regarding the deployment of FRT by the police: it is often governed by secrecy to protect important public interests during criminal investigations or in matters of national security, and frequently occurs without the knowledge or awareness of the individuals targeted, who cannot either consent or opt out.[145] In virtual absence of applicable regulation or supervisory control mechanisms, law enforcement agencies' subtle development and use of FRT, together with the ease of concealing these systems in CCTV cameras and even drones,[146] entails that there exist, at the moment, limited information – and even less public awareness – about *how* these technologies are used by law enforcement. In addition, the absence of comprehensive information about who can be included in watchlists and databases available to the police makes it harder to fully grasp the extent to which such technologies may infringe upon individuals' human rights and fundamental freedoms.[147] Aware of the potential invisibility of FRT deployment by law enforcement agencies against unaware protesters, in the case at hand the ECtHR accurately highlighted the applicant's difficulty in challenging FRT use by the Russian police anti-extremism unit and demonstrating the infringement upon his rights without direct evidence. The Court indeed decided to proceed with a circumstantial reasoning, based on (i) reports by local NGOs suggesting widespread (although concealed) FRT use by Russian authorities to identify protesters, (ii) the fact that the police were able to identify him in a few days solely through photos and screenshots of video regarding the protest, and (iii) the fact that the authorities did not contest such use in the judicial proceeding. The Court thus concluded that such use was plausible, by easing the burden of proof on the applicant.[148]

Second, the Court pointed out to the high intrusiveness and chilling effect of FRT, asserting that its use in the case at hand should be regarded as incompatible with the ideals and values core to democratic societies promoted by the Convention. In the views of the Court, FRT use requires robust safeguards, especially if sensitive data revealing the political position of targeted individuals are involved, and high levels of protection against abuse and arbitrariness. This entails that domestic legislation must establish precise limitations defining the nature of the situations giving rise to their use, the goals pursued, the categories targeted, as well as solid procedural safeguards concerning authorisation, data storage and processing, and oversight by a supervisory mechanism.[149]

[145] *Dowsett v UK* App no 39482/98 (ECtHR, 24 September 2003) para. 42; EDRi, *supra*, note 40, p 10 (describing mass surveillance as actions that "rely on watching [the public] indiscriminately, without reasonable suspicion, sufficient possibilities for them to have knowledge of what is happening, ability to consent, nor the genuine and free choice to opt in or out"; VL Raposo, "The Use of Facial Recognition Technology by Law Enforcement in Europe: A Non-Orwellian Draft Proposal" (2023) 29 European Journal on Criminal Policy and Research 515.

[146] Siatitsa, *supra*, note 36, p 185, noting that, recently, military grade drones have been equipped with facial recognition and emotion analysis software to deduce emotions, in order to "ensure that if authorities so decide, not a single person remains anonymous during a protest."

[147] O'Flaherty, *supra*, note, 10, pp 170–1; Zalnieriute, "Power and Protest," *supra*, note 3, p 101 (noting that law enforcement agencies worldwide "are experimenting with FRT with discretion and on an ad hoc basis, without appropriate legal frameworks to govern its use nor sufficient oversight or public awareness"); Siatitsa, *supra*, note 36, p 184.

[148] *Glukhin v Russia*, *supra*, note 7, paras 40, 69–73; Palmiotto, Menéndez González, *supra*, note 143, p 4; G Mobilio, "La Corte EDU condanna il ricorso alle tecnologie di riconoscimento facciale per reprimere il consenso politico: osservazioni a partire dal caso *Glukhin c. Russia*" (2024) 62 (1) DPCE online 695, 700, available at <www.dpceonline.it/index.php/dpceonline/article/view/2107>.

[149] *Glukhin v Russia*, *supra*, note 7, paras 83–90.

a. Ex-post and real-time FRT: what impact for human rights?

In its decision, the Court distinguished between the different FRT, namely those operating in real-time and post-remotely, highlighting how the former require stronger safeguards. However, some have suggested that the Court somewhat fails to directly address the distinct and specific legal implications deriving from both applications, revealing a superficial and overly abstract approach to the question matter of analysis.[150]

On the one hand, post-remote FRT do not necessarily entail a lesser degree of risks, as their intrusiveness prescinds from the purposes for which they are deployed and the delay in which the identification occurs. As underlined by the European Data Protection Board and European Data Protection Supervisor's *Joint Opinion 5/2021*, the fact that identification does not occur in real time shall not be considered a mitigating factor, since "a mass identification system is able to identify thousands of individuals in only a few hours" with the likelihood of "a significant chilling effect on the exercise of the fundamental rights and freedoms, such as freedom of assembly and association and more in general the founding principles of democracy."[151] For these reasons, as noted by Mobilio, an assessment of the intrusiveness of these systems necessarily implies an evaluation of how they are effectively used,[152] rather than when the identification takes place.

On the other hand, it is true that real-time or live FRT systems do carry intrinsic risks as they are "intimately linked to surveillance practices," an aspect that, according to some, the Court has perhaps neglected.[153] As such, the deployment of live FRT for the supposed legitimate aim of crime prevention during a peaceful assembly, for example to identify a suspect, would necessarily imply a large-scale automated processing of facial images of all the participants, including those who are not the subject of "attention" by the police, whose biometric templates would be acquired for comparison against a watch-list. Such a use of FRT would depart from "mere" targeted surveillance of certain individuals and would enable blanket surveillance,[154] with the plausible effect of discouraging individuals from taking part in demonstrations and protests.

The concerns on real-time FRT are not limited to risks of mass surveillance practices but are further exacerbated by the intrinsic characteristics of these technologies. As discussed above, FRT accuracy greatly diminishes when deployed in publicly accessible places, with increased risks of wrongly flagging individuals. Moreover, the inherent risk of unintended biases both on the technical side and the possibility of targeting individuals based on certain characteristics involves a number of additional dangers related to the possibility that their deployment in publicly available spaces amplifies and reinforces existing inequalities and discrimination.

Analogously to the reasoning of the ECtHR, the recent EU AI Act draws a distinction between "real-time" and "ex-post" biometric identification systems, categorising the former a "prohibited practice" and the latter as "high-risk," implying different levels of

[150] I Neroni Rezende, "Glukhin and the EU Regulation of Facial Recognition: Lessons to Be Learned?" (European Law Blog, 19 September 2023) available at <www.europeanlawblog.eu/pub/glukhin-and-the-eu-regulation-of-facial-recognition-lessons-to-be-learned/release/1>; Mobilio, *supra*, note 148, p 701.

[151] EDPB/EDPS, *supra*, note 38, paras 30–1.

[152] Mobilio, *supra*, note 148, p 700 et sqq.

[153] Palmiotto and Menéndez González, *supra*, note 143, p 5.

[154] These conclusions were also reached by the Italian Data Protection Authority, which gave an unfavourable opinion on the deployment of SARI Real time, a facial-recognition system, by the Ministry of the Interior since it lacked a sufficient legal basis. The Authority considered FRT for crime prevention "highly problematic" and requiring an appropriate legal basis taking into account the human rights and freedoms at stake, as well as the key features of these systems, including the criteria to select the individuals to be included in the watch-list, the consequences in case of false-positives, or the full reliability of the system as for processing the data of individuals belonging to ethnic minorities. See Italian Data Protection Authority, *Parere sul sistema Sari Real Time* (25 March 2021) 9575877.

control and safeguards.[155] Real-time remote biometric identification systems in public places for the purposes of law enforcement are subjected to a general prohibition, since they are regarded as inaccurate, biased, and particularly intrusive to the human rights and fundamental freedoms of those concerned, to such an extent that they may "affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights."[156] Despite these serious and worrisome considerations, Article 5(1)(h) introduces significant exceptions to this prohibition, allowing the use of these systems by law enforcement when they are "strictly necessary" to (i) search missing persons or victims of abductions, trafficking in human beings or sexual exploitation; (ii) prevent threats to the life or the physical safety of persons or of terrorist attacks; and (iii) the localisation and identification of a person who is suspected of having committed a serious criminal offence, when it is necessary for the investigation, prosecution or execution of a penalty, provided that such offence is punishable under national law for a maximum period of at least four years. Annex II contains an exhaustive list of the criminal offences that can be covered by this exception and for which real-time FRT may be used.[157]

Under the regulation, the use of real-time biometric identification, when allowed by virtue of the exceptions specified, should be limited to situations that are serious in nature (specifically in terms of the consequences that are expected if the system were not used), and is anyway subjected to a pre-authorisation by a judicial or administrative authority, except in cases of urgency whereas the authorisation must be obtained within 24 hours, an assessment of necessity and proportionality with regards to the purposes for which it is used (especially as regards the temporal, geographic and personal limitations), and a prior fundamental rights impact assessment.[158]

The exceptions to the general prohibition of real-time remote biometric identification have raised several concerns about whether the safeguards provided are adequate to protect individuals' rights and freedoms against the serious risks that these systems entail. In particular, the broad and quite general formulation of the situations that would make real-time biometric systems in publicly accessible spaces *permitted* may lead to a fragmentation in the implementation of the AI Act among Member States, where the same offences do not share a common definition nor provide for the same punishments, and may pave the way to *de facto* legitimising their use, especially in emergency situations. It has been noted, for example, that in the prevention of a threat of a terrorist attack or other *ticking-bomb* scenarios, it would be probable that these exceptions will allow that persons who are not formally involved in a criminal investigation are targeted.[159]

[155] AI Act, *supra*, note 6. Under recital 17 of the regulation, in the case of "'real-time' systems, the capturing of the biometric data, the comparison and the identification occur all instantaneously, near-instantaneously or in any event without a significant delay. [...] 'Real-time' systems involve the use of 'live' or 'near-live' material, such as video footage, generated by a camera or other device with similar functionality. In the case of 'post' systems, in contrast, the biometric data has already been captured and the comparison and identification occur only after a significant delay. This involves material, such as pictures or video footage generated by closed circuit television cameras or private devices, which has been generated before the use of the system in respect of the natural persons concerned".

[156] Ibid, recital 32.

[157] These include including terrorism, murder and grievous bodily injury, rape and other sexual offences, international crimes that are within the jurisdiction of the International Criminal Court, illicit trafficking of narcotics, nuclear materials or weapons, and others. See Annex II of AI Act, *supra*, note 6.

[158] Ibid, Art 5(2)–(7).

[159] See, eg, A Giannini and S Tas, "AI Act and the Prohibition of Real-Time Biometric Identification. Much Ado About Nothing?" (*Verfassungsblog*, 10 December 2024) available at <https://verfassungsblog.de/ai-act-and-the-prohibition-of-real-time-biometric-identification/>; EDRi, "How to Fight Biometric Mass Surveillance After the AI Act: A Legal and Practical Guide" (*EDRi*, 27 May 2024) available at <https://edri.org/our-work/how-to-fight-biometric-mass-surveillance-after-the-ai-act-a-legal-and-practical-guide/>.

Analogous concerns in terms of human rights guarantees are raised by post-remote biometric identification systems, which, as anticipated, are not prohibited under the AI Act. As high-risk practices under Article 6(2), ex-post FRT is subjected to some guarantees and safeguards, narrower than those applicable to real-time systems. For example, their deployment by the police does not always require a prior judicial or administrative authorisation (eg, in cases where it is used to identify a suspect "based on objective and verifiable facts linked to the offence")[160] nor a proportionality and necessity assessment, leaving broader freedom to Member States in their regulation. As already argued, however, the fact that the identification of a person takes place within a few seconds, days or months after the event occurred does not in practice reduce the risks of infringement upon human rights, if not the opposite. Retrospective identification allows the possibility that law enforcement authorities apply an identification system to *any* recorded material, either photo or video, providing them the ability to "look back in the past," regardless of the time lag between the acquisition/recording and the application of FRT.[161] This practice is associated to the risk that States' authorities exert a "persistent tracking" on individuals, with serious impacts on human rights and fundamental freedoms, no matter *when* the identification occurs.[162]

It is submitted that the guarantees afforded by the AI Act, especially relating to the deployment of live and ex-post FRT in publicly available places by law enforcement, may not be entirely in line with respect to ECtHR's approach in *Glukhin v Russia*.[163] As suggested by the Court, when deploying these technologies for the purposes of law enforcement, a "high level of justification" is required in order for them to be considered "necessary in a democratic society," and the level of protection accorded should be even higher in cases that data revealing a person's political opinion are processed. It remains to be seen whether the safeguards for the deployment of biometric identification systems under the AI Act will satisfy the ECtHR's standards, especially with regards to the ex-post FRT.

b. The ECtHR approach in addressing law enforcement deployment of FRT during peaceful protest: between "procedural fetishism" and "self-restraint"?

Another category of criticism directed against the Court relates to its approach towards biometric identification systems. By focusing on the absence of procedural safeguards regulating the police deployment of FRT within the Russian system, according to some the Court has avoided the fundamental question on whether these are fundamentally compatible with the ECHR. As noted by Zalnieriute, consistent with a "procedural fetishism" adopted in precedent case-law related to surveillance, the judges have put an emphasis on "procedural micro-issues" concerning the proportionality, functionality and effectiveness of the Russian surveillance system. As such, not only the Court circumvented the question on the substantial legality of FRT, but implicitly endorsed their use if effective safeguards are in place.[164] The position adopted by the Court in *Glukhin v Russia* appears to

[160] AI Act, *supra*, note 6, Art 26(10).

[161] Murray, "Police use of Retrospective Facial Recognition," *supra*, note 15, pp 836–7.

[162] European Parliamentary Research Service (ERPS), *Person Identification, Human Rights and Ethical Principles. Rethinking Biometrics in the Era of Artificial Intelligence* (Scientific Foresight Unit (STOA), 2021) available at <www.europarl.europa.eu/RegData/etudes/STUD/2021/697191/EPRS_STU(2021)697191_EN.pdf>.

[163] Mobilio, *supra*, note 148, p 704. For a discussion on the fundamental rights standards and the AI Act, see F Paolucci, "Shortcomings of the AI Act. Evaluating the New Standards to Ensure the Effective Protection of Fundamental Rights" (*VerfassungsBlog*, 14 March 2024) available at <https://verfassungsblog.de/shortcomings-of-the-ai-act/>.

[164] M Zalnieriute, "Glukhin v. Russia," *supra*, note 9, pp 698–9. On the ECtHR's "procedural fetishism," see also M Zalnieriute, "Procedural Fetishism and Mass Surveillance Under the ECHR: Big Brother Watch v. UK" (*Verfassungsblog*, 2 June 2021) available at <https://verfassungsblog.de/big-b-v-uk>.

align with the international and supra-national debate, where the prevailing trend – despite the permanence of opposing voices calling for a total ban – seems to have come to accept facial recognition systems under the strict condition of procedural safeguards and limitations.[165]

For example, the CoE's Framework Convention on Artificial Intelligence, the first-ever international legally binding treaty on AI, does not directly regulate biometric systems, but provides for principles of, *inter alia*, human dignity, transparency and oversight, accountability and responsibility and equality and non-discrimination, as well as privacy and personal data protection applicable to the lifecycle of artificial intelligence systems that may potentially interfere with human rights, democracy and the rule of law. The Convention significantly introduces an exception to its applicability for activities within the AI systems related to national security interests, as long as such activities respect international law, including IHRL.[166] Similarly, as discussed, the AI Act introduces important exceptions to the general prohibition of live FRT, while it does not ban post-remote FRT.

In light of the above, we cannot help but wonder whether the approach of the ECtHR in *Glukhin v Russia* has missed a chance to firmly set the bar high in favour on human rights guarantees. In the decision, the Court set high standards when it comes to law enforcement use of these systems, as it held that, to satisfy the quality of law requirements, the Russian domestic system should have envisaged procedures for a prior authorisation and for examining, using and storing the data obtained through FRT, as well as supervisory control mechanisms or the available remedies. In addition, domestic law lacked 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 the processing of sensitive personal data."[167]

However, a few crucial questions emerge concerning the approach adopted by the Court and the wider debate on FRT regulation. In the judgment, the Court admittedly reveals a certain restraint in clearly positioning itself on their fundamental compatibility with the ECHR. In its reasoning, the Court acknowledges how modern techniques of investigation and identification have a role to play in the fight against crime and how useful they can be in relation to organised crime and terrorism – "one of the challenges faced by today's European societies"[168] –, to some extent indirectly condoning their use. At the same time, the Court emphasises not only the chilling effect on human rights that FRT may cause, but also their incompatibility with the "ideals and values of a democratic society governed by the rule of law" when used to identify a peaceful protester exercising his right to freedom of expression, thus requiring high levels of protection, the "highest", when real-time FRT are involved.

This difficulty in balancing security and protective interests with the intrusiveness of FRT creates an ambiguity that cannot be ignored, especially given the urgent need of

[165] For a detailed discussion on the ECtHR's approach in *Glukhin v Russia*, see C Nardocci, "Il riconoscimento facciale sul 'banco' degli imputati. Riflessioni a partire, e oltre, Corte EDU *Glukhin c. Russia*" (2024) 1 BioLaw Journal 279, pp 290–1 (noting that "[n]onostante non siano in tutto sopite le voci che vorrebbero vietare in modo assoluto l'utilizzo dei sistemi di riconoscimento facciale per ragioni di sorveglianza pubblica [. . .], l'orientamento prevalente sembra essersi spostato in favore di una ammissibilità condizionata" and, as such, the ECtHR aligns with this position, which does not advocate for an absolute ban, but presupposes "un impiego soggetto a limitazioni e rispettoso dei diritti individuali grazie alla tipizzazione di specifici requisiti procedurali"); Murray, "Facial Recognition and the End of Human Rights as We Know Them?" *supra*, note 5, p 146 et sqq.

[166] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (adopted, 17 May 2024) CETS 225. Within the UN, the Convention of Cybercrimes, adopted on 8 August 2024, raised concerns about its human rights implications, namely with respect to vague provisions authorising predictive policing and the creation of shared biometric databases. K Rodriguez, "The UN Cybercrime Convention: Analyzing the Risks to Human Rights and Global Privacy" (*JustSecurity*, 27 August 2024) available at <www.justsecurity.org/98738/cybercrime-convention-human-rights/>.

[167] Glukhin, *supra*, note 7, para 83.

[168] Ibid, para 85.

regulation advocated by many. If this ambiguity could ideally be attributed to the "procedural fetishism" mentioned by some – where the Court focuses on the minor nature of the offense, the protester's peaceful behaviour and the lack of safeguards domestically – such an approach is not new to the Court's surveillance caselaw.[169] This approach suggests that it is the responsibility of the (either national or supra-national) legislator, rather than an international court, to establish an appropriate legal framework to mitigate the risks of abuse and arbitrariness: the ECtHR's role is to adjudicate specific cases, rather than to determine the compatibility of facial recognition systems with the ECHR in general terms.[170] In addition, given the diverse applications of FRT, the varying goals pursued, and tasks performed, the Court might be reluctant to endorse a general ban, especially considering current international regulatory trends.

At the same time, the Court's minimalist stance leaves crucial questions unanswered. If the evaluation on FRT lawfulness is on the minor offence and peaceful behaviour of the applicant, what would happen if the protester was, in fact, not peaceful? Assuming that the Russian system was equipped with a clear legal basis, it would be plausible for enforcement authorities to be entitled to deploy real time FRT in case of suspected serious crimes. Such deployment would require the systematic biometric processing of *all* persons in the monitored public space to check for potential matches against a watch-list, potentially causing serious interferences with their right to a private life. Even if the data collected were deleted afterwards, the scan and acquisition of facial images of hundreds, even thousands of individuals would shift the very nature of surveillance from targeting specific individuals for crime prevention to the potentially universal monitoring of the public space, in lack of effective safeguards.[171] When FRT is deployed in political or social demonstrations, surveillance would target individuals exercising their legal right to protest, with potential significant chilling effects on the freedoms of expression, assembly and association. Another aspect that should not be overlooked relates to the kind of sensitive data collected through FRT. Since data collected during peaceful protest can reveal the participants' political affiliations, such use of FRT could effectively enable political motivated profiling or persecution under the pretext of crime prevention.[172]

To date, legal challenges at the national level regarding police use of FRT have revealed gaps in domestic regulation, along with the risks of bias and misidentification inherent to these systems. These cases underscore the consequences of unchecked police surveillance in the absence of a robust accountability framework.[173] In this context, the Court may have missed an opportunity to establish authoritative, human rights-informed standards, by clarifying the (strict) conditions under which FRT could be deployed by police. As noted by Nardocci, in *Glukhin v Russia* the ECtHR overlooks key principles related to AI systems, which were conversely highlighted by domestic case-law and at a European level, such as transparency, reliability and human oversight.[174] Similarly, the notions of "general public

[169] See, eg, *supra*, notes 87 and 91.

[170] The Court itself notes that "[t]he question here is not whether the processing of biometric personal data by facial recognition technology may in general be regarded as justified by the Convention. The only issue to be considered by the Court is whether the processing of the applicant's data was justified under Article 8§2 of the Convention *in the present case*". *Glukhin v Russia*, *supra*, note 7, para 85 (emphasis added). See also Mobilio *supra*, note 148, pp 702–703.

[171] Italian Data Protection Authority, *Parere sul sistema Sari*, *supra*, note 154.

[172] OVD-Info, *supra*, note 15, noting that, in the Russian case, "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."

[173] See *supra*, note 119.

[174] Nardocci, *supra*, note 165, pp 301–3; CoE's Framework Convention on Artificial Intelligence, supra, note 157, Arts 7 et sqq.

interest" or "national security" which could justify FRT use were not explored. By clarifying these terms in the specific situation, the Court could have provided essential guidance to relevant stakeholders and legislators on when the deployment of FRT for legitimate national security or public interest purposes is proportional. As crime prevention interests will likely continue to pose challenges for the Court, it remains to be seen where the line will be drawn between security concerns and the protection of human rights.[175]

V. Concluding remarks

Protest is an essential right that contributes to the promotion and the affirmation of inclusive, pluralistic, and democratic societies and enables the full enjoyment of a broad range of civil, political, economic, social and cultural rights. The ability to freely express one's opinions, discuss and debate them in the public sphere without external surveillance not only fosters individual personal development, but also benefits the communities to which they belong.

In this context, the dangerous practice of monitoring publicly available places during peaceful assemblies and public gatherings to identify individuals for alleged public security purposes in practice restricts the ability of people to freely develop, express and discuss their ideas in the public sphere, both alone and with others. Intrusive facial recognition technologies pose serious risks for the individuals involved, as they have the potential to infringe on various rights and fundamental freedoms, *inter alia* the right to privacy, freedom of expression and freedom of assembly. Additionally, these systems carry inherent risks of inaccuracy and bias, which may disproportionately impact the most vulnerable individuals or groups in society – those who, in principle, would benefit the most from participating in public, whether political or social, activities and demonstrations. In the hands of public authorities, FRT often operates invisibly and without regulation, significantly enhancing and reinforcing state surveillance capabilities in the name of national security and public order.

In *Glukhin v Russia* the ECtHR has had the chance to rule on FRT's compatibility with human rights for the first time. The judgment clearly underlined the potential dangers that these technologies imply and, in the case under consideration, deemed them difficult to reconcile with the ideals and values of a democratic society governed by the rule of law, thus requiring strong safeguards against the risks of abuse. At the same time, the decision met with some criticism, for failing to directly address key concepts that could guide a more human rights-driven approach to police use of these technologies. If the Court appears to have aligned itself with the most recent trends sanctioning biometric mass surveillance practices on the condition that detailed regulatory frameworks and procedural safeguards are in place, the question of whether these will ever suffice remains wide open.

Acknowledgments. This work was supported by the MUR National Recovery and Resilience Plan funded by the European Union – NextGenerationEU – Mission 4 Component 2, Investment 1.3 "Partenariati estesi a Università, centri di ricerca, imprese e finanziamento progetti di ricerca", MUR notice n. 341 del 15/03/2022, Project SERICS – SEcurity and RIghts in the CyberSpace, proposal: PE00000014, CUP: J33C22002810001, funded by MUR decree n. 1556 of 11/10/2022. The author wishes to express her sincere gratitude to the anonymous reviewer for their insightful feedback on earlier versions of this article.

Competing interests. The author has no conflicts of interest to declare.

[175] Palmiotto and Menéndez González, *supra*, note 143, p 6.

Cite this article: G Gabrielli, "The Use of Facial Recognition Technologies in the Context of Peaceful Protest: The Risk of Mass Surveillance Practices and the Implications for the Protection of Human Rights". *European Journal of Risk Regulation*. https://doi.org/10.1017/err.2025.26