Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the rights to freedom of peaceful assembly and of association; the Special Rapporteur on the right to privacy and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism

Ref.: OL IRL 3/2022
(Please use this reference in your reply)

30 September 2022

Excellency,

We have the honour to address you in our capacities as Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; Special Rapporteur on the rights to freedom of peaceful assembly and of association; Special Rapporteur on the right to privacy and Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, pursuant to Human Rights Council resolutions 43/4, 50/17, 46/16 and 49/10.

In this connection, we would like to bring to the attention of your Excellency's Government information we have received concerning the proposal that the forthcoming **Garda Síochána (Recording Devices) Bill 2022**[1] may include measures to permit the use of facial recognition technology ('FRT') by law enforcement in the Republic of Ireland. Authorization of the use of FRT by law enforcement could significantly limit the exercise of fundamental freedoms, including the rights of freedom of expression (under article 19 of the International Covenant on Civil and Political Rights ("the Covenant")), privacy (article 17 of the Covenant), and freedom of peaceful assembly and of association (articles 20 and 21 of the Covenant). Further, such a proposal is out of step with the growing international consensus against the use of FRT, something reflected in the European Commission's current legislative proposals in the field of artificial intelligence ('AI').

In these circumstances, we urge your Excellency's Government to reconsider the proposal to include authority for the use of FRT by law enforcement in this legislation. Failure to do so risks violation of the Republic of Ireland's international human rights obligations.

I. Background

In April 2021, the Government published the General Scheme for the Garda Síochána (Digital Recording) Bill, setting out a series of legislative objectives relating to the increased use of surveillance technologies for law enforcement purposes, including provision for body-worn cameras, expanded authority for using mobile phones, mobile CCTV, and drone devices for surveillance purposes, and greater Gardaí access to third-party data (CCTV feeds and automatic number plate recognition). The Special Rapporteur on the rights to freedom of peaceful assembly and of association had previously expressed in a report concerns over overly broad and vague surveillance laws, which often fail to target specific individuals on the basis of a reasonable suspicion. These risks of abuse are increased as many laws and regulations governing surveillance do not keep pace with the rapid changes in

[1] Department of Justice, General Scheme of Garda Síochána (Digital Recording) Bill (April 2021), available at: https://www.gov.ie/en/publication/bc45c-general-scheme-of-garda-siochana-digital-recording-bill/

surveillance technology and its potential uses. With specific reference to domestic use of surveillance drones, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has expressly addressed the negative human rights implications of the domestic use of such technologies, which have been primarily developed in the context of counter-insurgency, counter-terrorism and armed conflict to domestic law enforcement arenas.[2] The General Scheme was subject to pre-legislative scrutiny by parliamentary committee in late 2021. The formal legislation (now named Garda Síochána (Recording Devices) Bill 2022 ('the Bill'))[3] has subsequently been drafted. It was introduced into the Dáil Éireann on 4 August 2022,[4] is expected to be considered at the committee stage in autumn 2022, and is scheduled by the Government to be enacted by the end of 2022.

The General Scheme does not provide further information as to whether or not FRT would be permitted or excluded under the detailed legislative provisions which would be drafted. However, at the time of the publication of the General Scheme, the Minister of Justice advised that she intended to seek Cabinet approval to include amendments to the Bill during the committee stage to include authority for law enforcement to use FRT.[5] That intention was reiterated by the Minister on 14 June 2022.[6]

The Minister of Justice's stated intention contradicts the Joint Committee on Justice's recommendation issued at the pre-legislative scrutiny stage in December 2021 that steps should be taken to ensure that information and data proposed to be collected by recording devices, such as body-worn cameras and CCTV should not use FRT.[7]

The plans for the extension of legislative authority under the Bill to FRT come at a time when the European Union is considering comprehensive legislative action in

[2] See: Remarks of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism at the International Expert Group Meeting on the Protection of Vulnerable Targets and Unmanned Aircraft Systems (6 October 2021), available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/remarks_of_the_un_sr_ct_hr_at_the_egm_vulnerable_targets_and_uas.pdf

[3] Garda Síochána (Recording Devices) Bill 2022 (Bill 79 of 2022).

[4] See: https://www.oireachtas.ie/en/bills/bill/2022/79/

[5] See: Minister for Justice's Written Answer to Question 587, available at: https://www.justice.ie/en/JELR/Pages/PQ-31-05-2022-587

[6] See: Minister for Justice's Written Answer to Question 1286, available at: https://www.oireachtas.ie/en/debates/question/2022-06-14/1286/

[7] See: An Comhchoiste um Dhlí agus Ceart/Joint Committee on Justice, Tuarascáil maidir leis an nGrinnscrúdú Réamhreachtach ar Scéim Ghinearálta Bhille an Gharda Síochána (Taifeadadh Digiteach)/Report on Pre-Legislative Scrutiny of the General Scheme of the Garda Síochána (Digital Recording) Bill, December 2011, p8, available at: https://data.oireachtas.ie/ie/oireachtas/committee/dail/33/joint_committee_on_justice/reports/2021/2021-12-17_report-on-pre-legislative-scrutiny-of-the-general-scheme-of-the-garda-siochana-digital-recording-bill_en.pdf

the field of AI following the European Commission's April 2021 proposal.[8] That proposal contemplates that *'the use of 'real time' remote biometric identification systems (such as FRT) in publicly accessible spaces for the purpose of law enforcement is prohibited unless certain limited exceptions apply*.'

II. Assessment and concerns with regards to the proposals for FRT

The proposal to include amendments to the Bill at the committee stage so as to allow for the use of FRT, especially FRT which operates in 'real time' as a tool for identification and targeted interference with individuals, raises significant concerns.

(a) Absence of proper pre-legislative scrutiny

Given the potential significant human rights impact of FRT as a novel surveillance technology, we regret to note that the detail of the government's proposals for authorizing the use of FRT by the Gardaí was not included in the General Scheme and, as a result, has not been subject to the sort of proper pre-legislative scrutiny ordinarily contemplated by Irish parliamentary procedure. We further note that, the proposal that the amendments relating to FRT will be introduced and then considered at the parliamentary committee stage prior to final legislative decision. Nevertheless, the bypassing of the pre-legislative review stage denies stakeholders other than those with parliamentary representation the opportunity to provide focused submissions on the detail of the proposed FRT provisions.

The absence of a procedure for a searching pre-legislative review of the FRT proposals is particularly concerning in light of the fact that international experts, in recognition of the novel challenges raised by FRT systems and practice, have called for particular caution with respect to reforms in this area.[9] The United Nations High Commissioner for Human Rights, has notably recommended in a report that States:

'[i]mpose a moratorium on the use of remote biometric recognition [i.e. facial recognition] technologies in public spaces, at least until the authorities responsible can demonstrate compliance with privacy and data protection standards and the absence of significant accuracy issues and discriminatory impacts, and until all the following recommendations are implemented:

(i) Systematically conduct human rights due diligence before deploying facial recognition technology devices and throughout the entire life cycle of the tools deployed;

(ii) Establish effective, independent and impartial oversight mechanisms for the use of facial recognition technology, such as independent data protection authorities, and consider imposing a requirement of prior authorization by an independent body for the use of facial recognition technologies in the context of assemblies;

---

[8] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts,' COM(2021) 206 final ('Commission Proposal').

[9] In addition to the position of the OHCHR see, for instance, the position of the EU Fundamental Rights Agency set out in: EU FRA, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (2020), available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

(iii) Put in place strict privacy and data protection laws that regulate the collection, retention, analysis and otherwise processing of personal data, including facial templates;

(iv) Ensure transparency about the use of image recordings and facial recognition technology in the context of assemblies, including through informed consultations with the public, experts and civil society, and the provision of information regarding the acquisition of facial recognition technology, the supplies or such technology and the accuracy of the tools;

(v) When relying on private companies to procure or deploy these facial recognition technologies, request that companies carry out human rights due diligence to identify, prevent, mitigate and address potential and actual adverse impact on human rights and, in particular, ensure that data protection and non-discrimination requirements be included in the design and the implementation of these technologies.'[10]

These pre-conditions do not seem to have been met, particularly in the absence of a robust pre-legislative scrutiny process. Accordingly, in addition to the substantive concerns raised in this letter, we urge your Excellency's Government to reconsider the procedure which has been followed in this instance, and instead to subject the proposed FRT provisions to the regular mechanism of pre-legislative review contemplated by Irish parliamentary process. The latter is accepted to be the most likely means to address the relevant human rights concerns.

(b) Timing of proposals

Further, we note that the question of whether or not FRT (and in particular 'real time' FRT systems) is lawful is currently subject to debate and legislative consideration between European Union institutions. The European Commission has proposed the harmonization of rules regulating AI systems, including FRT. While the European Commission no longer advocates its original proposal of a five-year total ban on FRT systems,[11] the Commission has recommended that FRT should not be used in publicly accessible spaces for law enforcement purposes unless its use is strictly necessary to limited objectives,[12] and that any use should be subject to prior specific authorization granted by a judicial or independent administrative authority.[13] As part of this process, the European Data Protection Board and the European Data Protection Supervisor have delivered a joint opinion calling for a moratorium on any use of AI for automated recognition of human features in public spaces.[14]

Given the paucity of domestic consideration of the impacts of FRT, we express further concerns that your Excellency's Government proposes effectively to prejudge the European Union legislative process, when that process has already raised significant concerns with FRT use. Accordingly, we respectfully recommend that your Excellency's Government delay any consideration of authorizing the use of FRT

---

10 A/HRC/48/31 (13 September 2021), [59(d)].

11 J Espinoza and M Murgia, 'EU backs away from call for blanket ban on facial recognition technology,' *Financial Times* (11 February 2020), available at: https://www.ft.com/content/ff798944-4cc6-11ea-95a0-43d18ec715f5

12 Commission Proposal, proposed Article 5(1)(d) and Article 5(2).

13 Commission Proposal, proposed Article 5(3).

14 See: 'EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination,' Press Release (21 June 2021), available at: https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en

for law enforcement. Such consideration should not only be delayed until such time as proper pre-legislative scrutiny ordinarily contemplated by Irish parliamentary procedure has been undertaken, but also until the same question has been properly considered at the European Union level.

(c) Substantive human rights concerns

The proposed use of FRT by law enforcement for 'real time' analysis of footage of large numbers of persons to identify them, then possibly track and apprehend them, raises significant human rights concerns, particularly with regards to the exercise of the right to freedom of peaceful assembly. Such a system necessarily requires the analysis and review of the biometrics of very large numbers of people who are not persons of interest to law enforcement, but whose sensitive and unique biometric data is nonetheless collected and considered by State authorities. As stated by the Special Rapporteur on the rights to freedom of peaceful assembly and of association in a report, these forms of identification and data collection violate the individual's anonymity in public spaces and exert significant "chilling effects" on decisions to participate in public gatherings.

Nor do FRT systems simply provide a mechanism of matching identities to images. As the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism set out in her 2020 report on States' use of biometric data,[15] sophisticated FRT systems allow for significant amounts of additional sensitive information not immediately detectable to human observers to be discerned. Tools can make assessments of health information such as body mass index from subjecting facial images to FRT algorithms,[16] and some research suggests that traits such as sexual orientation may also be identifiable.[17] Further, FRT is being used to assess facial expressions with the aim of identifying the subject's emotional state, albeit that the accuracy of these attempts is a matter of serious dispute.[18] As biometric investigation techniques grow more sophisticated, it is to be expected that any analysis of facial images through FRT systems will lead to increasingly detailed and personal information becoming available on the individuals whose images are analysed.

FRT represents a clear interference with individuals' rights to privacy. Under international human rights law, every person enjoys the right to private and family life without undue interference.[19] Both the General Assembly and the Human Rights Council have stressed that the right to privacy serves as one of the foundations of democratic societies and, as such, plays an important role in the realization of a host of other rights, including the rights to freedom of assembly and of association, freedom of religion, as well as freedom of opinion and expression.[20] But given the interconnected nature of human rights, the adverse impacts of privacy violations may

[15] 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?' (University of Minnesota Human Rights Center, 2020) ('Biometric Data Report').

[16] Ibid., p24.

[17] M Kosinski and Y Wang, 'Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation from Facial Images' (2018) 114(2) *Journal of Personality and Social Psychology* 246-257.

[18] Biometric Data Report, p25. See also: M Fairhurst, C Li, and M Da Costa-Abreu, 'Predictive Biometrics: A Review and Analysis of Predicting Personal Characteristics from Biometric Data,' IET Biometrics, The Institute of Engineering and Technology (2017), pp369-378.

[19] ICCPR, Article 17.

[20] A/RES/71/199; A/RES/73/179; A/HRC/RES/34/7.

entail more widespread rights infringements, including upon the right to equal protection of the law, the right to life, the right to liberty and security of the person, the rights to fair trial and due process, and the right to freedom of movement.

The context in which FRT is deployed – typically crowds of people, often brought together for purposes of assembly, including in respect of political demonstration or religious observance – also risks violations of the rights to freedom of peaceful assembly, freedom of expression, and to freedom of religion.

Interferences with the rights to privacy, freedom of assembly and expression, and other associated rights are only permissible in limited circumstances where they not only serve a legitimate objective,[21] but are strictly necessary and proportionate in their effect. Even if your Excellency's Government considers that the use of FRT - and the analysis of biometric personal data it entails - pursues the legitimate objective of preventing and investigating crime by identifying and assisting in the apprehension of criminal suspects, the degree of interference must be considered in light of the necessity of the measure to achieve the aim and the actual benefit it yields.[22]

In another context,[23] the United Nations Human Rights Committee has clarified that such consideration requires that the infringement is the *'least intrusive instrument amongst those which might achieve their protective functions*,'[24] and has counselled that, *'[i]n adopting laws providing for restrictions permitted [for legitimate aims], States should always be guided by the principle that the restrictions must not impair the essence of the right … the relation between the right and restriction, between norm and exception, must not be reversed. The laws authorising the application of restrictions should use precise criteria and may not confer unfettered discretion on those charged with their execution*.'[25]

A system which necessarily requires the harvesting of biometric data from a large crowd without any discrimination between potential persons of interest and those raising no law enforcement interest inevitably casts its net too widely, and appears incapable of complying with the *'least intrusive instrument*' criterion devised by the Human Rights Committee. Further, the public context of such biometric data gathering makes it impossible for individuals to opt out.[26] These are the reasons why the Special Rapporteur on the rights to freedom of peaceful assembly and of association has stated that surveillance against individuals should *'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 supervision*.'[27] Similarly, the United Nations High Commissioner for Human Rights has recommended that States should *'[r]efrain from recording footage of*

---

21 Article 17 of the ICCPR does not expressly set out that interferences may be justified on the basis of a legitimate objective, but the consistent approach of the Human Rights Committee, in common with regional human rights courts, is to read that implied limitation into the scope of the right. See, for instance the decision of the Human Rights Committee in *Van Hulst v Netherlands*, UN Doc. CCPR/C/82/D/903/1999 (2004), [7.6]-[7.10].

22 A/HRC/27/37, [24].

23 The right to freedom of movement under Article 12 of the Covenant.

24 HRC, *General Comment 27*, UN Doc. CCPR/C/21/Rev.1/Add/9 (1999), [14]; and HRC, *General Comment 34*, UN Doc. CCPR/C/GC/34 (2011), [34].

25 HRC, *General Comment 27*, [13].

26 Biometric Data Report, p8.

27 A/HRC/41/41, [57].

assembly participants, unless there are concrete indications that participants are engaging in, or will engage in, serious criminal activity, and such recording is provided by law, with the necessary robust safeguards.'[28]

In addition to the interferences which FRT appears inevitably to entail for those actually subject to monitoring, the human rights of persons more broadly are affected by the introduction of ever-greater surveillance capacities deployed in civic space. As the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has previously observed,[29] disproportionate use of surveillance powers *per se* undermines freedom of expression, particularly through the creation of a chilling effect whereby persons engage in self-censorship so as to avoid State scrutiny. That concern is particularly keenly felt by persons who already perceive themselves as targeted by State authority, including members of religious or ethnic minorities.[30] The Special Rapporteur had previously called for an immediate moratorium in the sale, transfer, and use of surveillance tools including FRT until robust human rights safeguards are in place to regulate such practice.[31]

These concerns are made all the more significant by the fact that evidence suggests that FRT systems are highly inaccurate at identifying individuals, leading to very high false positive rates, particularly in respect of persons other than white males.[32] The accuracy of FRT with respect to more sophisticated inferences about subject's emotional state similarly appears to display insufficient sensitivity to cultural differences.[33]

We further underline that States should not rely on the improvement of accuracy rates as the technology is used more widely and refined in practice to justify the well-known limitations of the technology. We further reaffirm that the legitimate exercise of fundamental freedoms ought not to be sacrificed or suspended for an indefinite period in the interests of remedying the defective programming of FRT developers. Even if accuracy rates were to drastically improve in short order, the more significant human rights concerns with respect to the disproportionate impact of the technology on non-suspects and the chilling effect on civic space would persist, without any path to reduction.

We would welcome your Excellency's response to the concerns raised *supra*, and stand ready to provide technical support on the various issues.

In the absence of proper examination of the regulatory safeguards contemplated in respect of FRT, we recommend that your Excellency's Government not pursue the proposal to authorize the use of FRT in law enforcement via amendments to the Bill at the committee stage.

---

28 A/HRC/44/24, [53(i)].
29 A/HRC/32/38, [57].
30 Ibid. See also: A/HRC/29/32.
31 A/HRC/41/35.
32 See, for instance: D Harwell, 'Federal study confirms racial bias of many facial-recognition systems, casts doubt of their expanding use,' *The Washington Post* (19 December 2019), available at: https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/; and National Institute of Standards and Technology, 'NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software', 19 December 2019, available at https://www.nist.gov/ news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software. See also: Biometric Data Report, p25.
33 Biometric Data Report, p25.

This communication, as a comment on pending or recently adopted legislation, regulations or policies, and any response received from your Excellency's Government will be made public via the communications reporting website after 48 hours. They will also subsequently be made available in the usual report to be presented to the Human Rights Council.

Please accept, Excellency, the assurances of our highest consideration.

Irene Khan
Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

Clement Nyaletsossi Voule
Special Rapporteur on the rights to freedom of peaceful assembly and of association

Ana Brian Nougrères
Special Rapporteur on the right to privacy

Fionnuala Ní Aoláin
Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism