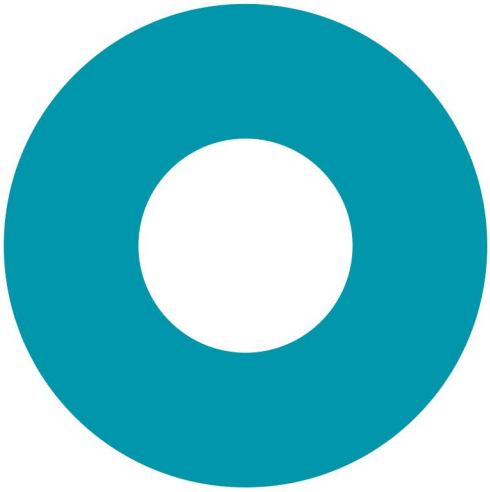
Legislative Observation

Submission to the Minister for Justice on the General Scheme of the Garda Síochána (Recording Devices)(Amendment) Bill

Irish Human Rights and Equality Commission
May 2024



Coimisiún na hÉireann um Chearta an Duine agus Comhionannas
Irish Human Rights and Equality Commission

Published by the Irish Human Rights and Equality Commission.

Copyright © Irish Human Rights and Equality Commission 2024

The Irish Human Rights and Equality Commission was established under statute on 1 November 2014 to protect and promote human rights and equality in Ireland, to promote a culture of respect for human rights, equality and intercultural understanding, to promote understanding and awareness of the importance of human rights and equality, and to work towards the elimination of human rights abuses and discrimination.

Contents

Abbreviations

The Charter	Charter of Fundamental Rights of the European Union
The ECHR	European Convention on Human Rights
EctHR	European Court of Human Rights
The General Scheme	General Scheme of the Garda Síochána (Digital Recording)(Amendment) Bill
The Commission	Irish Human Rights and Equality Commission
LED	Law Enforcement Directive
The Principal Act	The Garda Síochána (Recording Devices) Act 2023
CJEU	Court of Justice of the European Union

Recommendations

Equality and Non-Discrimination

The Commission recommends that:

- the human rights and equality implications of these technologies are subject to independent and effective scrutiny, by either an existing body, such as the new Policing and Community Safety Authority, or the establishment of a new body, such as an independent group on emerging technologies. This oversight should occur prior to and after these technologies are deployed to examine compliance with human rights and equality principles. Such oversight should take account of developing international positions.

Biometric Data and Biometric Identification (Head 2)

The Commission recommends that:

- further consideration is given to the definition of "Biometric Data" to ensure that there is no contradiction or confusion caused with existing definitions in Irish or EU law.
- the necessary safeguards for processing special category data are clearly set out in the legislation.
- the definition of "Biometric Identification" should clearly set out that for the purposes of this Bill, "biometric Identification" is intended to mean only retrospective or 'post' remote biometric identification in accordance with the definition set out in Article 3(38) of the EU Artificial Intelligence Act.

Power to use Biometric Identification (Heads 3 and 4)

The Commission recommends that:

- careful consideration is given to the offences that are to be included in the Schedule to ensure that the list contains only relevant and proportionate offences that are appropriate for the use of biometric identification and to prevent the unnecessary and disproportionate use of biometric identification.

- ‘security of the State’ is defined in the Bill so that it is clear what it encompasses with regard to the use of biometric identification.
- the Bill includes the necessary procedural safeguards and limitations to ensure the power to use biometric identification is not left open to potentially discriminatory, biased and/or arbitrary use.
- it should be clearly set out in the Code of Practice the circumstances in which the use of biometric identification will be deemed to be necessary and proportionate, taking account of the requirements of Article 10 of the Law Enforcement Directive.
- it must also be demonstrable by An Garda Síochána that the processing of biometric data for the purposes of biometric identification cannot be achieved in a more reasonable and proportionate way, and by less intrusive means.

Scope of Materials Accessible (Heads 2, 4, and 7)

The Commission recommends that:

- the Bill must clearly and precisely set out the specific sources of material that can be used for the purposes of biometric identification. The Commission also recommends that the Bill set out the lawful basis for the use of such sources and ensure that it is compliant with EU Law.
- the Bill should set out the precise circumstances in which it would be legal for An Garda Síochána to obtain/hold images and video material to be used for the purposes of biometric identification.
- provisions detailing how the integrity of the images and video material obtained/held by the Garda Síochána will be maintained should be set out in primary legislation.
- for the Bill to adequately protect the rights of the persons subject to it, it must provide clarity and foreseeability in terms of its effect on such persons to ensure that the processing of personal data by An Garda Síochána is lawful.
- the Bill should set out that where images and video materials are obtained by An Garda Síochána for a different original purpose, are then utilised for the purpose of biometric

identification, it will be necessary to demonstrate that processing the data is strictly necessary and proportionate and in accordance with law.

- search warrants issued under the Garda Síochána (Recording Devices) Act 2023 pertaining to the collection and/or recording of images and video materials in private places should authorise with particularity their subsequent use and retention for biometric identification.
- where An Garda Síochána obtain images and video material from third parties for the purpose of biometric identification, such as other national or international organisations, the legal basis that allows for the processing of such personal data must be clearly set out in the Bill.
- clarity is provided in the Bill as to what is meant by a national or international organisation.

'Live Feed' Biometric Identification (Head 4)

The Commission recommends that:

- the Bill should clearly define what constitutes 'live feed' for the purposes of the Bill to ensure the prohibition of the use of biometric identification in the context of live feed is fully operational.
- particular protocols should be provided in the Bill in relation to live feed obtained pursuant to Part 6 of the Garda Síochána (Recording Devices) Act 2023 to ensure that the prohibition of the use of biometric identification in the context of live feeds is fully operational.

Application and Approval (Heads 5 and 6)

The Commission recommends that:

- judicial authorisation must be sought for the power to use biometric identification. An authorisation granted should set out the nature, scope and duration of the approval.
- due to the sophistication of the technology and the developing national and international positions on artificial intelligence as well as the human rights and data protection implications, any judge involved in the authorisation process should be required to have knowledge and/or training in this area.

- all applications for the use of biometric identification should identify a specific and limited set of data sources that can be used in a biometric search.
- all written records concerning applications made for the use of biometric identification should be made available to a suitable independent oversight body at a minimum, on an annual basis to assess compliance with human rights, equality and data protection obligations.

Human Verification (Head 7)

The Commission recommends that:

- the code of practice should provide detail on what is involved in the human verification process and should provide specific detail as to the role of the Garda personnel in that process, including the level of training and expertise required.

Code of Practice

The Commission welcomes the requirement for the draft codes of practice to be laid before the Oireachtas, particularly given the importance of the code of practice as referenced throughout the General Scheme.

The Commission recommends that:

- consideration should be given as to whether provisions or fundamental issues designated for inclusion in the code of practice should be more appropriately dealt with in the primary legislation.
- the obligations on Garda personnel under this Bill are set out clearly and precisely. The Bill should also set out clearly the consequences that follow from a failure to observe a provision of the Act or the code of practice.
- it should be explicitly stated that the use of biometric identification will not become operational until the code of practice is published.

Introduction

The Irish Human Rights and Equality Commission ('the Commission') is both the national human rights institution and the national equality body for Ireland, established under the Irish Human Rights and Equality Commission Act 2014 (the '2014 Act'). The Commission has a statutory mandate to keep under review the adequacy and effectiveness of law and practice in the State relating to the protection of human rights and equality, and to examine any legislative proposal and report its views on any implications for human rights or, equality.[1] In this regard, we welcome the opportunity to provide the Minister for Justice with our submission on the General Scheme of the Garda Síochána (Digital Recording)(Amendment) Bill (the 'General Scheme').

The introduction of facial recognition technologies for use by An Garda Síochána further compounds the human rights and equality concerns we have previously raised with regard to the range of powers proposed in the General Scheme of the Garda Síochána (Digital Recording) Bill (now the Garda Síochána (Recording Devices) Act 2023 which the General Scheme sets out to amend). By way of context, in April 2022 we published our Legislative Observations to the Minister for Justice in response to the publication of the General Scheme of the Garda Síochána (Digital Recording) Bill. With regard to facial recognition technology, we raised the following general concerns with regard to its use: [2]

- The impact on the rights to privacy, freedom of peaceful assembly and association, freedom of expression and freedom of movement;
- The risk of profiling or the flagging and tracking of individuals on the basis of a protected characteristic which can give rise to discriminatory outcomes;
- The accuracy of facial recognition technology in terms of skin colour, ethnicity or gender of the person involved which may result in discrimination;
- The need for additional safeguards with regard to technology capable of facial recognition – whether ANPR/CCTV or body-worn camera technology – as such data constitutes biometric data under the Data Protection Act 2018;

[1] Section 10(2)(c) of the Irish Human Rights and Equality Commission Act 2014.
[2] See IHREC, Submission to the Minister for Justice on the General Scheme of the Garda Síochána (Digital Recording) Bill (April 2022), pp. 18-21.

- The European Commission's proposal for a Regulation laying down harmonised rules on artificial intelligence, states that facial recognition technology should not be used in publicly accessible spaces for law enforcement purposes unless its use is strictly necessary to a number of listed objectives and, if used, should be subject to a prior authorisation granted by a judicial authority or by an independent administrative authority;3
- The European Data Protection Board and the European Data Protection Supervisor called for a ban on any use of artificial intelligence for automated recognition of human features, such as faces, in publicly accessible spaces, and a ban on artificial intelligence systems using biometrics to categorize individuals into clusters based on ethnicity, gender, political or sexual orientation, or other grounds on which discrimination is prohibited under Article 21 of the Charter of Fundamental Rights;
- The UN High Commissioner for Human Rights recommends that states impose a moratorium on the use of remote biometric 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 certain stated recommendations are implemented.

The European Union Agency for Fundamental Rights accurately highlights that a person's facial image constitutes biometric data as it is "more or less unique, cannot be changed, and cannot be easily hidden. Facial images are also easy to capture: in contrast to other biometric identifiers, such as fingerprints or DNA, as a person is typically unable to avoid having their facial image captured and monitored in public." [4] Due to their sensitive nature, facial images fall into the 'special categories of personal data' or sensitive data and as such, EU data protection law provides for enhanced protection, and additional safeguards, compared to other personal data.[5] Thus, there is a heightened requirement for the State to ensure that this legislation adequately protects the rights of the persons subject to it.

[3] Regulation of the European Parliament and of the Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) 2021/0106(COD).
[4] FRA, Facial recognition technology: fundamental rights considerations in the context of law enforcement, p. 5.
[5] *Ibid.*

We recognise that the development of this legislative proposal forms part of a wider programme of legislative reform of policing powers and structures in the State, with which we have been engaging on an ongoing basis. We previously flagged concerns with the expansion of Garda powers provided for within this legislative reform and have called for stronger provisions and protections that ensure there are adequate safeguards governing the powers, and that there is adequate and effective independent oversight of the powers.[6] We have similar concerns with regard to the introduction of facial recognition technologies for use by An Garda Síochána.

We consider the use of facial recognition technologies by the State a serious interference with individual rights but also recognise that in order to support a modern police service in Ireland, there is a need for An Garda Síochána to transform its digital technologies.[7] However, respect for human rights and fundamental freedoms is an essential part of democracy and the rule of law, and an appropriate balance must be struck between competing rights. Whilst we will have a consultative role with regard to the code of practice relating to this Part 6A of the legislation, we have set out in this submission our concerns with regard to what the General Scheme indicates in terms of its considerations and compliance with human rights and equality law and standards.

We reiterate that in implementing legislative reforms with regard to policing powers and structures, it is important to recall the Commission on the Future of Policing's assertion that:

> "human rights are the foundation and purpose of policing".[8]

[6] See, IHREC, Submission on the Policing, Security and Community Safety Bill (March 2023); IHREC, Submission on the General Scheme of the Criminal Justice (Hate Crime) Bill (March 2022); IHREC, Submission on the General Scheme of the Garda Síochána (Powers) Bill (May 2022); IHREC, Submission on the General Scheme the Garda Síochána (Digital Recording) Bill (April 2022); IHREC, Submission on the General Scheme of the Criminal Justice (Hate Crime) Bill (March 2022).

[7] As set out under the 10th principle of the Commission on the Future of Policing in Ireland Report (September 2018). IHREC, Submission on the General Scheme the Garda Síochána (Digital Recording) Bill (April 2022) at p.4.

[8] Commission on the Future of Policing in Ireland, The Future of Policing in Ireland (2018) p. ix.

Relevant Human Rights and Equality Standards

The General Scheme engages and interferes with a number of fundamental rights protected under the Constitution, the Charter of Fundamental Rights of the European Union ('the Charter'), the European Convention on Human Rights ('the ECHR'), and international human rights law.

The Commission considers the following human rights and equality standards to be relevant:

- The right to privacy;[9]
- Protection of personal data;[10]
- The inviolability of the home;[11]
- Equality and non-discrimination;[12]
- Fair trial rights and procedural fairness;[13]
- Right to an effective remedy;[14]
- Freedom of assembly;[15] and

[9] The right to privacy was recognised in *Kennedy v Ireland* [1987] IR 587 as an unenumerated right under Article 40.3 of the Constitution; The right to respect of private and family life is also protected under international law under Article 8 of the European Convention on Human Rights ('ECHR'), Article 7 of the Charter of Fundamental Rights of the European Union ('the Charter'), Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights ('ICCPR').

[10] The right to data protection is protected by the *Data Protection Act 2018.* Part 5 of that Act transposed the *EU Law Enforcement Directive* into Irish law which concerns the processing of personal data by data controllers for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The right to personal data has also been recognised under Article 8 ECHR and Article 8 of the Charter.

[11] The right to the inviolability of the dwelling is protected under Article 40.5 of the Constitution. The right to respect for the home is also protected under Article 8 ECHR.

[12] Article 40.1 of the Constitution and Article 14 ECHR guarantee respectively; equality under the law and the right to enjoy rights and freedoms without discrimination. The right to equality before the law and the prohibition of non-discrimination is also protected under Articles 20 and 21 of the Charter and Articles 2, 3, 14, 15 and 26 ICCPR.

[13] The right to a fair trial and fair procedures are protected under Articles 34, 38 and 40.3 of the Constitution;[13] as well as under Article 47 of the Charter, Article 6 ECHR and Article 14 ICCPR.

[14] The right to an effective remedy for an individual whose rights and freedoms are violated is guaranteed under Article 47 of the Charter, Article 13 ECHR and Article 2(3) ICCPR.

[15] The right of citizens to assemble peaceably is protected under Article 40.6.1°.ii of the Constitution, Article 12 of the Charter, Article 11 ECHR and Article 21 ICCPR. However this right is not absolute, and is subject to qualifying proviso under Article 11(2) ECHR and Article 21 ICCPR which provide that restrictions on the right must be prescribed by law and necessary in a democratic society in the interests of national security or public safety, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others.

- Freedom of expression.[16]

There is inevitably a tension between meaningfully vindicating individual rights and permitting law enforcement authorities to use and access technology to address the commission of serious crime.[17] Therefore, any interference with the rights engaged under this legislation must comply with the principles of legality, necessity and proportionality.

Equality and Non-Discrimination

In its submission on the General Scheme of the Digital Recording Bill, the Commission noted the equality issues arising as a result of the proposed legislative basis for the use of recording devices, particularly with minority groups' experience of racial profiling in Ireland.[18] Similar issues arise with regard to the use of facial recognition technology where the inbuilt biases and discriminatory effects of the technology have been documented.[19]

The use of facial recognition technologies can lead to profiling or the flagging and tracking of the individuals on the basis of a protected characteristic; which can give rise to discriminatory outcomes. The practice of racial profiling violates the principles of non-discrimination and equality before the law, as well as having a negative effect on people's enjoyment of civil and political rights including the rights to privacy, freedom of movement and fair trial.[20]

The use of this technology by police, with no objective and reasonable justification, on the grounds of race, colour, descent, national or ethnic origin or their intersection with other relevant grounds, such as religion, sex or gender, sexual orientation and gender identity, disability and age,

---

[16] The right to freedom of expression is guaranteed under Article 40.6.1°.i of the Constitution, subject to the qualifying condition that it shall not be used to undermine public order or morality or the authority of the State. The right to freedom of expression is also guaranteed under Article 11 of the Charter, Article 10 ECHR and Article 19 ICCPR.

[17] The European Court of Human Rights has established there is a positive obligation on public authorities to investigate crimes. The right to investigate constitutes an element of the right to an effective remedy under Article 13 ECHR and as a procedural element of the right to life, the right to freedom from torture and ill-treatment, and the right to respect for private life amongst other core civil rights. See *Osman v UK* [1998] ECRR 101.

[18] IHREC, Submission on the General Scheme the Garda Síochána (Digital Recording) Bill (April 2022) at p.9.

[19]Leslie, D. (2020). Understanding bias in facial recognition technologies: an explainer. *The Alan Turing Institute* https://doi.org/10.5281/zenodo.4050457; *R (On the Application of Edward Bridges) v. The Chief Constable of South Wales Police & Ors* where the Court of Appeal found that the automated facial recognition system used by South Wales Police was not in compliance with significant aspects of the European Convention on Human Rights, data protection law, and the Public Sector Equality Duty.

[20] See United Nations Committee on the Elimination of Racial Discrimination, General recommendation No. 36 (2020) on preventing and combating racial profiling by law enforcement officials, CERD/C/GC/36 (17 December 2020). IHREC, Submission to the Minister for Justice on the General Scheme of the Garda Síochána (Digital Recording) Bill (April 2022).

migration status, or work or other status in surveillance or investigation activities constitutes racial profiling.[21] There are also particular concerns around the accuracy of facial recognition technology in terms of skin colour, ethnicity or gender of the person involved; which may result in discrimination.

The Commission recommends that the human rights and equality implications of these technologies are subject to independent and effective scrutiny, by either an existing body, such as the new Policing and Community Safety Authority, or the establishment of a new body, such as an independent group on emerging technologies. This oversight should occur prior to and after these technologies are deployed to examine compliance with human rights and equality principles. Such oversight should take account of developing international positions.

[21] See European Commission against Racism and Intolerance, ECRI General Policy Recommendation No 11 on Combatting Racism and Racial Discrimination in Policing, adopted on 29 June 2007 (4 October 2007); United Nations Committee on the Elimination of Racial Discrimination, General recommendation No. 36 (2020) on preventing and combating racial profiling by law enforcement officials, CERD/C/GC/36 (17 December 2020).

Observations on the General Scheme

Biometric Data and Biometric Identification (Head 2)

Head 2 of the General Scheme sets out the definitions of "biometric identification" and "biometric data". "Biometric identification" is defined as 'identifying, or attempting to identify, natural persons, by comparing their "biometric data" against "biometric data" legally held by AGS.' The General Scheme provides that "biometric data" is defined as having the same meaning as Section 69 of the Data Protection Act 2018[22], but is restricted to facial images only and does not include DNA, fingerprints or any other data. This creates a new specific definition of biometric data that is not accurate outside the confines of this Bill, which may lead to confusion in law, and which contradicts the definition of biometric data set out in Irish and EU Law.

The Commission recommends that further consideration is given to the definition of "Biometric Data" to ensure that there is no contradiction or confusion caused with existing definitions in Irish or EU law.

"Biometric data" is also one of the identified "special categories of personal data" under Part 5 of the Data Protection Act 2018. Article 10 of the Law Enforcement Directive ('LED')[23] also includes "biometric data for the purpose of uniquely identifying a natural person" in the list of special category data that may be processed only where strictly necessary and subject to appropriate safeguards for the rights and freedoms of the data subject. Therefore, the use of biometric identification under the General Scheme is liable to encompass the processing of special category data and extra safeguards are necessary.

With regard to "biometric identification", the definition should clearly indicate that the power only permits the use of retrospective or 'post' remote biometric identification (as the General Scheme

[22] Section 69, Data Protection Act 2018 -' "biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual that allow or confirm the unique identification of the individual, including facial images or dactyloscopic data;'
[23] Article 10 of the Law Enforcement Directive.

prohibits the use of live feed biometric identification).[24] The definition of biometric identification should also reflect the definition set out in Article 3(38) of the EU Artificial Intelligence Act.[25]

The Commission recommends that the necessary safeguards for processing special category data are clearly set out in the legislation.

The Commission recommends that the definition of "Biometric Identification" should clearly set out that for the purposes of this Bill, "biometric Identification" is intended to mean only retrospective or 'post' remote biometric identification in accordance with the definition set out in Article 3(38) of the EU Artificial Intelligence Act.

Power to use Biometric Identification (Heads 3 and 4)

Heads 3 and 4 of the General Scheme address the powers of An Garda Síochána to use biometric identification. The proposed Section 43(B)(1) sets out that a member shall not utilise biometric identification unless it is for the "the prevention, investigation, detection or prosecution of one or more of the criminal offences listed in the Schedule," or for the "protection of the security of the State". The use of biometric identification is limited to those offences in the Schedule only and may not be used for the purposes of any other offence. Given the nature of the technology being deployed this is appropriate, and care will have to be taken to ensure that the Schedule contains relevant offences that are appropriate for the use of biometric identification. However, there would appear to be some variation among the offences listed in the Schedule/proposed to be added to the Schedule,[26] where some could be deemed to be less serious than the "most serious of offences" the Bill was said to be intended for.[27] It was also highlighted during pre-legislative

[24] Retrospective biometric identification has been described as the use of facial recognition technology on either still images or video recordings taken in the past to compare faces to photographs held on police databases or watch lists. See: Big Brother Watch, Biometric Britain: The Expansion of Facial Recognition Surveillance (2023), p. 30.
[25] Article 3(38) of the EU AI Act provides: *''post' remote biometric identification system' means a remote biometric identification system other than a 'real-time' remote biometric identification system."*
[26] For example, obstruction of a peace officer punishable on summary conviction to a fine not exceeding €2,500 or to imprisonment for a term not exceeding 6 months or to both (section 19(4) of the Criminal Justice (Public Order)Act 1994), and murder which carries a mandatory sentence of life imprisonment.
[27] Press Release, Department of Justice, Minister McEntee receives Cabinet approval for draft Facial Recognition Technology Bill (14 December 2023 - updated on 31 January 2024). a person Public Order offences are included and the Minister for Justice, Helen McEntee recently confirmed that obstruction of a Peace Officer is also to be included in the offences

scrutiny by the victim/survivor groups that there are other very notable serious offences that have not been included for consideration in the Schedule.[28]

Given the highly intrusive nature of this technology, the inclusion of a given offence in the Schedule to this legislation must be afforded careful scrutiny including consideration of the resulting impact on the range of fundamental rights engaged in order to guard against 'mission creep' and the potential for the unnecessary and disproportionate use of biometric identification by An Garda Síochána. In this regard, we have concerns that the inclusion of offences such as 'riot' and 'violent disorder' may have implications in relation to the rights to freedom of expression and freedom of assembly. While assemblies with violent intent are not protected by the right to freedom of assembly, isolated acts of violence do not deprive an assembly as a whole of protection, and individuals do not lose the right to peaceful assembly as a result of acts of violence committed by others.[29]

The UN High Commissioner for Human Rights recommends that states: "Establish a moratorium on the use of facial recognition technology in the context of peaceful assemblies, at least until the authorities responsible can demonstrate compliance with privacy and data protection standards as well as the absence of significant accuracy issues and discriminatory impacts," and until certain conditions are implemented.[30]

The European Data Protection Board has also provided that in respect of law enforcement carrying out a search pertaining to a riot, the creation of a database of images for that search, based on material sourced from citizens, public transport, CCTV, police owned surveillance material, and material sourced from the media, without first establishing that a person included in the database has displayed severe criminal behaviour and meeting other criteria, may be unlawful.[31] The

[28] See submissions from Rape Crisis Network Ireland and Safe Ireland in the Joint Committee on Justice, Report on Pre-Legislative Scrutiny of the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023 (February 2024).
[29] See submission from Dr. Daragh Murray in the Joint Committee on Justice, Report on Pre-Legislative Scrutiny of the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023 (February 2024).
[30] United Nations Human Rights Council, The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights, A/HRC/48/31 (13 September 2021) para. 59(d). See also United Nations Human Rights Council, Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests: Report of the United Nations High Commissioner for Human Rights, A/HRC/44/24 (24 June 2020) para. 53(j).
[31] European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (Adopted 26 April 2023), pp. 43-45.

'chilling effects' of surveillance, whereby individuals may modify otherwise lawful behaviours due to a fear of being observed by the police, is a serious issue for concern in a democratic society.[32] These rights are foundational to democratic societies, as the European Court of Human Rights and the United Nations Human Rights Committee repeatedly make clear.[33]

The Commission recommends that careful consideration is given to the offences that are to be included in the Schedule to ensure that the list contains only relevant and proportionate offences that are appropriate for the use of biometric identification and to prevent the unnecessary and disproportionate use of biometric identification.

Biometric identification may also be used for "the protection of the security of the State." However, the definition of 'security of the State' is not set out in the General Scheme. It may be presumed that this is because in substance it refers to very serious crimes, such as wide scale organised crime or terrorism, which are self-evidently suitable for rigorous law enforcement investigation (a matter accepted by the European Court of Human Rights in the leading case of Glukhin v Russia)[34]. Nonetheless, it is something that should be defined so that it is clear what it encompasses with regard to the use of biometric identification.[35]

The Commission recommends that 'security of the State' is defined in the Bill so that it is clear what it encompasses with regard to the use of biometric identification.

The proposed Section 43B(2) is broad and subjective and provides excessive discretion to An Garda Síochána. Having the power to "locate a person or to follow the movements of a person in order to progress an investigation…" could in practice encompass any individual or group that is of interest to An Garda Síochána. The provision is absent of any procedural safeguards and limitations, and without these, the power provided for in this provision is subjective and gives An

[32] Amy Steven and others, "I Started Seeing Shadows Everywhere": The Diverse Chilling Effects of Surveillance in Zimbabwe' [2023] *Big Data & Society* 1, 3-4. https://journals.sagepub.com/doi/10.1177/20539517211065368
[33] European Court of Human Rights, *Kudrevičius and Others v. Lithuania*[GC], para. 91 ("the right to freedom of assembly is […] one of the foundations of [democratic] society."); and Human Rights Committee, General comment No. 37 (2020) on the right of peaceful assembly (article 21), (17 September 2020), para.1 ("[the right to peaceful assembly] also constitutes the very foundation of a system of participatory governance based on democracy, human rights, the rule of law and pluralism.")
[34] *Glukhin v Russia*, ECtHR, App no. 11519/20 (4 July 2023) at para 84.
[35] It is noted that a detailed definition of the term 'protecting the security of the State' is set out in Section (3)(1)(a) of the Policing, Security and Community Safety Act 2024.

Garda Síochána a very broad discretion to carry out surveillance on individuals in a manner that is potentially open to discriminatory, biased and/or arbitrary use.[36]

The highly intrusive nature of biometric identification requires strong rules and justifications, heightened protection in law, and strong safeguards against possible abuse. The European Data Protection Board in its guidance provides that the processing of biometric data under all circumstances constitutes a serious interference with rights.[37] The European Court of Human Rights has also stressed this point, stating that the use of facial recognition technology as a surveillance technology requires a 'high' level of justification to be deemed 'necessary in a democratic society'.[38]

The Commission recommends that the Bill includes the necessary procedural safeguards and limitations to ensure the power to use biometric identification is not left open to potentially discriminatory, biased and/or arbitrary use.

We note that under Head 4 of the General Scheme, the use of biometric identification will be presumed to be "necessary and proportionate if its use is in accordance with the applicable code of practice under Section 47." Article 10 LED provides that special categories of personal data may be processed for law enforcement purposes only where, "strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject". Necessity entails that processing should be a reasonable and proportionate method of achieving a given goal, taking into account the overarching principle of data minimisation, and that personal data should not be processed where there is a more reasonable and proportionate, and less intrusive way to achieve a goal.[39]

This means the strict necessity requirement applies where An Garda Síochána proposes to process biometric data for the purposes of biometric identification, and it must be demonstrable that the

[36] Notably, in *R(Bridges) v South Wales Police* the Court of Appeal held that the implementation of FRT technology did not have a sufficient legal framework and that too much discretion was left to individual police officers in the use and deployment of FRT, and so, did not satisfy the 'in accordance with the law' requirement; in *Glukhin v Russia*, the European Court of Human Rights found that law (in this case) was too broad and lacked limitations and procedural safeguards.

[37] European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (Adopted 26 April 2023), p. 5.

[38] Cristina Cocito, Gluhkin v Russia: Facial Recognition Considered Highly Intrusive but not inconsistent with Fundamental Rights (January 2024).

[39] Data Protection Commission, Guidance Note: Legal Bases for Processing Personal Data (December 2019), pp. 5-6.

purpose of the processing cannot be achieved in a more reasonable and proportionate way, and by a less intrusive means.[40]

The Commission recommends that it should be clearly set out in the Code of Practice the circumstances in which the use of biometric identification will be deemed to be necessary and proportionate, taking account of the requirements of Article 10 of the Law Enforcement Directive.

The Commission recommends that it must also be demonstrable by An Garda Síochána that the processing of biometric data for the purposes of biometric identification cannot be achieved in a more reasonable and proportionate way, and by less intrusive means.

Scope of Materials Accessible (Heads 2, 4, and 7)

Head 2 of the General Scheme provides that biometric identification will use a comparison of a person's biometric data with the biometric data which is "legally held" by An Garda Síochána. The power to use biometric identification set out under the proposed section 43B(3) under Head 4 of the General Scheme provides that for the prevention, investigation, detection or prosecution of one or more of the criminal offences listed in the Schedule, or for the protection of the security of the State,[41] An Garda Síochána will only utilise images and video that have "already been gathered and are legally held or legally accessed by An Garda Síochána". However, we note that under Head 7, it is stated that following approval, a member of Garda personnel may utilise biometric identification to search any images or footage that An Garda Síochána legally retains and any images or footage that An Garda Síochána can legally access (emphasis added). The latter suggests that approval may be given to search material that has not yet been obtained by the Garda Síochána, whereas Head 4 implies that only material already held will be searched.

It is not clear which specific sources of images and video material are encompassed within the legislation. For example, the source material could potentially include surveillance camera

[40] In *Schecke, Eifert v Hessen*, the CJEU held that, when examining the necessity of processing personal data, the controller needed to take into account alternative, less intrusive measures, and any interference with data protection rights arising from the processing in question should be the least restrictive of those rights. In general, to satisfy the necessity test, there ought to be no equally effective available alternative; See, CJEU, Joined Cases C 92/09 and C 93/09, *Schecke, Eifert v Hessen*, 9 November 2010, para 86.
[41] Proposed section 43B(1) under Head 4.

footage, CCTV footage, Automatic Number Plate Recognition images, body cam footage, images from social media, images from a member of the public's smartphone etc.[42] The EU Artificial Intelligence Act sets out that the untargeted scraping of facial images from the internet or CCTV footage for the purpose of creating or expanding facial recognition databases should be prohibited as this practice adds to the feeling of mass surveillance and can lead to gross violations of fundamental rights, including the right to privacy.[43] The EU Artificial Intelligence Act also provides that post biometric systems "should always be used in a way that is proportionate, legitimate and strictly necessary, and thus targeted, in terms of the individuals to be identified, the location, temporal scope and based on a closed data set of legally acquired video footage."[44]

It is also not clear from the General Scheme in which precise circumstances it would be legal for An Garda Síochána to obtain/hold such images. This is an issue of central importance as it is the content of such databases that is searched for the purposes of biometric identification. Given that the use of biometric identification will be ordered on a case-by-case basis, to identify the suspect/person being searched for, the persons whose rights are potentially most at risk are those unsuspected persons who are wrongly identified as a match because they are contained in this image database. The provision is also silent on who would be included in a database search and leaves the power open to data collection of persons who will have no knowledge their biometric data may be collected and/or used in a biometric identification search.

A further issue arises in the General Scheme given the absence of any provisions dealing with security, retention, and any other use to which this database can be put. This is a serious omission, and whilst the Principal Act provides that such issues should be covered in the relevant Code of Practice, in view of the unique importance and sensitivity of this database, provisions detailing how the integrity of same will be maintained should be set out in primary legislation.

The European Data Protection Board has noted that "the processing of a person's biometric data allows conclusions to be drawn concerning the private lives of the relevant persons. Those conclusions may refer to the racial or ethnic origins, health, religion, habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out,

[42] Darragh Murray, Police Use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Law Framework (2023), pp. 3-4.
[43] Recital 26(b) of the EU Artificial Intelligence Act.
[44] Recital (58e) of the EU Artificial Intelligence Act.

the social relationships of those persons and the social environments frequented by them." The information revealed by the application of facial recognition technology clearly shows the possible impact its use has on the right to the protection of personal data and the right to privacy (both of which are protected under EU and Irish law).[45]

The LED sets out specific requirements, at a high level, for legislation intended to provide for the processing of personal data by law enforcement authorities. Recital 33 LED states that any such legislative measure "should be clear and precise and its application foreseeable for those subject to it, as required by the case-law of the Court of Justice and the European Court of Human Rights. Member State law regulating the processing of personal data within the scope of this Directive should specify at least the objectives, the personal data to be processed, the purposes of the processing and procedures for preserving the integrity and confidentiality of personal data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness." This is given legal effect by Article 8(2) LED which requires that "Member State law regulating processing within the scope of this Directive shall specify at least the objectives of processing, the personal data to be processed and the purposes of the processing."

Section 71(1)(b) of the Data Protection Act 2018 requires that personal data shall be collected for one or more specified, explicit and legitimate purposes and shall not be processed in a manner that is incompatible with such purposes. At the time of obtaining images or video material for the specific purpose of biometric identification, An Garda Síochána must be able to justify doing so on the basis of strict necessity and proportionality. Similarly, where images and video material that were obtained by An Garda Síochána for a different original purpose are then utilised for the purpose of biometric identification, it will be necessary to demonstrate that processing it is strictly necessary and proportionate on a case-by-case basis.

In addition, images and video material lawfully obtained under the Garda Síochána (Recording Devices) Act 2023 will presumably be available for the purposes of biometric identification as they will have been lawfully obtained and/or held by An Garda Síochána. Given that the collection of such materials under the Act can be in a place other than a public place (by way of warrant), the database available for comparison would include materials taken in public and private places. This

[45] European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (Adopted 26 April 2023), para 34.

includes the home, which has particular constitutional protection[46], as well as being protected under Article 8 ECHR. Arguably, such a search warrant should authorise with particularity not just the creation of images or footage, but also their retention for the purposes of subsequent biometric identification. The grounds for such an application should be recorded in writing.

Head 4 also provides for the processing and storing by An Garda Síochána of images which have been legally provided by other national or international organisations, however, there is no stipulation that these images must have been legally obtained by these organisations, nor indeed what is meant by a national or international organisation.

The Commission recommends that the Bill must clearly and precisely set out the specific sources of material that can be used for the purposes of biometric identification. The Commission also recommends that the Bill set out the lawful basis for the use of such sources and ensure that it is compliant with EU Law.

The Commission recommends that the Bill should set out the precise circumstances in which it would be legal for An Garda Síochána to obtain/hold images and video material to be used for the purposes of biometric identification.

The Commission recommends that provisions detailing how the integrity of the images and video material obtained/held by the Garda Síochána will be maintained should be set out in primary legislation.

The Commission recommends that for the Bill to adequately protect the rights of the persons subject to it, it must provide clarity and foreseeability in terms of its effect on such persons to ensure that the processing of personal data by An Garda Síochána is lawful.

The Commission recommends that the Bill should set out that where images and video materials are obtained by An Garda Síochána for a different original purpose, are then utilised for the

[46] In *Damache v D.P.P*. [2012] 2 IR 266, paras. 40–44 Denham C.J. quoted Carney J. in DPP v Dunne [1994] 2 I.R. 537, at p. 540, who held: *"The constitutional protection given in Article 40, s.5 of the Constitution in relation to the inviolability of the dwelling house is one of the most important, clear and unqualified protections given by the Constitution to the citizen."*

purpose of biometric identification, it will be necessary to demonstrate that processing the data is strictly necessary and proportionate and in accordance with law.

The Commission recommends that search warrants issued under the Garda Síochána (Recording Devices) Act 2023 pertaining to the collection and/or recording of images and video materials in private places should authorise with particularity their subsequent use and retention for biometric identification.

The Commission recommends that where An Garda Síochána obtain images and video material from third parties for the purpose of biometric identification, such as other national or international organisations, the legal basis that allows for the processing of such personal data must be clearly set out in the Bill.

The Commission recommends that clarity is provided in the Bill as to what is meant by a national or international organisation.

'Live Feed' Biometric Identification (Head 4)

The General Scheme specifies that the use of biometric identification in the context of live feed is prohibited. This is a welcome provision; however, there is a need to define what constitutes live feed for the purposes of the Bill to ensure that the prohibition is fully operational. Commentators on facial recognition technology have noted that whilst retrospective facial recognition technology involves recorded material, "it may actually be deployed in near real time, in a manner proximate to live facial recognition. For example, surveillance camera footage may be stored to a database, and facial recognition technology applied to this recorded material. The time lag between the recording of the footage and the application of a RFR algorithm may be negligible, and if, for example, the system is configured to identify specific individuals, it could be used to generate an alert capable of influencing events in real time."[47]

The General Scheme fails to specify how long after material is recorded that it may be utilised for retrospective biometric identification. It is also noted that pursuant to Part 6 of the Garda

[47] Darragh Murray, Police Use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Law Framework (2023), pp. 3-4: https://onlinelibrary.wiley.com/doi/epdf/10.1111/1468-2230.12862.

Síochána (Recording Devices) Act 2023, An Garda Síochána can operate live footage. In this regard, particular protocols may be necessary to ensure there are no loopholes to the prohibition.

The Commission recommends that the Bill should clearly define what constitutes 'live feed' for the purposes of the Bill to ensure the prohibition of the use of biometric identification in the context of live feed is fully operational.

The Commission recommends that particular protocols should be provided in the Bill in relation to live feed obtained pursuant to Part 6 of the Garda Síochána (Recording Devices) Act 2023 to ensure that the prohibition of the use of biometric identification in the context of live feeds is fully operational.

Application and Approval (Heads 5 and 6)

Heads 5 and 6 of the General Scheme provide that the application to use biometric identification may be made to a member of An Garda Síochána not below the rank of Chief Superintendent. who is independent of the investigation to which the application relates. The General Scheme also provides that an approval may be subject to conditions as the approving member of the Garda Síochána considers appropriate, having regard to the information contained in the application. This suggests a large amount of discretion on the part of the Chief Superintendent and there is no obligation to set conditions with regard to the nature, scope and duration of the approval. Whilst the Chief Superintendent must believe on reasonable grounds that the use of biometric identification is necessary and proportionate, there is no detail provided as to the criteria against which the Chief Superintendent must determine the necessity and proportionality of the use of biometric identification.

In light of the extremely intrusive nature of biometric identification involving the use of biometric data which, given its sensitive nature, requires enhanced protection and additional safeguards, we have concerns with the application and approval process set out in the General Scheme being one that is carried out entirely internally within An Garda Síochána. Whilst there is a requirement that the approving Chief Superintendent be independent of the investigation to which the application relates, we do not consider this a sufficiently strong safeguard for a measure as intrusive as this and consider that external independent approval should be required. The provisions under Heads 5 and 6 providing for an internal Garda Síochána approval process without incorporating sufficient

oversight may not satisfy applicable human rights standards such as the right to privacy and protection of personal information. The Special Rapporteur on the right to privacy has noted that 'judicial authorization of intrusive measures generally raises the degree of privacy protection.'[48] In the case of Digital Rights Ireland, the Court of Justice of the European Union (the 'CJEU') criticised the absence of a requirement for judicial or independent administrative authorisation for access to retained data, under the Data Retention Directive.[49] Authorisation is required to limit the access and use of such data to what is strictly necessary for the purpose of attaining the objective pursued.[50] We consider that given the potential impact on the rights of the individual, approval of the use of biometric identification must only be given by an independent and impartial judge.

We also note the test laid down by the European Court of Human Rights ('ECtHR'), in the context of surveillance, when examining whether measures impermissibly interfered with the enjoyment of Article 8 ECHR. The ECtHR considers the nature, scope and duration of the possible measures; the grounds required for ordering them; the authorities competent to authorise, carry out and supervise them; and, the kind of remedy provided by national law.[51]

We have also previously highlighted the need for training for the judiciary tasked with considering authorisation of intrusive surveillance measures, and the guidance of the UN Special Rapporteur on the right to privacy in this regard:

> "[Judges] must have the knowledge and facts necessary to consider requests for such measures thoroughly and understand the potential implications of their decisions, particularly in terms of the technology to be employed and the consequences of using that technology. Hence, States should provide the required training and resources necessary to equip judges for this complicated task."52

---

[48] United Nations Human Rights Council, Report of the Special Rapporteur on the right to privacy, A/HRC/34/60 (6 September 2017) para. 28.
[49] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Joined Cases C-293/12 and C-594/12, 8 April 2014.
[50] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Joined Cases C-293/12 and C-594/12, 8 April 2014, para. 62. See also Maria Helen Murphy, Surveillance and the Law (Routledge 2019) pp. 53–54. See also IHREC, Submission on the General Scheme of the Garda Síochána (Digital Recording) Bill, p. 34.
[51] *Zakharov v Russia* [2015] ECHR 1065, para. 232.
[52] United Nations Human Rights Council, Report of the Special Rapporteur on the right to privacy, A/HRC/34/60 (6 September 2017) para. 28. See also IHREC, Submission on the General Scheme of the Garda Síochána (Digital Recording) Bill, p. 34.

The Commission recommends that judicial authorisation must be sought for the power to use biometric identification. An authorisation granted should set out the nature, scope and duration of the approval.

The Commission recommends that due to the sophistication of the technology and the developing national and international positions on artificial intelligence as well as the human rights and data protection implications, any judge involved in the authorisation process should be required to have knowledge and/or training in this area.

As highlighted under 'scope of material accessible', there is a need for the Bill to be specific regarding sources of material that can be used for the purposes of biometric identification. The provision under Head 5 should be amended to provide that the application process to use biometric identification must specify a specific and limited set of sources t to be used in a search.

The Commission recommends that all applications for the use of biometric identification should identify a specific and limited set of data sources that can be used in a biometric search.

Head 6 provides that An Garda Síochána shall create and maintain a written record concerning all applications made for the utilisation of biometric identification. These records shall contain the details of each application and the reasons why each application was approved or refused, and any further information provided for in an applicable code of practice. This is a welcome safeguard and will be important for oversight and monitoring the use of biometric identification, but it should go further to protect rights and there should be a requirement set out for this information to be provided to a suitable independent oversight body to assess compliance with human rights, equality and data protection obligations, at a minimum, on an annual basis. This would create a positive opportunity for specific ongoing learning outcomes to improve compliance, necessity and proportionality.

The Commission recommends that all written records concerning applications made for the use of biometric identification should be made available to a suitable independent oversight body at a minimum, on an annual basis to assess compliance with human rights, equality and data protection obligations.

Human Verification (Head 7)

The General Scheme includes a key safeguard that "the result of any use of biometric identification must be verified by a member of Garda Personnel prior to that result being forwarded to the investigation team". This is a welcome provision that is compliant with Article 11 LED and follows guidance provided by the European Data Protection Board that the verification process should not be fully automated.[53]

Concerns arise as to the quality of judgment in the verification process as it may depend inter alia on the quality and level of training received and any potential innate biases that may arise.[54] In addition, the General Scheme does not set out in specifics the Garda rank or Civilian grade of Garda Personnel who can verify the result. Whilst it may be intended to set out further details regarding this verification in the accompanying code of practice, consideration is needed as to whether this provision contains the adequate or sufficient oversight measures and safeguarding mechanisms to ensure the accuracy of the verification process.

The Commission recommends that the code of practice should provide detail on what is involved in the human verification process and should provide specific detail as to the role of the Garda personnel in that process, including the level of training and expertise required.

Code of Practice

The adequacy and effectiveness of safeguards in the legislation are crucial to ensure the use of technology is necessary and proportionate. Specific reference is made in the General Scheme to compliance with, the statutory code of practice (Heads 3, 4, 6, and 8) that will be required under section 47 of the Principal Act. Further provision is made with regard to the inclusion of provisions relating to the procedures to be followed by members of Garda personnel, and relating to the confidentiality, security, storage, access, retention, erasure and destruction of data gathered under the Act.

The code of practice under the General Scheme diverges from the other codes of practice in the Principal Act in that the draft codes of practice under the General Scheme must instead be laid

[53] European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (Adopted 26 April 2023).
[54] Big Brother Watch, Biometric Britain: The Expansion of Facial Recognition Surveillance (2023), p. 15; See also, Christan Meissner and John Brigham, Thirty years of investigating the own-race bias in memory for faces: A meta-analytic review, Psychology, Public Policy, and Law (2001).

before the Houses of the Oireachtas before being declared a code by Order. The other codes of practice under the Principal Act are to be sent to the Minister for review and signature.

The Commission welcomes the requirement for the draft codes of practice to be laid before the Oireachtas, particularly given the importance of the code of practice as referenced throughout the General Scheme.

The Commission welcomed the inclusion of provisions for codes of practice in the Principal Act, but highlighted the importance of the fundamental legal rules governing An Garda Síochána's powers being set down in the legislation (rather than being left to be addressed in codes of practice). This is to ensure that the fundamental legal principles are subjected to adequate and effective democratic scrutiny during the legislative process.[55] The precise scope of the powers provided to An Garda Síochána should be outlined within the legislation; while the codes of practice should set out further information on the circumstances in which the powers may be exercised and the procedures to be followed by members of An Garda Síochána when exercising these powers.

The Commission recommends that consideration should be given as to whether provisions or fundamental issues designated for inclusion in the code of practice should be more appropriately dealt with in the primary legislation.

There is also no provision in the General Scheme (nor the Principal Act) regarding what practical consequences, such as disciplinary proceedings, should occur where Garda personnel fail to observe any provision of the Act or the code of practice. Given the use of biometric identification poses a significant interferences with fundamental rights, and therefore any breach could have a profound consequence for the rights of individuals, the Commission considers this is an important omission that should be rectified and be included in the Bill.[56]

[55] IHREC, Submission on the General Scheme of the Garda Síochána (Digital Recording) Bill, p. 41.
[56] The Commission notes that Head 3(3) of the General Scheme of what became the Principal Act provided that a failure to observe any provision of this Act or of any code of practice made thereunder on the part of the member of the Garda Síochána shall render that member liable to disciplinary proceedings. This provision was omitted from the final Act.

The Commission recommends that the obligations on Garda personnel under this Bill are set out clearly and precisely. The Bill should also set out clearly the consequences that follow from a failure to observe a provision of the Act or the code of practice.

It is also not clear in the General Scheme (nor the Principal Act) whether provisions related to recording technologies and facial recognition technology will not become operational until the Minister publishes a code of practice and it comes into operation. This omission is concerning as it may mean these technologies are utilised in the community before the codes of practice are published or the data protection and human rights impact assessments are carried out, and before the Garda Members and Staff have read and understood the codes of practice.

The Commission recommends that it should be explicitly stated that the use of biometric identification will not become operational until the code of practice is published.