SUBMISSION

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

Irish Human Rights and Equality Commission

April 2022

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

Published by the Irish Human Rights and Equality Commission.

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.

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

Irish Human Rights and Equality Commission

April 2022

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

Contents

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]

The Commission welcomes the opportunity to provide the Minister for Justice with its submission on the General Scheme of the *Garda Síochána (Digital Recording) Bill* (the 'General Scheme'). The Commission and its predecessor body, the Irish Human Rights Commission ('the IHRC'), have previously highlighted a range of human rights and equality concerns relating to the recording and storing of images, and the adequacy and effectiveness of safeguards in Irish law surrounding the use of CCTV cameras for the investigation or detection of offences.[2] The Commission has a number of specific concerns with the proposals under the General Scheme to provide a legislative basis for the deployment and use of body-worn cameras and other recording devices by An Garda Síochána and the extension of the circumstances in which Closed Circuit Television ('CCTV') and Automatic Number Plate Recognition ('ANPR') devices may be used by An Garda Síochána. While the Commission will have consultative role in the development of the codes of practice under the legislation, the Commission's concerns extend beyond the parts of the legislation where the codes of practice are required. The Commission recommends a number of strengthened safeguards in the use of these technologies for the prevention of

[1] Section 10(2)(c) of the Irish Human Rights and Equality Commission Act 2014.

[2] The Commission made a submission to the Department of Justice in February 2020 with preliminary observations on this legislation; see IHREC, Preliminary Observations of the Irish Human Rights and Equality Commission in relation to the forthcoming Garda Síochána (Recording of Images) Bill: Submission to the Department of Justice and Equality (18 February 2020). See also IHRC, Observations on the Criminal Justice (Surveillance) Bill 2009 (May 2009); IHREC (designate), Review of the Garda Síochána Act 2005 (April 2014) para. 35; IHREC, Memorandum: Review of the Law on Access to Communication Data (13 June 2016); IHREC, Submission to the Commission on the Future of Policing (February 2018) pp. 18–19; IHREC, Submission to the United Nations Human Rights Committee on the List of Issues for the Fifth Periodic Examination of Ireland (August 2020) pp. 47–48.

crime and disorder.[3] The Commission remains available to assist the Minister if further scrutiny of the General Scheme is required and on any specific issue that may arise.

This submission focusses on the following matters:

- Intrusion on rights for law enforcement purposes;
- Equality implications in the use of technology;
- Access and retention of data;and
- Adequacy of safeguards and oversight mechanisms.

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

- Privacy;
- Protection of personal data;
- The inviolability of the home;
- Equality;
- Guarantee of a fair trial/proceeding;
- Adequacy of remedy/procedural fairness;
- Freedom of assembly; and
- Freedom of expression.

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;[4] however, the State must endeavour to balance the different rights at play.

The Commission notes that this legislation is being developed at the same time as the Data Protection Commission ('the DPC') is carrying out inquiries into surveillance of citizens for law enforcement purposes by An Garda Síochána and by the 31 local authorities through

[3] In accordance with human rights law, the State is required to provide adequate and effective safeguards to ensure a balance between the rights of individuals and the interest of the State in investigating crime; see *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* [GC], no. 931/13, ECHR 2017 (extracts), §§ 137.

[4] 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.

the use of technologies such as CCTV, body-worn cameras, ANPR, and drones.[5] In 2019, the DPC made 13 findings in relation to infringements of the *Data Protection Act 2018*, after an inquiry into Garda-operated CCTV schemes under section 38(3)(a) of the *Garda Síochána Act 2005*.[6] While the inquiries into the 31 local authorities are still ongoing,[7] the DPC has identified:

> "significant data protection compliance issues in relation to matters such as the use of covert CCTV cameras, the use of CCTV to detect illegal dumping, the use of body-worn cameras, dash-cams, drones and ANPR cameras, CCTV cameras at amenity walkways or cycle-tracks, and a lack of policies and data protection impact assessments."[8]

In its inquiries, the DPC raised data protection and privacy concerns with the increased deployment of ANPR and the use of CCTV devices which may be able to zoom in on individuals and their property from a greater distance.[9] The DPC's inquiry relating to Limerick City and County Council found concerning practices in the sharing of personal data

---

[5] In June 2018, the DPC launched own volition inquiries, under the *Data Protection Act 2018*. The purpose of these inquiries is to probe whether the processing of personal data that occurs with the use of these technologies is compliant with data protection law. The inquiries are also examining the legal basis underpinning the use of these surveillance technologies for law-enforcement purposes. The inquiries have been split into a number of modules, the first focussing on the use of video surveillance by the 31 local authorities and the second focussing on the use of video surveillance by An Garda Síochána. See Data Protection Commission, Annual Report 2018 (2019) pp. 45–46; Data Protection Commission, Annual Report 2019 (2020) pp. 49–50; Data Protection Commission, DPC Ireland 2018–2020 Regulatory Activity under GDPR (2020) pp. 63–72; Data Protection Commission, Annual Report 2020 (2021) pp. 54–55.

[6] Data Protection Commission, Decision of the Data Protection Commission regarding CCTV Schemes Authorised under Section 38(3)(a) of the Garda Síochána Act 2005 (23 August 2019). "These infringements relate to a number of matters such as governance issues (including record-keeping of downloads, retention periods, training, auditing of access logs); transparency in relation to informing the general public by signage and other means; the absence of data processor contracts; and the deployment of ANPR cameras on one Garda scheme in the absence of the implementation of appropriate data protection policies by An Garda Síochána and its failure to carry out a data protection impact assessment before rolling out the scheme." See Data Protection Commission, Annual Report 2019 (2020) pp. 49–50.

[7] The Data Protection Commission has issued decisions related to Kerry County Council, Waterford City and County Council and Limerick City and County Council. See Data Protection Commission, Decision of the Data Protection Commission relating to Kerry County Council (25 March 2020); Data Protection Commission, Decision of the Data Protection Commission relating to Waterford City and County Council (21 October 2020); Data Protection Commission, Decision of the Data Protection Commission relating to Limerick City and County Council (9 December 2021).

[8] Data Protection Commission, Annual Report 2020 (2021) p. 55. See also Data Protection Commission, DPC Ireland 2018–2020 Regulatory Activity under GDPR (2020) pp. 71–72.

[9] Data Protection Commission, Annual Report 2020 (2021) pp. 54–55.

captured by CCTV and ANPR with An Garda Síochána and providing members of An Garda Síochána with access to CCTV cameras or monitoring centres without a valid legal basis.[10] In particular, one of the findings was that the Council failed to demonstrate it had a legal basis to conduct targeted surveillance on behalf of An Garda Síochána.[11] The Commission is of the view that the development and implementation of this legislation, including the publishing of codes of practice under the legislation, should take account of the findings of the DPC's inquiries into the use of these technologies.

The Commission also recognises that the development of these legislative proposals forms part of a wider programme of legislative reform of policing powers and structures in the State, alongside the *Garda Síochána (Powers) Bill* and the *Policing, Security and Community Safety Bill*. In implementing such legislative reforms, it is important to recall the Commission on the Future of Policing's assertion that:

> "human rights are the foundation and purpose of policing".[12]

[10] Data Protection Commission, Decision of the Data Protection Commission relating to Limerick City and County Council (9 December 2021).
[11] Data Protection Commission, Decision of the Data Protection Commission relating to Limerick City and County Council (9 December 2021) paras. 6.214–6.217.
[12] 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 right to privacy

Commentary and case law on the human rights implications of the use of technological devices for law enforcement purposes have primarily focussed on balancing their use with the right to privacy. The right to privacy was recognised in *Kennedy v Ireland* as an unenumerated right under Article 40.3 of the Constitution of Ireland.[13] The right to respect of private and family life, home and communications is also protected under international law.[14]

The right to privacy is not an unqualified right, in *Kennedy v Ireland*, Hamilton P. stated that its:

> "exercise may be restricted by the constitutional rights of others, by the requirements of the common good and is subject to the requirements of public order and morality."[15]

Under the Constitution, an interference with any right, including the right to privacy must be proportionate.[16] In *Kane v Governor of Mountjoy Prison*, the Supreme Court stated that an individual has a right to enjoy privacy and that the absence of a specific justification for surveillance could constitute an infringement of his constitutional right to privacy.[17] In *DPP v Idah*, the Court of Criminal Appeal stated that there:

> "can be no doubt that the State may make incursions into the right of privacy in accordance with law"

[13] [1987] IR 587.
[14] 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').
[15] *Kennedy v Ireland* [1987] IR 587, at pp. 592–593.
[16] *Meadows v Minister for Justice, Equality and Law Reform* [2010] 2 IR 701.
[17] *Kane v Governor of Mountjoy Prison* [1988] 1 IR 757.

Nevertheless the:

> "law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which public authorities are entitled to resort to such covert measures and it must provide necessary safeguards for the rights of individuals potentially affected."[18]

The right to privacy is similarly qualified under the Charter[19] and Article 17 of the *International Covenant on Civil and Political Rights* ('ICCPR')[20]. The right to privacy is also subject to restrictions under Article 8(2) ECHR, which allows the State to justify interference with this right where such interference is in accordance with law and is necessary in a democratic society in the interests of national security, public safety, and for the prevention of disorder or crime among other grounds.[21]

The European Court of Human Rights ('the ECtHR') has developed a threefold test to assess whether an interference is in accordance with the law: first: the interference must have a basis in national law; second: the law must be accessible; and third: the law must be must be sufficiently foreseeable to enable individuals to act in accordance with the law.[22] Importantly, this does not mean always being advised in advance that one's data is about to be accessed, as this could defeat the purpose; rather, it means that the rules of the system are clear to all.[23] The ECtHR have stated that for an interference to be regarded as necessary in a democratic society, it should be proportionate to the legitimate aim pursued and there

---

[18] *Sunny Idah v The DPP* [2014] IECCA 3, para. 37.

[19] Article 52(1) of the Charter provides that: "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."

[20] Article 17(1) provides that no one shall be subjected to arbitrary or unlawful interference with their privacy.

[21] Article 8(2) provides that: "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[22] *Silver and Others v the United Kingdom*, 25 March 1983, Series A no. 61, § 87.

[23] The ECtHR have stated that citizens should not be able to predict when surveillance will occur, but legislation "must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures"; see *Szabó and Vissy v Hungary*, no. 37138/14, 12 January 2016, § 62.

should be adequate and effective safeguards in place to prevent arbitrary interferences with rights.[24]

The ECtHR has recognised that the systematic collection and the storing of visual data of a person in a public place may raise issues of privacy under Article 8 ECHR.[25] In *S. and Marper v the United Kingdom*, the ECtHR held:

> "The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 ... The subsequent use of the stored information has no bearing on that finding ... However, in determining whether the personal information retained by the authorities involves any ... private-life [aspect] ..., the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained ...".[26]

The United Nations Special Rapporteur on the right to privacy has set out a four-fold test that any legitimate infringement of privacy cannot be:

> "(a) arbitrary and must be provided for by law;
>
> (b) for any purpose but for one which is necessary in a democratic society;
>
> (c) for any purpose except for those of "national security or public safety, public order, the protection of public health or morals or the protection of the rights and freedoms of others"; and,
>
> (d) the measure must be proportionate to the threat or risk being managed."[27]

In its General Comment on the right to privacy, the United Nations Human Rights Committee stated that:

> "relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted"

---

[24] *A.-M.V. v Finland*, no. 53251/13, 23 March 2017, §§ 82-84.
[25] *Peck v the United Kingdom*, no. 44647/98, ECHR 2003-I, § 59; *Perry v the United Kingdom*, no. 63737/00, ECHR 2003-IX (extracts), § 38.
[26] S*. and Marper v the United Kingdom*, judgment (Grand Chamber) of 4 December 2008, § 67
[27] United Nations Human Rights Council, Report of the Special Rapporteur on the right to privacy, A/HRC/40/63 (16 October 2019) para. 18.

and

> "[a] decision to make use of such authorised interference must be made only by the authority designated under the law, and on a case-by-case basis."[28]

The protection of personal data

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 principles of necessity and proportionality apply to the processing of data for law enforcement purposes.[29] The right to protection of personal data has been recognised under Article 8 ECHR,[30] and is also expressly enshrined in Article 8 of the Charter[31].

The inviolability of the dwelling

The legislation provides that a member of An Garda Síochána may operate a recording device or a body-worn camera:

> "in a public place or any other place under a power of entry authorised by law or to which or in which he or she was expressly or impliedly invited or permitted to be."[32]

This has implications for the inviolability of the dwelling protected under Article 40.5 of the Constitution.[33] The Supreme Court has emphasised the importance of the vindication and protection of this constitutional right for the quiet enjoyment of our homes and therefore any potential interference with this enjoyment is to be heavily circumscribed in law.[34] The

---

[28] United Nations Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy) (1988). See also United Nations Human Rights Council, The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37 (30 June 2014).
[29] Section 71(5)(b) of the *Data Protection Act 2018*.
[30] *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* [GC], no. 931/13, ECHR 2017 (extracts), §§ 133-134.
[31] Article 8 provides: "1. Everyone has the right to protection of personal data concerning him or her; 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified; 3. Compliance with these rules shall be subject to control by an independent authority".
[32] Under Head 5(1) and Head 6(1) of the General Scheme.
[33] "The dwelling of every citizen is inviolable and shall not be forcibly entered save in accordance with law."
[34] Per Denham C.J. in *Damache v DPP, Ireland & The Attorney General* [2012] 2 IR 266, paras. 40–44; quoting Carney J., in *Director of Public Prosecutions v Dunne* [1994] 2 I.R. 537, at p. 540, who stated: "The constitutional protection given in Article 40, s. 5 of the Constitution in relation to the inviolability of the

right to respect for the home is also protected under Article 8 ECHR. In regard to the legality of entry and searches, the ECtHR have concentrated on the requirements that searches be lawful and accompanied by appropriate safeguards against misuse.[35]

Equality and non-discrimination

The legislative basis for the use of recording devices, body-worn cameras, CCTV and ANPR gives rise to equality issues, particularly with minority groups' experience of racial profiling in Ireland.[36] The United Nations Special Rapporteur on the right to privacy has noted that:

> "gender, race, class, social origin, religion, opinions and their expression can become factors in determining who is watched in society, and make certain individuals more likely to suffer violations of their right to privacy".[37]

The use by police, with no objective and reasonable justification, of 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, migration status, or work or other status in surveillance or investigation activities constitutes racial profiling.[38] The United Nations Committee on the Elimination of Racial Discrimination have warned that racial profiling can lead to the overcriminalisation of

---

dwellinghouse is one of the most important, clear and unqualified protections given by the Constitution to the citizen."

[35] See for example *Funke v France* [1993] 16 EHRR 287.

[36] An internal study found negative attitudes amongst significant sections of members of An Garda Síochána towards minority ethnic groups. The Commission has noted reports which indicate that minority ethnic communities can be under-protected and over-policed, including due to racial profiling. There are reports as well of racial profiling in the use of stop and search powers, including reports from young minority ethnic people. See European Commission against Racism and Intolerance, ECRI Report on Ireland (fifth monitoring cycle): Adopted on 2 April 2019 (2019) CRI (2019)18, para 52; Conor Gallagher, Gardaí have negative view of Travellers, survey finds (The Irish Times, 20 August 2020). See also IHREC, Submission to the Commission on the Future of Policing (February 2018) pp. 10-13; IHREC, Ireland and the Convention on the Elimination of Racial Discrimination: Submission to the United Nations Committee on the Elimination of Racial Discrimination on Ireland's Combined 5th to 9th Report (October 2019) pp. 136-138; IHREC, Submission to the United Nations Human Rights Committee on the List of Issues for the Fifth Periodic Examination of Ireland (August 2020) p. 47; IHREC, Developing a National Action Plan Against Racism: Submission to the Anti-Racism Committee (August 2021).

[37] United Nations Human Rights Council, Report of the Special Rapporteur on the right to privacy, A/HRC/40/63 (16 October 2019) para. 76.

[38] 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).

certain groups[39] and the reinforcing of stereotypical associations between crime and ethnicity.[40] The practice of racial profiling violates the principles of non-discrimination and equality before the law,[41] 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.[42]

Fair trial rights and procedural fairness

The right to a fair trial and fair procedures are protected under Articles 34, 38 and 40.3 of the Constitution;[43] as well as under Article 47 of the Charter, Article 6 ECHR and Article 14 ICCPR. For a trial to be regarded as fair, a person charged must be provided with certain rights, including:

> "to be adequately informed of the nature and substance of the accusation, to have the matter tried in his presence by an impartial and independent court or arbitrator, to hear and test by examination the evidence offered by or on behalf of his accuser, to be allowed to give or call evidence in his defence, and to be heard in argument or submission before judgment be given."[44]

The fundamental requirement of basic fairness applies from the time of arrest, and any breach of this requirement can lead to an absence of a trial in due course of law.[45] In *D v Director of Public Prosecutions*, it was held that:

---

[39] The Committee has recognised that specific groups, such as migrants, refugees and asylum seekers, people of African descent, indigenous peoples, and national and ethnic minorities, including Roma, are the most vulnerable to racial profiling. 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) para. 11.

[40] 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) para. 30.

[41] 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.

[42] 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).

[43] Per O'Higgins C.J in *State (Healy) v Donoghue* [1976] IR 325, at pp. 349–350.

[44] ibid.

[45] *DPP v Gormley and White* [2014] 2 IR 591, para. 82.

"on a hierarchy of constitutional rights there is no doubt that the applicant's right to fair procedures is superior to the community's right to prosecute".[46]

Right to an effective remedy

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. An effective remedy must be known and accessible to anyone who has an arguable claim that their rights have been violated.[47] An effective remedy includes a prompt, thorough and impartial investigation of alleged violations of rights.[48] A failure by a state to investigate allegations of violations could in and of itself give rise to a separate violation of the rights of individuals.[49] Individuals whose rights have been violated must be provided with reparation which involves appropriate compensation, restitution, rehabilitation and measures of satisfaction such as public apologies, guarantees of non-repetition and changes in relevant laws and practices.[50]

Freedom of assembly and freedom of expression

The potential widespread public use of the technologies, both current and future, for the policing of protests and public assemblies may result in a chilling effect on the exercise of the rights of freedom of assembly and freedom of expression. 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[51] and Article 21 ICCPR[52] which provide

---

[46] [1994] 2 IR 465.
[47] United Nations Human Rights Council, The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37 (30 June 2014) para. 40.
[48] United Nations Human Rights Council, The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37 (30 June 2014) para. 41.
[49] United Nations Human Rights Committee, General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, CCPR/C/21/Rev.1/Add.13 (26 May 2004) para. 15.
[50] United Nations Human Rights Committee, General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, CCPR/C/21/Rev.1/Add.13 (26 May 2004) para. 16.
[51] "No restrictions shall be placed on the exercise of these rights other than such as are prescribed by law and are 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. This Article shall not prevent the imposition of lawful restrictions on the exercise of these rights by members of the armed forces, of the police or of the administration of the State."
[52] "No restrictions may be placed on the exercise of this right other than those imposed in conformity with the law and which are necessary in a democratic society in the interests of national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others."

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.

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. This right includes the freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. As the exercise of this right carries special duties and responsibilities, it may be subject to certain conditions or restrictions which are provided by law and necessary in a democratic society.[53]

In the context of public assemblies, the United Nations High Commissioner for Human Rights has said that authorities should be transparent in their use of recording and facial recognition technology and should notify members of the public when they are or may be recorded and/or when their images may be processed in a facial recognition system.[54] The High Commissioner for Human Rights recommended that States:

> "[r]efrain from recording footage of assembly participants, unless there are concrete indications that participants are engaging in, or will engage in, serious criminal activity, and such recording is provided by law, with the necessary robust safeguards".[55]

---

[53] Article 10(2) of the ECHR provides: "The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."
Article 19(3) of the ICCPR sets out: The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals.

[54] 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. 37.

[55] 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(i).

The United Nations Special Rapporteur on the rights to freedom of peaceful assembly and of association has stated that surveillance against individuals exercising their rights of peaceful assembly and association 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."[56]

[56] United Nations Human Rights Council, Rights to freedom of peaceful assembly and of association: Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, A/HRC/41/41 (17 May 2019) para. 57.

Observations on the General Scheme

Adequacy and effectiveness of safeguards within the legislation

The General Scheme proposes radical change in the area of the recording of personal information by members of An Garda Síochána. The General Scheme attempts to reconcile the conflict between allowing law enforcement to get on with the difficult job of protecting the public and ensuring that rights are not dissolved to disappearance. The recording of persons by law enforcement personnel is generally lawful under the Constitution and international human rights law, subject to the requirement that:

- the interference with rights is based on law (i.e. clear, foreseeable and accessible);
- pursues a legitimate aim;
- is proportionate to that aim; and
- necessary in a democratic society.

While recognising that the lawful collection and use of personal data for law enforcement purposes is important for the prevention of crime, maintenance of public order and in the interests of national security; the Commission would draw attention to the '*Practical guide on the use of personal data in the police sector*' produced by the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, which provides that:

> "All data processing has to comply with the necessity, proportionality and purpose limitation principles. This implies that personal data processing within the police should be based on predefined, clear and legitimate purposes set out in the law; it should be necessary and proportionate to these legitimate purposes and should not be processed in a way incompatible with those purposes. Data processing should be carried out lawfully, fairly and in a transparent manner. Personal data within the police should furthermore be adequate, relevant and non-excessive in relation to the

purposes. Finally they should be accurate and up-to-date to ensure the highest data quality possible."[57]

Accordingly:

> "[t]he collection of personal data for police purposes should be limited to what is necessary and proportionate for the prevention of a real danger or the prevention, investigation and prosecution of a specific criminal offence."[58]

While being in a public area may mean enjoying a lesser degree of privacy, individuals should not be deprived of their rights.[59] The Commission is of the opinion that the more serious the intrusion is on the rights of an individual, the higher the justifying threshold should be for the use of the technology.

The Commission is of the view that the question of whether the use of these technologies and the collection of personal data for law enforcement purposes are consistent with the principles of legality, necessity and proportionality will require consideration of the proposed codes of practice under Head 7 and Head 10 and the analysis contained within the proposed Data Protection Impact Assessments and Human Rights Impact Assessments. While the General Scheme provides for data protection and human rights impact assessments to be conducted with regard to the matters set out in Parts 2 and 3 of the General Scheme, there is currently no requirement to conduct these assessments with regard to any of the matters under the other parts of the General Scheme. The Commission recommends that consideration be given to broadening out the reach of data protection and human rights impact assessments to other parts of the General Scheme due to the proposed interference of the General Scheme with the fundamental rights of individuals. While the full implication of the provisions of this General Scheme for the enjoyment of human rights will not be apparent until the publication of draft codes of practice and the data protection and human rights impact assessments, the Commission considers that there are measures that can be taken now within the drafting process to strengthen the safeguards for individual rights within the legislation; which will be detailed below in

---

[57] Council of Europe, Practical guide on the use of personal data in the police sector (2018) p. 2.
[58] Council of Europe, Practical guide on the use of personal data in the police sector (2018) p. 2.
[59] European Commission for Democracy through Law (Venice Commission, Opinion on video surveillance in public places by public authorities and the protection of human rights, adopted by the Venice Commission at its 70th Plenary Session (2007) para. 25.

relevant subsections. The Commission would particularly emphasise the importance of ensuring that the rights of persons who may be the subject of a recording by a device or who may face criminal proceedings due to recordings or images obtained by the means under the General Scheme are adequately and effectively addressed under this legislation. The recent Supreme Court judgement in *The People (DPP) v Hannaway and Ors*[60] is instructive in regard to the safeguards required for the appropriate balancing of rights with regard to surveillance, under the *Criminal Justice (Surveillance) Act 2009*; O'Malley J states:

> "In my view, the safeguards in this legislation lie in the requirements that surveillance may not be carried out other than on foot of an authorisation granted by an independent judge, for the purposes specified in the Act and having due regard to the rights of the individuals concerned and the proportionality of the proposed measures; in the obligation imposed on all relevant persons (not just the Minister) to ensure that the information gathered as a result of surveillance is used only for the permitted purposes and is kept securely; and in the oversight functions of the Referee and the designated judge of the High Court."[61]

The Commission recommends that the examination of the General Scheme includes consideration of whether the legislative proposals are provided by law (clear, foreseeable and accessible), have a legitimate aim, are necessary in a democratic society and proportionate to that aim. A particular focus should be on the adequacy of the safeguards to mitigate against intrusions on the fundamental rights of individuals with the use of recording technologies under the General Scheme.

The Commission recommends that consideration be given to requiring a Data Protection Impact Assessment and a Human Rights Impact Assessment be conducted under Part 4 and Part 5 of the General Scheme.

[60] [2021] IESC 31.
[61] ibid, para. 111.

Interpretation of key terms and application of the Act (Head 2 and Head 3)

Scope of the meaning of recording device and emerging technologies (Head 2)

The Commission notes that the definition of 'recording device'[62] under Head 2 is intended to be broad enough to encompass current technologies and emerging technologies in the future.[63] This is an important safeguard as the legislation and the associated codes of practice have to be adaptable to keep pace with technological advancements and developments. The nature of this legislation means that it will be addressing future technologies whose operation and pervasiveness one cannot actually envisage at this juncture. This may mean that certain laws and legal tests, such as those relating to the exclusion of illegally or unconstitutionally obtained evidence, will have to be further refined to take account of the emerging technologies. As the definition of 'recording device' is quite broad by design, it will undoubtedly impact rights; therefore, it will be important for the courts to keep pace with current technologies and technological advancements such as the recording facilities of personal computers, wearable devices or other devices (including in private spaces), live audio transcription software or intelligent personal assistant, cloud-based voices services like Alexa.

Due to the potential far-reaching human rights implications of emerging technologies, the Commission is of the opinion that the legislation should include strengthened safeguards to address significant changes in technological evolution, including developments in other jurisdictions or under consideration at EU level. Consideration should be given to including safeguards within the legislation requiring legislative review or amendment if there is such a significant technological evolution. These strengthened safeguards and laws are necessary to keep pace with the advancements in technology, otherwise emerging technologies pose a threat of intruding more and more on individual rights. The Commission is also of the view that emerging technologies should be subject to an independent oversight or advisory framework. In this regard, the Commission would draw attention to Scotland's independent advisory group on emerging technologies in policing[64] whose purpose is:

---

[62] "recording device" means a non-fixed device capable of recording or processing, including through the use of Automatic Number Plate Recognition, visual images, on any medium, from which a visual image or moving visual images may be produced and includes any accompanying sound or document.

[63] Explanatory notes for Head 2 of the General Scheme.

[64] See https://www.gov.scot/groups/independent-advisory-group-on-emerging-technologies-in-policing/.

> "To report to the Cabinet Secretary for Justice on whether the current legal or ethical frameworks need to be updated in order to ensure Police Scotland's use of emerging technologies in relation to operational policing is compatible with equality and human rights and other applicable legislation and best practice; and to provide specific recommendations or potential outputs to address any identified issues."

The Commission recommends that the legislation should include sufficient safeguards to address emerging technologies and technological developments; such safeguards could include legislative amendment or review.

The Commission recommends that emerging technologies be subject to independent and effective oversight by either an existing body, such as the Policing Authority, or the establishment of a new body, such as an independent group on emerging technologies.

Facial Recognition (Head 2)

The General Scheme is silent on whether the use of facial recognition technologies is permitted or excluded under the provisions. This omission is concerning as the increasing global use of facial recognition and surveillance technologies to track and control specific demographic groups raises concerns with respect to many human rights, including the right to privacy, freedom of peaceful assembly and association, freedom of expression and freedom of movement.[65] 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. There are also 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.[66] The Commission considers that additional safeguards are required 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*.

---

[65] 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) para. 35. See also European Parliamentary Research Service, Regulating facial recognition in the EU (September 2021) p. 6.

[66] 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) para. 35. See also European Parliamentary Research Service, Regulating facial recognition in the EU (September 2021) p. 7.

The European Commission's proposal for a Regulation laying down harmonised rules on artificial intelligence,[67] 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.[68] If facial recognition technology is used, each individual use shall be subject to a prior authorisation granted by a judicial authority or by an independent administrative authority.[69]

In a joint opinion on the European Commission's proposal, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) called for a ban on any use of artificial intelligence for automated recognition of human features, such as faces, in publicly accessible spaces.[70] They also recommend 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.[71]

---

[67] See 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, 2021/0106 (COD) (April 2021).

[68] The objectives are: (i) the targeted search for specific potential victims of crime, including missing children; (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack; (iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State. The use shall also take into account the following elements: (a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system; (b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences. See Article 5(1)(d) and Article 5(2) of the 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, 2021/0106 (COD) (April 2021).

[69] The competent judicial or administrative authority shall only grant the authorisation where it is satisfied, based on objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system at issue is necessary for and proportionate to achieving one of the objectives specified in paragraph 1, point (d), as identified in the request. In deciding on the request, the competent judicial or administrative authority shall take into account the elements referred to in Article 5, paragraph 2. See Article 5(3) of the 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, 2021/0106 (COD) (April 2021).

[70] European Data Protection Board, 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 (21 June 2021, press release).

[71] See also the Consultative Committee of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data's '*Guidelines on Facial Recognition*' which provide that the "use of facial recognition for the sole purpose of determining a person's skin colour, religious or other beliefs, sex, racial or ethnic origin, age, health condition or social condition should be prohibited unless

The UN High Commissioner for Human Rights recommends that states:

> "[i]mpose 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 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;
>
> (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 suppliers of 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

---

appropriate safeguards are provided for by law to avoid any risk of discrimination"; Consultative Committee of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Guidelines on Facial Recognition (January 2021) p. 5.

protection and non-discrimination requirements be included in the design and the implementation of these technologies".[72]

The Commission recommends that the legislation explicitly set out whether technology capable of facial recognition is covered under its provisions. If facial recognition technologies are permitted, the Commission recommends that the human rights and equality implications of these technologies be subject to independent and effective scrutiny, by either an existing body, such as the Policing 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, such as the European Commission rules on artificial intelligence.

Obligations for Gardaí in using the technology (Head 3)

Head 3(3) provides 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."

The Commission is concerned that the phrase 'shall render that member liable' is unclear on what will happen if a member of An Garda Síochána breaches the Act or a code of practice. As currently drafted, it appears that there may be no practical consequence if the Act or code of practice is breached. This is worrying from a human rights and equality perspective as the findings of the DPC's inquiries into An Garda Síochána and local authorities illustrates that the practices of An Garda Síochána in relation to this technology can breach relevant Acts and codes of practice.[73] The different technologies, covered in the General Scheme,

---

[72] 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).

[73] Data Protection Commission, Decision of the Data Protection Commission regarding CCTV Schemes Authorised under Section 38(3)(a) of the Garda Síochána Act 2005 (23 August 2019); Data Protection Commission, Decision of the Data Protection Commission relating to Kerry County Council (25 March 2020); Data Protection Commission, Decision of the Data Protection Commission relating to Waterford City and

pose significant interference with the fundamental rights of individuals, and therefore a breach can have profound consequences for the rights of individuals. While it is intended for the Act and codes of practices to set out the duties and responsibilities which the members of An Garda Síochána have to comply with, the reality of implementing this legislation may be different as shown by the findings of the DPC's inquiries. Accordingly, this legislation has to be clear on the obligations on the members of An Garda Síochána in using the technology covered under the legislation and the practical consequences which follow from a breach of the Act or code of practice.

The Commission recommends that the Heads of the General Scheme be revised to ensure that the obligations on the members of An Garda Síochána under this legislation are clear and precise, and that the General Scheme sets out clearly the consequences which follow from a failure to observe a provision of the Act or any code of practice.

Recording by the Garda Síochána for specified purpose (Part 2)

Body-worn cameras (Head 6)

The proposal to deploy body-worn cameras arose from a recommendation of the Commission on the Future of Policing in Ireland.[74] Body-worn cameras can be an important resource for promoting accountability and transparency for human rights violations, improving the quality of engagements, and modifying police behaviour.[75] Body-worn cameras have a human rights value as they can offer protection and vindicate the rights of members of An Garda Síochána and members of the public who they engage with by acting as a deterrent against the misuse of force and discrimination.[76] Body-worn cameras can be an important policing resource by enhancing trust between communities and An Garda

---

County Council (21 October 2020); Data Protection Commission, Decision of the Data Protection Commission relating to Limerick City and County Council (9 December 2021).

[74] The report of the Commission on the Future of Policing in Ireland recommended that An Garda Síochána should develop a plan to deploy body-worn cameras. The Commission on the Future of Policing in Ireland noted that body-worn cameras "can help to improve front line capability with the accurate recording of incidents, expedite analysis, enhance situational awareness, and sometimes protect police from harm". See Commission on the Future of Policing in Ireland, The Future of Policing in Ireland (2018) p. 79.

[75] European Union Agency for Fundamental Rights, Preventing unlawful profiling today and in the future: A guide (2018) pp. 85–86; 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. 12.

[76] European Union Agency for Fundamental Rights, Preventing unlawful profiling today and in the future: A guide (2018) p. 82; Cynthia Lum et al., 'Body-worn cameras' effects on police officers and citizen behaviour: A systematic review' (2020) Campbell Systematic Reviews, 1–40, p. 5.

Síochána.[77] If operated correctly, body-cameras can provide an objective record of an interaction.[78] Therefore, if subject to the necessary safeguards body-worn cameras can be a valuable tool in policing.

However, there is a discussion around the effectiveness of body-worn cameras in reducing crime or the use of force by police officers. In particular, a review of 70 empirical studies of body-worn cameras found that the effects of body-worn cameras have been overestimated, including the impact on police and citizens behaviour.[79] In the United Kingdom, a 2015 study on the use of 500 body-worn cameras by 814 Metropolitan police officers found:

> "no overall impact on the number or type of stop and searches conducted; no effect on the proportion of arrests for violent crime; and no evidence that the cameras changed the way officers dealt with either victims or suspects".[80]

Body-worn cameras may also have negative consequences for relations between the Garda Síochána and minority groups, particularly if they feel they are being specifically targeted.[81] The use of body-worn cameras also raises fundamental human rights concerns. Regard has to be given to the intrusion on the right to privacy of an individual, specifically if persons are recorded in distressing circumstances or if they are victims of domestic violence, sexual violence or rape.[82] Due to the implications for the rights of individuals, in using body-worn cameras, the legislation should include adequate safeguards to ensure that body-worn cameras are used in a legal and legitimate manner.[83] A particular focus should be on the

---

[77] European Union Agency for Fundamental Rights, Preventing unlawful profiling today and in the future: A guide (2018) p. 82.

[78] Cynthia Lum et al., 'Body-worn cameras' effects on police officers and citizen behaviour: A systematic review' (2020) Campbell Systematic Reviews, 1–40, p. 3.

[79] Cynthia Lum et al., 'Research on Body-worn cameras, What we know, what we need to know' (2019) Criminology and Public Policy, 1–26. See also Cynthia Lum et al., 'Body-worn cameras' effects on police officers and citizen behaviour: A systematic review' (2020) Campbell Systematic Reviews, 1–40.

[80] European Union Agency for Fundamental Rights, Preventing unlawful profiling today and in the future: A guide (2018) p. 87.

[81] European Union Agency for Fundamental Rights, Preventing unlawful profiling today and in the future: A guide (2018) p. 88.

[82] Amnesty International, Use of Force: Guidelines for Implementation of the UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials (August 2015) p. 81.

[83] United Nations Human Rights Council, Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Christof Heyns: Use of information and communications technologies to secure the right to life, A/HRC/29/37 (24 April 2015) para. 119; 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. 12.

policing of protests and public assemblies, as body-worn cameras and recording devices can have a chilling effect on the exercise of the right to freedom of assembly.[84]

The Commission is also concerned about the potential impacts that the use of footage from body-worn cameras in criminal proceedings may have on the right to a fair trial. With respect to the reliability of body-worn camera footage for criminal investigations, concerns have been raised about the accuracy of recordings.[85] For example, in Baltimore, police officers were accused of staging drug discoveries for their body cameras which raises questions about the probative value of these recordings and their admissibility in criminal proceedings.[86]

The Commission recommends that the development of this legislation requires careful examination of whether the interference with the right to privacy, protection of data, freedom of expression and assembly, and right to a fair trial that is presented by the use of body-worn cameras is proportionate and necessary in the prevention of disorder or crime.

If the operation of body-worn cameras is provided for under the legislation, the Commission recommends each individual use of a body-worn camera should be subject to independent oversight to ensure its use remains proportionate, and in compliance with human rights and equality principles.

Use of drones (Head 5)

The Explanatory Notes for Head 5 provide that the definition of recording devices may include drones. The use of drones raises implications for the rights of individuals, as drones have the ability to extensively capture a location which means that images of individuals who have no links to a suspected offence may be recorded and stored as well as images of

[84] Recording peaceful assembly participants in a context and manner that intimidates or harasses is an impermissible interference on the exercise of rights, including freedom of assembly, association and expression. See United Nations Human Rights Council, 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, A/HRC/31/66 (4 February 2016) para. 76. See also OSCE Office for Democratic Institutions and Human Rights, Handbook on Monitoring Freedom of Peaceful Assembly (2020) p. 62.

[85] Upturn, 'The Illusion of Accuracy: How body-worn camera footage can distort evidence' (2017).

[86] Jeffrey Bellin and Shevarma Pemberton, 'Policing The Admissibility Of Body Camera Evidence' (2019) 87(4) Fordham Law Review 1425, pp. 1427, 1441.

private dwellings. The Data Protection Commission has stated that drones, by their nature, pose:

> "a high risk to the rights and freedoms of individuals."[87]

The human rights and equality implications of drones have been recently considered by the Scottish Parliament's Justice Sub-Committee on Policing which published a report on 18 March 2021 on '*Police Scotland's use of remote piloted aircraft systems and body worn video cameras*'.[88] The report references an Equality and Human Rights Impact Assessment produced by Police Scotland and the Scottish Police Authority which revealed that the use of drones may potentially infringe Article 8 ECHR as they:

> "are capable of obtaining personal information and of flying in areas where people could have high expectations of maintaining their privacy. In addition, individuals may not necessarily be aware that they are being recorded."[89]

Drones may also infringe Article 9 (Freedom of Thought, Conscience and Religion) and Article 10 (Freedom of Expression) ECHR as the potential for a person to be recorded may deter them from exercising and make them less likely to exercise these rights.[90] The assessment also revealed that there may be a likelihood of a negative impact within the age, disability, pregnancy and maternity, and race protected groups in the usage of drones for law enforcement purposes.[91]

Due to the human rights and equality implications of the use of drones, the Commission is of the view that further consideration should be given to the effectiveness of drones as tool

---

[87] In particular, the right to protection of personal data in Article 8 of the Charter. See Data Protection Commission, Decision of the Data Protection Commission relating to Limerick City and County Council (9 December 2021) para. 6.274.

[88] The Scottish Parliament Justice Sub-Committee on Policing, Police Scotland's use of remote piloted aircraft systems and body worn video cameras (18 March 2021).

[89] The Scottish Parliament Justice Sub-Committee on Policing, Police Scotland's use of remote piloted aircraft systems and body worn video cameras (18 March 2021) para. 164. See also Police Scotland and Scottish Police Authority, Equality and Human Rights Impact Assessment (EqHRIA): Air Support Unit National Guidance (December 2020).

[90] The Scottish Parliament Justice Sub-Committee on Policing, Police Scotland's use of remote piloted aircraft systems and body worn video cameras (18 March 2021) para. 164. See also Police Scotland and Scottish Police Authority, Equality and Human Rights Impact Assessment (EqHRIA): Air Support Unit National Guidance (December 2020).

[91] The Scottish Parliament Justice Sub-Committee on Policing, Police Scotland's use of remote piloted aircraft systems and body worn video cameras (18 March 2021) para. 164. See also Police Scotland and Scottish Police Authority, Equality and Human Rights Impact Assessment (EqHRIA): Air Support Unit National Guidance (December 2020).

of policing. The Commission considers that the recommendations of the Justice Sub-Committee on Policing on the operation of drones are relevant to the examination of this General Scheme, including the recommendations:

> "The use of drones by Police Scotland can infringe human rights. An equalities and human rights assessment and a community impact assessment should be carried out prior to the use of a drone. These assessments must include consideration of whether the deployment is necessary, and if so, identify measures to mitigate the risks to the public…..
>
> The Sub-Committee recommends that the SPA [Scottish Police Authority] carries out periodic audits as part of its oversight function, to ensure that Police Scotland's use of drones complies with human rights requirements."[92]

The Commission recommends that the case for the use of drones for policing purposes should be substantially evidenced before the inclusion of drones under the definition of a 'recording device' in this legislation. If there is no substantive evidence demonstrating the effectiveness of drones in the prevention and detection of crime, the Commission recommends that Head 2 be amended to state the definition of a 'recording device' excludes a drone.

If the use of drones for policing purposes is provided for under the legislation, the Commission recommends that the use of drones for policing purposes be subject to a Human Rights Impact Assessment prior to the first use of drones under this legislation. Furthermore, the Commission recommends that the use of drones for policing purposes should be subject to independent oversight either by existing body, such as the Policing Authority, or a new independent mechanism; as a means of ensuring the use of drones is in compliance with human rights and equality standards.

[92] The Scottish Parliament Justice Sub-Committee on Policing, Police Scotland's use of remote piloted aircraft systems and body worn video cameras (18 March 2021) paras. 166–170.

Proportionality assessments in the use of a recording device and a body-worn camera by the Garda Síochána (Heads 5 and 6)

The General Scheme sets out the legal basis for the operation of a recording device (Head 5) and a body-worn camera (Head 6) by a member of An Garda Síochána in a public place or any other place under a power of entry authorised by law or to which or in which he or she was expressly or impliedly invited or permitted to be. Head 5(3) and Head 6(4) provide respectively that any use of a recording device or body-worn camera must be necessary and proportionate in relation to the functions of the Garda Síochána and the purpose of: (a) preventing, investigating, detecting or prosecuting criminal offences, (b) securing public order and public safety, or (c) safeguarding against, and the prevention of, threats to public security[93].

The Commission welcomes these provisions requiring that the members of An Garda Síochána must ensure that the exercise of their powers must be necessary and proportionate; moreover, the Commission notes a number of other Heads also require members of An Garda Síochána or the Garda Commissioner to conduct a proportionality assessment before exercising certain powers under those Head.[94] However, it is unclear at the moment within the legislation how the requirements of proportionality and necessity will be satisfied. Therefore, the requirement that the law be clear and accessible is not satisfied. In this regard, the Office of the United Nations High Commissioner for Human Rights state that:

> "'Accessibility' requires not only that the law is published, but that it is sufficiently precise to enable the affected person to regulate his or her conduct, with foresight of the consequences that a given action may entail."[95]

The Commission considers that the principles of necessity and proportionality will need to be clarified in the codes of practices and in the data protection and human rights impact assessments to guide the implementation of these provisions; as it appears that it would be the subjective view of the individual Garda operating the device as to whether its use is

[93] As provided under Head 5(2) and Head 6(2).
[94] Principally Head 8(2), Head 9(3) and Head 12(2).
[95] United Nations Human Rights Council, The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37 (30 June 2014) para. 28.

necessary or proportionate. In this regard, the Commission notes that both Head 7(9) and Head 10(9) set out that the Garda Commissioner:

> "shall take such steps as are necessary to ensure that all members of the Garda Síochána have read and understood a code of practice established under this Head and that a record is kept of the steps so taken in relation to each member."

It is important that the codes of practice set out how members of An Garda Síochána will be trained in the use of the technologies and also how it is envisaged that the use of these technologies will not only be proportionate but also become necessary. In providing guidance on the necessary elements of the proportionality assessments required to be carried out by members of An Garda Síochána when exercising certain powers under the Bill, the Commission would draw attention to the Police Service of Northern Ireland's ('PSNI') Privacy Impact Assessment on body worn videos ('BWV').[96] In Part 4 '*Legislative considerations relating to use of BWV*', it provides the following guidance on the elements of a proportionality assessment:

> "[T]he rationale for using the equipment must be clearly outlined prior to use.
>
> **Legislation underpinning its use**
>
> The use by PSNI of BWV must be shown to be proportionate, legitimate, necessary and justifiable. In addition, the Service must be able to demonstrate that the use of this equipment addresses a "pressing social need".
>
> …
>
> Under the legislation [European Convention of Human Rights Act 1998], Article 8 is a qualified right and, police forces are required to consider this article when dealing with recorded images, whether they are made in public or private areas. This assessment looks to address the issues raised by this Article and introduces safeguards, associated with how PSNI deploys this equipment in both private and public arenas. Throughout, the principle objective is ensuring that any interference with the rights of parties can only be justified if it is:

[96] Police Service of Northern Ireland, Body Worn Videos (BWV): Privacy Impact Assessment (August 2016).

- Necessary;
- In pursuit of a legitimate aim; and
- In accordance with the law.

Legal advice indicates that the use of BWV would be in accordance of the law. All images taken via a BWV device have the potential for use in court proceedings whether they provide information that is beneficial to the prosecution or defence. The information will be safeguarded by an audit trail in the same way as other evidence that is retained for court. It should be emphasised that BWV does enable police to collect valuable evidence for use in criminal prosecutions, ensures the police act with integrity and transparency and potentially provides objective evidence of controversial events. It offers protection for both citizens and the police.

The justification is likely to be closely scrutinised by the court and it is critical that recordings are not retained where there is no clear evidence of an offence, unless some other good reason exists for their retention.

Recordings of conversations between members of the public must always be considered private, even in public spaces. In a similar way, recordings made in public places are only public to those there at the time and must therefore be considered as potentially private. Users of BWV must consider this article when recording and must mot record beyond what is necessary for policing purposes. PSNI has established process and procedure which provide clear guidelines where BWV is planned to be used in private places or where a person or persons being recorded would reasonably have a strong expectation of privacy. These guidelines include:

Intimate searches – BWV will not, under any circumstances, be used for recording intimate searches or in any other circumstances where persons are in a state of undress.

Legal privilege – users must respect legal privilege and must not record material that is, or is likely to be, subject to such protections.

Expectation of Privacy – individuals will almost certainly have a strong expectation of privacy in places not generally not open to the public, such as a private residence especially at a time of day when people are likely to be in bed. Clear justification of

the need to use BWV will be required. Furthermore, circumstances may dictate an expectation of privacy even when an incident has occurred in a public area, such as where someone may be the subject of an accident in the street.

Likely to cause offence – care should be exercised in using BWV where it may cause serious offence, for example during a religious ceremony. BWV should not be used for formal investigative interviews.

The use of BWV for the interview of suspects is not permitted as it would be in contravention of PACE Code C."[97]

The Commission recommends that the legislation should be sufficiently clear and transparent to ensure that it is accessible and that individuals can foresee the circumstances in which the respective powers under the legislation may be used.

The Commission recommends that the codes of practices under Head 7 clearly set out the necessary elements of the proportionality assessment to be conducted by members of An Garda Síochána before exercising their powers under Heads 5 and 6 of the General Scheme.

Visibility of recording device (Head 5)

Head 6(3) provides that a body-worn camera being operated by a member of the Garda Síochána in accordance with this Head shall be visible on the clothing or uniform of the member wearing it and shall have a visible indicator when it is being operated. There is no corresponding requirement, under Head 5, for the recording device to be visible or have a visible indicator when it is being operated. This may give rise to covert recording or surveillance, particularly if members of An Garda Síochána are not in uniform when operating a recording device, as members of the public may be unaware that they are being recorded by a member of An Garda Síochána. While individuals do not have a right to predict when surveillance measures will occur, the legislation should be clear to individuals on the circumstances and conditions in which the measures may be used. [98] Therefore, if the intention is for a 'recording device' to be used for covertly recording or surveilling an

[97] See Police Service of Northern Ireland, Body Worn Videos (BWV): Privacy Impact Assessment (August 2016) pp. 8–10.
[98] *Szabó and Vissy v Hungary*, no. 37138/14, 12 January 2016, § 62.

individual, the legislation should be clear on this use and it should be explicit within the text that the use of a device may lead to covert recording. Given the intrusive nature of a recording device, the Commission is of the view that strengthened safeguards are needed to ensure the use of such a device remains proportionate. The Commission recommends that a recording device should be visible when operated by a member of An Garda Síochána. The Commission recognises that a requirement that a recording device be visible when being operated may not be practical in terms of the use of a recording device such as a drone; however, it should extend to the use of handheld recording devices.

If the intention is to provide for covert recording in the General Scheme, the Commission recommends that it should be explicit in the text that the use of these recording technologies may lead to covert recording.

The Commission recommends that consideration be given to amending Head 5 to provide that a handheld recording device shall be visible when operated by a member of An Garda Síochána.

Informing people that they are being filmed and recorded (Head 5 and Head 6)

The General Scheme is silent on whether members of An Garda Síochána have to inform individuals or groups that they are being filmed and recorded. While it may be intended to address this matter within the code or codes of practice under Head 7, the Commission considers that this issue needs to be addressed within the legislation as it is of fundamental importance to the rights of individual. Members of An Garda Síochána may be engaging with members of the public who due to an intellectual disability, visual impairment or hearing impairment are not aware or do not understand that they are being filmed and recorded or how this footage may be used. Persons with disabilities already face challenges in their interactions with An Garda Síochána;[99] therefore, this legislation should take a rights based approach[100] to ensure that members of An Garda Síochána adopt an "inclusionary,

[99] Including difficulties in communication, lack of awareness and skills, and lack of resources and support to engage meaningfully. See Gautam Gulati et al., 'Challenges for people with intellectual disabilities in law enforcement interactions in Ireland; thematic analysis informed by 1537 person-years' experience' (2021) 75 International Journal of Law and Psychiatry 1–9.

[100] Article 13 of the United Nations Convention on the Rights of Persons with Disabilities provides that States should ensure the "effective access to justice for persons with disabilities on an equal basis with others, including through the provision of procedural and age-appropriate accommodations".

disability-sensitive approach" in their interactions with persons with disabilities.[101] The legislation should clearly emphasise the duty of care that members of An Garda Síochána have towards individuals to inform them in an accessible language and format that they are being filmed and recorded. Consideration should also be given to including a requirement that a victim or victims of a crime may request for a recording device or body-worn camera to be turned off to protect their privacy.

The Commission recommends that Head 5 and Head 6 be amended to provide that a member of An Garda Síochána operating a recording device or body-worn camera under these Heads should inform an individual in an accessible language or format that they are being filmed and recorded.

Use of a recording device and a body-worn camera in a private dwelling (Heads (5(1) and 6(1))

Heads 5(1) and 6(1) provide that a member of An Garda Síochána acting in the course of their duties may operate a recording device or body-worn camera in:

> "any other place under a power of entry authorised by law or to which or in which he or she was expressly or impliedly invited or permitted to be."

This could mean that recordings could be made in private dwellings if the member of An Garda Síochána has a lawful search warrant or where they may have been invited in. It is unclear what amounts to an implied invitation or permission under the General Scheme. Due to the importance placed on the constitutional right to the inviolability of the dwelling, the Commission considers that these terms should be sufficiently clarified to ensure that individuals are aware of the circumstances and conditions in which members of An Garda Síochána may operate a recording device or body-worn camera in their private dwelling. To further strengthen the safeguards for the use of a recording device or a body-worn camera in a private dwelling, the Commission is of the view that members of An Garda Síochána should inform persons within a private dwelling that they are being filmed and recorded.

[101] Gautam Gulati et al., 'Challenges for people with intellectual disabilities in law enforcement interactions in Ireland; thematic analysis informed by 1537 person-years' experience' (2021) 75 International Journal of Law and Psychiatry 1–9, p. 3.

The Commission recommends that the precise scope of the phrase "in which he or she was expressly or impliedly invited or permitted to be" under Heads 5(1) and 6(1) should be clarified to ensure its compliance with the principle of legal certainty.

The Commission recommends that the Head 5 and Head 6 be amended to provide that a member of An Garda Síochána should inform persons within a private dwelling that a recording device or body-worn camera is being operated.

Mobile and fixed CCTV (Part 3)

Installation and operation of CCTV (Head 8 and Head 9)

Head 4 proposes to repeal and revoke the current statutory provisions in relation to Garda CCTV and community CCTV under section 38 of the *Garda Síochána Act 2005*[102] and Garda Síochána (CCTV) Order 2006.[103] The proposals to amend the law on CCTV is welcome, as the IHRC highlighted that there was insufficient regulation and a lack of safeguards in the use of CCTV cameras for the investigation or detection of offences.[104]

Head 8 largely reproduces the existing statutory provision in section 38; which provides that the Garda Commissioner may authorise the installation and operation of a CCTV scheme for the sole or primary purpose of securing public order and safety in public places or the prevention, detection, investigation and prosecution of criminal offences. The Commission acknowledges that the installation of community CCTV can play a positive role in reducing the fear of crime in communities.[105] However, research on the effectiveness of CCTV in preventing crime in four locations across Ireland revealed inconclusive results, showing increases in some categories of crime in one area but decreases in another.[106] Other commentators have stated that the installation of community CCTV schemes in some parts of the country, e.g. in Duleek, County Meath, where six cameras and five ANPR cameras

---

[102] Section 38 of the Garda Síochána Act 2005 currently allows for the installation and operation of CCTV 'for the sole or primary purpose of securing public order and safety in public places by facilitating the deterrence, prevention, detection and prosecution of offences'.

[103] Statutory Instrument No. 289/2006.

[104] The IHRC recommended that the use of CCTV cameras should be further regulated by law with adequate and effective safeguards concerning its use, particularly where CCTV footage is used for purposes which are not reasonably foreseeable. See IHRC, Observations on the Criminal Justice (Surveillance) Bill 2009 (May 2009) paras. 16, 18.

[105] In a report of the Joint Oireachtas Committee on Justice and Equality, it was noted that "CCTV can play an important role in crime prevention and in providing reassurance to people in rural communities"; Joint Committee on Justice and Equality, Report on Community Policing and Rural Crime (March 2019) p. 41.

[106] Aidan Donnelly, To CCTV or not? An examination of community-based CCTV in Ireland (DIT 2012).

were installed in 2017, has been driven by the perceived threat of crime rather than the reality, given that the spike in burglaries during the economic recession had returned to pre-recession levels by 2017.[107] This highlights the need to consider the evidence of the effectiveness of CCTV for policing purposes early in the legislative process so as to ensure that the use of CCTV complies with the principles of legality, necessity and proportionality. In a comparative analysis of CCTV schemes, the Oireachtas Library and Research Service compared the installation of CCTV and ANPR technology in Duleek with the installation of ANPR cameras in the town of Royston, Hertfordshire, UK and noted that the Information Commissioner's Office in the UK found the use of five cameras monitoring traffic with ANPR technology in Royston to be unlawful and excessive.[108] This comparison, as well as the evidence from the DPC inquiries of failings in the CCTV system, clearly demonstrate the need for a strong proportionality test to be built into the legislation to ensure the intrusion caused by the use of this technology complies with human rights and equality principles, and the need to ensure adequate and effective safeguards for the rights of individuals.

In this regard, the Commission considers that the provisions, under Head 8(1) and Head 9(1), that the Garda Commissioner may authorise the installation and operation of CCTV and mobile CCTV may not satisfy applicable human rights standards such as fair trial rights and rights to privacy and protection of personal information. While the human rights implications of this provision will become more apparent as part of the Human Rights Impact Assessment, the provision grants substantial executive power to the Garda Commissioner without incorporating sufficient oversight of this power. 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 Direction.[109] 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.[110]

---

[107] TJ McIntyre, 'Duleek use of CCTV to fight crime based on flawed logic' *Irish Times* (20 November 2017).
[108] Oireachtas Library and Research Service, Note on Data Privacy and Community CCTV Schemes (January 2019) p. 23.
[109] *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.
[110] *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.

The:

> "requirement for an independent review of surveillance measures at the authorisation stage is designed to realise the requirements of 'necessity' and proportionality in practice."[111]

Therefore, the Commission is of the opinion that either the Garda Commissioner or a senior Garda member on their behalf should be required to apply for judicial authorisation for the installation and operation of a CCTV scheme. This is not a burdensome or excessive requirement, as Part 4 of the General Scheme also requires applications to court to access Third Party CCTV. Each authorisation should be time-limited, and the Garda Commissioner or a senior Garda member on their behalf should be required to apply to the courts for a variation or renewal of an authorisation. The obligation to carefully document and justify intrusions on privacy rights would serve to create a culture of accountability and transparency. The Commission would draw attention to the guidance of the UN Special Rapporteur on the right to privacy on measures to support the judicial authorisation process for intrusive surveillance measures:

> "[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."[112]

Moreover, to address the potential profiling of communities in the use of CCTV the Commission considers that applications for authorisation of CCTV/mobile CCTV should be subject to the requirement that an application is notified to the public; so that an interested party may apply to challenge or set aside an application or authorisation. In this circumstance, an interested party should be provided with any documentation or information grounding the application for authorisation; subject to any claim of privilege or privacy issue that may arise in regards to the documentation or information relied upon by An Garda Síochána.

---

[111] Maria Helen Murphy, Surveillance and the Law (Routledge 2019) pp. 53–54.
[112] United Nations Human Rights Council, Report of the Special Rapporteur on the right to privacy, A/HRC/34/60 (6 September 2017) para. 28.

The Commission recommends that the development of this legislation should examine whether the interference with the right to privacy, protection of data, freedom of expression and assembly, and right to a fair trial that is presented by the use of CCTV is proportionate and necessary in the prevention of disorder or crime.

The Commission recommends that Head 8(1) be amended to require that judicial authorisation must be sought by the Garda Commissioner or a senior Garda member on their behalf for the installation and operation of CCTV. An authorisation granted under this subhead should be time-limited, and the Garda Commissioner or a senior Garda member on their behalf should be required to apply to court to vary or renew an authorisation. The Commission further recommends that the General Scheme be amended to set out a process for interested parties to challenge an application or authorisation.

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.

Transparency in the location of CCTV and ANPR cameras (Head 8)

The DPC inquiry concerning An Garda Síochána highlighted that inadequate signage was a repeated issue across Garda operated CCTV schemes and the use of ANPR cameras.[113] The inquiry found that:

> "In relation to the schemes inspected, it is clear that members of the public are not adequately on notice in relation to the processing that is taking place via CCTV operated by AGS [An Garda Síochána']. In many instances inspected, the first layer of signage is not present or, where it is present, it is not adequate as no contact details for the controller are supplied nor purposes for processing stated. Nor is there a second layer of information available to the public, either on the garda.ie website or on leaflets in Garda stations. Were they aware, individuals may opt to use a different

[113] Data Protection Commission, Decision of the Data Protection Commission regarding CCTV Schemes Authorised under Section 38(3)(a) of the Garda Síochána Act 2005 (23 August 2019) pp. 18–20. See also Data Protection Commission, DPC Ireland 2018–2020 Regulatory Activity under GDPR (2020) pp. 67–69.

> route or may continue and enter a CCTV-monitored area but secure in the knowledge that they can contact the relevant data controller if they wish to make inquiries or exercise any of their data protection rights."[114]

The DPC also found in relation to the Duleek and Donore schemes that none of the signs inspected mentioned that ANPR is in use.[115] The CCTV policy does not adequately address the purposes for which ANPR cameras have been installed or communicate to explain to public about what is ANPR, the capability of ANPR cameras, how it processes personal data and why it is necessary.[116] The inquiry concluded that the practices of An Garda Síochána in relation to signage and transparency on the usage of CCTV infringed the *Data Protection Act 2018*,[117] and stated that An Garda Síochána:

> "needs to identify and procure a consistent form of signage that meets the requirements of the Data Protection Act, 2018 and that will be easily recognisable by members of the public no matter where they travel in Ireland."[118]

The DPC has affirmed that the provision of information and communication relating to the processing personal data must comply with the principle of transparency; in that information must be easily accessible and easy to understand, and that clear and plain language is used to explain the processing of personal data.[119]

While it may be intended to address the issue of signage in the code of practice, the Commission consider that a requirement for appropriate signage should be set down within the legislation. This is due to the importance of ensuring that members of the public know the circumstances of when they may be recorded and the processing of their data.

---

[114] Data Protection Commission, Decision of the Data Protection Commission regarding CCTV Schemes Authorised under Section 38(3)(a) of the Garda Síochána Act 2005 (23 August 2019) p. 19.
[115] Data Protection Commission, Decision of the Data Protection Commission regarding CCTV Schemes Authorised under Section 38(3)(a) of the Garda Síochána Act 2005 (23 August 2019) p. 19.
[116] Data Protection Commission, Decision of the Data Protection Commission regarding CCTV Schemes Authorised under Section 38(3)(a) of the Garda Síochána Act 2005 (23 August 2019) p. 19.
[117] Namely section 71(1)(a) and section 90(2) – the right to information, specifically the information which should be provided to a data subject.
[118] Data Protection Commission, Decision of the Data Protection Commission regarding CCTV Schemes Authorised under Section 38(3)(a) of the Garda Síochána Act 2005 (23 August 2019) p. 20.
[119] Data Protection Commission, Decision of the Data Protection Commission regarding CCTV Schemes Authorised under Section 38(3)(a) of the Garda Síochána Act 2005 (23 August 2019) p. 17. See also guidance from the European Data Protection Board on the information to be provided to the data subject; European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices (adopted 29 January 2020) pp. 26–27.

The Commission recommends that Head 8 be amended to require that appropriate signage, which complies with the Data Protection Act 2018 and follows the Data Protection Commission's guidance, be erected in areas where CCTV and/or ANPR is in operation to ensure that individuals are informed of the processing of their personal data. The Commission further recommends that Head 8 should set out that information on the processing of personal data by CCTV and ANPR cameras should be available in an accessible format to the public on the Garda website and on leaflets in Garda stations.

Profiling in the location of CCTV (Head 8(2))

Head 8(2) provides that the Garda Commissioner shall, based on the information available to them, specify the areas within which, the installation and operation of CCTV is necessary and proportionate. The Commission is concerned about the adequacy of safeguards within this provision to prevent the blanket surveillance of particular communities such as those with a high proportion of ethnic minorities or in border areas. There is no description in the General Scheme or the explanatory notes of what evidence or data will be used to support the installation of CCTV in a given area.

Law enforcement organisations are increasingly using algorithmic profiling for determining the likelihood of criminal activity either in certain localities, or by certain groups or even individuals.[120] One such example is predictive policing:

> "which draws on the use of crime statistics and algorithmically based analysis to predict crime hotspots and make them the priorities for law-enforcement agencies."[121]

The suggested benefits of predictive policing are that it allows law enforcement agencies to deploy their resources more efficiently and effectively by identifying areas at increased risk of criminal activity, indicating when criminal activity may occur and identifying individuals who may potentially be involved in an act of crime – either as a perpetrator or as a victim.[122] However, predictive policing can reproduce and reinforce discriminatory outcomes,

---

[120] 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) paras. 31, 33.

[121] United Nations General Assembly, Report of the Special Rapporteur of the Human Rights Council on the right to privacy, A/72/540 (19 October 2017) para. 67.

[122] Albert Meijer and Martijn Wessels, 'Predictive Policing: Review of Benefits and Drawbacks' (2019) 42 International Journal of Public Administration 1031, pp. 1033–1034.

particularly if it relies on historical arrest data of a neighbourhood or community for determining the likelihood of criminal activity either in certain localities, or by certain groups or even individuals.[123] It can lead to over policing of the same communities, which in turn may lead to more arrests and convictions in that community, creating a dangerous feedback loop which exposes persons who are already disadvantaged and marginalised to a higher risk of arrest and punishment.[124] The United Nations Committee on the Elimination of Racial Discrimination have warned of a:

> "real risk of algorithmic bias when artificial intelligence is used in decision-making in the context of law enforcement."[125]

The Commission notes that profiling that results in discrimination against an individual on the basis of a special category of personal data is prohibited under section 89(3) of the *Data Protection Act 2018*. The Commission notes that the DPC's inquiries relating to Waterford City and County Council and Limerick City and County Council found that the operation of CCTV cameras at Traveller accommodation sites had no lawful basis for the processing of a special category of personal data.[126] The operation of CCTV cameras at Traveller accommodation sites also potentially interferes with the right to privacy and family life under Article 8 ECHR.[127] The Commission would draw attention to the Public Sector Equality and Human Rights Duty, under section 42 of the IHREC Act 2014, which binds public bodies to have due regard to the need to protect human rights and eliminate discrimination in the exercise of their functions. This may be beneficial in terms of thinking ahead to avoid the

---

[123] 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. 24.
[124] United Nations General Assembly, Report of the Special Rapporteur of the Human Rights Council on the right to privacy, A/72/540 (19 October 2017) para. 67; 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) paras. 12, 33.
[125] 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) para. 12.
[126] Data Protection Commission, Decision of the Data Protection Commission relating to Waterford City and County Council (21 October 2020) paras. 8.40–8.44; Data Protection Commission, Decision of the Data Protection Commission relating to Limerick City and County Council (9 December 2021) paras. 6.190–6.194.
[127] European Commission for Democracy through Law (Venice Commission, Opinion on video surveillance in public places by public authorities and the protection of human rights, adopted by the Venice Commission at its 70th Plenary Session (2007).

location of CCTV having a disproportionate impact on any one community or category of people.

The Commission recommends that the General Scheme be amended to prescribe the criteria for the selection of locations where CCTV is to be installed in order to safeguard against blanket surveillance of certain communities.

Criteria for authorisation (Heads 8(3)(b) and 8(4))

Head 8(3)(b) provides that authorisation may be given to persons who meet the established criteria and who are retained under a contract with Garda Commissioner. Head 8(4) sets out that the Garda Commissioner shall establish criteria for the purposes of subhead (3)(b). As these criteria will be crucial to the functioning of this provision and compliance with human rights and equality principles, it would seem apparent that before a Data Protection Impact Assessment and a Human Rights Impact Assessment, under Head 10, are conducted, that the Garda Commissioner should at minimum disseminate draft proposed criteria.

The Commission recommends that Head 8(4) be amended to require the Garda Commissioner to disseminate draft proposed criteria before any Data Protection Impact Assessment or Human Rights Impact Assessment is conducted.

Misuse of Mobile CCTV (Head 9)

The Commission notes that there is a criminal provision under Head 8(9)[128] in respect of the misuse of the installation of a fixed CCTV regime and in relation to the accessing of third party CCTV under Head 16[129]. It is unclear why there is not a similar provision in relation to the misuse of the installation or operation of mobile CCTV under Head 9.

The Commission recommends that consideration be given to including a provision under Head 9 criminalising the misuse of the installation or operation of mobile CCTV.

---

[128] Head 8(9) provides that "A person who, operates a CCTV scheme for the purposes prescribed in subhead (1) without authorisation, is guilty of an offence and is liable on summary conviction to a fine not exceeding €2,500 or imprisonment for a term not exceeding 6 months or both."

[129] Head 16(1) provides that "A person/third party who fails to comply with an authorisation in relation to the access to CCTV through a live feed under Head 13, Head 14 or Head 15 without lawful authority or reasonable excuse shall be liable – (a) on summary conviction to a class A fine or imprisonment for a term not exceeding 12 months or both, or (b) on conviction on indictment, to a fine or imprisonment for a term not exceeding 3 years or both."

Codes of practice (Heads 7 and 10)

Compliance with human rights and equality principles

The Commission welcomes the inclusion of provisions providing for a code or codes of practice to govern the operation of recording devices, body-worn cameras, CCTV and Mobile CCTV; and the requirements to conduct a Data Protection Impact Assessment and a Human Rights Impact Assessment as well as consulting with a number of bodies, including the Commission, on the content of the code of practice.

Head 7(2) and Head 10(2) set out a number a matters that shall be included within codes of practice including:

- procedures and standards to be followed in the operation of Part 2 and 3 of this Act; confidentiality, security, storage, access and retention of data gathered in accordance with Part 2 and 3 of this Act;
- data subject rights; and
- any other matters relevant to the operation of Part 2 and 3 of this Act.

Due to the implications for equality and human rights with the operation of recording devices, body-worn cameras and CCTV; it may be worth considering directly referencing human rights and equality considerations in the legislation.

The Commission consider that while codes of practice provide beneficial contextual guidance on how to apply the principles within the legislation, it is important to ensure that the fundamental legal rules governing the exercise of An Garda Síochána's powers are set down in the legislation rather than 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. 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.[130]

[130] In clarifying the powers under this legislation, the Commission recommends that the following non-exhaustive list of matters should be included in the codes of practice under Head 7 and Head 10: when should a recording device or a body-worn camera be turned on and when should it be turned off; are there particular policing scenarios where recording devices/body-worn cameras should or should not be used; the recording of protests and public assemblies; how it is communicated to an individual or group that they are being filmed

Head 7(3)(b) and Head 10(3)(b) set out that a Human Rights Impact Assessment shall be carried out, and this may include consultation with members of the public. Due to the broader implications for human rights and the potential for the use of these devices to profile communities, the Commission is of the opinion that it should be a requirement that consultation with members of the public is included in the carrying out of a Human Rights Impact Assessment. Members of the public should also be consulted in any review of a code or codes of practice under Head 7(6) and Head 10(6) as they may have lived experiences of the use of these devices/technologies.

Human rights proofing of Garda operational policies is of crucial importance in mainstreaming human rights standards, including the Public Sector Duty, in all aspects of policing. The Commission is of the view that the code or codes of practice should be underpinned by relevant equality and human rights standards.[131] Accordingly, the code or codes of practice should comprehensively set out the policies and procedures informing Garda decisions and regulating Garda powers under Part 2 and Part 3 of the legislation in a transparent and human rights compliant manner. In the context of ensuring that the legislation complies with the principles of legal certainty, the Commission has previously outlined that without publication of operational standards it cannot be assessed whether internal Garda policies contain adequate and effective safeguards to protect individuals from arbitrary or unjustifiable interference with the rights of individuals.[132] The publication of a code or codes of practice is an important measure for transparency, accountability and the public's reassurance that these devices are being operated proportionality.

In light of An Garda Síochána's obligations under the Public Sector Equality and Human Rights Duty, the Commission recommends that the codes of practice under Head 7 and

---

and recorded in public or in any other private place; formal recording or recording by members of An Garda Síochána when they are not on duty; the procedure if victims of crime ask for a body-worn camera to be switched off; and, the procedures around the storage, access to and dissemination of footage.

[131] See previous recommendations of the Commission: IHREC, Submission to the Commission on the Future of Policing (February 2018) p. 20. See also previous recommendations of the IHRC: IHRC, Policy Statement: Human Rights Compliance of An Garda Síochána (April 2009) pp. 12–14; IHRC, Observations on the Criminal Justice (Surveillance) Bill 2009 (May 2009) paras. 40, 42,

[132] See previous commentary of the Commission: IHREC, Submission to the Commission on the Future of Policing (February 2018) p. 20. See also previous recommendations of the IHRC: IHRC, Policy Statement: Human Rights Compliance of An Garda Síochána (April 2009) pp. 12–14.

Head 10 should be equality and human rights proofed and should be made accessible to the public.

The Commission recommends that Heads 7(2) and 10(2) be amended to set out that provisions in relation to human rights and equality considerations shall be included within codes of practice on the use of recording devices and body-worn cameras, and in relation to CCTV.

The Commission recommends that Heads 7(3)(b) and 10(3)(b) are amended to set out that the conducting of a Human Rights Impact Assessment shall include consultation with members of the public. The Commission further recommends that Heads 7(6) and 10(6) are amended to set out that members of the public shall be consulted in the review of a code or codes of practice.

Use of recording device or body-worn camera before a Minister orders that a code shall be a code of practice for the purpose of the legislation (Head 7(1))

Head 7(1) sets out that the Garda Commissioner shall, as soon as practicable after the coming into operation of Part 2 of this Act, and having had regard to the matters contained therein, prepare a draft code or codes of practice to set standards for the operation of Part 2 of this Act for submission to the Minister. This provision is quite loosely worded, and it is unclear whether a member of An Garda Síochána may operate a recording device or body-worn camera before the Minister, under Head 7(5), makes an order to declare that the code, scheduled to the order, shall be a code of practice for the purposes of this Act. This is potentially problematic as it may mean these technologies are utilised in the community before the code of practice is published or the data protection and human rights impact assessments are carried out, and before the members of An Garda Síochána have read and understood the code of practice.[133] In this regard, the Commission is of the view that the provisions under Part 2 should not become operational until members of An Garda Síochána receive training on the provisions under this Part including the necessary elements of a proportionally assessment to be conducted before the use of these devices.

[133] Head 7(9) provides that the Garda Commissioner "shall take such steps as are necessary to ensure that all members of the Garda Síochána have read and understood a code of practice established under this Head and that a record is kept of the steps so taken in relation to each member."

The Commission recommends that Head 7 of the General Scheme be amended to explicitly state that the provisions of Part 2 do not become operational until the Minister orders that a code shall be a code of practice for the purpose of the legislation.

The Commission recommends that Head 7 be amended to state that the provisions of Part 2 do not become operational until members of An Garda Síochána have received appropriate associated training.

Access to and dissemination of footage by members of An Garda Síochána (Heads 7 and 10)

The Commission notes that the DPC's inquiry into An Garda Síochána highlighted concerning practices in relation to excessive access to CCTV monitoring rooms by members of An Garda Síochána, no restrictions on bringing smart phones or recording devices into CCTV monitoring rooms, and the sharing of footage of a member of the public in a WhatsApp group.[134] The ECtHR, in *Peck v United Kingdom,*[135] found that the disclosure of the footage by the local council to the media had not been accompanied by sufficient safeguards and constituted disproportionate and unjustified interference with the applicant's private life, in breach of Article 8 ECHR. The Court found that the crime-prevention objective and context of the disclosures demanded particular scrutiny and care. The Court also held that there had been a violation of Article 13 ECHR (right to an effective remedy), read in conjunction with Article 8, finding that the applicant had had no effective remedy in relation to the violation of his right to respect for his private life. The Commission notes that the DPC recommended the prohibition of the use of personal audio or video recording devices in the area of the monitoring screens.[136] The Commission is of the view that the codes of practice should be robust in terms of the unauthorised access and dissemination of footage from body-cameras, recording devices and CCTV and the consequences which follow from breaching

[134] Data Protection Commission, Decision of the Data Protection Commission regarding CCTV Schemes Authorised under Section 38(3)(a) of the Garda Síochána Act 2005 (23 August 2019) p. 8.
[135] The case concerned the disclosure to the media of CCTV footage showing the applicant cutting their wrists in a street. See *Peck v. the United Kingdom*, no. 44647/98, ECHR 2003-I.
[136] Data Protection Commission, Decision of the Data Protection Commission regarding CCTV Schemes Authorised under Section 38(3)(a) of the Garda Síochána Act 2005 (23 August 2019) p. 9.

these provisions.[137] The codes of practice should comprehensively set out how the footage will be stored, and the proper procedures for accessing the footage.

The Commission recommends that the codes of practice comprehensively address the sharing and dissemination of footage by members of An Garda Síochána.

Third Party CCTV (Part 4)

Live feed access to third party CCTV (Head 11–14)

Under Head 12(1), a member of the Garda Síochána not below the rank of Superintendent may apply to a judge for authorisation to access the live feed of third party CCTV. The Explanatory Notes for Head 11 indicate that this power is envisaged where there is a large public event or where there is a requirement to provide protection to a visiting dignitary or where there is an increase in criminal activity in an area where there are 3rd party cameras. However, there is no such specification within the proposed legislation. If access is sought for the purpose of preventing the commission of offences, the applying member of An Garda Síochána need not specify a particular offence in respect of which the authorisation is being sought.[138] It is observed that under the *Criminal Justice (Surveillance) Act 2009*, where authorisation for surveillance in respect of the prevention of the commission of offences is sought, this must be in relation to arrestable offences (i.e. offences carrying a sentence of 5 years or more).[139]

It is unclear under the General Scheme the means by which an application will be made to a court by a member of An Garda Síochána not below the rank of Superintendent. Head 13(2) provides that the judge shall issue an authorisation if satisfied based on the information on oath provided by the superior officer.[140] If a member is only required to apply to the judge by way of information on oath, it may mean that no documentary evidence is required to

---

[137] The Commission recommended that clear guidelines on access to and disclosure of images should be enshrined in this legislation, supported by regulations and a code of practice, in its submission to the Department of Justice in February 2020; see IHREC, Preliminary Observations of the Irish Human Rights and Equality Commission in relation to the forthcoming Garda Síochána (Recording of Images) Bill: Submission to the Department of Justice and Equality (18 February 2020) pp. 13–15.

[138] Head 13(3) of the General Scheme.

[139] Section 4 of the *Criminal Justice (Surveillance) Act 2009*.

[140] Head 13(2) provides that "Subject to subhead (4), the judge shall issue such authorisation as he or she considers reasonable, if satisfied by information on oath of the superior officer concerned that—(a) the requirements specified in Head 12 (1) are fulfilled, and (b) to do so is justified, having regard to the matters referred to in Head 12 (2) and any other relevant circumstances.

ground the belief underlying the application. This is particularly concerning as the information on oath does not have to specify a particular offence in respect of which the authorisation is being sought.[141] Whilst the applying member must consider the likely impact on the rights of any person,[142] the General Scheme does not specify the nature of these rights. As this part of the Bill is not subject to a Human Rights Impact Assessment or code of practice, it may mean that the human rights and equality implications of these provisions are not fully understood or addressed by members of An Garda Síochána.

Head 14 sets out that authorisation can be given for up to one year, and can be renewed for a further period not exceeding one year. It is noted that under the *Criminal Justice (Surveillance) Act 2009*, authorisation for surveillance by An Garda Síochána may only be given for a period of up to three months, renewable for a further period not exceeding three months.[143] With regard to the circumstances outlined in the Explanatory Notes for Head 11, it is unclear why a period of up to one year is required, which can be renewed, is necessary when there is a public event or protection needs to be provided to a visiting dignitary. While the General Scheme provides that the judge may fix the date of expiry of the authorisation on a day they consider reasonable in the circumstances,[144] periods close to one year appear excessive and disproportionate when there is a lack of clarity around the circumstances which the provisions within this Part of the legislation aim to address. The duration of the permitted access to third party CCTV is an issue which could be considered as part of a human rights impact assessment. The Commission is also of the opinion that the implications for the rights to freedom of assembly and freedom of expression need to be considered if it is intended to provide access to live feed of third party CCTV where there is a large public event. This potentially has a chilling effect on the exercise of fundamental rights.

While an application for judicial authorisation to access third party CCTV is a welcome and necessary safeguard, the Commission considers that further measures could be taken to

[141] Head 13(3) provides that "Information on oath of a member of the Garda Síochána not below the rank of Superintendent specifying the grounds for his or her belief that the access to closed circuit television operated by a third party through a live feed is necessary for the purpose of preventing the commission of offences need not specify a particular offence in respect of which the authorisation is being sought.

[142] Head 12(2)(a) of the General Scheme.

[143] Sections 5 and 6 of the *Criminal Justice (Surveillance) Act 2009*.

[144] Head 13(6) of the General Scheme.

strengthen this safeguard. The proposal under Head 13, that an application for an authorisation, or a variation or renewal of authorisation"shall be heard otherwise than in public" is concerning as it an exception to the Constitutional guarantee that justice is administered in public. Moreover, there is an absence of any provision for a *legitimus contradictor*, or a provision akin to it, in relation to the application for authorisation. As applications are not made in public and on the basis of oaths, the Commission is of the opinion that strengthened oversight is required within the legislation given the potential for the infringement of fundamental rights. Such a safeguard could include requiring applications for authorisations to be reviewed by suitably qualified independent persons who can assess the material advanced by the members of An Garda Síochána to ground their application, and who can then report to the Court prior to the final orders being made. A procedure such as this measure would contribute to better informed judicial authorisation, and would also appear to satisfy the test laid down by the 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.[145]

The Commission reiterates its recommendation that Part 4 of the General Scheme provides for a Data Protection Impact Assessment and a Human Rights Impact Assessment to be conducted before this Part of the legislation comes into operation.

The Commission recommends that Head 13(1)(a) be amended to provide that an application for an authorisation or, the variation or renewal or an authorisation shall only be heard otherwise than in public on exceptional or emergency grounds.

The Commission recommends that the process for the application to court for authorisation be sufficiently clear within the General Scheme. Moreover, the Commission recommends that the standards required for grounding an application should be proportional to the impact these measures will have on the rights of individuals.

[145] *Zakharov v Russia* [2015] ECHR 1065, para. 232.

The Commission recommends that the period for the authorisation of access to third party CCTV be reviewed to ensure that the intrusion on the rights of individuals is proportionate.

The Commission recommends that the General Scheme be amended to require that the material grounding an application for an authorisation should be reviewed by a suitably qualified independent person before the Court makes an order on the authorisation.

Garda approval for temporary access to third party CCTV (Head 15)

Head 15 provides that a member of An Garda Síochána, not below the rank of Superintendent and independent of the investigation, may approve access to live feeds from third party CCTV for a period not exceeding 72 hours. Unlike Heads 12 and 13, there is no judicial oversight of this provision, which may lead to concerns that it becomes routine that members of An Garda Síochána will rely on this provision rather than apply for judicial authorisation for access. The Explanatory Notes for Head 15 provide that:

> "[t]his Head provides for internal Garda authorisation for access to live feeds for short-term access in cases where Gardaí have reasonable grounds to suspect a criminal offence has been, is being or will be committed in the vicinity of the third party CCTV."

However, the actual statutory language is more vague. Head 15(2) sets out that all that is required from the applicant for the approval is a belief on reasonable grounds that:

> "information relevant to a criminal offence under investigation can be obtained by accessing the third-party CCTV."

The vagueness of the language could mean that the provision is relied upon in circumstances different to those outlined in the explanatory notes. If the intention of Head 15 is to address circumstances where access to third party CCTV is required urgently and it is not possible to obtain judicial authorisation due to the urgent nature of the request, this circumstance should be explicitly provided for in the legislation. The current drafting does not appear to limit the circumstances in which a member of An Garda Síochána can apply for access under this Head. This broad understanding of the provision could lead to, as outlined above, this provision becoming a routine part of An Garda Síochána criminal

investigative powers rather than an emergency measure to address a specific urgent policing need.

The Commission recommends that judicial authorisation is required for all applications to request access to third party CCTV under Part 4.

Transfer of relevant data to the Garda Síochána (Part 5)

Consultation with the Data Protection Commissioner (Head 18)

Under Head 17, the Minister must consult with the Data Protection Commissioner prior to designating a relevant body. However, there is no corresponding requirement under Head 18 for the Minister and/or An Garda Síochána to consult with the Data Protection Commissioner in relation to all matters set out at Head 18 which deal with 'Disclosure of Data From Relevant Body'. Furthermore, there is no requirement for a Data Protection Impact Assessment or a Human Rights Impact Assessment with regard to the matters under Part 5. Excluding Part 5 from the remit of these assessments appear to pose concerns with regard to the rule of law, which:

> "[R]efers to a principle of governance in which all persons, institutions and entities, public and private, including the State itself, are accountable to laws that are publicly promulgated, equally enforced and independently adjudicated, and which are consistent with international human rights and standards. It requires, as well, measures to ensure adherence to the principles of supremacy of law, equality before the law, accountability to the law, fairness in the application of the law, separation of powers, participation in decision-making, legal certainty, avoidance of arbitrariness, and procedural and legal transparency."[146]

The Commission reiterates its recommendation that Part 5 of the General Scheme be amended to require that a Data Protection Impact Assessment and a Human Rights Impact Assessment be conducted before this Part of the legislation comes into operation.

The Commission recommends that Head 18 be amended to require that the Minister and/or An Garda Síochána must consult with the Data Protection Commissioner in relation to the matters falling under that Head.

[146] Maria Helen Murphy, Surveillance and the Law (Routledge 2019).

The sharing and storage of data and images of occupants of cars (Heads 17 and 18)

ANPR cameras produce clear images of a vehicle's driver and front-seat passenger, if there is one.[147] The Commission is of the view that the inside of a car amounts to a private place. In this regard, the PSNI's Privacy Impact Assessment on body worn videos sets out that individuals have a strong expectation of privacy in places not generally open to the public.[148] The Commission notes that the DPC inquiry concerning An Garda Síochána observed that:

> "[a]s no evidence was presented of any consideration being given to the issues of design in terms of what the ANPR cameras capture and how data can subsequently be aggregated, searched, consulted and reported, AGS failed to consider the privacy impact of such surveillance using ANPR cameras."[149]

This finding highlights that additional safeguards are needed around the transfer, sharing and storage of data and images of the occupants of cars, particularly images of passengers in cars who may have no relation to an incident or offence. This particular issue should be considered in the development of the human rights impact assessments, and measures should be set out to mitigate the impact on the rights to privacy and data protection.

The Commission recommends that particular consideration is given to the sharing and storage of images of occupants of cars, particularly images of passengers, in the drafting of this General Scheme and associated codes of practice to ensure that the intrusion on rights that the practice presents remains proportionate and necessary.

Miscellaneous provisions (Part 6)

No requirement for the exhibition of a device in proceedings (Head 20(1)(c))

Head 20(1)(c) sets out that a device from which evidence is sought to be adduced in court proceedings is not required to be exhibited as part of those proceedings. The Commission is concerned about the justification for this provision as it arguably represents a departure from the norm. The ability of the defence to have an expert examine such a device so that either the material it produces or aspects of concern as regards its operation can be looked into, is arguably an aspect of the right to a fair trial. Excluding a requirement for a device to

[147] Data Protection Commission, DPC Ireland 2018–2020 Regulatory Activity under GDPR (2020) p. 64.
[148] Police Service of Northern Ireland, Body Worn Videos (BWV): Privacy Impact Assessment (August 2016) p. 9.
[149] Data Protection Commission, DPC Ireland 2018–2020 Regulatory Activity under GDPR (2020) p. 64.

be produced in a proceeding potentially removes from a trial judge an aspect of their ability to guarantee a fair trial should issues relating to the operation and use of the device arise.

The Commission recommends that Head 20(1)(c) be removed from the General Scheme.

Admissibility of evidence (Head 20(4))

Head 20(4) provides that a failure to observe any provision of this Act or of any code of practice made thereunder on the part of any member of the Garda Síochána, shall not (without prejudice to the power of the court to exclude evidence at its discretion) of itself affect the admissibility of any evidence thereby obtained. While the Commission acknowledges that this provision is modelled on provisions within existing legislation,[150] the Commission would question the necessity of including this provision within this legislation as the Irish courts have shown they are prepared to apply evidential rules without supporting legislative provisions. The exclusionary rule, most recently formulated by the Supreme Court in *DPP v JC*,[151] governs the circumstances in which evidence obtained in breach of the constitutional rights of an accused may be admitted as evidence in a criminal trial. The Irish courts have also developed rules for determining whether evidence obtained unlawfully, but not in breach of constitutional rights, should be admitted.[152] As the admissibility of evidence is a matter for the courts, which this provision explicitly recognises, the Commission considers that this provision be removed as it may lead to unintended consequences for the existing rules of admissibility by creating an additional hurdle to the exclusion of evidence obtained unlawfully or in breach of constitutional rights.

The Commission recommends that Head 20(4) be removed from the General Scheme.

Review of the operation of the Act (Head 21)

Head 21 provides for a review of the operation of Part 4 and Part 5 of this legislation by a judge/the Independent Examiner to be established under the *Policing, Security and Community Safety Bill* will be responsible for this review. While the terms of Head 21 are welcome, the Commission is of the view that expanded oversight is required. Due to the implications for human rights and equality in the use of body-worn cameras, recording

---

[150] Including section 7(3) of the *Criminal Justice Act 1984*, section 14 of the *Criminal Justice (Surveillance) Act 2009* and section 164 of the *Criminal Justice (Forensic Evidence and DNA Database System) Act 2014*.
[151] [2015] IESC 31.
[152] *DPP v McMahon* [1986] IR 393.

devices and CCTV; consideration should be given to including an independent mechanism or body to review the operation of Part 2 and Part 3 of the Bill. Moreover, the initial findings of the DPC on the use of surveillance technology for law enforcement purposes underscores the necessity of putting in place an effective oversight mechanism to monitor and review the use of these technologies. The United Nations High Commissioner for Human Rights has commented that the:

> "[e]njoyment of the right to privacy depends largely on a legal, regulatory and institutional framework that provides for adequate safeguards, including effective oversight mechanisms."[153]

A more developed oversight regime would provide greater levels of accountability and transparency, and would provide reassurance to the public that the necessary checks and balances are in place in the use of these technologies. Such a mechanism would provide a strengthened safeguard against the potential intrusion on rights that are posed by the use of these technologies, and the potential blanket surveillance of communities in the deployment of technology.

While the Commission has no firm opinion on the structure or framework of an independent oversight regime, the following measures could be contemplated:

- Oversight by an existing body; such as the Policing Authority or its proposed replacement, the Policing and Community Safety Authority.[154]
- Creating an office similar to what they have in the UK, where there is the office of the 'Surveillance Camera Commissioner',[155] which was established under the Protection of Freedoms Act 2012 to further regulate CCTV. Its role is to: encourage compliance with the surveillance code of practice which sets out new guidelines for CCTV and ANPR; review how the code is working; and, provide advice to ministers on whether or not the code needs amending.

---

[153] 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/39/29 (3 August 2018) para. 26. See also United Nations Human Rights Council, The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37 (30 June 2014) para. 37.

[154] To be established under the Policing, Security and Community Safety Bill,

[155] See https://www.gov.uk/government/organisations/surveillance-camera-commissioner.

- Establishing an independent advisory group on emerging technologies which would regularly report to the Oireachtas or another designated body on key issues emerging, such as international developments, and on steps that might be required to ensure the appropriate balancing of rights.
- Establishing an expert judicial body akin to the 'Investigatory Powers Tribunal'[156] in the United Kingdom, which could hear complaints about surveillance related issues. The Tribunal is an independent judicial body which operates independently of government to provide a right of redress for anyone who believes they have been a victim of unlawful action by a public authority using covert investigative techniques.

Alongside an independent oversight mechanism, the Commission considers that this legislation should also be subject to regular legislative scrutiny including through the establishment of a Joint Oireachtas Committee on Human Rights, Equality and Diversity. The Commission has called for the establishment of a dedicated Oireachtas Committee on Human Rights, Equality and Diversity since 2016. In the context of this legislation, a dedicated committee would provide close parliamentary oversight of the implementation of the legislation and be able to monitor the human rights and equality implications arising in the use of the technologies and emerging technologies.

Furthermore, the Commission emphasises that an important aspect of the oversight of this legislation is the collection and publication of disaggregated data on the use of the powers under this legislation. The availability of disaggregated data is an important resource for monitoring compliance with human rights and equality principles, and assessing whether policies, such as the codes of practice, or legislation need to be reviewed or amended. Data could be collected on a number of powers under the General Scheme, including but not limited to: the number of times recording devices and body-worn cameras were operated; the geographic location of the use of recording devices and body-worn devices; the number of applications for authorisation of CCTV and Mobile CCTV and number of approvals; and, the geographic location of CCTV and ANPR. Such data should be published on a regular basis either by An Garda Síochána or a mechanism designated as an oversight body for the

[156] See https://www.ipt-uk.com/.

purposes of this legislation; and be considered by a dedicated Oireachtas Committee on Human Rights, Equality and Diversity. The collection of comprehensive disaggregated data is an important practice which:

> "may shed light on systematic patterns and institutional practices previously dismissed as individual-led bias, ultimately providing an opportunity to police the police by increasing transparency and, potentially, accountability".[157]

The Commission recommends that the operation of Part 2 and Part 3 of this legislation be the subject of independent oversight to ensure its compliance with human rights and equality standards.

The Commission recommends the establishment of a dedicated Joint Oireachtas Committee on Human Rights, Equality and Diversity.

The Commission recommends that the implementation of this legislation be accompanied by the collection and reporting of detailed disaggregated data.

Definition of surveillance device (Head 22)

Head 22 proposes to amend the definition of a surveillance device under section 1[158] of the *Criminal Justice (Surveillance) Act 2009* to exclude a body-worn camera or a recording device within the meaning of Part 2, a CCTV or mobile CCTV within the meaning of Part 3 of the General Scheme, an apparatus designed to enhance visual acuity or night vision, and a camera including a video camera, to the extent to which it is used to take photographs or video footage of any person who, or anything that, is in a place to which the public have access.

In considering this exclusion, it is worth drawing attention to the definition of surveillance under the *Criminal Justice (Surveillance) Act 2009*:

> "Surveillance means:

[157] Sarah Brayne, Predict and Surveil: Data, Discretion and the Future of Policing (Oxford University Press 2021) pp. 101–102.

[158] Section 1 provides that a "surveillance device" means an apparatus designed or adapted for use in surveillance.

(a) monitoring, observing, listening to or making a recording of a particular person or group of persons or their movements, activities and communications, or

(b) monitoring or making a recording of places or things,

by or with the assistance of surveillance devices".[159]

If it was not for the reference to 'surveillance device' in this definition, the Commission considers that the technologies that are the subject of this General Scheme could come within the definition of surveillance. Certainly if these technologies are used as part of covert investigative activity. The Commission notes that the Bill does not exclude the possibility that the data obtained through the use of a recording device or body-worn camera, under Part 2, be connected with other forms of digital recording such as CCTV and ANPR tracking in combination with phone tracking. Therefore, the exclusion of these devices from the definition of 'surveillance device' is concerning due to the potential for interplay of these technologies in the investigation of criminal activity.

The Commission would draw attention to IHRC's observations on the *Criminal Justice (Surveillance) Act 2009*. The IHRC expressed concern that a camera, to the extent to which it is used to take photographs of any person or anything that is in a place to which the public have access, is excluded from the definition of a surveillance device as the compilation and maintenance of a database of photographs would appear to give rise to an interference with the right to respect for private life.[160] The IHRC recommended that the definition of surveillance under the 2009 Bill should be extended to include the targeted, ongoing and repeated photographing of persons for the purposes of monitoring and/or recording the movements, activities and communications of such persons; and should be subject to the same safeguards as other forms of surveillance.[161]

The Commission recommends that consideration be given to the rationale for excluding the technologies under this legislation from the definition of a 'surveillance device' under the *Criminal Justice (Surveillance) Act 2009*.

[159] Section 1.
[160] IHRC, Observations on the Criminal Justice (Surveillance) Bill 2009 (May 2009) para. 17.
[161] IHRC, Observations on the Criminal Justice (Surveillance) Bill 2009 (May 2009) paras. 17, 19.

Additional provisions

The rights of data subjects

The General Scheme is generally silent on the rights of data subjects, including an absence of guidelines around access to and disclosure of data. This omission is particularly concerning as it is left unclear whether an individual charged with an offence should be provided with the footage from a recording device, body-worn camera or CCTV if this is to be used in evidence. While it appears that the intention is to address the rights of data subjects in the codes of practice, under Heads 7 and 10, the Commission considers the lack of guidelines within the legislation may weaken the protections available to affected individuals. The rights of data subjects include that individuals should have a right to access the data that is stored and request alterations or deletion of data that is stored without a legitimate and legal basis.[162] This right is particularly important for individuals who are inadvertently recorded as they are the vicinity of the use of the technology or in a dwelling where the technology is used. A framework should be in place to protect personal data including the immediate deletion of all data, except for the specific segments of the footage which is necessary for the conduct of a criminal investigation and the prosecution of serious criminal activity.[163] If material is being used in a civil or criminal context, access should be provided to the individual concerned of the material, or a copy of the material. The obligation to disclose material is an ingredient of the right to a fair trial and the right to an effective remedy.

The rights of data subjects is particularly important in circumstances where it is alleged that members of An Garda Síochána failed to observe or breached a provision or provisions of the legislation or any of the codes of practice. The disclosure of data in these circumstances would appear to go to the heart of the right to an effective remedy.[164] Consideration should also be given to addressing circumstances where it is revealed that an individual has been

---

[162] 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. 36.

[163] 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. 36.

[164] The ECtHR stated that what is required under Article 13 in the context of covert surveillance is a remedy that is as effective as can be having regard to the restricted scope for recourse inherent in any system of secret surveillance. See *Klass v Germany* (1979-80) 2EHHR 214, § 69.

the subject of recording in contravention of this legislation without their knowledge. There should a mechanism in place to inform the individual concerned so that they can exercise any further causes of action or remedies available to them.

In its Report on Disclosure and Discovery in Criminal Cases, the Law Reform Commission recommends that, in accordance with the Directive 2012/13/EU on the right to information in criminal proceedings, objective material, such as CCTV footage, should be disclosed at an early stage, including at the point where a person is detained in Garda custody and that further disclosure of scheduled materials should occur after this.[165] Moreover, the Law Reform Commission also recommended that when deciding on whether to order disclosure, a court should be required to take a number of factors into consideration including, but not limited to, the following:

(a) the probative value of the material,

(b) whether it is necessary for the accused's right to a trial in due course of law and the public interest in preserving the integrity of the criminal justice process,

(c) the rights of any person to whom the material held by the third party relates, including any reasonable expectation of privacy of that person, and any potential harm (whether physical or emotional), including the risk of secondary and repeat victimisation, which disclosure of the material held by the third party may cause to that person, and

(d) whether it is necessary to make an immediate order for disclosure and, in particular, whether it would be appropriate in the circumstances to postpone until the trial consideration of disclosure of the material, including having regard to other probative evidence that has already been disclosed concerning any person to whom the material held by the third party relates.[166]

In developing guidelines on access to and disclosures of images, the Commission would also draw attention to the guidance on the rights of data subjects set out in the '*Practical guide on the use of personal data in the police sector*' produced by the Consultative Committee of

[165] Law Reform Commission, Disclosure and Discovery in Criminal Cases (2014) p. 56.
[166] Law Reform Commission, Disclosure and Discovery in Criminal Cases (2014) pp. 57–58.

the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.[167]

The Commission recommends that clear guidelines on access to and disclosure of images should be enshrined in the forthcoming legislation and this should be supported by a code of practice.

The Commission recommends that the legislation set out effective remedies for individuals whose rights are violated under the legislation.

Procurement of technologies

While the matter of the procurement of the technologies that will be covered by Part 2 and Part 3 may not need to be addressed in this legislation, the Commission considers it important at this stage of the legislative process to remind and reaffirm that public procurement, as a function of public bodies, is subject to the Public Sector Duty.[168] This means that the public procurement process should be underpinned by the Public Sector Duty and international human rights standards.[169] In this regard, the Commission reiterates its previous recommendation that, in the context of government procurement, the State should consider introducing human rights due diligence as a mandatory requirement with legislative underpinning.[170]

The Commission recommends that the procurement of technologies under this legislation be underpinned by the Public Sector Equality and Human Rights Duty. Furthermore, the Commission reiterates it recommendation that human rights due diligence be placed on a statutory footing.

---

[167] Council of Europe, Practical guide on the use of personal data in the police sector (2018) pp. 5–7.
[168] IHREC, Implementing the Public Sector Equality and Human Rights Duty (March 2019).
[169] Such as the UN Guiding Principles on Business and Human Rights.
[170] IHREC, Ireland and the United Nations Convention on the Rights of the Child: Report by the Irish Human Rights and Equality Commission to the UN Committee on the Rights of the Child on Ireland's Combined Third and Fourth Periodic Reports (December 2015) p. 12; IHREC, Ireland and the Convention on the Elimination of Racial Discrimination: Submission to the United Nations Committee on the Elimination of Racial Discrimination on Ireland's Combined 5th to 9th Report (October 2019) p. 148.

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

The Irish Human Rights and Equality Commission

16 – 22 Sráid na Faiche,
Baile Átha Cliath, D07
CR20 16 – 22 Green Street,
Dublin, D07 CR20

Íosghlao/Lo-Call 1890 245 245
Guthán/Phone + 353 (0) 1 858 3000
Ríomhphost/Email info@ihrec.ie
Idirlíon/Web www.ihrec.ie
@_ihrec
/irishhumanrightsequality