ICCL Submission on the Garda Síochána (Digital Recording) Bill

August 2021

Irish Council for Civil Liberties

Contents

Executive Summary

This submission examines the Garda Síochána (Digital Recording) Bill, through the lens of privacy rights, data protection, the right to non-discrimination and the right to a fair trial. ICCL has identified a number of weaknesses in the legislation which give rise to a concern that these rights are at risk of being violated.

ICCL seriously questions the proposed expansion of surveillance powers in this Bill while there are ongoing inquiries by the Data Protection Commission (DPC) into the compliance of An Garda Síochána (AGS) with data protection law. We note deeply concerning findings by the DPC that suggest compliance with data protection law by AGS is exceptionally poor. This means privacy and data protection rights are already at risk by the failure by AGS to ensure existing surveillance capabilities comply with safeguards. ICCL considers that AGS must demonstrate a real commitment to upholding privacy and data protection law before the expansion of surveillance powers envisaged by this Bill can be considered.

ICCL considers that the tests of necessity and proportionality required for the introduction and expansion of surveillance technologies in the Irish context have not been met. In particular, there is no substantive evidence that body worn cameras are necessary or effective and we oppose their introduction. Further research is necessary into this issue and into the effectiveness of CCTV in preventing and detecting crime. We urge government to ensure that further research is carried out to prove its necessity and confirm its effectiveness in combating crime before surveillance technology is expanded for AGS.

In this submission, we analyse the Bill in detail on a Head by Head basis. We outline our concerns that the requirement for minimal interference with rights to achieve criminal justice aims will not be sufficiently met for the following reasons:

(a) The lawful purpose assigned to the use of recording devices is too broad,

(b) The definition afforded to 'recording device' is too broad and may pave the way for the introduction of controversial facial recognition technology and problematic future technology,

(c) The provision for use of recording devices for covert surveillance, in particular drones, is not accompanied by sufficient safeguards and

(d) The requirement for visibility of recording devices for overt surveillance is not sufficiently addressed.

The Bill is not clear regarding who has the authorisation to install, use and access devices. It does not specify the rank of garda, the training required, or whether a person wearing a recording device must be identifiable as a Garda.

ICCL considers that the legislation and the two codes of practice it provides for should be reviewed at early and regular intervals. The legislation must also include far more safeguards and oversight to protect against violations of privacy and data protection rights.

ICCL strongly opposes the inclusion of a provision on the admissibility of evidence. Decisions on evidence should remain strictly with the Courts.

Finally, ICCL are deeply concerned at the proposal to exclude gardaí from criminal liability under the legislation, given that the Bill introduces new offences, including tampering with recording devices.

We urge government to expend more time and resources examining whether expanding Garda surveillance powers is actually necessary. If it finds that it is then government must ensure that every time these powers are used robust safeguards are in place, including adequate oversight, to ensure that rights are not disproportionately interfered with.

Introduction

1. ICCL welcomes the opportunity to make a submission on the Garda Síochána (Digital Recordings) Bill, published on 29 April 2021.[1]

2. This Bill will amend the current statutory provisions in relation to Garda-operated CCTV and Community-based CCTV. Separately, it will allow gardaí to use new surveillance tools and technologies and gain live access to third party CCTV systems. As such, it will significantly expand the surveillance powers of An Garda Síochána (AGS), some of which will apparently be covert and potentially operate in private spaces. In summary, the Bill provides for:

- Body-worn cameras (BWCs), equipped with image, video and sound recording capabilities, in a public place or any other place where a member of the Garda Síochána has lawful authority or permission to be present;
- Non-fixed image, video and sound recording devices, such as camcorders, mobile phones, tablets, other handheld devices and drones, which will have recognition capabilities installed such as Automatic Number Plate Recognition (ANPR) and, in the future, other "emerging technologies", in a public place or any other place where a member of the Garda Síochána has lawful authority or permission to be present;
- CCTV in State-owned or operated vehicles designed for use on land, in water or in the air; and
- Live or real-time feed access to third party CCTV systems, i.e. CCTV systems used for private, domestic purposes and/or CCTV systems used by private commercial entities, or systems not controlled by gardaí; persons contracted with the

[1] This submission was written by ICCL Policy Officers Elizabeth Carthy and Olga Cronin.

Garda Commissioner; or a person approved by the local authority, as currently provided for under Section 38 of the Garda Síochána Act 2005.[2]

3. Surveillance powers intrude on the rights to privacy, protection of personal data, freedom of expression, non-discrimination, peaceful assembly and association. Laws that provide for State surveillance powers, without adequate safeguards to protect these rights and freedoms, risk arbitrary and unlawful infringement of these rights.[3]

4. With the commencement of the Data Protection Act 2018, Ireland now has a relatively robust legal framework providing for safeguards around privacy and data protection.[4] Despite this, ICCL is deeply concerned by findings of the Data Protection Commission (DPC) that AGS has repeatedly infringed data protection law.

5. Own-volition, ongoing inquiries being carried out by the DPC into the surveillance of citizens by local authorities and AGS, through the use of technologies such as CCTV, body-worn cameras, drones and other technologies such as ANPR-enabled systems, have raised serious concerns about AGS's compliance with data protection laws.[5]

---

[2] As of April 26, 2018, according to the Department of Justice there were (i) 35 Garda CCTV schemes throughout the State comprising in excess of 500 cameras, (ii) 45 Community-based CCTV schemes in operation, involving 367 cameras to which gardai have access, and (iii) 1,031 camera zones, under the Garda Safety Camera contract, providing a minimum of 90,000 hours of monitoring and surveying vehicle speed per year.

[3] Former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression Frank La Rue stated: "*National laws regulating what would constitute the necessary, legitimate and proportional State involvement in communications surveillance are often inadequate or non-existent. Inadequate national legal frameworks create a fertile ground for arbitrary and unlawful infringements of the right to privacy in communications and, consequently, also threaten the protection of the right to freedom of opinion and expression.*" Report of Special Rapporteur, Frank La Rue, United Nations, 2013, at paragraph 3. Accessible here: https://info.publicintelligence.net/UN-StateSurveillancePrivacy.pdf

[4] See also Directive (EU) 2016/680 of the European Parliament and of the Council (Law Enforcement Directive), Accessible here: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN. The LED was transposed into Irish law via the Data Protection Act 2018.

[5] Data Protection Commission, DPC Ireland 2018-2020 Regulatory Activity Under GDPR, June 2020, page 63. Accessible here: https://www.dataprotection.ie/sites/default/files/uploads/2020-06/DPC%20Ireland%202018-2020%20Regulatory%20Activity%20Under.pdf. See also Data

Specifically, the DPC has found that AGS has infringed several law enforcement provisions in the Data Protection Act 2018, in respect of the use of ANPR cameras, access to CCTV monitoring rooms, governance issues, appropriate signage and general transparency, and the absence of written contracts with third party processors.

6. Notably, these inquiries considered just five of the country's 500-plus Garda stations[6] (the DPC's inquiries are ongoing[7]). In response to the DPC's inquiries, a CCTV review has been carried out by AGS "to examine all Garda Commissioner CCTV authorisations and the policies, procedures and guidelines that apply to such authorisations".[8] The conclusions of this review and a subsequent examination of the same by the DPC are vital steps that must be undertaken before this Bill is passed, and this review should be made public.

7. The Bill as currently drafted includes some welcome provisions such as requirements to carry out Data Protection Impact Assessments and Human Rights Impact Assessments in some areas, and requirements to consult with the DPC and the Irish Human Rights and Equality Commission ahead of the creation of codes of practice for the use of body-worn cameras, recording devices, and CCTV. We also note the inclusion of some requirements for considerations of necessity and proportionality for authorising surveillance, which is welcome. However, to vastly expand AGS's surveillance powers at a time when the DPC's inquiries have cast serious doubt over data protection compliance by AGS and local authorities, who provide access to AGS through the Community-based CCTV schemes, is extremely concerning.

Protection Commission, Annual report for 2020. Accessible here: https://www.dataprotection.ie/sites/default/files/uploads/2021-05/DPC%202020%20Annual%20Report%20%28English%29.pdf

[6] An Garda Siochana, Garda numbers by station, July 2021, Accessible here: https://www.garda.ie/en/about-us/our-departments/human-resources-and-people-development/garda-hr-directorate/garda-numbers-by-station-31-july-2021.pdf

[7] Data Protection Commission, DPC Ireland 2018-2020 Regulatory Activity Under GDPR, June 2020, 63. Accessible here: https://www.dataprotection.ie/sites/default/files/uploads/2020-06/DPC%20Ireland%202018-2020%20Regulatory%20Activity%20Under.pdf

[8] Ibid, page 70.

8. ICCL urges government to delay this legislation until such time as the DPC is satisfied that AGS has in place proper and sufficient policies and practices to ensure that data protection law is upheld at all times.

Relevant human rights and legal framework

9. ICCL has consistently called for a human rights-based approach to policing[9]. The State is required to ensure that the actions of AGS comply with human rights law and standards as protected by the Irish Constitution, the European Convention on Human Rights (ECHR), the EU Charter of Fundamental Rights and Freedoms (CFR) and the UN human rights treaties that Ireland has ratified. AGS has a statutory duty to promote equality, eliminate discrimination, and protect the human rights of members, staff, and the persons to whom they provide services, which effectively includes all members of the public.[10]

10. ICCL considers that this legislation, in providing for powers in relation to digital recording and surveillance tools, will impact people's rights to privacy, protection of personal data, freedom of expression, non-discrimination, protest, and association.

11. The right to privacy is protected by the Irish Constitution, with the Irish courts holding that the right to privacy is one of the unenumerated rights which flow from Article 40.3.1.[11] Article 8 of the ECHR and article 7 of the CFR and article 17 of the ICCPR enshrine the right to respect for private and family life.[12] The European Court of

[9] See for example, Alyson Kilpatrick, ICCL, A Human Rights Based Approach to Policing in Ireland, 2018. Accessible here: https://www.iccl.ie/wp-content/uploads/2018/09/Human-Rights-Based-Policing-in-Ireland.pdf

[10] Section 42, Irish Human Rights and Equality Commission Act 2014.

[11] Article 40.3.1 provides that: "*The State guarantees in its laws to respect, and as far as practicable, by its laws to defend and vindicate the personal rights of the citizen*" The right to privacy can also be drawn from a number of Constitutional rights: the right to private property (Article 43); protection of family life (Article 41); the inviolability of the dwelling (Article 40.6.1); personal autonomy (Article 40.3.1 and Article 40.3.2; respect for human dignity (Preamble); privacy of the ballot (Article 16.1.4); litigation privacy (Article 34); right to form associations and unions (Article 40.6.1).

[12] ECHR article 8 provides: "(1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) 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

Human Rights (ECtHR) has previously urged the courts to scrutinise whether the growing sophistication of surveillance monitoring operations has been *"accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights"*.[13] The ECtHR has also stated that member states do not "*enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance*"[14]

12. The UN Human Rights Council recently adopted a resolution recognising the importance of "*a human rights-based approach to new and emerging digital technologies*" and of "*ensuring appropriate safeguards and human oversight in the application of new and emerging digital technologies*".[15]

13. In considering the right to privacy, the reasonable expectation of privacy while in public should also be considered. The independent regulator of the overt use and public operation of surveillance camera systems by the police in England and Wales, the Surveillance Camera Commissioner, has outlined that while a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. For example, two people having a conversation on a street or on a bus may have a reasonable expectation of privacy over that discussion, even though they are in public. The contents of such a conversation should therefore still be considered private

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."

[13] *Szabó and Vissy v Hungary* (Application no.: 37138/14) para 68. The monitoring techniques at the heart of this case included secret house search and surveillance with recording, opening of letters and parcels, as well as checking and recording the contents of electronic or computerised communications, all without the consent of the persons concerned. Accessible here: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-160020%22]}

[14] *Klass and Others v Germany* (Application no: 5029/71) para 49. Accessible here: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57510%22]}

[15] UN Human Rights Council, Resolution A/HRC/47/L.12/Rev.1, New and emerging digital technologies and human rights, July 13, 2021. Accessible here: https://undocs.org/A/HRC/47/L.12/Rev.1

information.[16] Similarly, the European Court of Human Rights has stated that there is *"a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'."*[17]

14. As noted by the Law Reform Commission, privacy is not merely instrumental to the achievement of other goals but is a basic human right that applies to all persons by virtue of their status as human beings[18]; it is closely connected to inherent human dignity and human freedom, autonomy and self-determination, and it is an organising principle of civil society closely connected to the democratic life of the polity.[19]

15. In respect of the right to freedom of expression, Article 40.6.1.i of the Constitution safeguards, *"The right of the citizens to express freely their convictions and opinions"*. The free exchange of ideas is the lifeblood of a democratic and free society and mature democracies require that a critique of ideas and institutions is not just tolerated but encouraged. The right to freedom of expression is also asserted in Article 11 of the CFR, Article 10.1 of the ECHR, Article 19 of the Universal Declaration of Human Rights, and Article 19 of the International Covenant on Civil and Political Rights (ICCPR).
16. The right to non-discrimination is enshrined in Article 14 of the ECHR, Article 21 of the CFR, Article 2 of the International Covenant on Economic, Social and Cultural Rights (ICESCR) and Article 2 of the ICCPR.
17. In a democracy, people have the right to express their views, peacefully protest, and gather together in public to do so. These rights to peaceful assembly and association are fundamental to the freedoms that lie at the heart of democracy. Numerous human

[16] UK Home Office, Covert Surveillance and Property Interference Revised Code of Practice, June 2018. Accessible here: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf
[17] *Peck v United Kingdom* (App no. 44647/98, para. 57. Accessible here: https://hdoc.echr.coe.int/eng#{%22itemid%22:[%22001-60898%22]}
[18] Law Reform Commission, Report Series: Privacy: surveillance and the interception of communications, LRC 57-1998, page 2. Accessible here: https://www.lawreform.ie/_fileupload/Reports/rPrivacy.pdf
[19] Ibid, pgs 3 & 4.

rights bodies have confirmed that States have a duty to facilitate protest, as well as the importance of this right to a functioning, democratic society.[20] The right to protest is protected by the Constitution, the ECHR, the CFR and the ICCPR through the rights to freedom of assembly, freedom of expression and freedom of association.[21]

18. The rights outlined above should be the guiding principles in the drafting of any legislation seeking to expand the powers of surveillance of AGS. This submission examines these rights and the relevant human rights and legal framework under each head of the Bill, considers the current surveillance powers of AGS, highlights concerns raised by the DPC and makes a number of recommendations on the basis of this analysis.

19. It should be noted that ICCL will only make reference to the heads of the Bill to which it wishes to comment on or make recommendations.

[20] See European Court of Human Rights, Guide to Article 11, Freedom of Assembly and Association, updated December 2020, Accessible here: https://www.echr.coe.int/Documents/Guide_Art_11_ENG.pdf For the scope of the right to protest, see also UN Human Rights Committee, General Comment 37 on article 21 Right of Peaceful Assembly, 23 July 2020, CCPR/C/GC/37, Accessible here:https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx

[21] The European Court of Human Rights has stressed the close symbiotic link between the Article 10 and 11 ECHR freedom of expression and freedom of assembly protections. Peaceful political protests are constitutionally protected pursuant to the Article 40.6.1 The Irish Constitution guarantees to freedom of expression and assembly "It is quite clear that persons who assemble peacefully on the public highway [to protest] are prima facie entitled to the benefit of the constitutional guarantee" – *Francis Hyland v. Dundalk Racing* [2014] IEHC 60 at para. 76. per Hogan J. see also: *The People (DPP) v. Kehoe* [1983] I.R. 136, 139 per McCarthy J.

Part One: Introductory provisions

Head 2: Interpretation

20. Head 2 provides that "*a 'recording device' means a non-fixed device capable of recording or processing, including through the use of Automatic Number Plate Recognition (ANPR), visual images, on any medium, from which a visual image or moving visual images may be produced and includes any accompanying sound or document*". An explanatory note under Head 2 further expands on this to say, "*Of particular importance is the definition of 'recording device' which is intended to be broad enough to encompass recording of an image/images where the device may have software installed such as ANPR to read licence plates, or possible emerging technologies in the future.*"

21. The broadness of this definition concerns ICCL. It includes the possible use of camcorders, mobile phones, tablets, other handheld devices and drones, while also intending to cover "*possible emerging technologies in the future.*" It may cover different types of intrusive surveillance technology that already exist, such facial recognition technology (FRT), and other future systems with intrusive capabilities. This is deeply problematic as certain existing surveillance technologies, which may fall under this definition, pose significant human rights concerns.

22. FRT systems have "*renowned ethnic, racial and gender biases against people of colour and women.*"[22] The International Network of Civil Liberties Organisations (INCLO), of which ICCL is a member, has conducted research which highlights serious concerns in respect of the use of this technology.[23] FRT and other biometric surveillance tools enable mass surveillance and discriminatory targeted surveillance. They have the capacity to identify and track people everywhere they go, undermining

[22] INCLO, Facial recognition tech stories and rights harms from around the world, 2021, available at https://files.inclo.net/content/pdf/19/in-focus-facial-recognition-tech-stories.pdf
[23] Ibid.

the right to privacy and data protection, the right to free assembly and association, and the right to equality and non-discrimination. The INCLO report, comprising of case studies from 13 countries, outlines how these rights are affected by FRT. ICCL strongly opposes the use of such technology and, with over 170 civil society organisations and activists from 55 countries around the world, is calling for an outright ban on biometric surveillance in public spaces.[24]

23. In addition, consideration must be given to the 'Internet of Things' and the proliferation of connected devices with sensors and recording capabilities that are now used in people's private homes and lives, i.e. smart doorbell cameras, virtual/digital assistants, Amazon Alexa's microphones which can capture private conversations inside homes and cars, or wearables such as Fitbit which can track a person's movements and vital signs. These devices, which can track a detailed description of people's lives, have already been used for law enforcement purposes in the US.[25] Serious privacy concerns have been raised in Ireland in respect of contractors capturing and listening to Siri users' private information and interactions.[26]

24. ICCL recommends that the definition of a recording device be narrowed to make clear that it does not encompass FRT or other forms of biometric surveillance given the significant risk of infringing a range of rights. Alternatively, if biometric tracking devices are introduced as "recording devices", the Bill must explicitly include much

[24] Access Now, et al., Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance, 7 June 2021.
[25] Wired, Alexa, Play My Alibi: The Smart Home Gets Taken to Court, August 31, 2020. Accessible here: https://www.wired.com/story/gadget-lab-podcast-470/ See also Cappellino A, Expert Institute, The Amazon Echo: Expert Witness in a Murder Trial?, February 21, 2021. Accessible here: https://www.expertinstitute.com/resources/insights/amazon-echo-expert-witness-murder-trial/ See also NBC News, Amazon's Alexa may have witnessed alleged Florida murder, authorities say, November 2, 2019. Accessible here: https://www.nbcnews.com/news/us-news/amazon-s-alexa-may-have-witnessed-alleged-florida-murder-authorities-n1075621
[26] The Journal, Hundreds of Cork-based Apple contractors lose jobs after hearing Siri users' private conversations, August 29, 2019. Accessible here: https://www.thejournal.ie/job-losses-apple-cork-siri-recordings-4786859-Aug2019/

greater safeguards to ensure any access to such devices is heavily regulated, monitored and minimised.

Head 3: Application of the Act

Transparency and accountability

25. ICCL welcomes the provision under Head 3(3) that any garda in breach of any code of practice made under this Bill will be subject to disciplinary proceedings. This is necessary to give real meaning and effect to the Code.

26. However, we express serious concern that under Head 3(4), a garda cannot be subject to criminal or civil proceedings for breach of the Act. This is unacceptable given the need for real accountability for breaches of data protection law. ICCL considers that there may be instances where abuse of surveillance technology may constitute harassment, which is a criminal offence. Decisions to authorise surveillance technology should be subject to judicial review to ensure transparency and accountability in the case of potential abuse of power. Gardaí should also be held criminally liable under the Act for offences created by the Act. ICCL can see no reason why a Garda should not be held criminally accountable for tampering with a device under Head 6(5) for example.

Part Two - Recording by AGS for specified purpose

Current surveillance powers of An Garda Síochána

27. Fundamental rights are generally not absolute, and it is acknowledged that states may interfere with fundamental rights in the pursuit of legitimate public interest objectives, provided the interferences are proportionate and are limited to what is necessary in a democratic society. A balance must be struck between ensuring that the state has effective and legitimate tools at its disposal in order to fulfil the functions of government, and the protection of fundamental rights and freedoms.

28. With this in mind, it is worth recalling that AGS already has significant surveillance powers which can be broadly divided into four types of surveillance, under three pieces of legislation. It is regrettable that just one of these powers is subject to judicial approval.[27]

i. Under the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993, in investigating serious offences or suspected serious offences, a garda can, with warrant authorisation from the Minister for Justice, tap telephones and/or intercept postal packets or telecommunications messages for up to three months.

ii. The Communications (Retention of Data) Act 2011, which is currently being challenged in the Court of Justice of the European Union[28], obliges mobile phone

[27] Dr TJ McIntyre of DRI and Privacy International, 'Stakeholder Report Universal Periodic Review 25th Session – Ireland', September 2015.

[28] *Graham Dwyer v. The Commissioner of An Garda Siochana& Ors* [2020] IESC 4, Accessible here: https://www.bailii.org/ie/cases/IESC/2020/2020IESC4_0.html . Supreme Court judge Mr Justice Clarke has sought clarification from the European Court of Justice regarding three areas of European law, namely: (i) Whether a system of universal retention of metadata for a fixed period of time is never permissible, irrespective of how robust any regime for allowing access to such data may be; (ii) The

and internet service providers in Ireland to retain the metadata relating to all telephone calls, text messages, emails (for up to two years) and communications on the internet (for up to one year). Under the Act, a member of AGS not below the rank of chief superintendent can, for the purposes of preventing, detecting, investigating or prosecuting a serious offence, safeguarding the security of the State and the saving of human life, seek and obtain access to that metadata.

Former Judge, Mr Justice John Murray, who examined the impact of this law on Irish journalists in 2017, stated that the Act provides for "*a form of mass surveillance of virtually the entire population of the State*" and "*...the retained data constitutes vital and comprehensive information concerning the private lives and professional activities of everybody, without exception.*" He found that the Act was "*universal and indiscriminate in reach and application*".[29]

iii. The Criminal Justice Surveillance Act 2009 allows for covert surveillance, or monitoring, observing, listening to or making a recording of a particular person or group of persons or their movements, activities and communications, or monitoring or making a recording of places or things, by way of using tracking and surveillance devices. Only "surveillance devices" (audio bugs and covert video cameras) require judicial authorisation; "tracking devices" (such as GPS trackers placed on cars or other

criteria whereby an assessment can be made as to whether any access regime to such data can be found to be sufficiently independent and robust; and (iii) Whether a national court - should it find that national data retention and access legislation is inconsistent with European Union law - can decide that the national law in question should not be regarded as having been invalid at all times but rather be regarded as invalid prospectively only. Also note: Digital Rights Ireland v Minister for Communications is an ongoing challenge by DRI in the High Court against data retention, following the Court of Justice of the European Union striking down the Data Retention Directive as incompatible with the Charter of Fundamental Rights of the European Union – the first time a directive was invalidated on fundamental rights grounds.

[29] Mr Justice John Murray, Review of the Law on the Retention of and Access to Communications Data, pages 2, 9 & 11. Accessible here: http://www.justice.ie/en/JELR/Review_of_the_Law_on_Retention_of_and_Access_to_Communications_Data.pdf/Files/Review_of_the_Law_on_Retention_of_and_Access_to_Communications_Data.pdf

vehicles) do not. A 'surveillance device' under this act does not include CCTV within the meaning of Section 38 of the Garda Síochána Act 2005, or a camera used to take photographs of any person who, or any thing that, is in a place to which the public have access. Judges can authorise covert surveillance for up to three months in case of surveillance devices. However, a garda can carry out this surveillance without judicial authorisation if it has been approved by a superior officer (of Superintendent rank or above) for up to 72 hours under certain conditions. In the case of planting tracking devices, a garda can use tracking devices for up to four months with internal approval from an AGS member of Superintendent rank or above (i.e. no judicial authorisation is necessary).

29. Concerns relating to the oversight of these powers have been highlighted by privacy experts, such as Dr TJ McIntyre of University College Dublin and Digital Rights Ireland. They include:

i. That systems of internal approval, as opposed to judicial approval, are particularly open to abuse;[30]

ii. Irish law does not provide for the notification of individuals who have been the subject of surveillance measures after the fact, even though this has been recognised by the ECtHR as an important safeguard for the right to privacy;[31]

iii. The system whereby a nominated High Court judge is tasked with reviewing the legislation, is inadequate as the judges' annual reports have "*consisted exclusively of a few formulaic paragraphs which recite that on a particular day certain (unspecified) documents were inspected, certain (unspecified) queries*

[30] Digital Rights Ireland and Privacy International, The Right to Privacy in Ireland Stakeholder Report Universal Periodic Review 25th Session – Ireland, September 2015, para 16.
[31] Ibid, para 20.

answered and as a result the judge is satisfied that the relevant authorities are in compliance with the law";[32]

iv. Lack of resources and specific expertise have been laid bare after the DPC identified issues which a designated judge did not;[33]

v. Although there are judges designated to oversee the various laws that provide for the interception of communications, access to retained communications data, and the use of "surveillance devices" and tracking devices respectively, the role of the judge is limited to examining the surveillance itself – there is no statutory power to examine the later use of surveillance material;[34] and

vi. Lack of transparency around the Complaints Referee mechanism makes it "impossible" to determine the mechanism's effectiveness.[35]

Head 5: Use of recording device by the Garda Síochána

Human rights concerns relating to the use of recording devices

30. This head expands the use of recording devices by members of AGS in a public place or where an on-duty Garda has lawful authority/permission to be present. As mentioned above, ICCL has serious concerns about the broad definition of a 'recording device' and how the inclusion of "emerging technologies in the future" could lead to the use of biometric surveillance tools such as FRT.

[32] Ibid, para 26.

[33] EU Fundamental Rights Agency, McIntyre, TJ, Short Thematic Report National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies: Legal update, page 16. Accessible here: https://fra.europa.eu/sites/default/files/fra_uploads/ireland-study-data-surveillance-ii-legal-update-ie.pdf

[34] Ibid, page 9.

[35] Digital Rights Ireland and Privacy International, 'The Right to Privacy in Ireland Stakeholder Report Universal Periodic Review 25th Session – Ireland', September 2015, para 32.

31. According to AGS's Modernisation and Renewal Programme 2016-2021, AGS plans to use FRT in order to "*track suspects from CCTV*"[36] while "*Technologies such as face in the crowd and shape in the crowd biometrics will be used to identify key targets*".[37] The inclusion of these plans diametrically opposes the Department of Justice's code of practice for Community-based CCTV schemes prohibiting the use of automatic FRT.[38]

32. These surveillance technologies pose a risk to the rights to privacy, data protection, freedom of expression, and freedom of assembly. Under human rights law, the government has to ensure that any infringement on rights must be necessary and proportionate to a legitimate aim. ICCL believes that the expansion of the use of recording devices has not been demonstrated as necessary or proportionate to the achievement of legitimate aims in the Irish context.

Need to clarify who can use a recording device

33. Head 5(1) provides that a Garda may operate a recording device "in the course of his or her duties". It does not specify that the Garda has to be of a specific rank, have received any specific training, or be identifiable as a Garda. ICCL recommends that these requirements be included to ensure that recording devices are only ever used in a lawful manner by fully qualified and fully trained Gardaí.

Need for clear and specific purpose to use a recording device

34. Head 5(2) specifies that the use of recording device by a Garda must be for a specific primary purpose, namely: (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.[39] This provides for an overly

[36] An Garda Siochana, An Garda Síochána Modernisation and Renewal Programme 2016-2021, page 44. Accessible here: https://www.garda.ie/en/about-us/publications/policing-plans/strategy/modernisation-and-renewal-programme/modernisation-and-renewal-programme-2016-2021.pdf
[37] Ibid, page 45.
[38] Department of Justice, Code of Practice for Community-based CCTV schemes, para 4.10 http://www.justice.ie/en/JELR/PD_001_Code_of_Practice_2019.pdf/Files/PD_001_Code_of_Practice_2019.pdf
[39] Garda Síochána (Digital Recordings) Bill, Heads 5 & 6.

broad range of purposes, which goes against the human rights requirement that any infringement on rights must be as minimal as possible to achieve a specified legitimate aim. The overuse of such recording devices to secure 'public order' could have a significant chilling effect on the exercise of the right to freedom of assembly in particular.

35. While we recommend narrowing the purposes outlined in this Head, the provision in Head 5(3) that any use of a recording device must be necessary and proportionate to the purposes stated is welcome. However, ICCL would welcome clarification from the Government as to how necessity can be proven in the Irish context, given that there is no apparent evidence-based justification for the expansion of surveillance in Ireland.

Lack of mention of visibility or signage of the recording device

36. There is no mention of the requirement for visibility or signage in respect of the use of recording devices under Head 5. This raises significant data protection concerns. Surveillance could be considered covert if it is carried out in a manner either calculated to ensure, or having the effect of ensuring, that any persons subject to the surveillance are unaware that it is or may be taking place. Covert surveillance requires much greater safeguards and is only permitted in exceptional circumstances. As referred to below, the DPC has very clearly set out that covert surveillance should not be used for the prevention of crime. It is therefore vital that the distinction between overt and covert is maintained.

37. The DPC has stated that "*The use of recording mechanisms to obtain data without an individual's knowledge is generally unlawful. Covert surveillance is normally only permitted on an exceptional case-by-case basis where the data are kept for the purposes of preventing, detecting or investigating offences, or apprehending or prosecuting offenders. This provision automatically implies that a written specific policy be put in place detailing the purpose, justification, procedure, measures and safeguards that will be implemented with the final objective being, an actual involvement of An Garda Síochána or other prosecution authorities for potential criminal investigation or civil legal proceedings being issued, arising as a*

consequence of an alleged committal of a criminal offence(s). Covert surveillance must be focused and of short duration. A DPIA should be carried out prior to the installation of any covert systems, to clearly assess whether the measure can be justified on the basis of necessity and proportionality to achieve the intended purpose. Only specific (and relevant) individuals/locations should be recorded. If no evidence is obtained within a reasonable period, the surveillance should cease. If the surveillance is intended to prevent crime, overt cameras may be considered to be a more appropriate measure, and less invasive of individual privacy."[40]

38. ICCL recommends that the use of all recording devices must have increased safeguards to ensure that their use is compliant with human rights and data protection concerns. Requiring that all recording devices are visible is one such safeguard. Other safeguards could include more frequent reviews of the code of practice in respect of recording devices than every five years as stipulated in this head, annual publication of reports/reviews/audits of the use of recording devices, streamlined data protection training/certification for all Garda users of these devices, and ongoing access to information and training about data protection/privacy for same.

Privacy risks of drones

39. The use of drones feature under two separate headings in the Bill - Head 5 and Head 9, given that drones fall under the definition of recording device outlined in the interpretation section and included at Head 5(1). It is worth recalling, and endorsing the recommendations previously made by the European Article 29 Working Party (WP29)[41] in respect of drone use by law enforcement purposes. WP29 states that the

[40] Data Protection Commission. CCTV Guidance for data controllers, https://www.dataprotection.ie/sites/default/files/uploads/2019-05/CCTV%20guidance%20data%20controllers_0.pdf

[41] The Article 29 Working Party was set up via Article 29, Directive 95/46/EC, providing independent non-binding advice on the meaning of Directive 95/46/EC. WP29 ceased to exist when the GDPR and LED came into effect. However, the work of the WP29 can be used in the interpretation and understanding of the GDPR where the European Data Protection Board has not issued any replacement guidance.

use of personal data collected by means of drones by the police and other law enforcement authorities should:

i. Comply with necessity, proportionality, purpose limitation, data minimisation and privacy by design principles; a strict and justified retention period should be set;

ii. The transparency principle should be respected. Data processing carried out by the use of drones should be prescribed by law to be transparent and foreseeable to data subjects. As far as possible, the latter should be informed of the processing and their corresponding rights;

iii. Law enforcement data processing carried out by means of drones should not allow for constant tracking of individuals or, at the very least, where constant tracking is found to be strictly necessary, this should be restricted to law enforcement warranted investigations. Technical and sensing equipment used must be in line with the purpose of the processing;

iv. The prohibition of automated enforcement of decisions also applies to these uses. The data processed via drones should be further scrutinised by a human operator before any decision adversely affecting an individual is made;

v. Courts should generally be able to review the use of drones for intelligence and law enforcement purposes in line with national practice;

vi. A regular review of the necessity to process personal data by the use of drones and of compliance of this use with evolving legal frameworks should be carried out;

vii. The use of drones for law enforcement, even in warranted investigations, should require a higher regime of approval in the organisational hierarchy. Depending on national law, personal data collected by the use of drones for these

types of investigations should be incorporated in the administrative files that may be used in court.[42]

viii. As previously identified by the WP29, drones pose several privacy risks in relation to the processing of data carried out by equipment on a drone. The difficulty of not being able to view drones from the ground poses specific transparency risks as it may be difficult, if not impossible, to ascertain (i) what data processing equipment is on the drone; (ii) what purpose the data is being collected for and (iii) who is collecting the data. Drones also provide the opportunity for the collection of a wide variety of information for long periods of time across large areas. As flagged by the WP29, *"Even higher risks for the rights and freedoms of individuals arise when the processing of personal data by means of drones is carried out for law enforcement purposes".*[43]

Need for a pilot scheme

40. Given the resource and rights implications of introducing these technologies, a pilot scheme is recommended. This was carried out in relation to the introduction of audio-visual recording of Garda interviews. This scheme could test the effectiveness of these devices and could facilitate the carrying out of a human rights impact assessment and data protection impact assessment (DPIA) of the operation of these devices.

Head 6: Use of body-worn cameras by An Garda Síochána

41. This head introduces the use of body-worn cameras by members of Garda Síochána. ICCL has serious concerns about the use of these surveillance technologies and the risk that they will disproportionately infringe on privacy and data protection rights. We oppose the introduction of body-worn cameras for Gardaí and, if they are introduced,

[42] Article 29 Working Party, Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones, June 16, 2015. Accessible here: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2015/06/wp231_en.pdf

[43] Ibid.

we call for a pilot roll-out to prove they are necessary in an Irish context. Stringent safeguards are required if they are to be introduced.

42. ICCL was concerned at the significant risk to human rights posed by the recommendation by the Commission on the Future of Policing in Ireland to introduce body-worn cameras (BWCs).[44] BWCs and other surveillance technologies pose a risk to the rights to privacy, data protection, freedom of expression, and freedom of assembly. Under human rights law, the government must ensure that any infringement on rights must be necessary and proportionate to a legitimate aim. ICCL believes that the necessity of introducing BWCs has not been demonstrated as necessary or proportionate to the achievement of legitimate aims in the Irish context.

Need for clear and specific purpose to use a BWC

43. The Bill specifies that the use of a BWC by a Garda must be for a specific primary purpose, namely: (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.[45]

44. This provides for an overly broad range of purposes, which goes against the human rights requirement that any infringement on rights must be as minimal as possible to achieve a specified legitimate aim. The use of BWCs to secure 'public order' could have a significant chilling effect on the exercise of the right to freedom of assembly in particular. ICCL recommends that if BWCs are rolled out in Ireland, the primary purpose must be connected to a demonstrated need and an extremely narrow purpose such as preventing serious harm or loss of life.

[44] Commission on the Future of Policing in Ireland, The Future of Policing in Ireland, 18 September 2018,"AGS should develop a plan to develop body work cameras. There is a significant amount of experience in other jurisdictions which could be tapped for best practice."
[45] Garda Síochána (Digital Recordings) Bill, Heads 5 & 6.

45. While we recommend narrowing the purposes outlined in this Head, the provision in Head 5(3) that any use of a recording device must be necessary and proportionate to the purposes stated is welcome. ICCL would again welcome clarification from government as to how necessity can be proven in the Irish context, in particular in relation to the efficacy of the use of BWCs to achieving these aims.

Data protection concerns around the introduction of body-worn cameras

46. The Data Protection Commission sets out that a detailed data protection assessment of the use of body-worn cameras should be carried out, such as a Data Protection Impact Assessment.[46] Key issues include minimising the amount of personal data recorded; ensuring that recordings are stored securely and kept only for a stated purpose; and responding appropriately to subject access requests.[47] These issues are not expressly addressed in this legislation. Given the importance of data protection and human rights considerations to the use of this technology, ICCL recommends that these concerns be addressed in the Bill.

47. Given the resource and rights implications of introducing these technologies, ICCL also recommends a pilot scheme be carried out. Such a scheme is crucial. In a previous submission to the committee on BWCs, ICCL highlighted how, after assessing research carried out in other jurisdictions where BWCs have been introduced, ICCL had not found consistent, conclusive or convincing evidence that BWCs have led to better policing or that evidence of crimes gathered by such cameras have generated better outcomes in the criminal justice system. On the contrary, ICCL found that flagship research carried out in Rialto, California - often cited to prove the benefits of BWCs by governments, police forces and those that stand to profit from the roll out of BWCs - has since been significantly undermined by other, larger research projects and by that study's own authors.[48]

[46] DPC, Guidance on the use of body worn cameras or action cameras, 2020.
[47] Ibid.
[48] Irish Council for Civil Liberties, Body-worn cameras for An Garda Síochána, October 16, 2019. Accessible here: https://www.iccl.ie/wp-content/uploads/2019/10/ICCL-Body-Worn-Cameras-DoJ-submission.pdf

Head 7: Code of practice under this part

48. This head includes a requirement that the Garda Commissioner shall draft a code of practice in relation to recording devices and body-worn cameras and that in preparing a draft code of practice, the Garda Commissioner shall ensure that a data protection impact assessment and human rights impact assessment is carried out. ICCL welcomes the requirement for both assessments and calls on the Commissioner to ensure that these assessments take into account the range of rights that may be affected by the use of this technology, including the right to dignity, privacy, non-discrimination, freedom of expression and assembly, and fair trial rights, including the presumption of innocence. We also call on the Commissioner to assess the impact of surveillance technology on community policing and relationships.

49. We consider that it should be made explicit in the Bill that there shall be no expansion of surveillance powers, as provided for under the legislation, until such time as a Code of Practice is adopted by the Minister. ICCL further recommends that the review be carried out on an annual or bi-annual basis given the ongoing risk to rights posed by rapid advances in surveillance technologies.

Part Three - Closed circuit television

(a) The current legal framework

50. Section 38 of the Garda Síochána Act 2005 currently provides that the Garda Commissioner may authorise 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. This section of the Garda Síochána Act 2005 (which will be repealed and replaced by this new Bill) in the main provides that:

- The Garda Commissioner can specify areas where CCTV is warranted.
- The Garda Commissioner can give authorisation to (a) a member of AGS, (b) persons who meet established criteria and who are retained under a contract with the Garda Commissioner, and (c) persons who meet the established criteria and whose application for authorisation in respect of a specified area within the administrative area of a local authority has been approved by the local authority after consulting with the joint policing committee for that administrative area.
- The Garda Commissioner can set criteria for the above.
- Persons given authorisation for community-based CCTV under local authority grounds must make sure gardaí have access "at all times" to the CCTV authorised by the Commissioner. The lawful basis for a council's sharing of live-feed CCTV footage with AGS is contained in section 38(7) of the An Garda Síochána Act 2005.
- The Garda Commissioner may issue directions to authorised persons pertaining to the CCTV and with the minister's consent, revoke authorisation. Person found guilty of not complying with a revocation order can be fined €2,500 or jailed for 6 months.
- The Minister shall issue guidelines to the Garda Commissioner concerning the supervision and control of the monitoring of CCTV by authorised persons. She can also revise/withdraw such guidelines.
- Section 38 of AGS Act 2005 does not apply to installation or operation of CCTV "*on any premises by the owner or occupier of the premises for the purpose of safeguarding persons or property on the premises or in its environs*".

51. S.I. No. 289/2006 - Garda Síochána (CCTV) Order, 2006 (to be revoked by this Bill) outlines the criteria to be met under section 38(3)(c) of the Garda Síochána Act 2005 for a person to be deemed an "authorised person" for the installation and operation of CCTV in specific area of a local authority.

(b) Inquiries carried out by Data Protection Commission into AGS and local authorities

52. In last year's DPC Ireland 2018-2020 Regulatory Activity Under GDPR report, the Data Protection Commission outlined that, in June 2018, it began a number of own-volition inquiries under the Data Protection Act 2018 into the surveillance of citizens by the state sector for law enforcement purposes through the use of technologies such as CCTV, BWCs, drones and other technologies such as ANPR enabled systems. The first module is focused on 31 local authorities in Ireland and their use of the Community-based CCTV schemes, and the second is on AGS and their Garda-operated CCTV schemes.

Inquiries into AGS

53. The inquiries concerning AGS followed the introduction of "smart" CCTV camera schemes, with the potential for FRT and ANPR, being introduced in locations such as Limerick and Duleek.[49] It was reported in the media that 14 towns in Limerick[50] were to introduce 44 smart CCTV cameras which would be linked with data from environmental and footfall sensors as well as number plate recognition.[51] Limerick City

[49] Buckley, R, Oireachtas Library and Research Service, Data Privacy and Community CCTV Schemes, 2019, page 21. Accessible here: https://data.oireachtas.ie/ie/oireachtas/libraryResearch/2019/2019-01-14_data-privacy-and-community-cctv-schemes_en.pdf

[50] The towns were: Abbeyfeale; Adare; Askeaton; Caherconlish; Castleconnell; Cappamore; Croom; Foynes; Kilmallock; Murroe; Newcastle West; Pallasgreen; Patrickswell and Rathkeale. See here: https://www.limerick.ie/council/newsroom/news/44-high-spec-smart-cctv-cameras-being-installed-14-county-limerick-towns

[51] Edwards, E, "Data Protection Commissioner to investigate State CCTV schemes" The Irish Times (01 March 2018), Accessible here: https://www.irishtimes.com/business/technology/data-protection-commissioner-to-investigate-state-cctv-schemes-1.3410181

and County Council also announced that the system would allow for remote access of the CCTV feed on smartphones enabling authorised users access to live footage, while a number of 'tourism' cameras would also be installed to allow for live online streaming. As of last year, the council planned to expand this system.[52]

54. Such plans were flagged in AGS' 120-page five-year programme Modernisation and Renewal Programme (2016-2021), the contents of which raise questions about the principles of legitimacy, necessity and proportionality. The programme clearly outlined AGS's plans to use FRT to track suspects from CCTV, and using ANPR technology to track suspected vehicles on the motorway.[53] The same programme explained that AGS planned to "*expand use of ANPR for both roads policing and as an investigative and intelligence tool*"[54]; "*expand Garda access to data from ANPR systems and CCTV cameras throughout the country by working with State and commercial organisations*"[55]; create a centralised system to store CCTV, audio files and ANPR data "*to allow for wider access and analysis*"[56]; and use "*technologies such as face in the crowd and shape in the crowd biometrics will be used to identify key targets*"[57]. It is notable that the term "data protection" is mentioned just once in the document.[58] We would highlight that the Department of Justice specifically states, in its code of practice for Community-based CCTV schemes, that the use of automatic FRT is prohibited.[59]

[52] Smart CCTV Pilot Project - Hinterland Study, Accessible here: https://www.limerick.ie/smart-limerick/programme-4-infrastructure/smart-cctv-pilot-project-hinterland-study
[53] An Garda Siochana: Modernisation and Renewal Programme 2016-2021, June 9, 2016, page 44, Accessible here: https://www.garda.ie/en/about-us/publications/policing-plans/strategy/modernisation-and-renewal-programme/modernisation-and-renewal-programme-2016-2021.pdf
[54] Ibid, page 53.
[55] Ibid.
[56] Ibid, page 101.
[57] Ibid, page 45.
[58] Ibid, page 50.
[59] Department of Justice, Code of Practice for Community-based CCTV schemes, para. 4.10 http://www.justice.ie/en/JELR/PD_001_Code_of_Practice_2019.pdf/Files/PD_001_Code_of_Practice_2019.pdf

55. The DPC's inquiry involved inspections in relation to Garda-operated CCTV schemes at Garda Stations in Tullamore; Henry Street, Limerick; Pearse Street, Dublin; Duleek and Ashbourne, Co Meath. It found AGS had infringed several law enforcement provisions in the Data Protection Act 2018, in respect of the use of ANPR cameras, access to CCTV monitoring rooms, governance issues, appropriate signage and general transparency, and the absence of written contracts with third party processors.

Automatic Number Plate Recognition (ANPR) cameras

56. The DPC found that 50 percent of cameras used in the Duleek and Donore Garda-operated CCTV scheme in Co Meath (seven of 14) were ANPR cameras. The DPC explained the capabilities of the ANPR cameras[60] before stating: "*As 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.*"[61]

Excessive access to monitoring rooms

57. The DPC found that the monitoring rooms at the Garda stations in Pearse Street, Ashbourne and Henry Street were co-located with the station's command centre and radio control centre. This had the effect of all Gardaí in Pearse Street station having access to 34 live-feed CCTV screens; 600 gardaí in Henry Street station having access

[60] The DPC found AGS infringed Section 75(3) of the Data Protection Act, 2018 as it has failed as controller to implement an appropriate data protection policy in respect of the ANPR cameras and associated activities; AGS infringed Section 76, as it acted passively as the controller in taking over a predesigned system and cannot have assessed the requirement for or implemented the appropriate data protection by design and default safeguards; and AGS was in breach of Section 84 by reason of its failure to carry out a data protection impact assessment on the ANPR surveillance system for which it is the data controller, to test the necessity of ANPR cameras and to demonstrate that the use of ANPR cameras is justified and proportionate vis a vis the crime levels in the area it is trying to address. In accordance with Section 84(1), this assessment should have been completed before the processing operations commenced. Accessible here: https://www.dataprotection.ie/sites/default/files/uploads/2020-06/DPC%20Ireland%202018-2020%20Regulatory%20Activity%20Under.pdf

[61] DPC Ireland 2018 - 2020 Regulatory Activity Under GDPR, June 2020, page 64. Accessible here: https://www.dataprotection.ie/sites/default/files/uploads/2020-06/DPC%20Ireland%202018-2020%20Regulatory%20Activity%20Under.pdf

to more than 50 monitoring screens; and all gardaí in Ashbourne station having access to one screen with several CCTV views.

58. The DPC found some Garda-operated CCTV systems appeared to have no capability to record who accessed the system and when. Elsewhere it found there was an electronic audit trail capable of identifying who accessed the system and when, but "*there was no evidence of proactive auditing of the access logs such that improper use could be detected*". The DPC also found, in one case, that a single generic login to the access the system posted on a whiteboard, making it near impossible to identify who had accessed the system.[62]

Training of staff

59. The DPC found there was an absence of a training programme on the use of Garda-authorised CCTV systems for gardaí attached to two CCTV schemes.

Privacy by Design and Default

60. Gardaí in Duleek and Donore routinely failed to manually return the 'pan, tilt and zoom' CCTV cameras to their original focus. In some cases, the cameras were left directed at private homes, while one camera was fixed on the front door of a local priest's home, resulting in his home activities being permanently on view at Ashbourne Garda Station.[63]

Retention

61. The DPC found an inconsistency in application of the AGS Code of Practice for CCTV in Public Places in respect of the retention of footage. The Duleek and Donore scheme operates a 56-day retention policy rather than the 31 days set out in the Code. The

[62] Ibid, page 65.
[63] Ibid, page 66

DPC found no jusitification for this extension and at one stage found CCTV footage that was 79 days old.[64]

Data-logging

62. Under Section 82(1) of the Data Protection Act 2018, data controllers must create and maintain a 'data log' in their automated processing systems so it can be ascertained when and if personal data was consulted by any person or whether personal data was disclosed or transferred to any other person. The DPC found, "No such analysis or justification was presented to this inquiry by AGS".[65]

Appropriate signage and general transparency

63. The DPC found that inadequate signage was an issue across all the Garda-operated CCTV schemes inspected. It found that members of the public are not adequately on notice in relation to the processing that is taking place via CCTV operated by AGS. Specifically, no CCTV signage was found on the approach roads to Duleek and Donore, while none of the signs that were erected in areas where ANPR cameras were deployed indicated that APNR was being used. At Pearse Street and Henry Street, the CCTV signage erected adjacent to the stations contained no purposes for the CCTV, nor any contact details for the AGS .

64. The DPC also found that the relevant Garda stations operating the CCTV schemes failed to provide callers at the public counter with information leaflets concerning the AGS CCTV operation in the area, and that the Garda website provided no information specific to the individual CCTV schemes authorised under Section 38 of the Garda Síochána Act, 2005.

Absence of written contracts between AGS and third party data processors

[64] Ibid, page 66.
[65] Ibid, page 66.

65. The DPC found AGS infringed Section 80 of the Data Protection Act 2018 for failing to put in place a written contract between itself and all third-party contractors servicing its CCTV systems under the authorised schemes, and by failing to ensure the processors in each case provide sufficient guarantees to implement appropriate organisational and technical measures.

66. In summary, the DPC found:

- No evidence that AGS considered and implemented the provisions of the Law Enforcement Directive as transposed by the Data Protection Act, 2018 in respect of the CCTV schemes.
- The AGS Code of Practice for CCTV in Public Places had remained unchanged since 2006 and did not appear to have been reviewed.
- In respect of systems found to be lacking digital tracing of individual access, no plans to upgrade were conveyed to the DPC.
- No actions were undertaken to account for the new legal framework for personal data with the exception of the appointment of a Data Protection Officer and a Record of Processing Activities (ROPA) across AGS, both implemented in 2018.
- AGS circulars accompanying responses to the DPC's questionnaire found nothing current and updated to take account of the Data Protection Act, 2018 was attached.
- Section 77(a) of the Data Protection Act 2018 specifically requires competent authorities to *"evaluate the risks to the rights and freedoms of individuals arising from the processing concerned"*, while section (b) requires them to implement a range of protective measures. The DPC found AGS had not demonstrated that it had complied with these sections.[66]

67. The DPC ordered AGS to bring its processing into compliance with the relevant provisions of the Data Protection Act 2018. It further issued a reprimand to AGS, stating that the number and extent of infringements "tend to demonstrate a

[66] The DPC made seven findings. More details in relation to these findings can be found in the DPC report referenced above.

generalised failure by AGS as data controller to implement appropriate technical and organisational measures in order to ensure that the personal data processed by it is processed in accordance with the provisions of the Data Protection Act 2018". Finally, it imposed a temporary ban on processing specifically in respect of the use of ANPR cameras under the schemes in Duleek and Donore. The DPC ordered AGS to switch off seven ANPR cameras, with the stipulation that they would not be reactivated without approval of the DPC.

Inquiries into local authorities

68. Since September 2018, the DPC has been inspecting County Councils in Kildare, Limerick, Galway, Sligo, Waterford, Kerry and South Dublin. According to the DPC, these seven local authorities have more than 1,500 CCTV cameras in operation for surveillance purposes. The focus of these inspections are the Community-based CCTV systems authorised under section 38(3)(c) of the Garda Síochána Act.

69. The DPC found that the issues of concern which arose were "far in excess of what we anticipated". They found "new issues of concern have arisen in every local authority inspected", with "significant data protection compliance issues in relation to matters such as the use of covert CCTV cameras, CCTV cameras at bottle-banks, the use of body-worn cameras, dash-cams, drones and ANPR cameras, CCTV cameras at amenity walkways or cycle-tracks, the lack of policies and data protection impact assessments, as well as several other issues. These include significant concerns about how some local authorities are discharging their data protection obligations."[67]

Head 8: Closed Circuit Television

70. This Head replaces Section 38 of the Garda Síochána Act 2005. It includes some additional provisions regarding the relationship with local authorities, which seems to seek to address some concerns raised by the DPC regarding the operation of

[67] Ibid, page 71.

Community-based CCTV schemes.[68] It also provides for a new offence where a person operates a CCTV scheme without authorisation.

Need for increased evidence into the effectiveness of CCTV

71. The use of CCTV has serious implications for the right to privacy. In order to ensure the interference with privacy is proportionate, their effectiveness in fighting crime must be proven. There is limited evidence of the effectiveness of CCTV in preventing crime in Ireland and in other contexts.[69] Research into whether CCTV has aided with the detection of crime has yielded "mixed results".[70] There is a need for evidence demonstrating the effectiveness of CCTV schemes including as to whether they effectively prevent or detect crime, secure public order or public safety, or safeguard against or prevent threats to public security, before expanding them further.

Need for a more regular review of authorisation granted under Head 8

72. This head states that the Garda Commissioner shall ensure that any authorisation of installation and operation of CCTV is reviewed on a regular basis, at least within 5 year intervals.[71] Given the significant impact of CCTV on human rights, ICCL recommends that this interval be shortened and that authorisation should be reviewed on an annual or bi-annual basis.

Need to include explicit safeguards regarding the operation and access of CCTV

73. ICCL recommends that strict safeguards be included regarding the operation of CCTV. CCTV footage can be shared publicly and cause untold damage. Dara Quigley took her own life after images of her arrest, while naked, taken from the Garda CCTV system, were circulated online in 2017.[72] No garda has ever been disciplined or held

[68] DPC, Data protection and community-based CCTV schemes, 2019.
[69] Roni Buckley, Oireachtas Library and Research Service, Data Privacy and Community CCTV Schemes, 2019.
[70] Ibid.
[71] Garda Síochána (Digital Recordings) Bill, Head 8(7).
[72] Irish Council for Civil Liberties, Justice for Dara, https://www.iccl.ie/justice-for-dara/

accountable for this egregious breach of privacy and dignity. Robust safeguards and protections are absolutely vital to prevent such abuse of power.

Need for narrower purpose

74. Head 8(1) allows for the Garda Commissioner to authorise the installation of CCTV for specific purposes. Given the absence of evidence in relation to the necessity and proportionality of installing CCTV, ICCL recommends that these purposes are narrowed. Head 8(2) provides that the Garda Commissioner may "specify the areas" within which the installation and operation of CCTV may be "necessary and proportionate". This provision is unclear and should be clarified. Assessing necessity and proportionality must be done for every decision to install and operate CCTV on a case-by-case basis and particular 'places' should be designated in a blanket fashion as automatically allowing for human rights compliant installation and operation of CCTV.

Head 9: Mobile Closed Circuit Television

75. This head provides for the installation of mobile CCTV, but does not outline in the same detail the protections as set out regarding fixed CCTV. There is no mention that the Garda Commissioner shall be satisfied that a Data Protection Impact Assessment (DPIA) has been carried out prior to granting an authorisation. There is also no mention of the need for visibility or signage in relation to mobile CCTV, as required by data protection law. These must be introduced.

Further use of drones

76. Head 9, in respect of mobile CCTV, provides for the installation of CCTV cameras in, or "fixed to",[73] any vehicle owned or operated by the State, including drones. This head does not stipulate that the use of these cameras will operate in "public" places.

[73] Note: "This Head sets out that the Garda Commissioner may provide for the installation and operation of CCTV in vehicles, as defined in Head 2, for purposes referred to in subhead (2). Although the camera may be fixed to the vehicle, the vehicle is not fixed and as such, CCTV in vehicles does not fall within the provisions of Head 8."

This is different to the use of drones under Head 5, which provide they can be used in either public places or where a member of the Garda Síochána has lawful authority or permission to be present. ICCL can only conclude that Head 9 will therefore allow for cameras attached in or to vehicles, such as drones, to be used in private spaces . ICCL is concerned at the lack of adequate safeguards in respect of this. Specifically, we note that the use of mobile CCTV, including drones, in addition to the use of BWCs and recording devices, will not come under the remit of the review process carried out by the designated judge, as per Head 21. This is concerning, particularly in respect of drones, because there is a reduced visibility of devices working at altitude, and such devices could yield private information about people who are completely unaware that they are being watched. This means that this head could lead to covert surveillance in private spaces and, ultimately, a clear expansion of AGS' current covert surveillance capabilities without any judicial oversight.

77. ICCL would again refer to the European Article 29 Working Party (WP29)[74] in respect of drone use by law enforcement purposes highlighted in our discussion under Head 5 above, including the specific risks and difficulties associated with drone use.

Head 10: Code of Practice under this part

78. The Data Protection Commission's inquiry of Garda-operated CCTV schemes, outlined in detail above, identified wide-ranging and concerning infringements of data protection law. Their report also identified the need for different safeguards to:

- Record access instances, outlining who has accessed the CCTV systems, when and where;
- Maintain records of downloads of CCTV footage;
- Implement a training programme for Gardaí who use the systems on the systems' capabilities and on correct handling and protection of personal data;
- Create and maintain a 'data log' to ascertain when and if personal data was consulted by any person or disclosed or transferred to any other person;

[74] Ibid.

- Ensure adequate signage that AGS is operating CCTV.[75]

79. ICCL recommends that all of the safeguards proposed by the DPC following their inquiries be explicitly included in the Code of Practice required under Part Three.

[75] Data Protection Commission, DPC Ireland 2018-2020, Regulatory Activity under GDPR, 2020. Accessible here: https://www.dataprotection.ie/sites/default/files/uploads/2020-06/DPC%20Ireland%202018-2020%20Regulatory%20Activity%20Under.pdf

Part Four - Third party CCTV

Head 11: Live Feed Access to Third Party CCTV

80. This head provides for an authorisation process to access third party CCTV through a live feed. The explanatory note highlights that it is "*considered that this may be necessary in relation to an increase in criminal activity in a particular area where 3rd party cameras may be located.*" This seems problematic as it could lead to general monitoring and profiling of certain areas or people, and amount to extended covert surveillance if AGS fail to flag this surveillance with affected members of the public. It's not clear from the heads of the Bill how AGS will provide for this signage, particularly if it is access that will be provided for 72 hours under specific circumstances without judicial authorisation. The ECtHR has previously held that an interference with private life through the use of covert surveillance is considered legitimate when certain conditions are met i.e. that the surveillance is in accordance with the law; it has a legitimate aim; and reasonable steps are taken to protect the privacy of the individual monitored.

81. It should be noted that section 89(1) of the Data Protection Act 2018 provides that, "*A decision that produces an adverse legal effect for a data subject or significantly affects a data subject shall not be based solely on automated processing, including profiling, of personal data that relate to him or her*", while section 89(3) prohibits "*Profiling that results in discrimination against an individual on the basis of a special category of personal data*" .

82. The Notes for Head 11 which provides for access by the Garda Síochána to third party CCTV via a live feed state that: "*It is envisaged that the Garda Síochána may request such an authorisation for access in circumstances where there is a large public event or where there is a requirement to provide protection to a visiting dignitary, for example.*" ICCL considers that the fact of a large public event should not of itself constitute sufficient grounds for accessing live CCTV. Individuals must be allowed to

exercise their constitutional and human rights without undue interference. ICCL considers that this provision would provide for a disproportionate interference with the right to protest. Surveillance of large public events should only take place where there is a particular and reasonable suspicion that criminal activity might take place during the event. If protesters are aware they will be surveyed during their protest, they may decide not to take part at all in order to preserve their privacy. This could have a significant chilling effect on the exercise of the right to protest.

Visibility of AGS access to third party CCTV through a live feed

83. ICCL assumes, as there is no definition in this head or Bill, that third party CCTV means CCTV used for private, domestic purposes or CCTV used for private commercial reasons. It is not clear to ICCL how AGS will ensure there is public signage and clear visibility regarding its use of private and commercial CCTV cameras and/or regarding its live feed access to same. ICCL also questions how this live access will work in respect of private residences or homes which are afforded a greater level of privacy[76], or with internal security camera systems, or third party cameras which are not being operated in accordance with law. This is an area of particular concern for ICCL, given Head 16 provides that a person who fails to comply with live feed access authorisation without lawful authority or reasonable excuse could face a fine or jail term of up to three years. ICCL recommends much clearer definitions in relation to third party CCTV and specific safeguards, including visibility, are required by this legislation.

(a) Head 12: Application for authorisation

84. This head notes that the Garda applying for the authorisation must have reasonable grounds that access to the CCTV is "*necessary and proportionate to its objectives…including its likely impact on the rights of any person and of a duration that is reasonably required to achieve its objectives.*" While ICCL welcomes the explicit requirement for the relevant Garda to have regard to the impact on rights, we

[76] Article 40.5 of the Irish Constitution provides, "The dwelling of every citizen is inviolable and shall not be forcibly entered save in accordance with law".

consider the need to avoid a disproportionate impact should be more explicitly stated. It must be acknowledged that the collection of data in respect of one person can lead to the collection of others who are not under suspicion of AGS, including children and vulnerable people. As such, this head should explicitly provide for the obligations set down by Article 6 and Article 7 of the LED as previously outlined in this submission.

85. Further, the explanatory note highlights it is envisaged that "*access may be sought for a duration of up to one year.*" This seems unreasonably lengthy. ICCL recommends that this process be strictly regulated and only used where it is necessary and for a much shorter, limited duration, with review of authorisation required on a frequent basis, such as weekly or monthly.

(b) Head 13: Authorisation and Head 14: Variation or renewal of authorisation

86. Head 13 provides that an AGS member of Superintendent rank or above can go before a judge to apply for authorisation without having to specify a particular offence in respect of which the authorisation is being sought. This is immensely troubling given the authorisation could be secured for up to a year. Further, Head 14 provides that when seeking a variation or renewal of authorisation for up to another year, there is still no requirement to make the judge aware of the offence the subject of the application. ICCL recommends that authorisation should require reasonable suspicion of a particular offence.

87. This head further provides that an application for authorisation shall be made *ex parte* and *in camera* to a district court judge. While this judicial oversight is positive, it is problematic that AGS will be able to obtain live feed access to third party CCTV secretly and monitor potentially large numbers of people without their knowledge. This raises significant privacy and data protection concerns. ICCL recommends that there be appropriate signage and visibility for the CCTV and the fact that AGS has

received live feed access to it. Applications for authorisation should be carried out in public except in exceptional cases with proven justification.

(c) Head 15: Approval for temporary access to third party CCTV

88. This head provides that a member of AGS of Superintendent rank or higher may approve access to third party CCTV through a live feed for up to 72 hours. This is a wide-reaching power which significantly infringes on the right to privacy and data protection and, as such, should be subject to judicial oversight. ICCL recommends that this provision be removed or that a judge must grant such access following application by AGS or the interested party.

Part Five - Transfer of relevant data to An Garda Síochána

(a) Legal and human rights framework

89. The right to protection of personal data is a fundamental right protected under Article 8 of the CFR. Further, the Data Protection Act 2018 (which itself must be complied with) gives effect to aspects of the EU General Data Protection Regulation (GDPR), which places obligations on organisations and individuals who collect and process data related to people in the EU. It also transposes the EU Law Enforcement Directive (LED), in respect of the processing of personal data by data controllers (persons who decide why and how personal data will be processed) for the purposes of the prevention, investigation, detection and prosecution of criminal offences and the execution of criminal penalties.

90. Article 2(2)(d) of the GDPR provides: *"This Regulation does not apply to the processing of personal data … by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."*[77] Instead, the LED provides specific rules with regard to the processing of personal data for such purposes. However, it's worth noting that some obligations under the GDPR also apply under the LED. They include:
    - The need for data controllers to implement appropriate technical and organisational measures to ensure that processing is performed in accordance with the respective law (Article 19 in LED; Article 24 in GDPR);
    - To implement data protection by design and by default (Article 20 in LED; Article 25 in GDPR);
    - To use a processor that provides sufficient guarantees and acts only on instructions from the controller (Article 22 in LED; Article 28 in GDPR);

[77] Article 2, General Data Protection Regulation (GDPR). Accessible here https://gdpr-info.eu/art-2-gdpr/

- To maintain a record of processing activities (Article 24 in LED; Article 30 in GDPR);
- To implement logging measures (Article 25 in LED; Article 30 in GDPR);
- To cooperate with the supervisory authority in the performance of its tasks on request (Article 26 in LED; Article 31 in GDPR);
- To carry out a Data Protection Impact Assessment (DPIA) when the processing is likely to result in a high risk to the rights and freedoms of natural persons (Article 27 in LED; Article 35 in GDPR);
- To consult the supervisory authority in advance in specific circumstances (Article 28 in LED; Article 36 in GDPR);
- To implement appropriate measures to ensure a level of security appropriate to the risk, in particular as regards the processing of special categories of personal data (Article 29 in LED; Article 32 in GDPR);
- To notify the supervisory authority of a personal data breach without undue delay not later than 72 hours after having become aware of it, when the breach is likely to result in a risk to the rights and freedoms of natural persons (Article 30 in LED; Article 33 in GDPR);
- To communicate the personal data breach to the data subject without undue delay where the personal data breach is likely to result in a high risk to his/her rights and freedoms (Article 31 in LED and Article 34 in GDPR);
- To designate a data protection officer under specific conditions (Article 32 LED; Article 37 in GDPR);
- To respect the conditions defined for the transfer of personal data to third countries or to international organisations (Article 35 and following in LED; Article 44 and following in GDPR).

Other obligations specific to the LED include:

- The data controller must make a clear distinction between personal data of different categories of data subjects (Article 6);
- The data controller must ensure that personal data based on facts are distinguished from personal data based on personal assessments, and ensure the quality of that data (Article 7);

- Processing must be lawful and based on Union law or Member State law (Article 8);
- Processing of special categories of data is allowed only where strictly necessary (Article 10).[78]

Head 17: Power of minister to designate relevant body

91. Head 17 allows the Minister to designate another body as a relevant body, after prior consultation with the DPC, for the purposes of the Act where he or she is satisfied that "*the relevant data to be provided by the body is necessary and proportionate for the purposes of- (i) the prevention, investigation, detection or prosecution of criminal offences; or (ii) safeguarding the security of the State.*" ICCL would highlight that data itself cannot be 'necessary and proportionate' but rather the provision of data must be necessary and proportionate. We recommend making this clearer in this provision.

Head 18: Disclosure of data from relevant body

92. This Head provides that a relevant body may disclose data, i.e. ANPR data, with or without images, to An Garda Síochána. It is important that this process complies with all relevant data protections laws and that a DPIA is carried out prior to any data-sharing.

[78] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Accessible here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG ; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Accessible here: https://eur-lex.europa.eu/eli/reg/2016/679/oj ; See also Commission nationale de l'informatique et des libertés (French Data Protection Authority), "Law enforcement Directive": What Are We Talking About?, June 2, 2021, Accessible here: https://www.cnil.fr/en/law-enforcement-directive-what-are-we-talking-about

Part Six: Miscellaneous

Head 20: Admissibility of evidence under this Act

93. Head 20 sets out an inclusionary rule for the admissibility of CCTV evidence if there is an error or omission on the face of the authorisation so long as the error or omission was inadvertent and the information ought to be admitted in the interests of justice. It also outlines specific matters for the court to consider in making this decision, including whether the error or omission was serious or merely technical in nature. This appears to unduly extend into the remit of the courts, which is the proper forum to determine whether evidence is admissible following submission from both prosecution and defence. Outlining an inclusionary rule in this manner may deprive a defendant of the opportunity to challenge evidence obtained in breach of his or her constitutional rights. ICCL considers that the admissibility of evidence should be a matter for the courts and not the legislature.

94. The Irish exclusionary rule applies to evidence obtained in breach of an accused's constitutional rights, including the right to privacy. The current exclusionary rule, set out in *DPP v JC*[79], permits the admissibility of unconstitutionally obtained evidence where the "*unconstitutionality concerned arose out of circumstances of inadvertence or by reason of developments in the law which occurred after the time when the relevant evidence was gathered.*"[80] However, this decision has been widely criticised for failing to properly define the scope of the new rule, failing to define what 'inadvertence' may mean and for unduly encroaching on the one effective remedy in Irish law for ensuring constitutional rights are respected at every stage of the criminal justice process.[81] We also note that this decision has been used to admit evidence that has been retained unlawfully in violation of the right to privacy.[82] ICCL has

[79] [2017] 1 IR 417.
[80] Ibid.
[81] Claire Hamilton, ICCL, A Revolution in Principle: Assessing the impact of the new evidentiary exclusionary rule, 2020.
[82] Ibid.

previously highlighted that this is problematic and recommended that Irish surveillance laws be brought in line with European Union and ECHR standards. As such, ICCL strongly recommends the removal of this provision.

Head 21: Review of Operation of Act

95. This head provides that a designated judge shall review the operation of Part 4 and 5 of the Act. ICCL recommends that this review mechanism be expanded to a review of the operation of the entire Act and that the judge's reports be as detailed and transparent as possible.

Recommendations

(1) Postpone the passing of this Bill until such time as the DPC ceases its inquiries into AGS and local authorities;

(2) Ensure AGS has carried out a robust CCTV review examining AGS's policies, procedures and guidelines and that this is examined by the DPC before this Bill is passed. Also ensure that review is published.

(3) Ensure that the use of recording devices and BWCs are necessary and proportionate to the achievement of legitimate aims.

(4) Narrow the purposes to use a recording device or BWC.

(5) Narrow the definition of recording device, in particular to ensure that it does not encompass facial recognition technology.

(6) Ensure that the use of a recording device for covert surveillance, in particular drones, is accompanied by increased safeguards to ensure that it is human rights compliant and compliant with data protection concerns.

(7) Clarify the visibility or signage procedures regarding the use of a recording device.

(8) Clarify who can use a recording device, whether a Garda has to be of a specific rank, have received any specific training, or be identifiable as a Garda.

(9) Expressly address data protection concerns and human rights considerations to the use of BWCs in the Bill.

(10) Specify that the review of the relevant code of practice should take place on an annual or bi-annual basis rather than within 5 years.

(11) Implement a pilot scheme to trial the use of recording devices and BWCs to test their effectiveness and conduct a human rights impact assessment and data protection impact assessment.

(12) Implement the recommendations previously made by Article 29 World Party (WP29 in respect of drone use by law enforcement purposes.

(13) Conduct further research into the effectiveness of CCTV in preventing, investigating or detecting criminal offences, securing public order and public safety, or safeguarding against and the prevention of, threats to public safety.

(14) Specify that the review of authorisation of installation or operation of CCTV should take place on an annual or bi-annual basis rather than within 5 years.

(15) Include specific safeguards, as recommended by the DPC, in relation to CCTV in the Bill.

(16) Include more detail and protections in relation to mobile CCTV, such as the need to carry out a DPIA before the granting of an authorisation and the need for sufficient signage and visibility of CCTV.

(17) Clarify if this Bill intends to provide AGS the power to carry out covert surveillance in private spaces via drones.

(18) Ensure that access to third party CCTV through a live feed is strictly regulated and only used where it is necessary and for a limited duration.

(19) Ensure that when an application for renewal of authorisation for live feed access to third party cameras, the AGS member must tell the judge the offence the subject of the request.

(20) Clarify how AGS will erect appropriate signage and visibility when AGS has received live feed access to third party CCTV, including CCTV used by private and commercial entities..

(21) Remove the provision (Head 15) enabling AGS to approve temporary access to third party CCTV through a live feed without judicial oversight.

(22) Remove the inclusionary rule that the Bill outlines.

(23) Expand the review of Part 4 and 5 of the Act to a review of the operation of the entire Act.

About ICCL

The Irish Council for Civil Liberties (ICCL) is Ireland's oldest independent human rights body. It has been at the forefront of every major rights advance in Irish society for over 40 years. ICCL helped legalise homosexuality, divorce, and contraception. We drove police reform, defending suspects' rights during dark times. In recent years, we led successful campaigns for marriage equality and reproductive rights.

Irish Council for Civil Liberties