



LAW SOCIETY  
OF IRELAND

# Submission on the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill

Joint Committee on Justice

18 January 2024



# Submission on the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill

---

## Introduction

The Law Society of Ireland (the '**Law Society**') appreciates the opportunity to respond to a request from the Joint Committee on Justice on the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023 (the '**General Scheme**').

Given the limited time available to consult on the General Scheme, any failure to comment on a particular head/note does not indicate a particular position on that head/note. We hope that publication of the General Scheme will be followed by publication of a draft Bill which will be subject to full legislative scrutiny, in which event we may contribute additional technical points at a that stage.

## Executive Summary

The Law Society notes possible weaknesses in the General Scheme which give rise to a concern that this legislation will be challenged on several grounds including through the lens of privacy rights, data protection, the right to non-discrimination and the right to a fair trial. The Law Society submits that the tests of necessity and proportionality required for the introduction of biometric identification in the Irish context merits further examination. In this submission, we look at the General Scheme on a Head-by-Head basis and outline our observations in a general manner. The legislation could provide more safeguards and oversight relating to when biometric identification can be used by An Garda Síochána, the recording of the use of this technology, the external monitoring of its use and reviews of the applicable Code of Practice.

## Part One – Preliminary and General

### Head 2 – Amendment to Section 2 of Principal Act - Interpretation

The definition of 'biometric identification' means identifying or attempting to identify, natural persons, through the comparison of a person's biometric data with the biometric data which is legally held by An Garda Síochána'.

It is noted that the definition of biometric data is to have the meaning as set out in section 69 of the Data Protection Act 2018, with the exclusion of DNA fingerprints and other data "except for facial images".

Section 69 (1) of the Data Protection Act 2018 defines biometric data;

"Biometric Data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual that allow or confirm the unique identification of the individual, including facial images or dactyloscopic data".

It is noted that section 69 of the Data Protection Act 2018 includes 'physiological or other behavioural characteristics'. If it is the intention that this Bill will only apply to facial images and not other physical characteristics of individuals such as their height, it would be preferable that this is set out more explicitly in the legislation. The definition does not specify what is meant by 'technical processing'. Does this include the creation of facial images by a camera phone or indeed the processing of physical photographs?

The definition of "biometric identification" is as follows:

"identifying or attempting to identify, natural persons to the comparison of a person's biometric data with the biometric data which is legally held by An Garda Síochána"

The definition of biometric identification, given the lack of clarity in the definition of biometric data, arguably does not exclude the comparison by An Garda Síochána without the assistance of intelligent automation, of two photographs.

## **PART 2 – The insertion of new Part 6A into the Principal Act**

### **Head 3 – New Section 43A – Application of this Part**

#### **Section 43A (2)(i)**

This subsection provides,

“nothing in this Part shall prevent An Garda Síochána from processing and storing images which have been legally provided by other national or international organisations”.

The draft does not specify what national or international organisations it refers to. Is it other law enforcement organisations only? Or is it envisaged that An Garda Síochána could lawfully obtain images from the Department of Social Protection for example, to obtain biometric data for the purposes of identification. The draft could be more explicit as to which type of organisation it refers to.

Also, the draft should place an onus on An Garda Síochána to only use images which have been legally obtained by those organisations. The Department of Social Protection has been implicated in the past for illegally processing biometric data (<https://www.iccl.ie/press-release/psc-facial-recognition-software-dpia/>). If that data is subsequently transferred to An Garda Síochána then the whole chain could be tainted.

Section 43A (3) provides that the use of biometric identification must be in compliance with a Code of Practice as set out in section 47. Section 47 of the Principal Act provides for consultation in relation to codes of practice and periodic reviews of the codes of practice. It is submitted that the use of intelligent automation to assist with the identification of suspects in the context of the investigation of offences requires more transparency and oversight. It is submitted that this should be explicit in primary legislation.

Political agreement was reached at EU level on 8 December 2023 in relation to the Artificial Intelligence Act (**AI Act**). The AI Act classifies what it calls ‘Post Remote Biometric Identification Systems’ as being high risk processing and requires that such systems by law are equipped with appropriate logging capabilities and that any final decisions impacting persons are made by human eyes.

The principles of this General Scheme should align with the principles agreed at political level on the AI Act, including stating specifically that the final decision around identification should be made by a person.

Searches conducted using biometric identification technology need to be fully documented at every stage of the identification process and logged accordingly. The technology must log the searches made, results returned, and a record of the images maintained for final review. The search and result logs could be available for review by way of disclosure by the defense in the event of prosecution. This could be expressly provided for in the primary legislation.

The General Scheme is silent on the oversight of the use of biometric identification systems. There is a requirement that An Garda Síochána keep a record of all applications but it is not clear whether such records will be reviewed by an independent authority to ensure that the use of biometric data is used in a proportionate manner. The high-risk nature of the processing would require that the use of such technology is the subject of oversight to assure the public

of the compliance by An Garda Síochána with both the legal requirements and the Code of Practice proposed under the General Scheme.

## **Head 6 – New Section 43D - Approval**

Section 43 (D) (1) provides that the Chief Superintendent may approve an application if the following circumstances are met:

- a) he or she is independent of the investigation to which the application relates,
- b) he or she believes on reasonable grounds that the use of biometric identification is necessary and proportionate, and
- c) he or she believes on reasonable grounds that the use of biometric identification is connected to an investigation of an offence in the schedule or a matter relating to the protection of the security of the State.

The provision does not set out how or against what criteria, the Chief Superintendent is to assess whether the use of biometric identification is both necessary and proportionate. It is assumed that such technology will only be required for complex investigations involving significant searches of CCTV footage or other digital data and where there are circumstances of urgency such as a threat to the public security, concern for a person's safety or the protection of life. The objectives of the bill could be set out in clearer detail so that the test as to what is necessary and proportionate can be better assessed and reviewed. It would be preferable if the General Scheme set out more clearly the underlying policy intention. It is submitted that judicial oversight might be more appropriate here namely an Application to a District Court Judge.

## **Head 7 – New Section 43E – Use of the Biometric Identification**

Subsection (1) provides that a Garda

“...may utilise biometric identification to search the following in order to locate, follow the movements or identify a person:

- (a) any images or footage that An Garda Síochána legally retains;
- (b) any images or footage that An Garda Síochána can legally access.”

On one reading of (b) above it infers that an authorisation by a Chief Superintendent would cover biometric identification using images not yet in the custody of An Garda Síochána, but that are legally accessible to them. This appears to contradict an earlier provision, Section 43(B)(3).

That section provides,

“Biometric identification referred to in subsection (1) will only utilise images and video that has already been gathered and are legally held or legally accessed by An Garda Síochána.”

This subsection confirms that An Garda Síochána must have already gathered the images and videos. Section 43E(1) could be reworded to make it clear that it refers to videos and images already gathered. It could read, a member “may utilise biometric identification to search the following in order to locate, follow the movements or identify a person, any images or footage already gathered and legally retained or legally accessible by An Garda Síochána.”

In addition, it is not clear how images and footage could be gathered by An Garda Síochána but not ‘retained’ by them. Is the term “legally accessible” required?

## **PART 3 – The insertion of consequential amendments into the Principal Act**

### **Head 12 - Amending section 47**

#### **Retention, erasure, destruction**

It is envisaged that retention, erasure and destruction of biometric data and the results of biometric identification is dealt with in a Code of Practice. Given the sensitivity of biometric data and purported fallibility of facial recognition, why would the legislation governing its use leave the destruction provisions to a Code of Practice? In contrast, the Criminal Justice (Forensic Evidence and DNA Database System) Act 2014 includes provisions in relation to the retention and destruction of forensic samples. The facial recognition legislation could do the same so that individuals know how long their data is retained.

#### **Scheduled of Offences**

The AI Act, as it currently stands, requires in the context of 'live' biometric identification systems (which is excluded under this General Scheme) that this technology can only be used for specified offences. It is not clear from the information available on the political agreement reached on 8 December 2023 whether that limitation applies equally to 'post review' biometric identification systems captured by this General Scheme.

As set out previously, the objectives against which an application for the use of biometric identification technology is to be assessed could be more clearly articulated. It is submitted that the use of the technology, to be necessary and proportionate, must be used for the more serious offences, where the requirements of efficiency and urgency are most acute. This will depend on the type of the investigation as opposed to the nature of the offence. It will likely apply to many cybercrimes, cyber enabled offences, offence presenting a threat to public safety and investigations seeking to preserve life.

The scheduled offences currently do not include any terrorist related offences such as offences contrary to the Explosive Substances Act 1883, Firearms Act 1925 - 1964 or offences relating to organized crime set out in part 6 of the Criminal Justice Act 2006. The scheduled offences do not include the offence of sexual assault, albeit aggravated sexual assault and rape offences are included.

It is submitted that the requirements of the AI Act be reviewed to assess whether individual offences must be scheduled for post review biometric identification.

#### **Conclusion**

The Law Society submits that more attention to precise drafting be given in the Bill to the recording, storing and accessing biometric data and using this data for biometric identification for the investigation or detection of offences.

We have outlined some specific points on the draft wording in this submission but generally the Law Society would like to see a number of strengthened safeguards in the use of these technologies by An Garda Síochána.

The Law society submits that an application made by An Garda Síochána to use biometric identification should be made to a District Court Judge rather than the Chief Superintendent.

We note that this legislation is being developed at the same time as the Data Protection Commission (the **DPC**) investigates surveillance of people for law enforcement purposes by

An Garda Síochána and the DPC has identified significant data protection compliance issues (Data Protection Commission, Annual Report 2020).

The Law Society acknowledges that there is inevitably a tension between vindicating individual rights to privacy and protection of personal data and permitting law enforcement authorities to use and access technology to address the commission of serious crime however the State must balance the different rights at play to ensure justice is done and seen to be done.

We appreciate the opportunity to contribute these comments and observations to the Committee's consideration of the General Scheme. We remain available to further assist the Committee in any way we can.

For further information please contact

Niamh Coyne  
n.coyne@lawsociety.ie



© Law Society of Ireland, 2023

Blackhall Place, Dublin 7

t. 01 672 4800

e. [general@lawsociety.ie](mailto:general@lawsociety.ie)

