Seirbhís Leabharlainne 7 Taighde
Library & Research Service

Briefing Paper

Garda Síochána (Recording Devices) (Amendment) Bill

Karen McLaughlin, Senior Parliamentary Researcher (Law)

17 July 2025

Abstract

The Draft General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill, published on 14 December 2023, proposes to insert a new Part, Part 6A, into the Garda Síochána (Recording Devices) Act 2023, to provide for the use of facial recognition technology by An Garda Síochána in certain circumstances. This paper provides an overview of the policy and legal context to this legislative proposal and an outline of the General Scheme.

Tithe an
Oireachtais
Houses of the
Oireachtas

Table of Contents

This L&RS publication may be cited as:

Oireachtas Library & Research Service, 2025, L&RS General Scheme Briefing Paper: Garda Síochána (Recording Devices)(Amendment) Bill

Legal Disclaimer

No liability is accepted to any person arising out of any reliance on the contents of this paper. Nothing herein constitutes professional advice of any kind. This document contains a general summary of developments and is not complete or definitive. It has been prepared for distribution to Members to aid them in their parliamentary duties. Some papers, such as a Bill Digest, are prepared at very short notice. They are produced in the time available between the publication of a Bill and its scheduling for second stage debate. Authors are available to discuss the contents of these papers with Members and their staff but not with members of the general public.

Executive Summary

The Draft General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill was published on 14 December 2023. The Scheme proposes to insert a new Part, Part 6A, into the Garda Síochána (Recording Devices) Act 2023 to provide for the use of retrospective facial recognition technology by An Garda Síochána.

An Garda Síochána has been advocating for this technology in recent years and has stated that digital crime can only be detected with digital tools. These calls for Facial Recognition Technology (FRT) have emerged in the context of wide-ranging policing reform and evolving Government policy on artificial intelligence. While facial recognition technology has been developing for several decades, its use by policing bodies has increased significantly in the last decade. This increased use has been controversial and has given rise to debates about accuracy of the technology, particularly its potential inherent biases and capacity to discriminate against particular groups.

Human rights lawyers and civil society groups have highlighted the impacts on the rights to privacy as well as several other rights and highlighted how this may create a chilling effect on how an individual may behave in society. However, it has been noted that human rights may be infringed upon legally if three tests can be satisfied, namely legality, proportionality and necessity and legitimacy. A case taken in the UK has also highlighted that the police, in its discharge of the public sector equality duty, must be able to satisfy themselves that the technology being used does not contain biases which could discriminate against certain protected groups[1]. A similar duty exists in this jurisdiction.

EU law also plays a significant role in the regulation of the use of facial recognition technology by law enforcement authorities. The processing of facial images by law enforcement authorities is already subject to significant regulation under the Data Protection Act 2018, which implements the General Data Protection Regulation (GDPR) and the Law Enforcement Directive. There has been reports of providers of facial recognition systems facing fines from data protection authorities in the EU for non-compliance with these obligations. In June 2024 the European Union Regulation on Artificial Intelligence (known as the EU AI Act) came into effect, which adopts a risk-based approach to the regulation of AI. The EU AI Act describes retrospective facial recognition technology as a high-risk AI system and places specific obligations on users of such systems.

The legal and policy landscape has significantly changed since the General Scheme was published in 2023. In particular, the EU AI Act has classified live FRT as a prohibited AI system which may only be used in limited circumstances and has placed wide-ranging obligations on users of high-risk AI systems. Thus, it is likely that the published Bill may be quite different to the General Scheme. Nevertheless, this paper discusses the developing policy and legislative environment relevant to the legislative proposal and provides contextual information to assist Members in navigating this complex and fast changing area.

[1] *The Queen (on application of Edward Bridges) v The Chief Constable of South Wales Police* [2020] EWCA Civ 1058.

Introduction

The Draft General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill was published on 14 December 2023. The Scheme proposes to insert a new Part, Part 6A, into the Garda Síochána (Recording Devices) Act 2023 (hereafter the 2023 Act). The 2023 Act was enacted on 5 December 2023 and some of the provisions were commenced on 15 May 2024.[2]

According to the Government Legislation Programme Summer 2025, the purpose of this Bill is:

> To provide for retrospective searching of images which are legally in the possession of An Garda Síochána through the safe and ethical use of facial recognition technology in limited circumstances only and in relation to specific serious offences which are subject to a penalty on conviction of up to life imprisonment.

Pre-legislative scrutiny of the General Scheme took place on 13 February 2024. The Joint Oireachtas Committee on Justice published its report on 27 February 2024 with 32 recommendations for amendments. A discussion of the recommendations is beyond the scope of this paper as it will be discussed in the forthcoming Bill Digest.

The purpose of this paper is to set out the legal and policy context related to this legislation – both in terms of the context leading up to the publication of the General Scheme as well as developments that occurred prior to the publication of this paper. It should be noted that artificial intelligence and its regulation is continually evolving and therefore, this paper is not an exhaustive consideration of issues related to this technology. This paper will focus primarily on the law, policy and research related to the use of facial recognition technology in policing.

Related Library and Research publications and resources:

- Bill Resource Page [internal only] Garda Síochána (Recording Devices) (Amendment) Bill
- L&RS Bill Digest on the Garda Síochána (Recording Devices) Bill 2022
- Bill Resource Page [internal only] Garda Síochána (Recording Devices) Bill 2022
- L&RS (2019) Note: Data privacy and community CCTV schemes
- L&RS (2024) Spotlight on 'Artificial Intelligence: Background and overview of the current regulatory landscape in Ireland and the EU'
- L&RS (2025) Research Matters: How AI can impact human rights and equality

[2] Garda Síochána (Recording Devices) Act 2023 (Commencement) Order 2024 (S.I. No. 215 of 2024), art. 2(b).

Origins and Operation of Facial Recognition Technology

Origins and evolution of FRT

It is generally accepted that Woodrow Bledsoe first attempted "facial recognition" in a computational form between 1964-65.[3] However, Taylor argues that FRT does not have a single origin and its evolution comes from a range of technological developments such as:

> "… mugshots in eighteenth-century France; mathematical analysis of caste in nineteenth-century British India; innovations by Chinese closed-circuit television companies and computer vision start-ups conducting bio-security experiments on farm animals."[4]

In the 1990s the US defence agency funded the development of this technology with early trials being carried out at Super Bowl games and later anti-terrorism measures. Birhane notes "enthusiasm for the technology lapsed following interventions from groups".[5]

In 1991 Turk and Pentland described their "near-real-time computer system that can locate and track a subject's head, and then recognize the person by comparing characteristics of the face to those of known individuals."[6] Discussing the historical context of FRT development, Raji and Fried divide the evolution into four periods as follows:

1. **Early Research Findings (1964 - 1995):** Bledsoe's initial approach was to encode each individual with a vector of computed distances between facial features, a method that would become popular but was very computationally expensive and slow.
2. **Commercial Viability as the "New Biometric" (1996 - 2006):** the creation of the Face Recognition Technology (FERET) database in 1996, the very first large-scale face dataset available for academic and commercial research (Phillips et al. 2000b);
3. **Mainstream Development for Unconstrained Settings (2007-2013):** the Labelled Faces in the Wild (LFW) dataset in 2007, as the first Web-sourced and unconstrained face dataset (Huang et al. 2007), and
4. **Deep Learning Breakthrough (2014 and onwards):** the development of DeepFace in 2014, the first facial recognition model to beat human performance on the face verification task and to be trained with the now-dominant technique of deep learning (Taigman et al. 2014).[7]

[3] Raji and Fried (2021) About Face: A Survey of Facial Recognition Evaluation, Association for the Advancement of Artificial Intelligence.
[4] Taylor SM. FRT in 'Bloom': Beyond Single Origin Narratives. In: Matulionyte R, Zalnieriute M, eds. The Cambridge Handbook of Facial Recognition in the Modern State. Cambridge Law Handbooks. Cambridge University Press; 2024, pp 44-59.
[5] Abeba Birhane "We're headed for big problems if gardaí get facial recognition technology", *Irish Times,* 20 March 2024. Abeba Birhane is a cognitive scientist, currently a senior adviser in AI accountability at Mozilla Foundation and an adjunct assistant professor at the School of Computer Science and Statistics at Trinity College Dublin.
[6] Turk, Pentland (1991) "Eigenfaces for Recognition" *Journal of Cognitive Neuroscience* Volume 3, Number 1.
[7] Raji and Fried (2021) About Face: A Survey of Facial Recognition Evaluation, Association for the Advancement of Artificial Intelligence.

General Use Cases

According to a leading academic and activist, Dr. Joy Buolamwini, Facial Recognition Technologies (FRTs) are “a set of digital tools used to perform tasks on images or videos of human faces”.[8] These tools are categorised by Buolamwini based on whether they answer certain questions, which are outlined in Table 1 below.

Table 1: Types of FRT used to answer specific questions

Questions	Tasks performed by FRT tools
Is there a face in the image?	Face detection
What kind of face is shown in the image?	Face attribute classification Face attribute estimation Face attribute detection Emotion, affect, and facial expression classification
Whose face is shown in the image?	Facial recognition, including: • Face verification • Face identification

Source: L&RS, based on Buolamwini et al (2020), Facial Recognition Technologies: A Primer

In recent years these tools have been used in a wide range of everyday life scenarios, which has been described by academics as pro-social’ applications of FRT[9]. These academics have described some of these uses as follows:

- **Retail sector:** using FRT to recognise repeat customers; target screen-based advertising to particular demographics; collect information on how different customers use retail space and engage with particular arrangements of goods; and gauge satisfaction levels by monitoring the facial expressions of shoppers waiting in checkout lines or engaging with particular advertisements
- **Financial uses or ‘Pay by Face’ systems:** the use of ‘facial authentication’ technology to facilitate payment for goods replacing the need to present a card.
- **Education**: students using ‘face ID’ to pay for canteen meals and to check out library books; the detection of unauthorised campus incursions; the automated proctoring of online exams; and even gauging students’ emotions, moods, and levels of concentration as they engage with content from the curriculum and different modes of teaching delivery
- **Employment**: facial recognition applications also allow factory and construction employees to clock in for work via contactless ‘facial time attendance’ applications.[10]

[8] Buolamwini et al (2020), Facial Recognition Technologies: A Primer

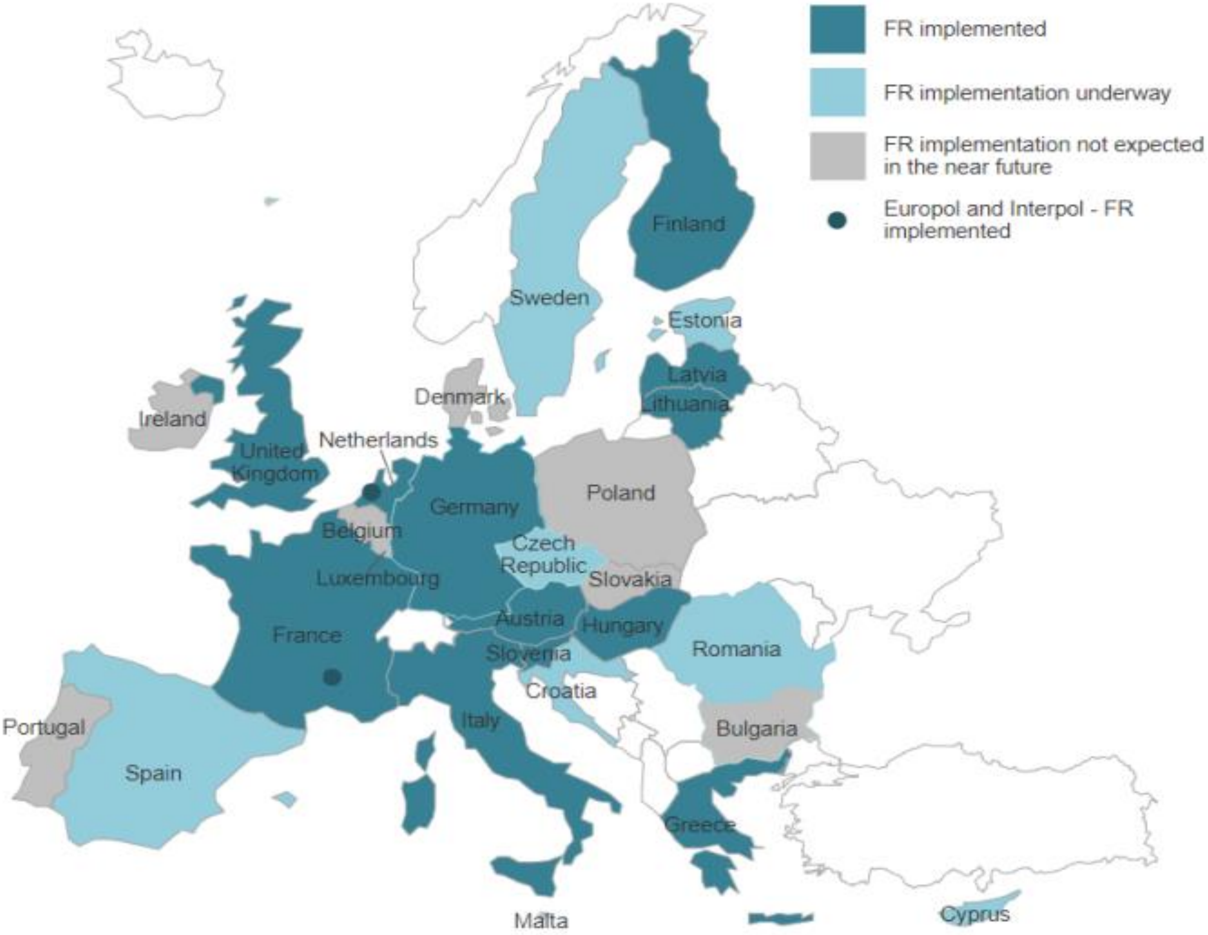
[9] Selwyn N, Andrejevic M, O’Neill C, Gu X, Smith G. Facial Recognition Technology: Key Issues and Emerging Concerns. In: Matulionyte R, Zalnieriute M, eds. The Cambridge Handbook of Facial Recognition in the Modern State. Cambridge Law Handbooks. Cambridge University Press; 2024:11-28.

[10] Ibid.

Use of FRT in the policing context

In the policing context, a study published by the EU Agency for Fundamental Rights (FRA) in 2019 revealed that there are few examples of national law enforcement authorities using live facial recognition technology in Europe.[11] The FRA study cites examples, mostly test cases, in the UK, Germany, France, Hungary and Sweden. Figure 1 below illustrates the findings of research conducted in 2020 related to the use of FRT in criminal investigations in EU Members States. Several Member States, including Ireland, cited legal issues (lack of legislation or existence of legal restrictions), as the primary reason for not using FRT. The TELEFI research also indicated that where FRT was being used, its most common use case in criminal investigations was its retrospective use.[12]

Figure 1: Use of FRT in Criminal Investigations in EU Member States



Source: TELEFI project Summary Report (2021), p 23.

[11] EU Agency for Fundamental Rights (2019) Facial recognition technology: fundamental rights considerations in the context of law enforcement, p 3.

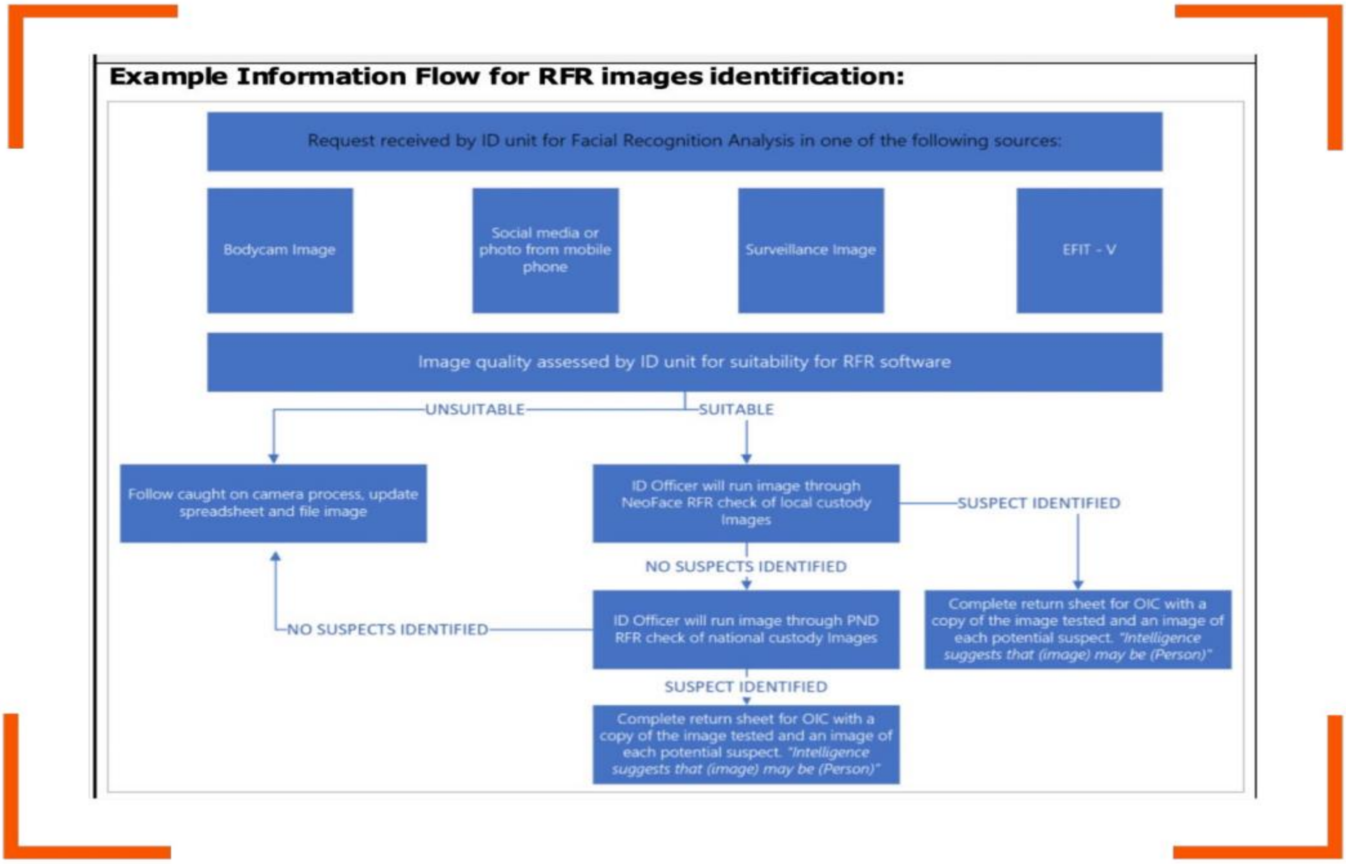
[12] TELEFI project Summary Report (2021), p 24. See also: Ragazzi, Kuskonmaz, Plájás, van de Ven & Wagner (2021), Biometric and Behavioural Mass Surveillance in EU Member States, Report for the Greens/EFA in the European Parliament.

In 2023, Murray described the use of three types of facial recognition technology by police forces in the UK as follows:

1. **Live facial recognition (LFR)** involves the application of facial recognition technology to live video feeds. If a match against the reference database (the 'watchlist') is returned an alert is generated so that officers can engage the individual in real time.
2. **Operator initiated facial recognition (OIFR)** is an 'in the field' technology also used to engage individuals in real time. Police officers take a photo of an individual using a dedicated app, and this is checked against a reference database composed primarily of local and national custody images.
3. **Retrospective facial recognition (RFR)** involves the after-the-fact application of facial recognition technology to any pre-recorded – i.e. not 'live' – digital content.[13]

Figure 2 below provides an example of information flow in relation to the use of retrospective facial recognition technology by law enforcement in the UK.

Figure 2: Practical application of retrospective facial recognition by law enforcement in the UK


Example Information Flow for RFR images identification:
Request received by ID unit for Facial Recognition Analysis in one of the following sources:
Bodycam Image
Social media or photo from mobile phone
Surveillance Image
EFIT - V
Image quality assessed by ID unit for suitability for RFR software
UNSUITABLE
SUITABLE
Follow caught on camera process, update spreadsheet and file image
ID Officer will run image through NeoFace RFR check of local custody images
SUSPECT IDENTIFIED
NO SUSPECTS IDENTIFIED
Complete return sheet for OIC with a copy of the image tested and an image of each potential suspect. "Intelligence suggests that (image) may be (Person)"
NO SUSPECTS IDENTIFIED
ID Officer will run image through PND RFR check of national custody images
SUSPECT IDENTIFIED
Complete return sheet for OIC with a copy of the image tested and an image of each potential suspect. "Intelligence suggests that (image) may be (Person)"

Source: Big Brother Watch (2023) Biometric Britain, p. 37.

[13] Murray (2023) Police Use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Law Framework, *Modern Law Review* 1-31, p. 4. See also Lynch (2024) Facial Recognition Technology in Policing and Security—Case Studies in Regulation, Special Issue Law and Emerging Technologies.

Operational issues: Accuracy

The accuracy of FRT has been questioned since the proliferation of its use in recent years. Researchers have cautioned against relying on a single percentage point when assessing accuracy and have suggested that the following factors be considered:

- different kinds of facial recognition technologies (from systems that detect the presence of a face, to those that assign attributes to a face, and finally those that attempt to verify or identify a unique individual),
- systems produced by different companies will produce different accuracy results,
- different types of errors a system makes,
- the distribution of those errors across different demographic populations,
- how real-world conditions differ from test conditions.[14]

Buolawmini and others provide an example of how an FRT system can make errors in Figure 3 below.

Figure 3: Falses and Positives in FRT

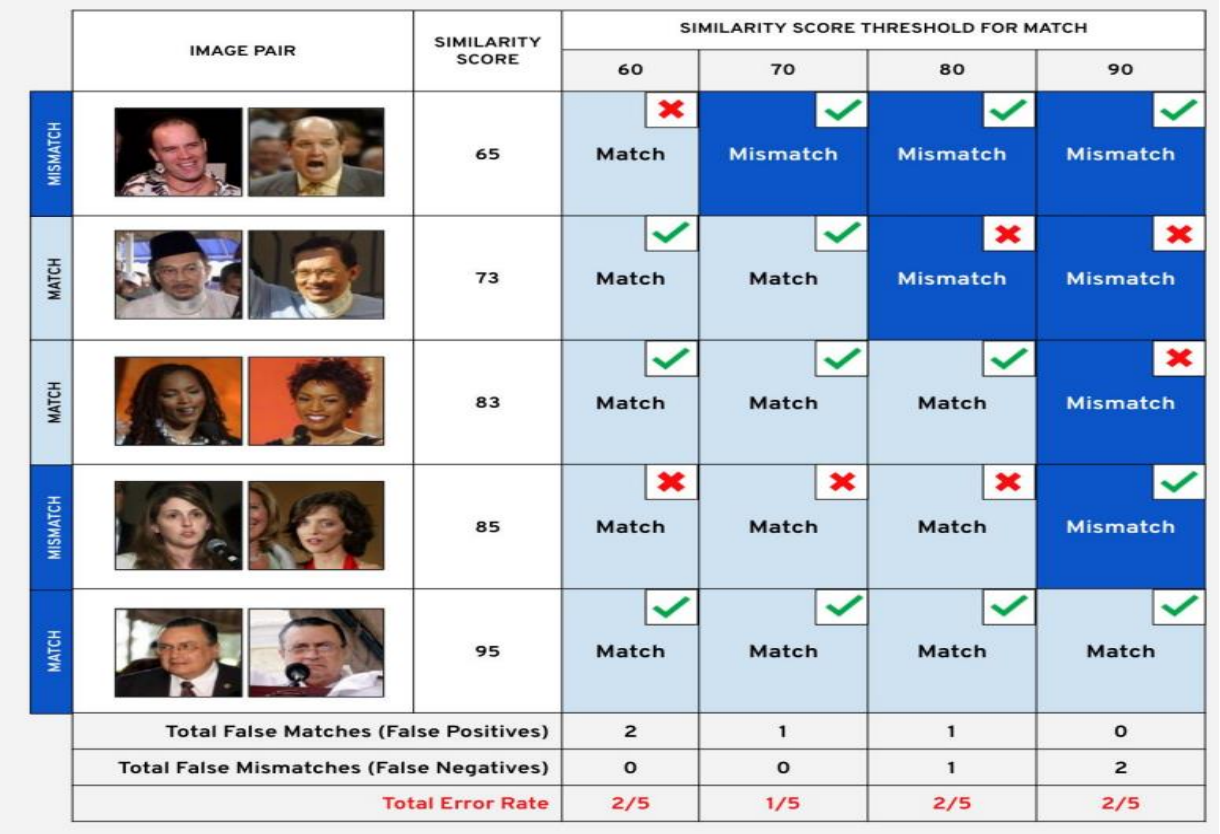


	IMAGE PAIR	SIMILARITY SCORE	SIMILARITY SCORE THRESHOLD FOR MATCH			
			60	70	80	90
MISMATCH		65	✗ Match	✓ Mismatch	✓ Mismatch	✓ Mismatch
MATCH		73	✓ Match	✓ Match	✗ Mismatch	✗ Mismatch
MATCH		83	✓ Match	✓ Match	✓ Match	✗ Mismatch
MISMATCH		85	✗ Match	✗ Match	✗ Match	✓ Mismatch
MATCH		95	✓ Match	✓ Match	✓ Match	✓ Match
	Total False Matches (False Positives)		2	1	1	0
	Total False Mismatches (False Negatives)		0	0	1	2
	Total Error Rate		2/5	1/5	2/5	2/5

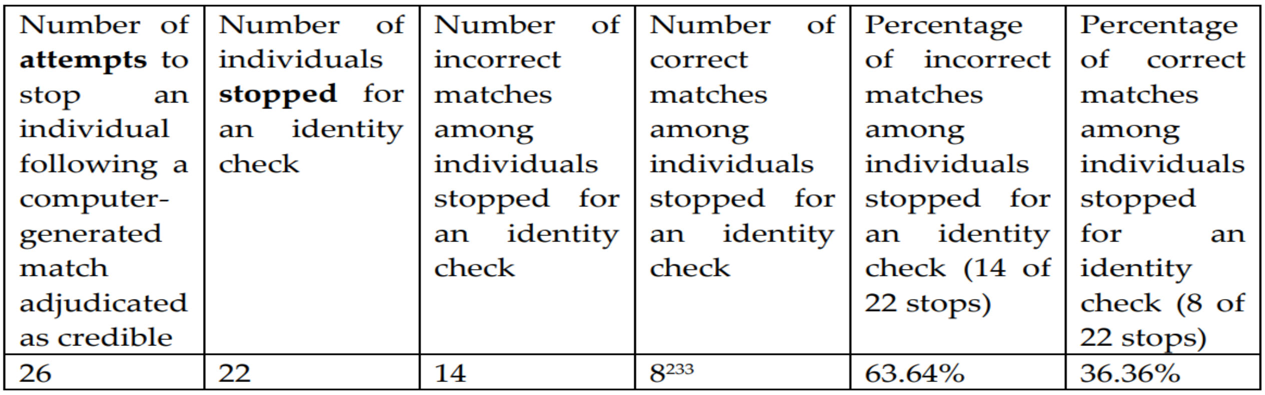
Source: Buolamwini et al (2020) Facial Recognition Technologies: A Primer

From 2016-2019 the Metropolitan Police Service (MPS) conducted 10 test deployments trialling live facial recognition technology during live policing operations. Researchers observed 6 of the 10 trials and studied the practices and procedures to provide an

[14] Buolamwini et al (2020) Facial Recognition Technologies: A Primer

independent assessment of the operation of FRT during the test deployments.[15] During the deployments the MPS used a database of individual images, known as a ‘watchlist’, against which live camera images were matched.[16] Overall, the FRT system generated 46 matches, involving 45 individuals, and MPS officers considered 26 of these matches credible enough to stop individuals and perform an identity check. Table 2 below provides a summary of the numbers and percentages of correct and incorrect matches from completed identity checks.

Table 2: Types of FRT used to answer specific questions



Number of **attempts** to stop an individual following a computer-generated match adjudicated as credible	Number of individuals **stopped** for an identity check	Number of incorrect matches among individuals stopped for an identity check	Number of correct matches among individuals stopped for an identity check	Percentage of incorrect matches among individuals stopped for an identity check (14 of 22 stops)	Percentage of correct matches among individuals stopped for an identity check (8 of 22 stops)
26	22	14	8[233]	63.64%	36.36%

Source: Fussey and Murray (2019) Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Recognition Technology, p. 70.

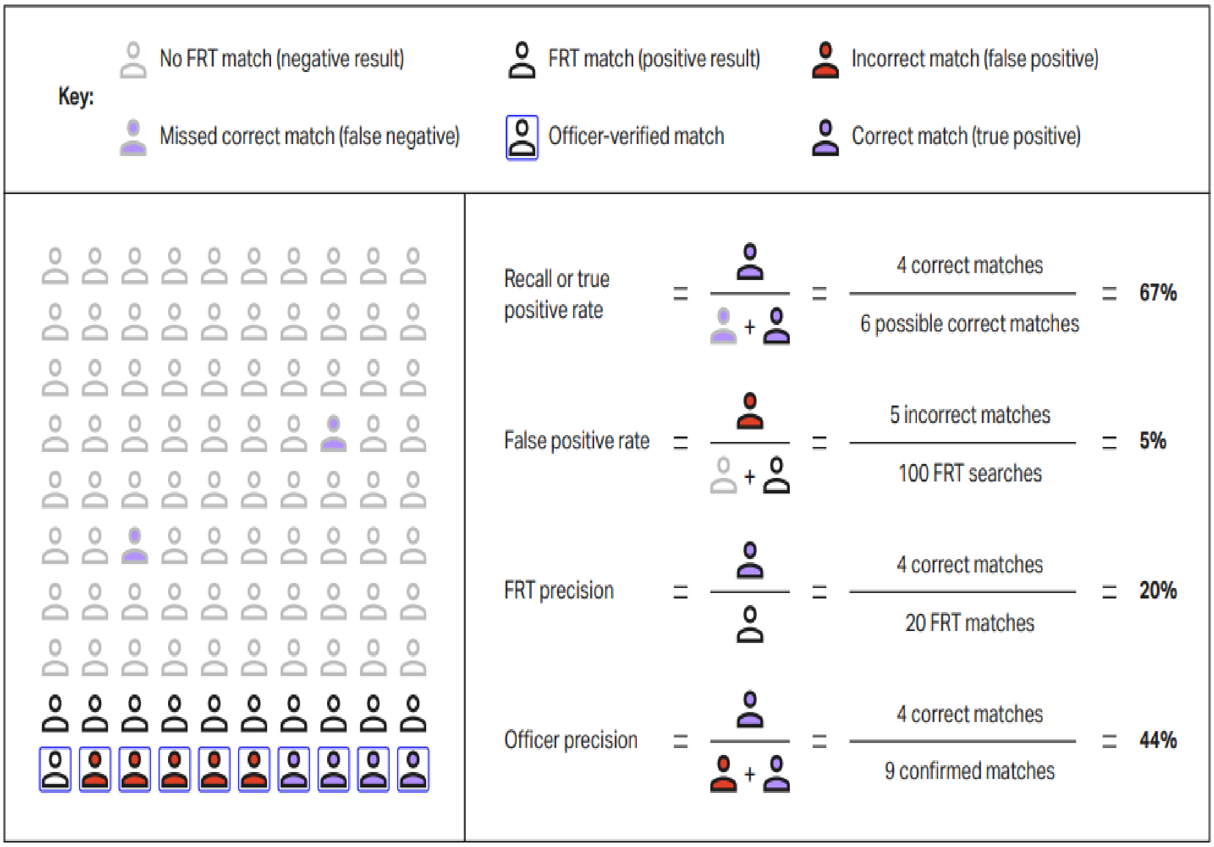
Fussey and Murray observed several issues relating to evaluating the performance of FRT.

- Firstly, the effectiveness of FRT cannot be judged on absolute numbers of matches. The researchers noted that calculations, outcomes and ratios may be influenced by numerous variables such as the time the camera was active for and the density of the crowd passing the camera.[17]
- Secondly, the methodology for measuring false positives is disputed. For example, the evidence from the MPS study indicates that the unreliability of human adjudication must be considered when calculating false positive rates.
- Thirdly, despite the use of different algorithms and cameras during test deployments, which were described as more accurate or capable, each deployment generated new and substantive issues.
- Fourthly, issues arose in relation to the creation and maintenance of watchlists. Such issues included scale, accuracy and currency of the data.[18]

Figure 4 below provides an illustration of how performance metrics have been calculated in another study on the use of FRT in policing in the UK.

[15] Fussey and Murray (2019) Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Recognition Technology. Further detail on the methodology used in this report is set out in chapter 1.
[16] Fussey and Murray (2019) Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Recognition Technology, p. 69.
[17] Fussey and Murray (2019) Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Recognition Technology, p. 73.
[18] Fussey and Murray (2019) Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Recognition Technology, p. 73.

Figure 4: Summary of performance metrics for FRT in the context of policing


Key:
No FRT match (negative result)
FRT match (positive result)
Incorrect match (false positive)
Missed correct match (false negative)
Officer-verified match
Correct match (true positive)
Recall or true positive rate
4 correct matches
6 possible correct matches
67%
False positive rate
5 incorrect matches
100 FRT searches
5%
FRT precision
4 correct matches
20 FRT matches
20%
Officer precision
4 correct matches
9 confirmed matches
44%

Source: Radiya-Dixit (2022), A Sociotechnical audit: Assessing Police Use of Facial Recognition, Minderoo Centre for Technology & Democracy

Fussey, Davies and Innes have also noted that:

> "Political and media-based discussions of AFR have been largely pre-occupied with outcomes and 'if it works'. But this position fails to define what appropriate measures of success should be (i.e. the number of convictions, arrests or accurate identifications or minimizing the volume of inaccurate 'matches'). For AFR critics, a key issue concerns purported high numbers of 'false positives' generated by the system".[19]

These views echo the observations of the UK Biometrics and Surveillance Camera Commissioner who has continued to express concerns about the accuracy of FRT, despite independent testing and has called upon the UK government to engage more fully with civil liberties groups on risks and benefits of FRT.[20]

[19] Fussey, Davies and Innes (2021) "'Assisted' Facial Recognition and the Reinvention of Suspicion and Discretion In Digital Policing", *British Journal of Criminology* (2021) 61, 325-344, at 332.

[20] Biometrics and Surveillance Camera Commissioner Annual Report – 2023/2024, para 48.

Irish context

The contested nature of the debate in relation to accuracy of FRT arose during the PLS hearings.[21] AGS presented a study from the US National Institute of Standards and Technology (February 2023), which found identification scores of over 99% accuracy for cloudwalk_mt_007 algorithm.[22] In its advice to Government, the AI Advisory Council noted that "NIST researchers have acknowledged significant issues with the accuracy and bias of FRT algorithms and challenges in evaluating real-world FRT using wild image data from sources like CCTV and bodycams".[23] Following the publication of the PLS Report, Dr. Abeba Birhane,[24] rebutted accuracy claims and noted that the operation of that algorithm is kept secret. [25] Dr. Birhane also commentated that "the debate on 'accuracy' only obscures the bigger issues: FRT is a threat to fundamental rights, accurate or not".[26]

In its advice to Government, the AI Advisory Council stated that the following factors must be considered when evaluating the performance of FRT:

- Real-World Conditions: Accuracy metrics derived from ideal datasets may not reflect real-world conditions, which are often more complex and challenging.
- Matched and Unmatched Domains: Reported accuracy is often based on matched domains, as in the NIST results, such as mugshot-to-mugshot comparisons, rather than more difficult real-world scenarios like mugshot-to-CCTV footage.
- Demographic Disparities: Presenting evaluation results as a single, averaged accuracy figure can obscure significant disparities in performance across different demographics, potentially masking poorer outcomes for specific groups.[27]

In light of this recommendation in relation to testing in real-world conditions, a 2023 evaluation of the Metropolitan Police Service's use of retrospective FRT found:

> "It should be noted that all the face images were taken by test staff, or Cohort in the case of selfies, and when a facial image taken considered unsatisfactory by the photographer, e.g., out of focus, motion blur, subject eyes shut, generally a second image would be taken. For evaluation of demographic equitability this was appropriate for the images need to be consistent across demographics. It should be acknowledged that using images of lower quality, or lower resolutions, may not achieve the same level of performance."[28]

[21] Joint Oireachtas Committee on Justice, Report on Pre-Legislative Scrutiny of the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023, February 2024, p. 22-23.

[22] Joint Oireachtas Committee on Justice, Report on Pre-Legislative Scrutiny of the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023, February 2024, p. 23.

[23] Artificial Intelligence Advisory Council, Advice to Government: FRT Use by An Garda Síochána, Advice Paper No. 1/2024 June 2024, p. 4.

[24] Dr. Abeba Birhane is a leading academic on artificial intelligence who appeared before the Joint Oireachtas Committee during one of its pre-legislative scrutiny hearings on the General Scheme. Dr. Birhane is also a member of the Government of Ireland's AI Advisory Council.

[25] We're headed for big problems if gardaí get facial recognition technology – The Irish Times

[26] We're headed for big problems if gardaí get facial recognition technology – The Irish Times

[27] Artificial Intelligence Advisory Council, Advice to Government: FRT Use by An Garda Síochána, Advice Paper No. 1/2024 June 2024, p. 4.

[28] Mansfield, Facial Recognition Technology in Law Enforcement Equitability Study Final Report, National Physical Laboratory, p 23-24.

Bias and discrimination

A study published by the European Parliament recognises:

> "AI is created by humans, which means it can be susceptible to bias. Systematic bias may arise as a result of the data used to train systems, or as a result of values held by system developers and users. It most frequently occurs when machine learning applications are trained on data that only reflect certain demographic groups, or which reflect societal biases."[29]

In research carried out by Buolamwini and Gebru it was found that "all classifiers perform better on lighter subjects than darker subjects" and "across the board, darker females account for the largest proportion of misclassified subjects".[30] Discussing this research, Birhane has noted that although there was resistance to the paper at first "the vendors of the facial-recognition software that they audited eventually responded positively".[31] Birhane also notes that:

> "Amid what can feel like overwhelming public enthusiasm for new AI technologies, Buolamwini and Gebru instigated a body of critical work that has exposed the bias, discrimination and oppressive nature of facial-analysis algorithms".[32]

In the policing context, another study has noted "when technology forms the basis of a police investigation, the bias is likely to lead to disproportionate incrimination and wrongful indictment among minority groups."[33] For example, in the USA, a Detroit resident, Robert Williams, was arrested after FRT used by the Michigan State Police erroneously matched him with a wanted watch thief.[34] In 2016 the world's largest corporate supplier of police body cameras (Axon) announced that it would not deploy facial recognition technology in any of its products because it was too unreliable for law enforcement work and "could exacerbate existing inequities in policing, for example by penalising black or LGBTQ communities".[35]

In addition, independent scientific research carried out in 2023 on the use of FRT by the South Wales Police and the Metropolitan Police Service found:

> "False positive identifications increase at lower face-match thresholds of 0.58 and 0.56 and start to show a statistically significant imbalance between demographics with more Black subjects having a false positive than Asian or White subjects."[36]

[29] Panel for the Future of Science and Technology, European Parliamentary Research Service, The ethics of artificial intelligence: Issues and initiatives, March 2020, p. 15.

[30] Buolawimi and Gebru (2018) Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Conference on Fairness, Accountability, and Transparency, p. 10. See also Buolawimi (2017) Gender Shades: Intersectional Phenotypic and Demographic Evaluation of Face Datasets and Gender Classifiers.

[31] Birhane (2022) The unseen Black faces of AI algorithms, Nature Vol 610, p. 452.

[32] Birhane (2022) The unseen Black faces of AI algorithms, Nature Vol 610, p. 452.

[33] International Network of Civil Liberties Organizations (INCLO)(2021) *In Focus: Facial Recognition Tech Stories and Rights Harms from Around the World*, p. 9.

[34] International Network of Civil Liberties Organizations (INCLO)(2021) *In Focus: Facial Recognition Tech Stories and Rights Harms from Around the World*, p. 10.

[35] Crawford, K. (2019), "Regulate facial-recognition technology", Nature 572 (2019), 29 August 2019, p. 565. See also OECD AI Incidents and Hazards Monitor (AIM).

[36] Mansfield, Facial Recognition Technology in Law Enforcement Equitability Study Final Report, National Physical Laboratory, para 1.4.5.

According to research published by the European Parliament, “unless developers work to recognise and counteract these biases, AI applications and products may perpetuate unfairness and discrimination.”[37] That study also noted that biases can be hard to detect and handle because ‘black boxes’ make it “impossible for the consumer to judge whether the data used to train them [AI applications] are fair or representative”.[38] Researchers have highlighted the challenge to “… ensure that the relevant values are embedded in AI systems”.[39]

Surveillance technology, including FRT, and police operations

In the L&RS Note: Data privacy and community CCTV schemes, which is referred to in the L&RS Digest on the Garda Síochána (Recording Devices) Bill, it is noted:

> “In Ireland few studies have been conducted into the effectiveness of CCTV in preventing crime. One doctoral study from 2012, however, showed inconclusive results on its effectiveness whereby some categories of crime reduced in CCTV operated areas, but equally increased in other areas”.[40]

Similar results are evident from a study in Dallas, Texas in 2023 which found that CCTV did not significantly impact violent crime reductions.[41]

Exploring the role of AI in crime prevention, Haley notes “public cooperation with police can be at the essence of whether investigations and solving crimes are hindered or improve case clearance rates”.[42]

A recently published undergraduate thesis examined data from the US National Incident Based Reporting System during the period 2017-2023 to determine the impact of facial recognition technology on crime.[43] During this period, a number of the cities studied banned FRT and the study examined crime rates before and after these bans[44]. Comparing the results to findings related to the use of CCTV, the author concludes :

> “… there is little evidence supporting the theory that the implementation of this technology deters crime, and the many police departments who have implemented this technology have no basis for believing it improves public safety”.[45]

[37] Panel for the Future of Science and Technology, European Parliamentary Research Service, The ethics of artificial intelligence: Issues and initiatives, March 2020, p.15.

[38] Panel for the Future of Science and Technology, European Parliamentary Research Service, The ethics of artificial intelligence: Issues and initiatives, March 2020, p. 16.

[39] Ethics of AI (Chapter 3) - The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence – section 3.4. See OECD, Catalogue of Tools and Metrics for Trustworthy AI.

[40] Donnelly, “To CCTV or not? An examination of Community Based CCTV in Ireland” (Dublin; DIT, 2012).

[41] Study cited in Haley, P. The Impact of Biometric Surveillance on Reducing Violent Crime: Strategies for Apprehending Criminals While Protecting the Innocent. Sensors 2025, 25, 3160.

[42] Haley, P. The Impact of Biometric Surveillance on Reducing Violent Crime: Strategies for Apprehending Criminals While Protecting the Innocent. Sensors 2025, 25, 3160.

[43] Davis Taliaferro, Facing the Facts: The Efficacy of Police Facial Recognition Technology, University of Virginia Department of Economics, 28 April 2025.

[44] Ibid.

[45] Ibid.

Furthermore, the author discusses the potential societal costs, such as distrust in the police, as well as financial implications in the case of impact of wrongful identification and arrest of individuals.[46]

Therefore, the literature suggests the impact of technology on crime prevention is unclear. Moreover, the limited literature available on the efficacy of FRT suggests that any potential efficiencies in police investigation must be balanced against impacts on rights and society.

[46] Ibid.

Policy context

Facial recognition technology is rapidly evolving. Similarly, the policy context surrounding the proposed legislation has developed quickly in recent years. These technological advancements also occur against the backdrop of an extensive programme of policing reform which began with the establishment of the Commission on the Future of Policing in Ireland (COFPI) in 2017. The purpose of this section of the paper is to track Government policy in relation to the use of AI in policing and outline how these fit within the police reform agenda.

Government policy on AI

In response to research funded by the European Commission, Ireland indicated that, as of December 2020, it had no plans to implement facial recognition technology in the near future, i.e. in the next 1-2 years.[47] However, the use of artificial intelligence tools in policing was indicated in AI - Here for Good A National Artificial Intelligence Strategy for Ireland (June 2021) which states:

> "AI can provide new tools and insights for policing and law enforcement. The principal areas of AI application in this field include predictive policing, and the gathering and analysis of evidence. Under An Garda Síochána's Digital Strategy 2019-2023, digital policing is evolving rapidly with innovations emerging around AI and robotics."[48]

The AI Strategy also recognised:

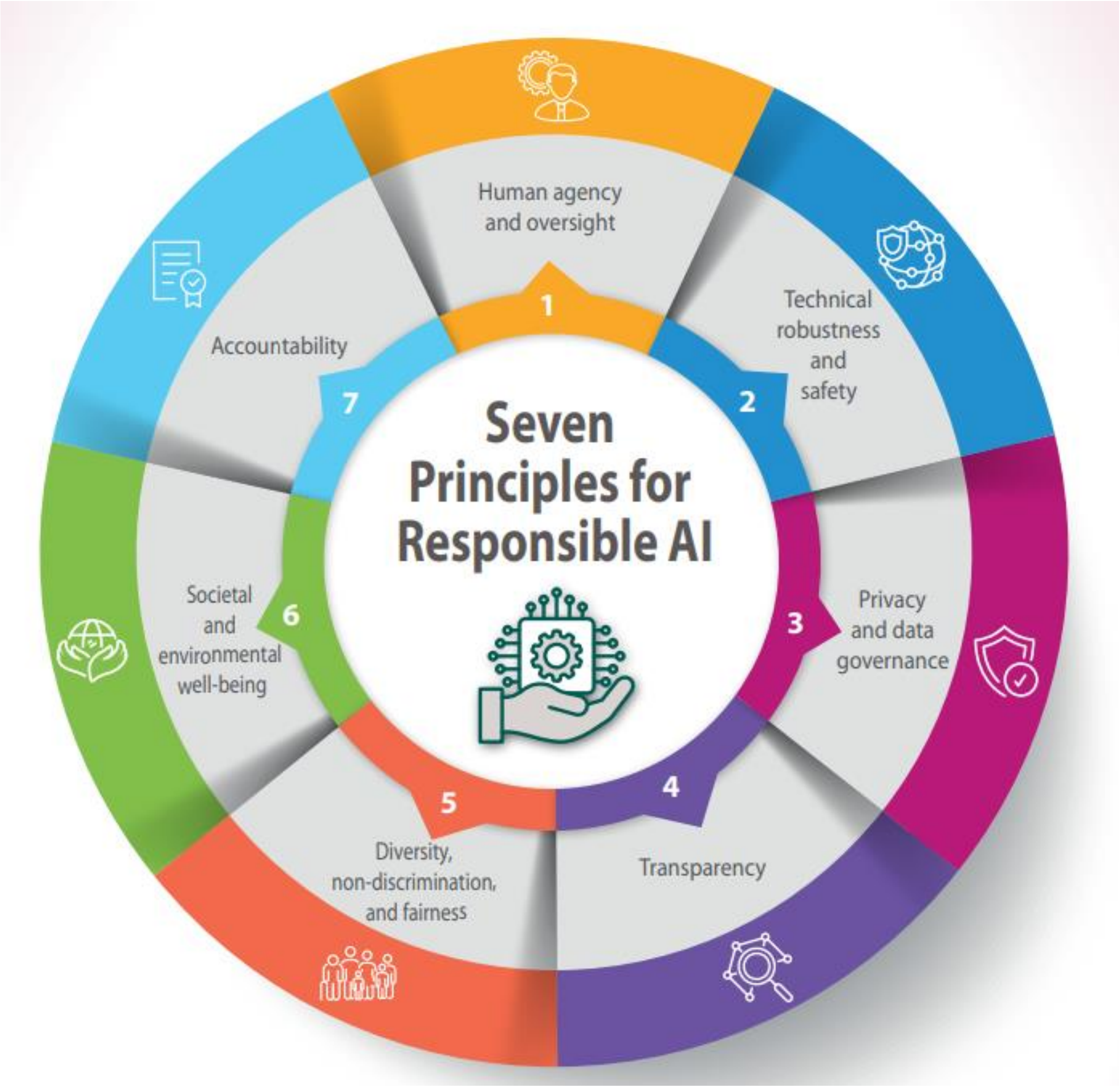
> "AI-based systems have the potential to exacerbate existing structural inequities and marginalisation of vulnerable groups. For instance, AI-based facial recognition technology that has been trained disproportionately on lighter skin tones may be significantly less accurate in relation to people of colour and can thus exhibit higher false positive rates for this population."[49]

In its refreshed National AI Strategy (2024) the Government committed to "a people-centred, ethical approach to AI development, adoption and use".

In the Interim Guidelines for Use of AI in the Public Service (February 2024), the Government asserted that AI tools used in the civil and public service must comply with the seven principles for responsible AI, which were informed and aligned with the European Commission's High Level Expert Group's seven principles for Trustworthy AI, depicted in Figure 5 below. In May 2025 this was reiterated in the Government's Guidelines for the Responsible Use of AI in the Public Service. In these Guidelines the Government outlines the benefits and risks associated with using AI in public services. The benefits listed include productivity, responsiveness and accountability. The EU AI Act's risk-based approach forms a central part of assessing risk in the Guidelines and it is also noted that data bias and discrimination, transparency and explainability, as well as dehumanisation of services are significant challenges when using AI to deliver public services.

[47] TELEFI_SummaryReport.pdf (telefi-project.eu), p 22.
[48] TELEFI_SummaryReport.pdf (telefi-project.eu), p 44.
[49]TELEFI_SummaryReport.pdf (telefi-project.eu), p 21.

Figure 5: Irish Public Service Responsible AI Framework

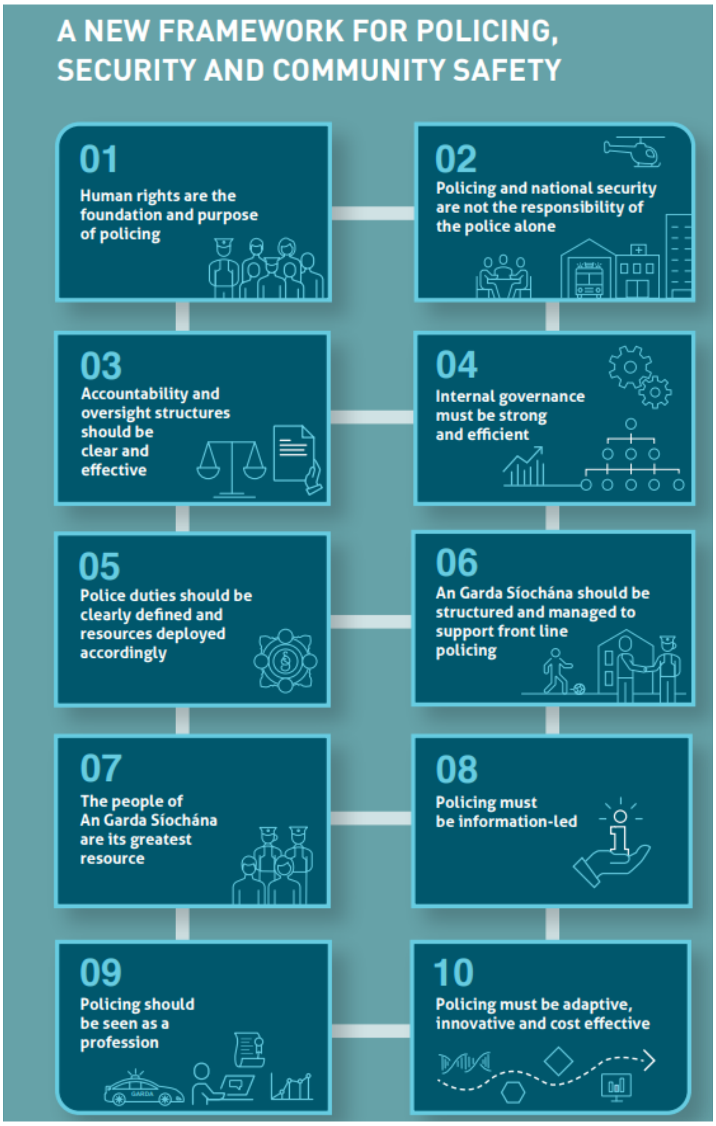

Seven Principles for Responsible AI
1
Human agency and oversight
2
Technical robustness and safety
3
Privacy and data governance
4
Transparency
5
Diversity, non-discrimination, and fairness
6
Societal and environmental well-being
7
Accountability

Source: Guidelines for the Responsible Use of AI in the Public Service (May 2025)

The Guidelines for the Responsible Use of AI in the Public Service also provide a Decision Framework to guide public service workers when considering using AI to solve a problem or improve a service. In this Framework, the first question is whether AI is the best solution for the problem and lists a number of factors to be discussed among a cross-functional team of experts.[50] The Guidelines then require public service workers to use the Responsible AI Canvas, which is described as “a simple, structured tool, designed to help develop, implement and oversee responsible AI solutions that meet the seven Principles for Responsible AI”.[51]

[50] Guidelines for the Responsible Use of AI in the Public Service, p. 38.
[51] Guidelines for the Responsible Use of AI in the Public Service, p. 42.

Policing policy on technology and AI



A NEW FRAMEWORK FOR POLICING, SECURITY AND COMMUNITY SAFETY

01 Human rights are the foundation and purpose of policing

02 Policing and national security are not the responsibility of the police alone

03 Accountability and oversight structures should be clear and effective

04 Internal governance must be strong and efficient

05 Police duties should be clearly defined and resources deployed accordingly

06 An Garda Síochána should be structured and managed to support front line policing

07 The people of An Garda Síochána are its greatest resource

08 Policing must be information-led

09 Policing should be seen as a profession

10 Policing must be adaptive, innovative and cost effective

The Commission on the Future of Policing in Ireland (COFPI) was established in 2017 to bring forward to the Government proposals for the future of policing. The COFPI recommended the introduction of body-worn cameras, which was legislated for in the Garda Síochána (Recording Devices) Act 2023.The final report noted that artificial intelligence:

"… will pose questions for policing, both practical and ethical. As in other professions, some functions now performed by police personnel will in future be performed by machines. Privacy issues arising from these developments will require a national, and international, debate going beyond policing."[52]

The Government's plan for implementing the COFPI's recommendations, A Policing Service for the Future (2018), included commitments related to body worn cameras but did not mention FRT. The Government's Final Report (2024) on the implementation of COFPI stated:

> "It is intended that Body Worn Cameras, supported by the underlying legislation, technology and training will act as an important evidentiary tool as well as increasing safety for Gardaí and the public."

In its review of the implementation of COFPI, the Irish Council for Civil Liberties noted that "Under human rights law, … surveillance technology should only be used … when the response is proportionate to meet a pressing need".[53]

In its PLS submission, AGS, relying on the 8thand 10th principles of COFPI illustrated in the graphic above, argues that "digital crime can only be detected with digital tools" and that it is

[52] COFPI, p. 92.

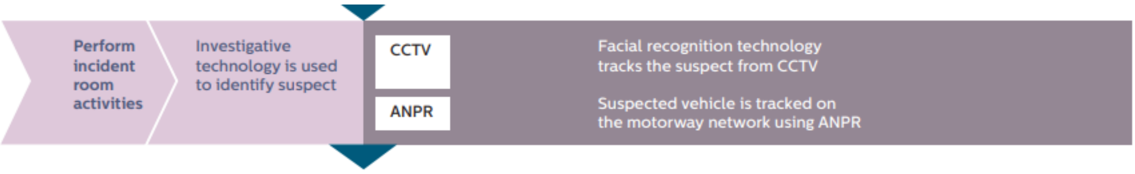
[53] ICCL (2024) Human Rights in Irish Policing Analysing the Implementation of the Recommendations from the Commission on the Future of Policing in Ireland.

necessary to have a “blend of the electronic world (data, devices and systems) with the human skills of Gardaí (human rights focus, tradecraft and decision making)”.[54]

AGS Corporate Plans

In An Garda Síochána’s Modernisation and Renewal Programme 2016-2021 the use of facial recognition technology was referred to in an example of a crime investigation process as illustrated in Figure 6 below:

Figure 6: Reference to FRT in Crime Investigation Process


Perform incident room activities
Investigative technology is used to identify suspect
CCTV
ANPR
Facial recognition technology tracks the suspect from CCTV
Suspected vehicle is tracked on the motorway network using ANPR

Source: An Garda Síohána’s Modernisation and Renewal Programme 2016-2021, p. 44.

The AGS Digital Strategy, Connect: An Garda Síochána Digital Strategy 2019 – 2023, also contained a priority action to “implement enhanced biometric identification services, including face recognition and mobile fingerprint capability”.[55]

While the AGS Strategy Statement 2022-2024 does not contain a specific reference to FRT, it does commit to cultivating “an information-led service, using data and technology to drive efficiencies, effectiveness and decision-making”.[56] In its Policing Priorities 2022-2024, the Policing Authority called upon the AGS to ensure that:

> “All policies existing and new are human rights proofed, to include any policy relating to the use of new technologies for policing”.[57]

In its assessment of policing performance in December 2024, the Policing Authority expressed the following views about policing and technology:

> “The Authority believes and has articulated its view to the Garda Commissioner and the Department of Justice that there is a need within the organisation for an overarching policy on technology. The same concerns that exist for the public with regard to policing – fairness, proportionality, legality and non-discrimination – are as relevant, if not amplified when technology increases policing capability. New technologies while they can assist policing can also be intrusive and infringe on the rights of individuals. Rather than address these concerns afresh with each device or platform that evolves, one overarching framework that sets out for the public the Garda Síochána’s

[54] An Garda Síochána, Submission on the General Scheme of the Recording Devices (Amendment) Bill 2023, 18 January 2024, available in the PLS Report, p 112.
[55] Connect: An Garda Síochána Digital Strategy 2019 – 2023, p 17.
[56] AGS Strategy Statement 2022-2024, p 19.
[57] Policing Authority, Policing Priorities 2022-2024, p 6.

> commitments to the public regarding its use of technology and how it will ensure that its use is informed by human rights and ethically deployed is essential."[58]

The AGS in its Human Rights Strategy recognises the issues of privacy, for example, it is stated:

> "There is a renewed focus on the privacy rights of those who encounter members of An Garda Síochána following the introduction of the General Data Protection Regulation (GDPR) and the Law Enforcement Directive. While specific issues of data protection are not the subject of this Strategy, issues in connection to the right to a private life under the Article 8 of the ECHR and Article 40.3 of the Constitution fall within the scope of this Strategy. Actions are proposed that address this issue, specifically in the context of covert policing and surveillance."[59]

Views on the use of FRT in policing

Discussions about legislating for FRT first arose in the context of the Garda Síochána (Digital Recording) Bill, which provided for the use of certain technologies by AGS, including body worn cameras and automatic number plate recognition (ANPR). In its 2021 Report on Pre-Legislative Scrutiny, the Joint Oireachtas Committee on Justice recommended that "CCTV devices will not use Facial Recognition Technology (FRT)."[60]

This section of the paper provides a summary of views that have been expressed on the introduction of FRT in recent years.

Government view

On 25 May 2022, former Minister for Justice, Helen McEntee TD, announced her intention to "provide for the use of facial recognition technology, Artificial Intelligence technology and other digital evidence management systems by An Garda Síochána" at the Garda Representative Association's Annual Delegate Conference. In this speech the Minister gave the following use case example:

> "Facial recognition software could be used where you might have a photo of a person that you need to search against recordings from a CCTV system".[61]

The Minister committed to not using such technology for "indiscriminate surveillance and mass data gathering" and to its use in "very clearly defined circumstances to help Gardaí search CCTV and video footage".[62] The Minister also noted that law enforcement partners in

[58] Policing Authority, Assessment of Policing Performance, December 2024, p 32.
[59] AGS, Human Rights Strategy 2022-2024, p. 11.
[60] 2021-12-17_report-on-pre-legislative-scrutiny-of-the-general-scheme-of-the-garda-siochana-digital-recording-bill_en.pdf (oireachtas.ie)
[61] gov - Speech by Minister for Justice Helen McEntee to the Garda Representative Association, Annual Delegate Conference (www.gov.ie)
[62] gov - Speech by Minister for Justice Helen McEntee to the Garda Representative Association, Annual Delegate Conference (www.gov.ie)

the UK and USA, as well as international agencies such as Europol and Interpol use facial recognition technology.

Furthermore, in response to a PQ, the Minister indicated her intention to bring forward a committee stage amendment to the Garda Síochána (Recording Devices) Bill to provide for the use of FRT, as follows:

> "The use of facial recognition technology, artificial intelligence and other digital evidence management systems would be used to search or process evidence held by An Garda Síochána. A number of safeguards will be built into the legislation to ensure that any potential intrusions into citizen's private lives are necessary and proportionate and are for justifiable policing purposes."[63]

During Second Stage debate of the Garda Síochána (Digital Recording) Bill 2023, the then Minister for Justice, Simon Harris TD, indicated that the proposals would relate to the use of retrospective facial recognition technology as a tool to aid the identification of suspects who are suspected of having carried out an arrestable offence, for example child sexual abuse.[64] The Minister also indicated that the use of FRT would be subject to safeguards and oversight including:

> "... judicial oversight over the operation of this technology, a strict prior approval mechanism for its use and Garda personnel remaining responsible as decision-makers, meaning that there would certainly not be any "machine" decision-making process."[65]

In April 2023, it was reported that this amendment gave rise to concerns from Justice Committee chairman James Lawless TD and it was not supported by the Green Party.[66] In June 2023, former Taoiseach, Leo Varadkar TD, indicated that the proposal to use FRT would be progressed through separate legislation rather than a Committee stage amendment.[67] The AGS (Digital Management and Facial Recognition Technology) Bill was then listed on the Autumn Legislation Programme 2023 as a priority for drafting.

On 14 December 2023, the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023 was published and was listed as a priority for publication in the Spring, Summer and Autumn Legislation Programmes in 2024. Pre-legislative scrutiny of the Bill took place on 13 February 2024 and the Joint Oireachtas Committee on Justice published its report in February 2024 with 32 recommendations for amendments. These recommendations will be considered in the forthcoming L&RS Bill Digest which will be published in advance of Second Stage debate.

Speaking at a conference in December 2024, the then Minister of State James Browne TD stated:

[63] Response to PQ on 'Legislative Programme', Dáil Éireann Debate, Tuesday - 31 May 2022. Question (587). Available here.

[64] Garda Síochána (Recording Devices) Bill 2022: Second Stage, Dáil Éireann debate - Wednesday, 1 Feb 2023, Vol. 1032 No. 5.

[65] Garda Síochána (Recording Devices) Bill 2022: Second Stage, Dáil Éireann debate - Wednesday, 1 Feb 2023, Vol. 1032 No. 5.

[66] Green Party urges scrapping of fast-track plan for Garda to use facial recognition technology – The Irish Times

[67] Dáil debates, Tuesday, 20 June 2023.

> "Given rapid developments in AI technologies over the past several years, it is of great importance that our justice systems, law enforcement agencies and policy makers are aware of, and prepared to engage with, the opportunities and the threats that advancements in artificial intelligence offers."[68]

The Programme for Government (January 2025) commits to the deployment of FRT "for serious crimes and missing persons, with strict safeguards" and the introduction of "live FRT in cases of terrorism, national security, and missing persons, with strict safeguards".[69] This is the first time that the Government has indicated its intention to permit the use of live facial recognition. In response to a PQ on 10 April 2025, Minister for Justice, Home Affairs and Migration, Jim O'Callaghan TD, confirmed that the Bill would not provide for the use of live FRT and instead this will be considered for inclusion in a subsequent Bill.[70]

On 16 July 2025, the Minister for Justice, Jim O'Callaghan TD, stated that he is working on two pieces of legislation in relation to FRT and describes their purposes as follows:

> "The first Bill will amend the Recording Devices Act 2023. This will only allow Gardaí to process retrospectively biometric data, with significant safeguards in place. It will allow for retrospective biometric analysis.
>
> …
>
> a second piece of legislation that will provide for retrospective and potentially live biometric identification and analysis beyond what is contained in the original Bill."[71]

AGS view

During Second Stage debate of the Garda Síochána (Digital Recording) Bill 2023, the then Minister for Justice, Simon Harris TD, indicated to Dáil Éireann that the Garda Commissioner and staff of AGS had called for the introduction of FRT.[72] During the pre-legislative scrutiny hearing, Garda Commissioner, Drew Harris, stated:

> "Digital crime and evidence can only be investigated with digital tools. Manual processing by Garda personnel sitting at screens is unfeasible and ineffective."[73]

The Garda Commissioner also addressed public concerns about AI, noting:

> "I wish to clarify that digitalisation in An Garda Síochána means that electronic tools act only in support of decisions taken by gardaí. There is never a question of

[68] gov.ie - Minister Browne in EU Re: combat migrant smuggling & child sexual abuse & how artificial intelligence may support justice systems
[69] Programme for Government 2025: Securing Ireland's Future, p. 117.
[70] An Garda Síochána Dáil Éireann Debate, Thursday - 10 April 2025, PQ No. 18323/25. See also Facial recognition: Work on law to introduce technology 'well advanced', says Minister – The Irish Times.
[71] Speech by Minister for Justice, Home Affairs and Migration, Jim O'Callaghan: A Contested Arena: Balancing competing human rights in the area of Justice, Home Affairs and Migration, 16 July 2025.
[72] Garda Síochána (Recording Devices) Bill 2022: Second Stage, Dáil Éireann debate - Wednesday, 1 Feb 2023, Vol. 1032 No. 5.
[73] Joint Committee on Justice debate - Tuesday, 13 Feb 2024

> autonomous machine decision-making. All decisions that can impact on a person are only taken by identifiable and accountable personnel."[74]

In its submission to the Joint Oireachtas Committee, An Garda Síochána identified the following use cases for image analysis and recognition technologies:

1. **Event Detection** – when something changes such as a person appearing on a deserted street;
2. **Object Recognition** – the ability to search for a certain type of object such as a car, a bicycle or a backpack;
3. **Object Clustering** – having identified an object of interest, the ability to search for all occurrences of it in the series;
4. **Person associated non-biometric search** – the ability to search for person wearing, carrying or using an object (such as a hi-vis jacket);
5. **Person associated non-biometric recognition** – having distinguished a person of interest (without associated identity), the ability to search for all occurrences of that person based on their association with objects;
6. **Person biometric recognition and search** – search for occurrences of a person (without associated identity) based on physical characteristics such as facial features;
7. **Person biometric clustering** – having distinguished a person of interest (without associated identity) in a series, find all instances of that person based on physical characteristics;
8. **Retrospective person remote biometric search** – search for all images in a digital evidence series for occurrences of a specific person of interest's image (with or without associated identity established);
9. **Retrospective person remote biometric identification** – Search a database of facial images (with associated identity) for a match with an image.[75]

Speaking during a Joint Oireachtas Committee on Justice debate, Garda Commissioner Drew Harris stated:

> "Facial recognition technology is not what we are seeking. We are seeking facial identification and the point of that is that we will have thousands of hours of CCTV and use AI to go through and find every incidence where we have the record of an individual who is present. We have no database of pictures to run them against so the object for us is to see what offences have been identified and make efforts then to identify that individual through normal police work. The AI assists us to the point of establishing the number of times an individual is seen and that individual may be engaging in criminal activity. It is just so much faster. It is months and months faster than individual gardaí sitting in front of laptops going through thousands of hours of CCTV.

[74] Joint Committee on Justice debate - Tuesday, 13 Feb 2024
[75] An Garda Síochána, Submission on the General Scheme of the Recording Devices (Amendment) Bill 2023, 18 January 2024, available in the PLS Report, p. 113-114.

> I refer to all the fears set out around facial recognition technology. We do not even wish to push as far as the European directive on AI. What we wish to do is retrospective investigation of serious criminality where CCTV or other images might play a part. Therefore, there has been a huge distortion in this. In doing so, the importance of its use in the expeditious of investigation and bringing serious offenders to justice has been lost to our detriment. As we sit here today, we have lost a very valuable investigative tool and I know the Government is working hard to make sure we have that as soon as possible."[76]

In an AGS information leaflet on Body Worn Cameras, it is stated that AGS will not use live FRT in conjunction with this technology. It is also stated:

> "While BWC footage is expected to be relatively small in volume and not a significant source for retrospective FRT, other CCTV evidence collected and stored on any future DEMS, as a result of a future procurement process, may be. All analysis tools (AI or FRT) must operate on a decision support basis only; Garda policy prevents autonomous machine decision-making where this could adversely impact a member of the public."[77]

Artificial Intelligence Advisory Council Advice (June 2024)

The Artificial Intelligence Advisory Council (AIAC) was established in January 2024 and in accordance with its Terms of Reference it is tasked with:

1. Providing expert guidance, insights, and recommendations in response to specific requests from government on emerging issues in artificial intelligence.
2. Developing and delivering its own workplan of advice to government on issues in artificial intelligence policy which it deems of particular priority in the current and future AI landscape, providing insights on trends, opportunities, and challenges.
3. Engaging in public communications aimed at demystifying and promoting trustworthy, ethical and person-centred AI. This may include media interviews, participation in public and sectoral events, or other communications activity.

In June 2024 a Sub-Group of the AIAC on Biometrics in the Public Service in Ireland issued an advice paper to Government on FRT Use by An Garda Síochána. Describing the opportunities and challenges presented by FRT, the advice notes:

> "FRT software can automate existing human-driven workflows and perform analyses previously impossible with human review. It provides the potential to speed up the processes of investigating and apprehending offenders and finding missing persons while using less police time and personnel. When used in law enforcement, potential efficiency gains must be balanced against the impact on rights. A complex range of harms may potentially occur in deploying FRT including misidentifying crime suspects.

[76] Joint Committee on Justice debate - Wednesday, 29 Nov 2023
[77] An Garda Síochána – Body Worn Cameras Frequently Asked Questions (FAQ)

> Therefore, as recognised in the AI Act, used in a law enforcement context, FRT is a high-risk technology given the potential consequences of its use for individuals."[78]

The advice considered the accuracy of FRT systems, referenced earlier in this paper, as well as public trust in AI, legal and regulatory considerations, procurement considerations and operationalisation. Some of the advice offered to Government included the following:

- Public trust must be a cornerstone in the use of AI by An Garda Síochána. Public transparency, engagement and accountability is crucial to building public trust around any contemplated use of FRT in policing and its operational parameters.
- Given the limitations of current evaluations, the AIAC advises against procuring or deploying FRT until satisfactory independent evaluations are conducted under real-world conditions relevant to Irish law enforcement. It is recommended that an independent Irish AI expert group be established to assess existing and emerging FRT evaluation methods from NIST and other international studies. Their goal would be to determine whether FRT algorithms are fit for intended law enforcement purposes in Ireland.
- If a decision is made to proceed to legislate, primary legislation must clearly establish the legal basis and use cases for FRT. The AIAC recommends close consultation with the Data Protection Commission, the Human Rights and Equality Commission and the EU AI Office to appropriately navigate the rights and regulatory considerations which FRT in law enforcement give rise to.
- In providing for and operationalising FRT, compliance with the EU AI Act framework should be built in. A Fundamental Rights Impact Assessment in alignment with the EU AI Act should be provided for before procurement and deployment of an FRT system by An Garda Síochána.
- Reference databases of images used in any matching exercise must have defined parameters and an express legislative basis provided for the data collected there.
- Applications for approval for deployment and applications for judicial redress should be from suitably trained members of the judiciary.
- To be suitably robust, the operational parameters should ideally be expanded upon in the form of secondary legislation rather than a Code of Practice.
- Access to an FRT system should be restricted to protect data privacy and to minimise the risk of errors as a result of deployment by personnel who are not appropriately trained.
- Robust complaints and judicial redress provisions should be expressly included in any legislation.
- Periodic independent auditing of the use of FRT should be provided for.
- We recommend the adoption of a bespoke procurement framework for FRT systems, in consultation with AI experts, to ensure their reliability in meeting best practice.
- If FRT is operationalised, ensuring legitimacy of data use and processing would be crucial.
- Accountability and securely storing and managing facial recognition data demand the development of extremely robust protocols.

[78] Artificial Intelligence Advisory Council, Advice to Government: FRT Use by An Garda Síochána, Advice Paper No. 1/2024 June 2024, p. 2.

- Adequate training, support and proper oversight around interpreting AI outputs is essential.[79]

The advice concludes that since no independent studies, including those by NIST, have evaluated FRT in real-world conditions “FRT systems should not be deployed in Ireland without independent review and evaluation by AI experts, considering unresolved risk factors and their potential impacts”.[80]

Stakeholder views

In June 2022, a group of academics and non-governmental organisations called upon the Minister not to introduce an amendment to the Garda Síochána (Recording Devices) Bill to allow for FRT, citing the risks associated with the technology. The letter also highlighted that such legislation would be premature given that Ireland would soon be subject to the provisions of the forthcoming European AI regulatory framework.[81]

During the pre-legislative scrutiny hearing on 13 February 2024, the Joint Oireachtas Committee on Justice engaged with An Garda Síochána and the Department of Justice as well as a wide range of stakeholders including academics, non-governmental organisations (Irish Council for Civil Liberties and Rape Crisis Network Ireland), the Law Society and the Data Protection Commission. According to the PLS report:

> “The submissions provided several observations on the General Scheme and commentary in relation to specific heads, in particular, outlining the impact of biometric identification technology on human and fundamental rights; outlining concerns with the accuracy of this technology and the potential for racial bias; and on provisions on the power to use the Biometric Identification [Head 4] and the Application for Approval of this technology [Head 5].”[82]

The PLS report also noted that some submissions highlighted the following advantages that FRT may bring for policing:

- Essential to be able to process complex digital evidence.
- Important for tackling transnational crime.
- Use of FRT saves resources and time.
- Current usage of image analysis and recognition technology in child sexual abuse material.[83]

[79] Artificial Intelligence Advisory Council, Advice to Government: FRT Use by An Garda Síochána, Advice Paper No. 1/2024 June 2024.

[80] Artificial Intelligence Advisory Council, Advice to Government: FRT Use by An Garda Síochána, Advice Paper No. 1/2024 June 2024, p. 8.

[81] Open letter to the Irish Times: Experts' red line on policing facial recognition technologies - UCD Centre for Digital Policy.

[82] Joint Oireachtas Committee on Justice, Report on Pre-Legislative Scrutiny of the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023, February 2024, p. 17.

[83] Joint Oireachtas Committee on Justice, Report on Pre-Legislative Scrutiny of the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023, February 2024, p. 35.

Following the hearings one of the stakeholders, Dr. Abeba Birhane, published an opinion in the Irish Times, March 2024 stating:

> "In seeking legislation to allow the use of facial recognition technology (FRT) in policing, Ireland risks introducing a technology that scientific evidence has demonstrated is ineffective, inherently flawed, opaque and discriminatory."[84]

In its Legislative Observations on the General Scheme, the Irish Human Rights and Equality Commission (IHREC) summarised the competing issues at play in relation to this legislation as follows:

> "We consider the use of facial recognition technologies by the State a serious interference with individual rights but also recognise that in order to support a modern police service in Ireland, there is a need for An Garda Síochána to transform its digital technologies. However, respect for human rights and fundamental freedoms is an essential part of democracy and the rule of law, and an appropriate balance must be struck between competing rights."[85]

[84] Birhane, We're headed for big problems if gardaí get facial recognition technology – The Irish Times, 20 March 2024.

[85] IHREC, Submission to the Minister for Justice on the General Scheme of the Garda Síochána (Recording Devices)(Amendment) Bill, May 2024, p 11.

Legal context

The Draft General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill, published on 14 December 2023, proposes to insert a new Part, Part 6A, into the Garda Síochána (Recording Devices) Act 2023. The operation of the 2023 Act will be discussed in more detail in the next section discussing the legislative proposals in the General Scheme.

As noted in the LRS Digest on the Garda Síochána (Recording Devices) Bill 2022, the use of technology by An Garda Síochána may impact on a range of human rights, which are protected by Bunreacht na hÉireann (Constitution of Ireland), the European Convention on Human Rights and EU Charter of Fundamental Rights.

Some of these rights, for example, the right to respect for private life and the protection of personal data, are further protected by the Data Protection Act 2018. The 2018 Act gives effect to the General Data Protection Regulation (GDPR) and transposes the Law Enforcement Directive (Directive (EU) 2016/680) into Irish law and gives rise to wide-ranging compliance obligations. The European Union Regulation on Artificial Intelligence (known as the EU AI Act) also adopts a risk-based approach to the regulation of AI. There is therefore a close connection between the data protection and artificial intelligence regulatory frameworks.

The Council of Europe has also published a Framework Convention on Artificial Intelligence. This has been signed, but not yet ratified, by the EU. It has not been signed by Ireland.

The purpose of this section is to outline both the human rights and regulatory legal framework which the legislative proposals on FRT must comply.

Human Rights Considerations

The EU Agency for Fundamental Rights (FRA) has identified the following fundamental rights as those most effected by FRT in the law enforcement context:

- Respect for private life and protection of personal data
- Non-discrimination
- Rights of the child and of elderly people
- Freedom of expression and freedom of assembly and of association
- Right to good administration
- Right to an effective remedy.[86]

Murray has identified two categories of potential human rights harms linked to retrospective FRT as follows:

> "First is the immediate impact on an individual's right to privacy caused by the recording of their movements in public, and by being subject to biometric processing. Second is a potentially more insidious long-term harm, associated with surveillance-related chilling effects."[87]

[86] Facial recognition technology: fundamental rights considerations in the context of law enforcement (europa.eu)

[87] Murray, Police Use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Law Framework (2023) *Modern Law Review* pp 1–31, at 8.

Expanding on his views in relation to the second category of human rights harms, Murray examines several studies on chilling effects, which found changes in behaviour and self-censorship as well as impacts on participation in political activities. [88] The Venice Commission noted similar concerns."[89]

Murray claims that facial recognition "is illustrative of the step change in State power and influence made possible by widespread digitisation and the emergence of AI" given the capacity to monitor the "minutiae of all individuals' day-to-day activities".[90] Murray also claims that "if human rights law is to respond to the challenges posed by facial recognition – and digital technologies generally – it must evolve." [91]

Necessity, Proportionality and Safeguards

The rights impacted by FRT listed above are protected by Bunreacht na hÉireann, the European Charter of Fundamental Rights, the European Convention on Human Rights (ECHR)[92] and various Council of Europe and United Nations treaties, which Ireland has ratified. However, these rights are not absolute any may be limited in certain circumstances. For example Article 8(2) ECHR states:

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

According to Murray:

> "… the advent of pervasive facial recognition is seen – if not as a *fait accompli* – then at least as an inevitability. The focus has been on limiting use, and establishing safeguards, rather than really questioning what the impact of facial recognition might be – particularly at a societal level – and whether certain applications of this technology should be used at all".[93]

During pre-legislative scrutiny some stakeholders raised questions as to the necessity of FRT and the Joint Oireachtas Committee suggested "that the rationale for introducing Facial Recognition Technology (FRT) be published in parallel with the progression of this legislation".[94] The PLS report also highlighted submissions from stakeholders that called for

[88] Murray, Police Use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Law Framework (2023) *Modern Law Review* pp 1–31, pp 11-12.
[89]Report on the Democratic Oversight of Signals intelligence Agencies, European Commission for Democracy Through Law (Venice Commission), Study No 719/2013, CDL-AD(2015)-11, 15 December 2015 at p 58.
[90] Murray, Facial recognition and the end of human rights as we know them? (2024) Netherlands Quarterly Journal of Huma Rights, Vol 42(2) (2024).
[91] Murray, Facial recognition and the end of human rights as we know them? (2024) Netherlands Quarterly Journal of Huma Rights, Vol 42(2) (2024).
[92]The ECHR has been indirectly incorporated into Irish law by the European Convention on Human Rights Act 2003.
[93] Murray, Facial recognition and the end of human rights as we know them? (2024) Netherlands Quarterly Journal of Huma Rights, Vol 42(2) (2024).
[94] PLS report, p 6.

the three tests of legality, necessity, and proportionality to be fulfilled where there is a restriction on human rights.[95]

The issue of legally permissible restrictions on the right to privacy through surveillance technology was discussed in the L&RS Digest on the Garda Síochána (Recording Devices) Bill.[96] It is well established in the case law of the European Court of Human Rights, the European Court of Justice and national courts that such encroachments upon the right to privacy may be permissible where it is necessary and proportionate to do so. This section will highlight some recent cases where these tests were considered in the context of FRT.

In the case of *Glukhin v. Russia*[97] the European Court of Human Rights held that use of live facial recognition technology in Russia violated an individual's right to respect for private life (Article 8 ECHR) and the right to freedom of expression (Article 10 ECHR).[98] The Court stated:

> "...the use of highly intrusive facial recognition technology in the context of the applicant exercising his Convention right to freedom of expression is incompatible with the ideals and values of a democratic society governed by the rule of law, which the Convention was designed to maintain and promote. The processing of the applicant's personal data using facial recognition technology in the framework of administrative offence proceedings – first, to identify him from the photographs and the video published on Telegram and, secondly, to locate and arrest him while he was travelling on the Moscow underground – cannot be regarded as "necessary in a democratic society".[99]

The European Court of Human Rights also noted that even though FRT was being used to pursue what may be deemed a legitimate aim in terms of "the prevention of disorder" and "the protection of the rights of others", it was not "necessary in a democratic society".[100]

The Court also held:

> "The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes ... and especially where the technology available is continually becoming more sophisticated ... . The protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests"[101]

The Court described the following as the minimum safeguards required :

- Procedures relating to duration of use,
- Storage of data,
- usage,

[95] Ibid.
[96] L&RS, Bill Digest on the Garda Síochána (Recording Devices) Bill 2022, p 23-25.
[97] Application no. 11519/20.
[98] *Glukhin v. Russia,* Application no. 11519/20.
[99] *Glukhin v. Russia,* Application no. 11519/20, para 90.
[100] *Glukhin v. Russia,* Application no. 11519/20, para 55.
[101] *Glukhin v. Russia,* Application no. 11519/20.para 75.

- access of third parties,
- procedures for preserving the integrity and confidentiality of data, and
- procedures for their destruction.[102]

Similarly in *The Queen (on application of Edward Bridges) v The Chief Constable of South Wales Police*[103] the Court of Appeal examined the use of live automated facial recognition technology by the South Wales Police force. The Court of Appeal found that "the policies did not sufficiently set out the terms on which discretionary powers can be exercised by the police and for that reason do not have the necessary quality of law".[104]

The Court of Justice of the European Union has also considered infringements on the right to privacy and data protection in the context of the automated analysis of passenger name records (PNR) for the purposes of preventing, detecting, investigating, and prosecuting terrorist offences and serious crime.[105] Discussing this case commentators noted that the automated matching of PNR data with patterns is comparable in its functioning to facial recognition systems and pointed out that the CJEU stated:

> "that the possibility of 'false negatives' and the fairly substantial number of 'false positives' resulting from the use of the system may limit the appropriateness of the system. However, automated processing has indeed already made it possible to identify air passengers presenting a risk in the context of the fight against terrorist offences and serious crime; this is why the system is not inappropriate. Moreover, according to the CJEU, the appropriateness of the system essentially depends on the proper functioning of the subsequent verification of the results obtained under those processing operations by non-automated means.[106]

Therefore, from this brief illustration of recent case law in this area, it is clear that the relevant tests may be satisfied is the law is sufficiently precise and achieves the correct balance between individual rights and police operations.

Public Sector Equality and Human Rights Duty

Section 42 of the Irish Human Rights and Equality Commission Act 2014 provides:

> A public body shall, in the performance of its functions, have regard to the need to—
>
> > (a) eliminate discrimination,
> >
> > (b) promote equality of opportunity and treatment of its staff and the persons to whom it provides services, and

[102] *Glukhin v. Russia,* Application no. 11519/20 para 77.
[103] [2020] EWCA Civ 1058.
[104] [2020] EWCA Civ 1058, para. 94.
[105] CJEU, Case 817/19, Ligue des droits humains v. Conseil des ministres [2022], ECLI:EU:C:2022:491, pp. 123–124.
[106] Matulionyte R, Zalnieriute M, eds. Facial Recognition Technology across the Globe: Jurisdictional Perspectives. In: The Cambridge Handbook of Facial Recognition in the Modern State. Cambridge Law Handbooks. Cambridge University Press; 2024:125-126, Chapter 9.2.

> (c) protect the human rights of its members, staff and the persons to whom it provides services.

A similar duty exists in the UK's Equality Act 2010, which is known as the Public Sector Equality Duty (PSED). In *The Queen (on application of Edward Bridges) v The Chief Constable of South Wales Police*[107] the appellant challenged the use of live automated facial recognition technology by the South Wales Police (WSP) Force. One of the grounds of complaint related to an alleged breach of the equality duty's requirement to have due regard to the need to eliminate discrimination on the basis of the protected grounds of race and sex. The appellant relied on "scientific evidence that facial recognition software can be biased and create a greater risk of false identifications in the case of people from black, Asian and other minority ethnic ("BAME") backgrounds, and also in the case of women."[108] The Court of Appeal stated:

> "Public concern about the relationship between the police and BAME communities has not diminished in the years since the Stephen Lawrence Inquiry Report. The reason why the PSED is so important is that it requires a public authority to give thought to the potential impact of a new policy which may appear to it to be neutral but which may turn out in fact to have a disproportionate impact on certain sections of the population".[109]

The Court held:

> "… SWP have never sought to satisfy themselves, either directly or by way of independent verification, that the software program in this case does not have an unacceptable bias on grounds of race or sex. There is evidence, in particular from Dr Jain, that programs for AFR can sometimes have such a bias. Dr Jain cannot comment on this particular software but that is because, for reasons of commercial confidentiality, the manufacturer is not prepared to divulge the details so that it could be tested. That may be understandable but, in our view, it does not enable a public authority to discharge its own, non-delegable, duty under section 149.[110]

The Court concluded that:

> "SWP have not done all that they reasonably could to fulfil the PSED. We would hope that, as AFR is a novel and controversial technology, all police forces that intend to use it in the future would wish to satisfy themselves that everything reasonable which could be done had been done in order to make sure that the software used does not have a racial or gender bias.".[111]

Given the similarity of the UK's Public Sector Equality Duty to the one applicable in this jurisdiction, it is worth noting that AGS may have to satisfy themselves that the FRT software that they may procure does not have an unacceptable bias which may result in discrimination. However, some research has revealed "explanations increased blind trust rather than

[107] [2020] EWCA Civ 1058.
[108] [2020] EWCA Civ 1058, at para. 164.
[109] [2020] EWCA Civ 1058 para 177
[110] [2020] EWCA Civ 1058 para 199.
[111] [2020] EWCA Civ 1058 para 201.

appropriate reliance on AI".[112] Therefore the individual interpreting the explanations of AI must understand how the technology operates in order to ensure appropriate reliance on AI.

Data Protection and FRT

Facial images are included in the definition of "biometric data" which may be processed by law enforcement authorities under the Data Protection Act 2018. Biometric data is classified as a "special category of personal data" and therefore law enforcement officials must demonstrate that such processing is required for one of the following purposes:

- to prevent injury or other damage to the data subject or another individual,
- to prevent loss in respect of, or damage to, property, or otherwise
- to protect the vital interests of the data subject or another individual;
- the processing is necessary for the administration of justice.[113]

When processing personal data for law enforcement purposes[114], the data must be:

- processed fairly and lawfully;
- collected for one or more specified, explicit and legitimate purposes and shall not be processed in a manner that is incompatible with such purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are collected;
- accurate, kept up to date if necessary, and every reasonable step should be taken to ensure (with due regard to the purpose they were collected) inaccurate data are rectified or erased;
- kept in a form that permits the identification of a data subject for no longer than is necessary for the purposes for which the data are collected;
- processed in a manner that ensures appropriate security of the data against unauthorised or unlawful processing and accidental loss damage or destruction.[115]

In its Guidelines on the use of FRT by law enforcement authorities, the European Data Protection Board (EDPB) notes that "a great deal of the increased interest in FRT is based on the efficiency and scalability of FRT" yet "the sheer size of processing of personal data, ... constitutes an interference with the fundamental right to protection of personal data."[116]

The EDPB Guidelines provide an overview of the properties of FRT and the applicable legal framework in the context of law enforcement, as well as practical guidance on procuring FRT

[112] Bansal et al Does the Whole Exceed its Parts? The Effect of AI Explanations on Complementary Team Performance. In CHI Conference on Human Factors in Computing Systems (CHI '21), May 8–13, 2021, Yokohama, Japan. ACM, New York, NY, USA.

[113] Section 69 of the Data Protection Act 2018.

[114] This relates to the processing of personal data by data controllers who are competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, where personal data is being processed for these purposes.

[115] Section 71(1) of the Data Protection Act 2018.

[116] European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, adopted 26 April 2023.

systems and potential use cases. In Scenario 4 of the Guidelines, the EDPB outlines a scenario where the police implement a way of identifying suspects committing a serious crime caught on CCTV by retrospective FRT.

To ensure the proportionate and necessary use of FRT, EDPB notes it should be considered whether "matching can be done manually within a reasonable amount of time, depending on the case at hand".[117] The EDPB concludes:

> In this scenario several measures have been put in place in order to limit the interference with data protection rights, such as the conditions for the use of the FRT specified in the legal basis, the number of people with access to the technology and the biometric data, manual controls etc. The FRT significantly improves efficiency in the investigatory work of the forensic department of the police, is based on law allowing for the police to process biometric data when absolutely necessary and therefore, within these perimeters may be considered a lawful interference of the rights of the individual.[118]

In recent years several data protection authorities in EU Member States have sanctioned Clearview AI for breaches of the GDPR in relation to its development of facial recognition databases. A comparison of these complaints illustrates that some authorities imposed fines of around 20 million Euro, while others did not impose any fines.[119]

EU AI Act and restrictions on the use of FRT in policing

Application in Ireland

The European Union Regulation on Artificial Intelligence (known as the EU AI Act) was published in the Official Journal of the European Union on 12 July 2024. Article 113 of the Regulation outlines the following timeline in relation to the entry into force of the Regulation:

- The Regulation will apply fully from **2 August 2026;**
- Chapters I and II will apply from **2 February 2025;**
- Chapter III Section 4, Chapter V, Chapter VII and Chapter XII and Article 78 will apply from **2 August 2025**, with the exception of Article 101;
- Article 6(1) and the corresponding obligations in this Regulation shall apply from **2 August 2027**.

[117] European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, adopted 26 April 2023, p. 47.
[118] European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, adopted 26 April 2023, p. 47.
[119] Authorities in Germany, France, Italy, Greece, Austria, and the UK concluded that the company breached the European Union (EU) General Data Protection Regulation (GDPR). In September 2024 the Dutch Supervisory Authority also decided to fine Clearview AI Inc. a total amount of € 30 500 000 – see further here. See Won Kyung Jung, Hun Yeong Kwon (2024) Privacy and data protection regulations for AI using publicly available data: Clearview AI case.

While it has been reported that the implementation of the AI Act may be delayed due to industry lobbying, a spokesperson for the European Commission stated on 4 July 2025 that there would be no delays given that the timeline is set out in the Regulation.[120]

Since the EU AI Act is a Regulation it will apply in full to Ireland and the Regulation of Artificial Intelligence Bill is listed in the Government's Summer Legislation Programme 2025 to give further effect to the Regulation.

In February 2025 a Parliamentary Question was asked about the applicability of the EU AI Act to policing given the reference to Article 6a of Protocol 21 to the Treaty of the Functioning of the European Union[121] in Recital 40[122] to the EU AI Act. The Minister for Justice, Jim O'Callaghan TD, responded:

> "I can inform the Deputy that Protocol 21 does not arise in respect of the EU AI Act (Regulation (EU) 2024/1689). Protocol 21 only applies in instances where the legal basis for a new legislative measure is drawn from Title V of Part 3 of the Treaty on the Functioning of the European Union. This is not the legal basis for the EU AI Act." [123]

It may be of interest to note that a similar recital appears in the Law Enforcement Directive (Recital 99), which was transposed into Irish law by the Data Protection Act 2018.

Aims of the EU AI Act

The aim of the EU AI Act is to promote innovation and the use of AI while also ensuring respect for fundamental rights, democracy and the rule of law. The EU AI Act uses specific terminology to refer to different forms of FRT which is set out below:

- **'biometric data'** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic [also known as fingerprint] data;
- '**biometric identification'** means the automated recognition of physical, physiological, behavioural, or psychological human features for the purpose of establishing the identity of a natural person by comparing biometric data of that individual to biometric data of individuals stored in a database;

[120] European Commission Midday press briefing from 04/07/2025, available here. See also Claudie Moreau, The EU will not budge on deadline for generative AI rules, *Euractiv* 4 July 2025.

[121] See further REVIEW OF PROTOCOL 21 TFEU

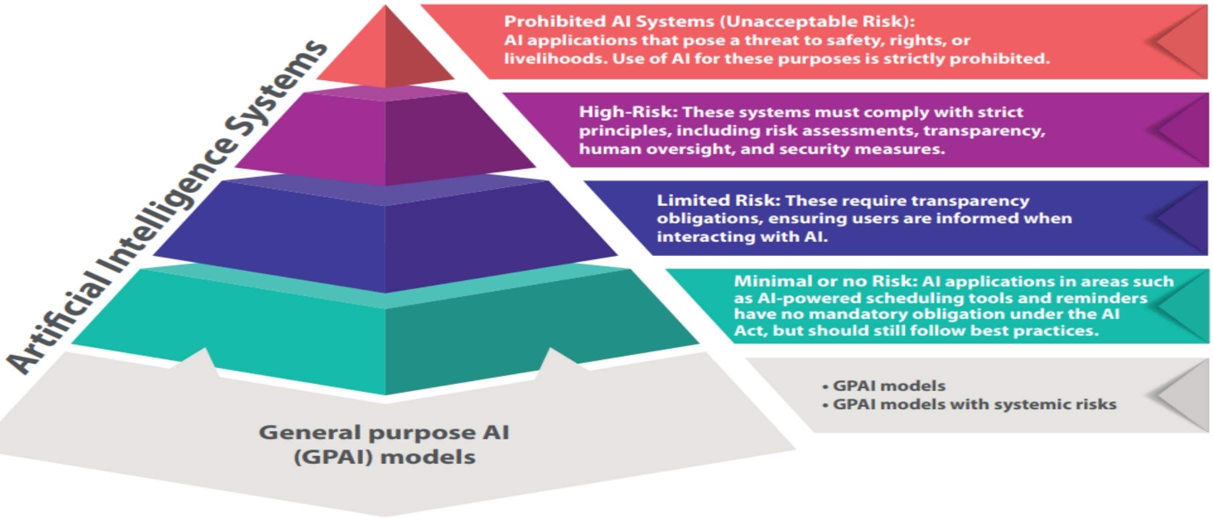
[122] Recital 40 to the EU AI Act states: "In accordance with Article 6a of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the TEU and to the TFEU, Ireland is not bound by the rules laid down in Article 5(1), first subparagraph, point (g), to the extent it applies to the use of biometric categorisation systems for activities in the field of police cooperation and judicial cooperation in criminal matters, Article 5(1), first subparagraph, point (d), to the extent it applies to the use of AI systems covered by that provision, Article 5(1), first subparagraph, point (h), Article 5(2) to (6) and Article 26(10) of this Regulation adopted on the basis of Article 16 TFEU which relate to the processing of personal data by the Member States when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU, where Ireland is not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16 TFEU."

[123] Artificial Intelligence – Wednesday, 12 Feb 2025 – Parliamentary Questions (34th Dáil) – Houses of the Oireachtas.

- **‘biometric verification’** means the automated, one-to-one verification, including authentication, of the identity of natural persons by comparing their biometric data to previously provided biometric data;
- **‘biometric categorisation system’** means an AI system for the purpose of assigning natural persons to specific categories on the basis of their biometric data, unless it is ancillary to another commercial service and strictly necessary for objective technical reasons;
- **‘remote biometric identification system’** means an AI system for the purpose of identifying natural persons, without their active involvement, typically at a distance through the comparison of a person’s biometric data with the biometric data contained in a reference database;
- **‘real-time remote biometric identification system’** means a remote biometric identification system, whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay, comprising not only instant identification, but also limited short delays in order to avoid circumvention;
- ‘**post-remote biometric identification system’** means a remote biometric identification system other than a real-time remote biometric identification system.

The AI Act follows a risk-based approach, classifying AI systems into four different risk categories, which are described in Figure 7 below.

Figure 7: EU AI Act risk-based approach


Artificial Intelligence Systems
Prohibited AI Systems (Unacceptable Risk): AI applications that pose a threat to safety, rights, or livelihoods. Use of AI for these purposes is strictly prohibited.
High-Risk: These systems must comply with strict principles, including risk assessments, transparency, human oversight, and security measures.
Limited Risk: These require transparency obligations, ensuring users are informed when interacting with AI.
Minimal or no Risk: AI applications in areas such as AI-powered scheduling tools and reminders have no mandatory obligation under the AI Act, but should still follow best practices.
• GPAI models
• GPAI models with systemic risks
General purpose AI (GPAI) models

Source: Guidelines for the Responsible Use of AI in the Public Service (May 2025), p. 18.

FRT or biometric identification systems fall into both the unacceptable risk and high-risk categories under Chapters 2 and 3, respectively, of the EU AI Act. The regulation of these AI systems will be set out briefly below.

Live FRT – a prohibited AI system

Article 5(1)(h) of the EU AI Act prohibits the use of live FRT, or real-time remote biometric identification ('RBI'), except if used by law enforcement for one of the following three purposes, subject to specific conditions:

1. the targeted search for victims of specific crimes or missing persons
2. prevention of a threat to the life or of a terrorist attack
3. identification of a person suspected of having committed a criminal offence[124]

Article 5(2) also provides:

> "The use of the 'real-time' remote biometric identification system in publicly accessible spaces shall be authorised only if the law enforcement authority has completed a fundamental rights impact assessment as provided for in Article 27 and has registered the system in the EU database according to Article 49. However, in duly justified cases of urgency, the use of such systems may be commenced without the registration in the EU database, provided that such registration is completed without undue delay."

In Guidance published by the European Commission, the rationale for the prohibition of RBI is outlined as follows:

> "Technical inaccuracies of AI systems intended for the remote biometric identification of natural persons can lead to biased results and entail discriminatory effects. Such possibly biased results and discriminatory effects are particularly relevant with regard to age, ethnicity, race, sex or disabilities. In addition, the immediacy of the impact and the limited opportunities for further checks or corrections in relation to the use of such systems operating in real-time carry heightened risks for the rights and freedoms of the persons concerned in the context of, or impacted by, law enforcement activities."[125]

Chapter 2 came into force on 2 February 2025. However, given that Minister O'Callaghan has indicated that this Bill will not provide for live FRT, further discussion is beyond the scope of this paper.

Retrospective FRT – a high-risk AI system

Article 6(2) in conjunction with paragraph 1(a) of Annex III of the EU AI Act classifies remote biometric identification systems as high-risk AI systems. Recital 95 of the EU AI Act recognises:

[124] Annex II of the EU AI Act lists the following as relevant criminal offences referred to: terrorism, trafficking in human beings, sexual exploitation of children, and child pornography, illicit trafficking in narcotic drugs or psychotropic substances, illicit trafficking in weapons, munitions or explosives, murder, grievous bodily injury, illicit trade in human organs or tissue, illicit trafficking in nuclear or radioactive materials, kidnapping, illegal restraint or hostage-taking, crimes within the jurisdiction of the International Criminal Court, unlawful seizure of aircraft or ships, rape, environmental crime, organised or armed robbery, sabotage, participation in a criminal organisation involved in one or more of the offences listed above.

[125] European Commission, Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), Brussels, 4.2.2025 C(2025) 884 final, para. 293.

> "Post-remote biometric identification systems should always be used in a way that is proportionate, legitimate and strictly necessary, and thus targeted, in terms of the individuals to be identified, the location, temporal scope and based on a closed data set of legally acquired video footage. In any case, post-remote biometric identification systems should not be used in the framework of law enforcement to lead to indiscriminate surveillance. The conditions for post-remote biometric identification should in any case not provide a basis to circumvent the conditions of the prohibition and strict exceptions for real time remote biometric identification."

Paragraph 6 of Annex III of the EU AI Act describes the use of AI systems by law enforcement in the following circumstances as high-risk AI systems:

> (a) assess the risk of an individual becoming the victim of criminal offences;
>
> (b) polygraphs or similar tools;
>
> (c) evaluate the reliability of evidence in the course of the investigation or prosecution of criminal offences;
>
> (d) assessing the risk of an individual offending or re-offending not solely on the basis of profiling[126], or to assess personality traits and characteristics or past criminal behaviour of individuals or groups;
>
> (e) for the profiling[127], of individuals in the course of the detection, investigation or prosecution of criminal offences.

Given the categorisation of remote biometric identification systems as a high-risk AI system, such systems are subject to a range of regulatory provisions set out in Chapter 3 of the EU AI Act. This designation triggers a range of compliance obligations, including requirements around risk management, data governance, human oversight and registration in the EU's database. While a full exploration of the obligations on providers and deployers of high-risk AI systems are beyond the scope of this paper, the specific obligations related to the use of retrospective FRT may be summarised as follows:

- **Judicial/administrative authorisation** must be requested prior to use or no later than 48 hours after use, except when it is used for the initial identification of a suspect.
  - If the authorisation is rejected, the use of retrospective FRT must be stopped immediately and the personal data must be deleted.
- **Limited use** to what is strictly necessary for the investigation of a specific criminal offence.
- **Specific use** linked to a criminal offence or threat of such offence, a criminal proceeding or the search for a specific missing person. Untargeted use of FRT is prohibited.
- **Human decision-making** by the law enforcement authorities required.

[126] As referred to in Article 3(4) of the Law Enforcement Directive (EU) 2016/680, which was transposed into Irish law by the Data Protection Act 2018.

[127] As referred to in Article 3(4) of the Law Enforcement Directive (EU) 2016/680, which was transposed into Irish law by the Data Protection Act 2018.

- **Annual reports on use of FRT** must be submitted to the relevant market surveillance and data protection authorities, excluding the disclosure of sensitive operational data related to law enforcement.[128]

Provisions related to high-risk AI systems identified in Annex 3 and Chapter 3 will come into force on 2 August 2026.[129] However, Article 26(10) of the EU AI Act provides that Member States may introduce more restrictive laws on the use of post-remote biometric identification systems.

Databases, the EU AI Act and Prüm II

As discussed above, FRT operates by comparing images to a reference database. The General Scheme does not contain any information on databases. During pre-legislative scrutiny, questions were raised as to what database would be used when using FRT and some recommendations were made to provide clarity in this regard.[130] Since the publication of the General Scheme, there has been some legislative developments in EU law which may shape the forthcoming Bill.

Article 5(1)(e) of the EU AI Act prohibits the expansion of facial recognition databases through "the untargeted scraping of facial images from the internet or CCTV footage;". According to Guidelines provided by the European Commission:

> "'Database' in this context should be understood to refer to any collection of data, or information, that is specially organized for rapid search and retrieval by a computer. A facial recognition database is capable of matching a human face from a digital image or video frame against a database of faces, comparing it to images in the database and determining whether there is a likely match between the two. Such a facial recognition database may be temporary, centralised or decentralised. Article 5(1)(e) does not require that the sole purpose of the database is to be used for facial recognition; it is sufficient that the database can be used for facial recognition."[131]

The European Commission also notes that the use of existing facial databases built up before 2 February 2025 must not be further expanded through AI-enabled untargeted scraping and must comply with data protection law.[132]

On 13 March 2024, a Regulation on police cooperation (known as Prüm II)[133] came into force. The Regulation requires Member States to establish a national database of the facial images

[128] Article 26(10) of the EU AI Act.

[129] Article 113 of the EU AI Act sets out the timelines in relation to entry into force and application. The Regulation itself was published in the Official Journal of the European Union on 12 July 2024.

[130] Joint Oireachtas Committee on Justice, Report on Pre-Legislative Scrutiny of the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023, February 2024, pp 25-26.

[131] European Commission, Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), Brussels, 4.2.2025 C(2025) 884 final, para. 226.

[132] European Commission, Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), Brussels, 4.2.2025 C(2025) 884 final, para. 236.

[133] European Union Regulation (EU) 2024/982 on automated data exchange for police cooperation. Further information available here.

(Article 19) of suspects, convicted persons and, potentially, victims and to allow for automated searching of facial images between Member States (Article 20). European Digital Rights has raised concerns about the inclusion of facial image exchange in Prüm II due to the serious risks of fundamental rights violations[134]. The Regulation is one of three legislative measures under the EU Police Cooperation Code which aims to enhance cooperation between police forces in the EU. The Department of Justice has indicated that a statutory instrument may be necessary to give effect to the Information Exchange Directive[135] and on 26 April 2022, Dáil Éireann passed a motion to opt in to the Prüm II Regulation[136].

Therefore, although there was no provision in the General Scheme for the establishment of a national database of facial images, it is evident that Ireland will be obliged to set up such a database under the Prüm II Regulation.

[134] Article 4(15) of Regulation (EU) 2024/982. See commentary here: EDRi-position-paper-Respecting-fundamental-rights-in-the-cross-border-investigation-of-serious-crimes-7-September-2022.pdf

[135] 2024-02-26_information-note-department-of-justice-directive-eu-2023-977_en.pdf

[136] Dáil Éireann debate -Tuesday, 26 April 2022.

Legislative Proposal

The Draft General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill was published on 14 December 2023 and proposes to insert a new Part, Part 6A, into the Garda Síochána (Recording Devices) Act 2023.

The 2023 Act provides for the use, in certain circumstances, of technology in policing, such as body worn cameras and drones (Part 2); automatic number plate recognition (ANPR) (Part 3); and CCTV (Parts 5 – 7)[137]. The 2023 Act was enacted on 5 December 2023 and some of the provisions were commenced on 15 May 2024.[138] Parts 8 and 9 of the 2023 Act include operational provisions, such as the requirement to develop codes of practice, admissibility of evidence and the review of the operation of parts of the Act.

Overview of the General Scheme

The General Scheme is comprised of 16 Heads, divided into three Parts, and a Schedule of offences in relation to which biometric identification may be used. As mentioned above, given the developments in the legal and policy landscape since the publication of the General Scheme in 2023, it is likely that the published Bill may be quite different to the General Scheme. Nevertheless, this section of the paper raises some thematic issues arising in the General Scheme which are likely to be of relevance to the forthcoming Bill.

Part 1 relates to preliminary and general matters and includes definitions of "biometric data" and "biometric identification". These definitions do not align to those set out in the EU AI Act outlined above. However, the General Scheme was published prior to the finalisation of the EU AI Act.

Part 2 proposes to insert a new Part, Part 6A (sections 43A-G), into the Garda Síochána (Recording Devices) Act 2023. This Part sets out the power to use biometric data (Head 3 – new section 43B), the approval process (Head 5 – new section 43C) and sets out parameters in relation to the use of biometric data (Head 7 – new section 43E). It also creates offences (Head 9 – new section 43G) in relation to the misuse of biometric identification. These offences are in line with offences listed under various parts of the 2023 Act.

Part 3 proposes to amend section 47 (Codes of Practice) of the Garda Síochána (Recording Devices) Act 2023, primarily to require the passage of a resolution by both Houses of the Oireachtas prior to the making of a Ministerial order in relation to a Code of Practice on biometric identification. This is a departure from process for the making of Codes of Practice in relation to other recording devices under Parts 2 – 6 of the Garda Síochána (Recording Devices) Act 2023.

Key thematic issues arising from these Heads will be discussed further below.

[137] See L&RS Bill Digest on the Garda Síochána (Recording Devices) Bill 2022

[138] Garda Síochána (Recording Devices) Act 2023 (Commencement) Order 2024 (S.I. No. 215 of 2024), art. 2(b). Ss. 6-7, 13-34, 49 had not yet been commenced at the time of writing.

Approval process

Head 5 proposes the insertion of a new section, section 43C, into the Garda Síochána (Recording Devices) Act 2023, which requires an application for the use of FRT to be made to a Garda Chief Superintendent. As outlined above, Article 26(10) of the EU AI Act requires judicial or independent administrative authorisation for the use of retrospective FRT (also known as post-remote biometric identification). The EU AI Act states that such authorisation must be requested prior to use or no later than 48 hours after use, except when it is used for the initial identification of a suspect. If the authorisation is rejected, the use of retrospective FRT must be stopped immediately and the personal data must be deleted.

In terms of operational issues, An Garda Síochána has raised the following concerns:

> "Within the context of an investigation and related analysis of large amount of evidentiary material where multiple offences may occur, it is not feasible to expect that the 'parameter of the search' are known a-priori. This is particularly the case in CSAM investigations and in the case of riots. As in any analytic work, search terms and hypotheses evolve and change as the material is inspected. Furthermore, search parameters may need to be adapted also depending on the specific capabilities and accuracy of the software used for biometric processing. The current wording is likely to cause an excessive administrative burden and delays to the investigation team."[139]

Codes of Practice

Head 3 states that the use of biometric identification under this Part must be in compliance with a Code of Practice as set out in section 47 of the Garda Síochána (Recording Devices) Act 2023.

Article 27 of the EU AI Act requires a fundamental rights impact assessment (FRIA) to be carried out for high-risk AI systems. As mentioned above, retrospective FRT would be considered a high-risk system under the AI Act. Therefore, in contrast to the 2023 Act, which provided no guidance on the contents of a FRIA, it is likely that the published Bill will specify the elements of the FRIA as follows:

> (a) a description of the deployer's processes in which the high-risk AI system will be used in line with its intended purpose;
>
> (b) a description of the period of time within which, and the frequency with which, each high-risk AI system is intended to be used;
>
> (c) the categories of natural persons and groups likely to be affected by its use in the specific context;
>
> (d) the specific risks of harm likely to have an impact on the categories of natural persons or groups of persons identified pursuant to point (c) of this paragraph, taking into account the information given by the provider pursuant to Article 13;

[139] An Garda Síochána, Submission on the General Scheme of the Recording Devices (Amendment) Bill 2023, 18 January 2024, available in the PLS Report, p. 119.

> (e) a description of the implementation of human oversight measures, according to the instructions for use;
>
> (f) the measures to be taken in the case of the materialisation of those risks, including the arrangements for internal governance and complaint mechanisms.[140]

In its PLS submission, AGS stated that "the development of a relevant code of practice for biometric identification would involve a Data Protection Impact Assessment (DPIA) of the anticipated use cases and approval/oversight mechanisms".[141] On 17 May 2024, a draft code of practice in relation to Body Worn Cameras was published under section 47(4) of the 2023 Act.[142] This Code of Practice was developed to coincide with the launch of the first phase for a Proof of Concept (PoC) for Body Worn Cameras (BWCs). According to the Final Implementation Report of 'A Policing Service for the Future':

> "Over 350 BWC trained Gardaí in three Dublin stations – Store Street, Pearse Street and Kevin Street have begun using Body Worn Cameras. Two other stations in Limerick and Waterford (Henry Street Garda Station and Waterford Garda Station) will follow in the coming months. It is intended that Body Worn Cameras, supported by the underlying legislation, technology and training will act as an important evidentiary tool as well as increasing safety for Gardaí and the public".[143]

In its observations on the General Scheme IHREC noted that it was unclear whether FRT could be deployed before a Code of Practice was developed and recommended that:

> "… consideration should be given as to whether provisions or fundamental issues designated for inclusion in the code of practice should be more appropriately dealt with in the primary legislation. The precise scope of the powers provided to An Garda Síochána should be outlined within the legislation; while the codes of practice should set out further information on the circumstances in which the powers may be exercised and the procedures to be followed by members of An Garda Síochána when exercising these powers".[144]

In the Code of Practice on Body Worn Cameras it is noted that:

> "The fundamental principle underpinning this COP is that any action taken must comply with the fundamental principles of legality, necessity, proportionality, and accountability and is applied in a non-discriminatory manner in accordance with the principles of the Constitution of Ireland 1937 and the European Convention on Human Rights."

The Code of Practice also states that both Human Rights Impact Assessment and Data Protection Impact Assessments have been carried out in accordance with the 2023 Act.[145]

[140] Article 27(1) of the EU AI Act.

[141] An Garda Síochána, Submission on the General Scheme of the Recording Devices (Amendment) Bill 2023, 18 January 2024, available in the PLS Report, p. 119.

[142] S.I. No. 216/2024 - Garda Síochána (Recording Devices) Act 2023 (Code of Practice) Order 2024

[143] Government Final Report on the implementation of the commitments contained in 'A Policing Service for the Future' (published in 2024).

[144] Submission to the Minister for Justice on the General Scheme of the Garda Síochána (Recording Devices)(Amendment) Bill, p. 27.

[145] Further discussion of this requirement is set out in L&RS Bill Digest on the Garda Síochána (Recording Devices) Bill 2022, p. 41—42.

These assessments are not appended to the code of practice. Therefore, it is not clear what, if any, impacts were found and what actions, if any, were required to be taken to ameliorate the impacts.

It may be of interest to note that non-compliance with a Code of Conduct will not automatically affect the admissibility of evidence[146]. In its PLS recommendations the Joint Oireachtas Committee on Justice had recommended that "Head 9 should be amended to provide for a disciplinary process arising from deliberate breaches of a Code of Practice".[147]

Review of operation of FRT and potential regulatory issues

Head 16 proposes to amend section 49 of the Garda Síochána (Recording Devices) Act 2023,which currently provides for the appointment of a serving High Court judge to review the operation of Parts 3 and 6 of the 2023 Act. Part 3 relates to the use of automatic number plate recognition, which had not yet been commenced at the time of writing. Part 6 relates to the Processing by Members of Garda Personnel of CCTV Operated by Third-Party Through Live Feed. Parts 3, 6 or section 49 of the 2023 Act had been commenced at the time of writing.

In the L&RS Digest on the Garda Síochána (Recording Devices) Bill, it was noted that similar judicial oversight roles created under the Communications (Retention of Data) Act 2011, have been critiqued for the following reasons:

> "...when the oversight role is a part-time function of a busy judge with no staff, specialist training or technical advisors, this lack of detail does not instil confidence and suggests an over-reliance on the entities supposedly being monitored."[148]

As outlined above, Article 26(10) of the EU AI Act requires annual reports on the use of post-remote biometric identification to be submitted to the relevant market surveillance and data protection authorities, excluding the disclosure of sensitive operational data related to law enforcement. The relevant national authorities in Ireland would be the Competition and Consumer Protection Commission[149] and the Data Protection Commission. These authorities are listed on the Department of Enterprise, Tourism and Employment's website, which indicates that the Government has approved a recommendation that Ireland adopt a distributed model of implementation of the EU Artificial Intelligence (AI) Act.

Article 77 of the EU AI Act also requires member states to provide a list of authorities which will supervise or enforce obligations related to fundamental rights, including the right to non-discrimination, in relation to certain high-risk uses of AI systems specified in the Act. According to the Department of Enterprise, Tourism and Employment's website, Ireland's list of fundamental rights authorities are as follows:

- An Coimisiún Toghcháin
- Coimisiún na Meán

[146] Section 48(3) of the Garda Síochána (Recording Devices) Act 2023.
[147] PLS Report, p. 11.
[148] TJ McIntyre (2016) Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective. See also Mr Justice Murray (2017) Review of the Law on the Retention of and Access to Communications Data, pp 47-48.
[149] Article 3(26) of the EU AI Act defines 'market surveillance authority' means the national authority carrying out the activities and taking the measures pursuant to Regulation (EU) 2019/1020.

- Data Protection Commission
- Environmental Protection Authority
- Financial Services and Pensions Ombudsman
- Irish Human Rights and Equality Commission
- Ombudsman
- Ombudsman for Children's Office
- Ombudsman for the Defence Forces

It should be noted that these public bodies do not yet have any obligations arising out of the EU AI Act but it is expected that they "will get additional powers to facilitate them in carrying out their current mandates in circumstances involving the use of AI systems".[150] Such mandates will likely be of relevance to the review of the operation of FRT in policing and therefore it remains to be seen whether such functions will be assigned in this or forthcoming legislation.

In addition, it has been suggested that the overlaps between the GDPR and the AI Act may present a regulatory challenge, for example:

> "A company using a biometric tool internally may act simultaneously as a controller under the GDPR and a deployer under the AI Act, triggering distinct compliance obligations. At the same time, providers of biometric tools — who may typically consider themselves processors under the GDPR — face the most extensive requirements under the AI Act, particularly for high-risk systems."[151]

While there is only one reference to the Data Protection Act 2018 in the General Scheme, there are numerous references to the 2018 Act in the Garda Síochána (Recording Devices) Act 2023. Therefore, it may be necessary to provide further clarity on how these regulatory regimes will operate in practice and which public bodies will be responsible for the oversight mechanism required by EU law.

Implementation issues: Admissibility of Evidence

Section 48 of the Garda Síochána (Recording Devices) Act 2023 relates to the admissibility of evidence and provides:

> "Documents obtained in accordance with this Act may, subject to this section and any applicable rules of evidence, be admitted as evidence in criminal and civil proceedings and in disciplinary actions."

While the General Scheme does not make any reference to admissibility of evidence, there have been some developments on identification evidence which may be of interest. *DPP v McHugh* 2024 [IECA] 176 concerned the legal basis for the exclusion by a judge of identification evidence in a criminal trial for murder. There was no direct evidence of the accused killing the victim and the prosecution wanted to introduce video evidence which they proposed showed the accused on CCTV in the vicinity. Two members of An Garda Síochána

[150] Department of Enterprise, Tourism and Employment's website.

[151] Richard Lawne, Biometrics in the EU: Navigating the GDPR, AI Act, published on 23 April 2025 on iapp.org. According to the website the IAPP is a policy neutral, not-for-profit association founded in 2000 with a mission to define, promote and improve the professions of privacy, AI governance and digital responsibility globally.

testified before the trial judge that the person captured by the video image was the accused; such evidence was excluded from consideration of the jury by the trial judge based on the argument that members of the Gardai identifying suspects had to be independent of the investigation.[152] The court concluded:

> "The evidence of identification, asserted by the prosecution to be proximate in time and place to the murder of the victim, should be restored for the consideration of the jury. The Court avoids any comment on the reliability or strength of that evidence. That is not for judges. It is for the jury to consider that evidenc[e]."[153]

Therefore, it may be the case that juries will have to grapple with issues related to the use of FRT in future trials.

Offences for which FRT may be used

The Schedule includes a list of offences, in relation to which biometric identification or data may be used. According to the Government press release[154] accompanying the General Scheme, issued on 14 December 2023, Minister for Justice, Helen McEntee TD requested the Joint Oireachtas Committee on Justice, to consider an additional list of offences for possible inclusion in the Bill. In its report on PLS, the Joint Oireachtas Committee made the following recommendation:

> "The Committee recognises the very serious nature of the additional list of offences set out in Appendix 2 and calls on the Government to include each of these offences in the Schedule of the Garda Síochána (Recording Devices) (Amendment) Bill 2023. The offences that the Minister asked the Committee to consider are very serious, such as defilement of a child under the age of 17, as well as a number of child pornography offences and offences relating to encouraging a sexual offence to be committed against a child. These offences carry heavy prison sentences and should be included in the Bill when published."[155]

In their respective PLS submissions, Dr. Darragh Murray and Dr. Ciara Bracken-Roche note that the inclusion of offences relating to 'riot' and 'violent disorder' may have a chilling effect on the rights to freedom of expression and freedom of assembly.[156] Both of these offences may be classified as serious criminal offences[157] since they both attract a maximum custodial sentence of 10 years.

It should be noted that Recital 33 of the EU AI Act states that the use of 'real-time' remote biometric identification (also known as 'live FRT') should only be used for offences that attract a custodial sentence of at least four years. The EU AI Act does not provide similar guidance on

[152] Kane, Evidence and Procedure Update, Irish Criminal Law Journal 2024, 34(4), 90-95.
[153] *DPP v McHugh* [2024] IECA 176, para.30.
[154] gov - Minister McEntee receives Cabinet approval for draft Facial Recognition Technology Bill (www.gov.ie)
[155] Joint Oireachtas Committee on Justice, Report on Pre-Legislative Scrutiny of the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023, February 2024, p. 11.
[156] Joint Oireachtas Committee on Justice, Report on Pre-Legislative Scrutiny of the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023, February 2024, p. 93.
[157] These offences are listed in the Schedule to the Bail Act 1997 as serious criminal offences.

which offences may be subject to post-remote biometric identification (also known as ‘retrospective FRT’).

Table 3 below sets out the offences listed in the Schedule to the General Scheme as well as the additional list of offences published by the Minister in December 2023.

Table 3: Offences listed in Schedule and additional offences proposed

Offences listed in Schedule to the General Scheme	**Additional offences referred to Joint Oireachtas Committee on Justice**
Non-Fatal Offences against the Person	
Section 15 – false imprisonment	Sections 16 - 17 (abduction of a child by a parent and abduction of a child by a person other than their parent is punishable by imprisonment for a term not exceeding 7 years
Section 4 and section 4A	
Sexual offences	
Criminal Law (Rape) (Amendment) Act 1990, section 3(1) and section 4(1)	Criminal Law (Rape) (Amendment) Act 1990, section 2 (sexual Assault, punishable by imprisonment for a term not exceeding 14 or 10 years)
Criminal Law (Sexual Offences) Act (2017), section 21(4).	Criminal Law (Sexual Offences) Act 2006, section 3 and 3A (defilement of child under 17 years and the same offence but by a person in authority, punishable by imprisonment for a term not exceeding 15 years and 10 year respectively)
Child Trafficking and Pornography Act 1998, section 3	an offence under sections 4, 4A, 5, 5A, of the Child Trafficking and Pornography Act 1998
Criminal Law (Sexual Offences) Act 2006, section 2	Criminal Law (Human Trafficking) Act 2008, section 5 (soliciting or importuning for purposes of prostitution of trafficked person, punishable by imprisonment for a term not exceeding 5 years)
The Common Law offence of Rape	Criminal Justice Act 2006, section 176 (reckless endangerment of children,

	punishable by imprisonment for a term not exceeding 10 years)
Criminal Law (Rape) (Amendment) Act 1990, section 4	section 249 of the Children Act 2001
	an offence under sections 4-8 of the Criminal Law (Sexual Offences) Act 2017
Homicide	
Offences Against the Person Act 1861, section 4	
Any offence under section 3 of the Criminal Justice Act 1990	
The Common Law offence of Murder	
The Common Law offence of Manslaughter	
Public order offences	
Criminal Justice (Public Order) Act 1994, sections 14 and 15	Criminal Justice (Public Order) Act 1994, section 19 (Assault or obstruction of peace officer)
Property offences	
Criminal Justice (Theft and Fraud Offences) Act, 2001, section 13	Criminal Damage Act (1991), section 2 (includes arson and criminal damage with intent to endanger life)
Criminal Justice (Theft and Fraud Offences) Act (2001), section 14	
Drugs offences	
	sections 15A and 15B of the Misuse of Drugs Act (1977), (drug trafficking offences for drugs over the value of €13,000, which subject to maximum penalties of life imprisonment)
Other	Section 2 of the Criminal Justice (UN Convention against Torture) Act (2000)

Source: L&RS (2025), based on the General Scheme and Department of Justice press release.

Conclusion

Artificial intelligence and its regulation have evolved rapidly in the last few years. The EU AI Act is the first regulatory framework in relation to AI and it remains to be seen how it will interact with the existing data protection regulatory framework. While the Garda Síochána (Recording Devices) (Amendment) Bill proposes to provide for the "safe and ethical use of facial recognition technology" it is clear from the research highlighted above that ethical and operational concerns remain in relation to the use of FRT.

This General Scheme proposes to amend the Garda Síochána (Recording Devices) Act 2023 which had not yet, at the time of writing, been fully commenced. Therefore, the operation of the new technologies provided for within that Act have not yet been tried and tested. The inclusion of FRT within this legislative framework would widen the scope of technologies available to AGS in policing. Given that the General Scheme was published before the finalisation of the EU AI Act, some Heads will have to be redrafted to ensure compliance with EU law.

Contact:

Houses of the Oireachtas
Leinster House
Kildare Street
Dublin 2
D02 XR20

www.oireachtas.ie
Tel: +353 (0)1 6183000
Twitter: @OireachtasNews

Library & Research Service
Tel: +353 (0)1 6184701
Email: library.and.research@oireachtas.ie