

REMOTE BIOMETRIC IDENTIFICATION FOR LAW ENFORCEMENT PURPOSES

FUNDAMENTAL RIGHTS IMPLICATIONS

REPORT



FRA

Remote Biometric Identification for Law Enforcement Purposes: Fundamental Rights Implications

Vienna, 2026

© European Union Agency for Fundamental Rights, 2026

Reproduction is authorised provided the source is acknowledged.

For any use or reproduction of photos or other material that is not under the European Union Agency for Fundamental Rights copyright, permission must be sought directly from the copyright holders.

Neither the European Union Agency for Fundamental Rights nor any person acting on behalf of the agency is responsible for the use that might be made of the following information.

Luxembourg: Publications Office of the European Union, 2026

PRINT	ISBN 978-92-9489-814-2	doi:10.2811/9903465	TK-01-26-020-EN-C
PDF	ISBN 978-92-9489-813-5	doi:10.2811/7982830	TK-01-26-020-EN-N

Photo credits:

Cover: © Kara / Adobe Stock

Page 19: © deagreez / Adobe Stock

Page 25: © Vedi altro / Adobe Stock

Page 31: © Ernest / Adobe Stock

Page 57: © Gérard Bottino / Adobe Stock

Page 65: © InfiniteFlow / Adobe Stock

Page 68: © jittawit21 / Adobe Stock

Foreword

Remote biometric identification (RBI) is rapidly becoming part of the technology available to law enforcement authorities in Europe. By comparing facial or voice data captured at a distance, and holding it in reference databases, these AI-driven systems can help to prevent, detect and investigate serious crime, identify suspects and search for victims or missing persons.

Such uses may contribute to public security. Yet, the capacity to identify people remotely – sometimes in publicly accessible spaces – also creates challenges for the protection of fundamental rights. Inaccurate or biased matches may have serious consequences for individuals, and the prospect of identification may discourage people from taking part in demonstrations, from attending gatherings in public, or otherwise exercising their rights in public.

FRA's research has shown how quickly measures framed as exceptional can start to feel routine, particularly when it comes to Member States strengthening their internal security. That is precisely why strict safeguards must be built in from the outset, not added once a system is already in use.

The European Union (EU) has established an important legal framework for addressing these risks. The EU Artificial Intelligence Act recognises the risks associated with RBI technologies and limits their use, particularly real-time use by law enforcement in publicly accessible spaces. It permits only narrowly defined exceptions under specific conditions. These rules complement the wider safeguards provided by the EU Charter of Fundamental Rights and EU data protection law.

The effectiveness of this legal framework will depend on its implementation and enforcement. This means clear national legal bases, and necessity and proportionality assessments carried out before – and not after – a system is deployed. It means reliable, independently tested technology and meaningful human oversight. And it means that transparency, independent supervision and access to effective remedies must remain in place throughout a system's use, not only at the point of implementation.

This report examines how remote biometric identification is regulated, considered, tested and used for law enforcement purposes across selected EU Member States. Drawing on legal analysis, interviews with practitioners and experts, observations of police work and public perceptions of RBI, it identifies both the potential contribution of these technologies and the fundamental rights challenges they present.

The report's central message is clear: public security and fundamental rights are not competing objectives. Rights-compliant policing bolsters public trust, democratic accountability and the rule of law. As Member States put the EU's legal framework into practice, FRA's evidence-based findings and opinions offer concrete guidance to ensure that the use of remote biometric identification is lawful, necessary, proportionate and subject to effective oversight.

Sirpa Rautio
Director

Contents

Foreword	1
Key findings and FRA opinions	5
PROVIDING FOR A RIGHTS-COMPLIANT NATIONAL LEGAL BASIS FOR LAW ENFORCEMENT AGENCIES' USE OF REMOTE BIOMETRIC IDENTIFICATION	7
INCREASING TRANSPARENCY ABOUT REMOTE BIOMETRIC IDENTIFICATION TOOLS USED BY LAW ENFORCEMENT	8
ENSURING A NECESSARY HIGH LEVEL OF ACCURACY AND DATA QUALITY	9
MITIGATING THE RISK OF ABUSE WHEN USING REMOTE BIOMETRIC IDENTIFICATION TOOLS	10
PREVENTING GENERAL AND INDISCRIMINATE SURVEILLANCE AND SOCIAL HARM	12
ENSURING EFFECTIVE EXTERNAL OVERSIGHT AND ACCESS TO EFFECTIVE REMEDIES	13
Introduction	15
ENDNOTES	20
1 LEGAL FRAMEWORK APPLICABLE TO REMOTE BIOMETRIC IDENTIFICATION SYSTEMS USED FOR LAW ENFORCEMENT PURPOSES	23
1.1. EU AI ACT AND THE EU DATA PROTECTION <i>ACQUIS</i> – SPECIAL RULES ON WHAT IS BANNED AND WHAT IS PERMITTED	25
1.2. REQUIREMENTS FOR INTERFERENCES WITH FUNDAMENTAL RIGHTS TO BE JUSTIFIED	30
ENDNOTES	33
2 FUNDAMENTAL RIGHTS CHALLENGES WHEN USING REMOTE BIOMETRIC IDENTIFICATION – SELECTED KEY ISSUES	35
2.1. LEGALITY OF USING REMOTE BIOMETRIC IDENTIFICATION – THE NEED FOR A CLEAR LEGAL BASIS IN NATIONAL LAW	35
2.2. LACK OF INFORMATION AND TRANSPARENCY ABOUT THE USE OF REMOTE BIOMETRIC IDENTIFICATION	41
2.3. ACCURACY AND DATA QUALITY	43
2.4. RISKS OF ABUSE	47
2.5. RISK OF SURVEILLANCE AND SOCIAL HARM	51
2.6. EXTERNAL OVERSIGHT AND EFFECTIVE REMEDIES	56
ENDNOTES	62
Conclusions: Hard-wiring fundamental rights when considering remote biometric identification for law enforcement purposes	65
ANNEX I – ABOUT REMOTE BIOMETRIC IDENTIFICATION SYSTEMS	67
FACIAL RECOGNITION TECHNOLOGY	67
VOICE RECOGNITION TECHNOLOGY	68
ANNEX II – METHODOLOGY	69
FIELDWORK	69
ENDNOTES	72

Key findings and FRA opinions

Law enforcement agencies are constantly seeking new technologies to improve the successful prevention, detection and investigation of crime to keep people safe. In recent years, biometric technology has advanced considerably. Such technologies allow for the identification of people at a distance without their active involvement or participation – a technique called remote biometric identification (RBI). For example, facial recognition technology (FRT) can scan crowds of people with video cameras and identify individuals based on their faces, by comparing the digital facial images obtained with images in databases. The technology works even if parts of the face are covered, such as when wearing a mask. While RBI tools provide opportunities to enhance public security, protect people from crime and find victims of crime or missing people, this artificial intelligence (AI)-driven power raises serious fundamental rights issues.

The European Union (EU) has adopted new legislation, the AI Act (**Regulation (EU) 2024/1689**), which, among other things, regulates the use of RBI by law enforcement agencies and partly prohibits its real-time use. The AI Act complements other applicable EU and national law governing the use of such systems, such as EU fundamental rights law and the EU data protection *acquis*. These bodies of law set stringent requirements for RBI's use, restricting or prohibiting its use by public and private actors, including those outside law enforcement.

This report is based on legal analysis, interviews with law enforcement practitioners and other experts in the field, and non-participant observations of work relating to RBI by selected law enforcement agencies. The empirical analysis was complemented by a quantitative survey with a limited number of people conducted in publicly accessible spaces to capture people's views on the use of RBI technology by law enforcement in public places.

The analysis provides insights into how to better protect fundamental rights when considering the use of such powerful technology. The European Union Agency for Fundamental Rights (FRA) carried out fieldwork in 2024 and early 2025, before the entry into application of the provisions of the AI Act relevant to RBI. Several interviewees were therefore still awaiting further guidance and discussing its possible implementation and impact. The findings in this report, which reflect issues arising at the time the fieldwork was carried out, can usefully inform the implementation of the AI Act and, more broadly, the fundamental-rights-compliant use of RBI for law enforcement purposes.

The key fundamental rights considerations for RBI development and use, elaborated in the opinions of this report, are summarised in **Table 1**.

The fieldwork shows that the use of RBI tools is relatively recent in the EU Member States covered. At the time of the research, most RBI systems under scrutiny were not real-time systems as defined in the AI Act. This means that these AI-driven systems do not perform the capture of biometric data, comparison and identification instantaneously, or almost instantly (i.e. without a significant delay), within the meaning of Article 3(42) of the AI Act, but rather do so in a retrospective manner (*ex post*), as per Article 3(43) of the AI Act.

TABLE 1 KEY CONSIDERATIONS FOR MEMBER STATES AND DEPLOYERS TO ENSURE FUNDAMENTAL-RIGHTS-COMPLIANT REMOTE BIOMETRIC IDENTIFICATION

Relevant party (or parties)	Action needed
Member States (government/ legislator)	— Provide a clear, specific and comprehensive legal basis that governs the use of both real-time and <i>ex post</i> remote biometric identification (RBI) for law enforcement purposes and aligns with the AI Act. It should indicate if RBI can be used in real time or <i>ex post</i>, while respecting necessity and proportionality and assessing all the fundamental rights impacted; determine the permissible purposes of RBI use; specify the criminal offences for which RBI can be deployed from the list in Annex II to the AI Act; lay down detailed conditions for the authorisation of RBI use, including judicial or independent oversight; and clarify in detail when and how deployers must conduct fundamental rights impact assessments (FRIAs), as per the AI Act. — Do not use RBI for law enforcement purposes until adequate national legal frameworks and designated oversight mechanisms are in place. — Consider adopting stricter (more protective) rules for the deployment of RBI than those provided for in the AI Act. — Provide effective safeguards, as provided for in the AI Act, EU data protection law and fundamental rights law, against their potential abuse (see Section 2.4), both when enacting legislation on the matter and when setting out more detailed rules and practical guidance. — Clearly define the reference databases and watch lists against which collected biometric data are compared. — Put in place standard operating procedures governing the operational aspects of using RBI tools, with rights-compliant solutions built in by design and in line with the procedures and guidelines set up to comply with the AI Act. — Consult a full range of stakeholders, including the general public and civil-society organisations, before adopting RBI tools and putting them into operation. — Ensure that law enforcement authorities publish the results of their FRIAs of the RBI system. — Provide meaningful information to the general public about the planned and real use of RBI for law enforcement purposes. — Ensure that regular transparency reports are published by both technology vendors and the law enforcement agencies deploying RBI. — Ensure that the RBI systems deployed by law enforcement agencies are sufficiently accurate across various population groups. — Explore possibilities of ensuring independent testing processes for RBI tools for both providers and deployers within the EU. — Never permit the use of real-time or <i>ex post</i> RBI to identify participants in peaceful demonstrations or political gatherings. — Ensure that data collection practices that do not use RBI, such as the visible use in highly frequented publicly accessible spaces of CCTV cameras that do not have RBI functionality, are subject to a thorough data protection impact assessment that also takes their potential chilling effect into account. — Provide sufficient resources to oversight bodies and ensure that they have sufficient powers and expertise to prevent and assess fundamental rights violations and effectively support those whose fundamental rights are affected by RBI tools used for law enforcement purposes. — Provide those seeking redress with the opportunity to request clear and meaningful explanations about the role of AI-driven tools in their case, including appropriate information about their functioning, and make sure every law enforcement deployer designates a contact person for such queries.
Deployers (law enforcement agencies)	— Ensure that the RBI system has undergone independent or external tests of its accuracy and potential bias before the system's deployment and that such tests are regularly repeated during its use. — Conduct a FRIA of the system, in line with Article 27 of the AI Act, duly considering all affected fundamental rights in a comprehensive manner. Particular attention should be paid to the right to human dignity; the right to privacy and the protection of personal data; non-discrimination; the freedoms of expression, assembly and association; the rights of the child and the elderly; the right to good administration; and the right to an effective judicial remedy. Obtain all necessary information from the providers of these systems. — Ensure system results are interpreted by staff with appropriate expertise and experience who are not involved directly in the investigation, prior to any action being taken on the basis of the results.

Providing for a rights-compliant national legal basis for law enforcement agencies' use of remote biometric identification

RBI technologies offer law enforcement agencies a powerful but highly intrusive tool to combat crime. Some respondents interviewed for this study underscored the need for a sufficient, specific and clear legal basis for the use of RBI, and highlighted that this is currently not the case for each RBI system in the Member States covered. Respondents to the FRA survey conducted in public places expressed concern that domestic law does not sufficiently limit the use of RBI technologies. They also noted the potential unethical use of the technology by the police and a consequent risk of 'function creep', that is, a gradual expansion of RBI tools' use beyond their original purpose.

Article 5(5) of the AI Act obliges Member States to lay down in their national legislation detailed rules governing authorisations for real-time RBI technologies for law enforcement purposes. National law must clearly state the purposes for which such technology can and cannot be used by law enforcement agencies – to avoid function creep – and also the concrete criminal offences covered, based on the list of offences in Annex II to the AI Act. When it comes to the use of *ex post* RBI systems for law enforcement purposes, their use is permitted insofar as it is authorised under EU and national law (recitals 54 and 59 of the AI Act). Additional requirements apply for law enforcement authorities' use of *ex post* RBI systems for criminal investigation purposes, implying the need for clear legal rules governing the authorisation of these systems' use (Article 26(10) of the AI Act). Member States can opt for stricter rules – by establishing wider-ranging prohibitions – than those required under the AI Act, as specified in its Articles 5(5) and 26(10).

Besides these legality requirements stemming from the AI Act, a clear legal basis for any limitation of fundamental rights is always required under EU fundamental rights law, including under Article 52(1) of the Charter of Fundamental Rights of the European Union (the Charter).



FRA OPINION 1

Member States must provide for a clear, specific and comprehensive legal basis governing the use of RBI for law enforcement purposes – both real-time and *ex post* – which must align with the AI Act. To comply with the EU fundamental rights law framework and the requirements in the AI Act, and to prevent function creep, domestic law should:

- indicate if RBI can be used in real time or *ex post*, duly respecting necessity and proportionality and assessing all the fundamental rights impacted;
- determine the permissible purposes for its use, beyond;
- specify the criminal offences from the list in Annex II to the AI Act for which RBI can be deployed;
- lay down detailed conditions for authorisation, including judicial or independent oversight;
- clarify in detail when and how deployers must conduct FRIAs, as per the AI Act.

FRA OPINION 2

Until adequate national legal frameworks and designated oversight mechanisms are in place (see **FRA opinion 11**), Member States should not use RBI for law enforcement purposes.

Given the potential serious and far-reaching fundamental rights implications of RBI, Member States should consider opting for more restrictive laws as per Articles 5(5) and 26(10) of the AI Act, prohibiting wider uses of RBI at the national level, beyond what is banned under the AI Act.

Increasing transparency about remote biometric identification tools used by law enforcement

FRA OPINION 3

To ensure greater transparency and understanding of the uses of RBI, Member States should consult a full range of stakeholders, including the general public and civil-society organisations, before adopting RBI tools and putting them into operation.

Member States should make sure that law enforcement authorities also publish the results of their FRIAs of RBI systems, which should be undertaken prior to deployment and when any changes to the system are made, to increase public trust.

FRA OPINION 4

Member States should take appropriate measures to provide meaningful information to the general public about their planned and real use of RBI for law enforcement purposes. This is particularly essential for exceptionally permitted uses of real-time RBI technologies, especially when people's facial images are captured by cameras in publicly accessible spaces without their knowledge and consent.

When an RBI tool is in operation, Member States should ensure that regular transparency reports are published by both technology vendors and law enforcement agencies deploying RBI. Reports should include information about the nature of deployments, the types of criminal offences concerned, the number of individuals impacted and the performance of the given RBI tool. These reports can help Member States assess the overall necessity and proportionality of the use of such systems in practice. They can also inform the statistics to be provided by the European Commission under the AI Act.

Transparency about the use of AI-driven RBI tools for law enforcement purposes and informing the general public about these tools are of crucial importance. Little information is available in the public domain about the use of RBI by national law enforcement authorities. Reasons for the 'secrecy' that some fieldwork respondents mentioned include maintaining the confidentiality of police operations, including any potential use of RBI tools. In several of the Member States covered, there is no dedicated transparency mechanism for informing the public or reporting publicly on the system's operation and effectiveness. There is limited public consultation prior to deployment. Research findings also point to a limited understanding among the judiciary of how RBI works.

This lack of transparency mechanisms is also reflected in the findings from the FRA survey conducted in public places, where views differed on whether FRT is being used in a specific Member State or not, pointing to a lack of knowledge about its use in practice. Two thirds of respondents think that FRT 'should only be used in public places where people are informed of its use and purpose'. Transparency is essential for enhancing the general public's trust.

Transparency is important not only for reasons of legality but also because it allows people to understand the reasons behind any decision supported by RBI tools, which is part of the right to good administration (Article 41 of the Charter) and allows people to exercise their right to an effective judicial remedy (Article 47 of the Charter). It also enables affected individuals to turn to other oversight mechanisms. Ultimately, it also upholds respect for human dignity (Article 1 of the Charter).

In addition to the information provision requirements established under Article 13 of the Law Enforcement Directive (**Directive (EU) 2016/680** (LED)), which can be limited to avoid obstructing or prejudicing law enforcement work or to protect public security and national security, some transparency measures are required under the AI Act.

The AI Act obliges providers and deployers of RBI systems for law enforcement purposes to register themselves and their systems in a secure non-public section of the EU database for high-risk AI systems. The European Commission and the competent national data protection supervisory authorities (as market surveillance authorities) have access to this database (Articles 49(1), (3) and (4), 71 and 74(8) of the AI Act). While law enforcement deployers of RBI systems need to share their FRIAs with market surveillance authorities under Article 49(4)(c) of the AI Act, they do not need to register summaries of them in the EU database. However,

Article 5(7) of the AI Act states that the European Commission must publish annual statistics on the law enforcement use of real-time RBI tools in publicly accessible spaces, aggregated to the Member State level.

Ensuring a necessary high level of accuracy and data quality

Notwithstanding potential accuracy gains, technical inaccuracies in RBI systems can lead to wrong outputs, including biased results and discriminatory outcomes. During the fieldwork, interviewees shared limited information about the accuracy rates (statistics) of specific RBI tools. Voice recognition experts within law enforcement authorities were the most familiar with and transparent about the accuracy rates and related statistics of the voice recognition technology used. The accuracy of RBI systems is strongly influenced by the quality of data used to create the systems and the data used during their deployment, as acknowledged by some interviewees. Some respondents underlined the importance of adequate testing, given that real-life conditions impact the performance of the technology. When it comes to FRT, a number of interviewees mentioned the practice of submitting the technologies used for standardised external assessment, for example to the US National Institute of Standards and Technology. Respondents from civil society and oversight bodies, including data protection authorities and other statutory human rights institutions or bodies, often expressed concerns about facial recognition systems working less accurately for certain groups and system biases that could lead to discrimination.

The AI Act acknowledges the technical challenges related to RBI systems (recital 32). It also requires that providers of RBI systems must ensure appropriate levels of system accuracy, which are to be declared in the instructions for use given to deployers (Article 15(1) and (3)). Under Article 13(3)(b)(v) of the AI Act, the instructions must include, when appropriate, information regarding the performance of the system in relation to persons or groups subjected to the system. Further obligations concerning accuracy apply under EU data protection law, where the principle of data accuracy (Article 4(1)(d) of the LED) requires that national authorities use information and data that are accurate and up to date. Pursuant to Article 15(2) of the AI Act, the European Commission has to encourage the development of benchmarks and measurement methodologies in cooperation with relevant stakeholders.

The AI Act also contains several requirements concerning data quality for both providers (Article 10) and deployers (Article 26(4)). The human oversight of RBI systems, required under Articles 14 and 26(2) of the AI Act, will also play an important role during the deployment of such systems, as deployers need to be aware of how the systems actually work and what their accuracy limitations are. At the same time, ensuring high levels of accuracy may require access to large and representative datasets, which may not be compatible with the principles of purpose limitation and data minimisation protected by EU data protection law.



FRA OPINION 5

Member States should ensure that RBI systems deployed by law enforcement agencies are sufficiently accurate across various population groups (e.g. women, people of colour, children, the elderly) who are subjected to such systems, duly considering the settings in which the technology will be deployed. This is needed to minimise discriminatory outputs and accuracy-related risks of wrongly flagging people.

Law enforcement authorities should ensure that an RBI system underwent independent or external tests concerning accuracy and potential bias before the system's deployment and that such tests are regularly undertaken during its use.

FRA OPINION 6

The European Commission should, under Article 15(2) of the AI Act, encourage the development of rigorous EU-wide benchmarks for the accuracy of RBI systems, taking into account diverse real-world conditions, the requirement of data minimisation under the EU data protection legislation and the need for accuracy assessments concerning different population groups, as general accuracy rates might convey a distorted picture.

The European Commission and Member States should explore possibilities for ensuring processes for the independent testing of RBI tools for both providers and deployers within the EU.

Mitigating the risk of abuse when using remote biometric identification tools

FRA OPINION 7

Member States should clearly set out the purpose-specific rules and conditions for the use of RBI technologies and provide effective safeguards against their potential abuse – both when enacting legislation on the matter and when setting out more detailed rules and practical guidance. Clearly defining reference databases and watch lists against which the biometric data collected are compared is equally important. The systematic logging of every time the tools are used or the data produced by them are viewed would ensure a clear audit trail, which is a precondition for effective oversight. Where data obtained through the use of RBI tools are later used in criminal proceedings, this information should be included in the case file to safeguard the right to a fair trial and equality of arms (see also the key finding ‘**Ensure effective external oversight and access to effective remedies**’).

Member States should put in place standard operating procedures governing the operational aspects of using RBI tools, with rights-compliant solutions built in by design, in line with the guidance on fundamental rights compliance stemming from the AI Act and EU data protection legislation. To avoid abuses by individual users, such procedures should include assurances that results produced by RBI systems are interpreted by staff with appropriate expertise and experience who are not involved directly in the investigation, prior to any action being taken on the basis of the results. Standard operating procedures for law enforcement agencies should also provide sufficiently detailed guidance to officers on how to proceed in interpreting results produced by RBI tools, to keep the intrusion into people’s rights to the minimum.

RBI technologies, a powerful tool for law enforcement to combat terrorism and other forms of serious crime, which is a legitimate aim under the AI Act, allowed certain fundamental rights to be restricted in some clearly defined cases.

Findings from the fieldwork revealed that the absence of a clear legal framework carries the risk that RBI is used disproportionately and beyond its intended purpose. Some respondents added that RBI tools can be used for not only public security but also national security purposes, which may lead to blurred lines and unauthorised use. The findings also show that law enforcement officers may not always rely on officially approved tools. Interviewees highlighted that the lack of transparency in the use of RBI also leads to concerns over the potential abuse of such systems. This includes a lack of clarity as to which reference databases and watch lists are consulted by the RBI systems or which persons can be included in such databases and watch lists and on what basis. Certain tools with functionalities that can significantly extend the scope of their use inherently contain the risk of ‘function creep’. In some cases, abuse has occurred, as acknowledged by both law enforcement and civil-society respondents.

A separate issue, connected to access to RBI systems, is the interpretation of these systems’ results and their role in investigations. Some law enforcement interviewees emphasised that results from RBI systems only support investigations and are not used for automated decision-making, as they ultimately undergo human review.

FRA’s survey conducted in public places showed that, while most people feel generally comfortable with the use of FRT, there is always a share of respondents who do not feel comfortable at all with it. Differences exist when it comes to live (real-time) and *ex post* use. Importantly, people’s level of acceptance of the use of FRT changes depending on its purpose. Most are concerned that the captured information might be used for purposes other than the officially authorised ones.

The AI Act sets forth several rules that aim to address, at least indirectly, concerns about the potential abuse of RBI for law enforcement purposes. These include the transparency and information sharing requirements that apply to system providers vis-à-vis deployers (Article 13) and the obligation of deployers to ensure that staff overseeing the system have the necessary competence, training and authority (Article 26(2)). The AI Act also requires deployers of such AI-powered systems to conduct a FRIA, which can help to identify, prevent and address potential abuse. Such an assessment, which may rely on assessments previously conducted by the provider, needs to be conducted prior to the deployment

of the system and then updated if any of the assessment's elements change or are no longer up to date during the deployment of the system (Article 27). FRA's **2025 report *Assessing High-risk Artificial Intelligence: Fundamental rights risks*** further underlined the importance of FRIAs.

FRA OPINION 8

When Member States' law enforcement agencies conduct *ex ante* and *ex post* FRIAs of RBI systems, they should evaluate the fundamental rights affected in a comprehensive manner, which serves to mitigate the risk of abuse. As set out in FRA's 2025 report *Assessing High-risk Artificial Intelligence: Fundamental rights risks* (**FRA opinion 4** and **Section 2.3**) and 2019 focus paper '**Facial recognition technology: fundamental rights considerations in the context of law enforcement**' (Section 7), these include, but are not limited to, the right to human dignity, the right to privacy and the protection of personal data, non-discrimination, the freedoms of expression and assembly, the rights of the child and the elderly, the right to good administration and the right to an effective judicial remedy.

To enable national law enforcement authorities to carry out thorough FRIAs, they need to obtain all necessary information from the providers that is required under the AI Act. This information is needed to assess the technology's impact on fundamental rights both when used in line with its intended purpose and under conditions of reasonably foreseeable misuse. Trade secrets and confidentiality requirements should not hinder such efforts.

FRA OPINION 9

Member States should not use real-time or *ex post* RBI to identify participants in peaceful demonstrations or political gatherings. Such a strict ban is essential to avoid normalising general and indiscriminate surveillance and to prevent chilling effects on the exercise of a number of fundamental rights, such as the freedoms of assembly, expression and association (as identified in recital 32 to the AI Act).

If, in the aftermath of such events, *ex post* RBI needs to be used on available recordings for the purposes of criminal investigations, such use should be permitted only on the same grounds as those on which the use of real-time RBI is exceptionally permitted (Article 5(1)(h)(i)–(iii) of the AI Act) and should have no repercussions for participants solely on the basis of their peaceful participation in an event. Such use should also comply with EU fundamental rights law, including the Charter, applicable EU data protection legislation and Article 26(10) of the AI Act.

FRA OPINION 10

To take people's fear of surveillance seriously, Member States should ensure that data collection practices that do not use RBI, such as the visible use in highly frequented publicly accessible spaces of CCTV cameras that do not have RBI functionality, are subject to a thorough data protection impact assessment that also takes their potential chilling effect into account.

The potential societal impact of RBI misuse is significant. A key concern arising from the fieldwork is that deploying RBI technologies in public spaces amounts to general and indiscriminate surveillance. A similar concern expressed is linked to its 'chilling effect': it dissuades individuals from exercising their rights and modifies people's behaviour in public. In a different but related context, the Court of Justice of the European Union also expressed similar concerns about surveillance by means of retaining telecommunications data and its impact on the freedom of expression (Joined Cases C-203/15 and C-698/15, *Telez Sverige*). Many respondents in the fieldwork underscored that public anonymity is a precondition for the enjoyment of rights in publicly accessible spaces. Civil-society respondents and oversight bodies warned that using RBI during demonstrations leads to a significant risk of it being abused against political opponents or people expressing critical views of government and also expressed concerns about the potential disproportionate impact on certain communities.

The findings from the quantitative survey confirm this. They clearly show that the use of RBI tools has a negative impact on people's decisions to attend public events or protests, with 29 % of respondents indicating that the use of such technologies by the police would negatively affect their decision to attend public events or protests. Most notably, people who consider themselves to belong to ethnic minorities in the Member State where they were interviewed say they would attend public events or protests less often.

Articles 11 and 12 of the Charter guarantee everyone the freedoms of expression and peaceful assembly. Recital 32 to the AI Act acknowledges the chilling effect of the use of real-time RBI systems, which may 'evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights'. Recital 95 also stresses that the use of *ex post* RBI systems for law enforcement purposes should not lead to indiscriminate general surveillance. More specifically, Article 5(1)(h) of the AI Act sets out clear purpose limitations: real-time RBI systems can only be used for law enforcement purposes in publicly accessible spaces when it is strictly necessary for the targeted search for victims of certain offences or missing persons; to prevent specific, substantial and imminent threats to life or physical safety or terrorist attacks; or to localise or identify a person suspected of having committed a serious criminal offence.

Ensuring effective external oversight and access to effective remedies

Given that interferences with fundamental rights are not easy to predict due to constantly developing technology, close monitoring of RBI tools by independent oversight bodies is essential. Oversight mechanisms help ensure that RBI tools used for law enforcement purposes have a basis in law, are strictly necessary to achieve well-circumscribed legitimate aims and are not excessive in relation to the objective pursued. Existing oversight mechanisms under EU and national law continue to apply to the development and use of RBI systems. As the fieldwork showed, some internal oversight structures are in place, such as disciplinary bodies with monitoring power or an internal committee reviewing each report made on the use of RBI tools. Most of the interviewees underscored that human resources are limited, which impacts oversight. Some data protection authorities and civil-society organisations that were interviewed described limitations in providing consistent external oversight, as dedicated oversight bodies are often constrained in resources and technical and legal expertise and by their mandate. External oversight bodies stressed that (data protection) impact assessments would be necessary to ensure accountability and that internal regulations should exist within both law enforcement agencies and external oversight bodies.

The AI Act reinforces the oversight of RBI systems: it enables data protection authorities to act as market surveillance authorities for RBI systems used for law enforcement purposes (Article 74(8)). At the same time, Article 77 empowers national authorities protecting fundamental rights to access documentation and, where this is insufficient, ask market surveillance authorities to organise the testing of RBI systems. FRA's 2025 report *Assessing High-risk Artificial Intelligence: Fundamental rights risks* provides evidence that the self-assessments required under the AI Act need to be complemented by the effective oversight of such systems by independent bodies that are sufficiently resourced and possess the necessary fundamental rights expertise.

Article 47 of the Charter and Articles 6 and 13 of the European Convention on Human Rights (ECHR) guarantee the right to an effective remedy and to a fair trial. This right covers all types of procedures, together with the requirement that the remedy sought for must be before a judge. Access to an effective judicial remedy must also cover decisions made with the support of RBI technologies used for law enforcement purposes. In line with relevant case-law under Article 47 of the Charter and Article 13 of the ECHR, the remedy must be 'effective in practice as well as in law' (*). Fieldwork respondents raised concerns that, while necessary legal avenues are in place, this right is not effectively guaranteed in practice and it is often hard to mobilise non-judicial avenues for



FRA OPINION 11

Member States should maintain effective accountability systems by earmarking additional resources for oversight bodies to enable them to upskill and diversify their staff. Oversight bodies should also be equipped with sufficient powers and expertise to prevent and assess fundamental rights violations and effectively support those whose fundamental rights are affected by RBI tools used for law enforcement purposes.

Facilitating cooperation between appropriate oversight bodies at the national and European levels can also help them share expertise and experience, as well as the burden of scrutiny. When implementing actions to facilitate cooperation between oversight bodies at the national level, Member States should consider mobilising available EU funds.

FRA OPINION 12

Effective judicial remedies must be available in case the use of RBI systems creates fundamental rights violations. To ensure that remedies are available in practice, Member States – in particular their law enforcement authorities using RBI systems – should provide those seeking redress with the opportunity to request clear and meaningful explanations about the role of such AI-driven tools in their case, including appropriate information about their functioning. This obligation would help achieve equality of arms if affected individuals seek justice for alleged wrongdoings by RBI-supported decisions. It would also support the effectiveness of the fundamental rights oversight of RBI systems used for law enforcement purposes.

submitting complaints about the alleged unlawful use or the outcome of the use of RBI tools for law enforcement purposes to data protection authorities or ombudspersons. The very low number of initiated cases for redress can be attributed to several reasons. One is that the use of RBI systems for law enforcement purposes is not widespread yet. Some respondents pointed out the lack of transparency to the public, including potential complainants, as another reason. In some Member States covered, the fieldwork revealed that the ombudsperson had not received any complaints – possibly due to a lack of information, the need to first go through the police complaint mechanism, and uses of RBI not yet being widespread or well known about.

Individuals impacted by the use of RBI systems continue to have all their rights under the LED, including their rights to information (albeit limited) on, access to, the rectification of or the erasure of their personal data. On top of this, the AI Act introduces the right to obtain a clear and meaningful explanation from deployers about the role of AI in making individual decisions (Article 86). The right applies with some exceptions; notably, it does not apply where other EU or national law provides for an exception from the right or restricts it (Article 86(2) and (3) of the AI Act). At the same time, the AI Act offers only limited possibilities for filing a complaint (Article 85). The right to an explanation can, therefore, be used as a basis for exercising remedies afforded under other applicable law, such as data protection legislation.

Introduction

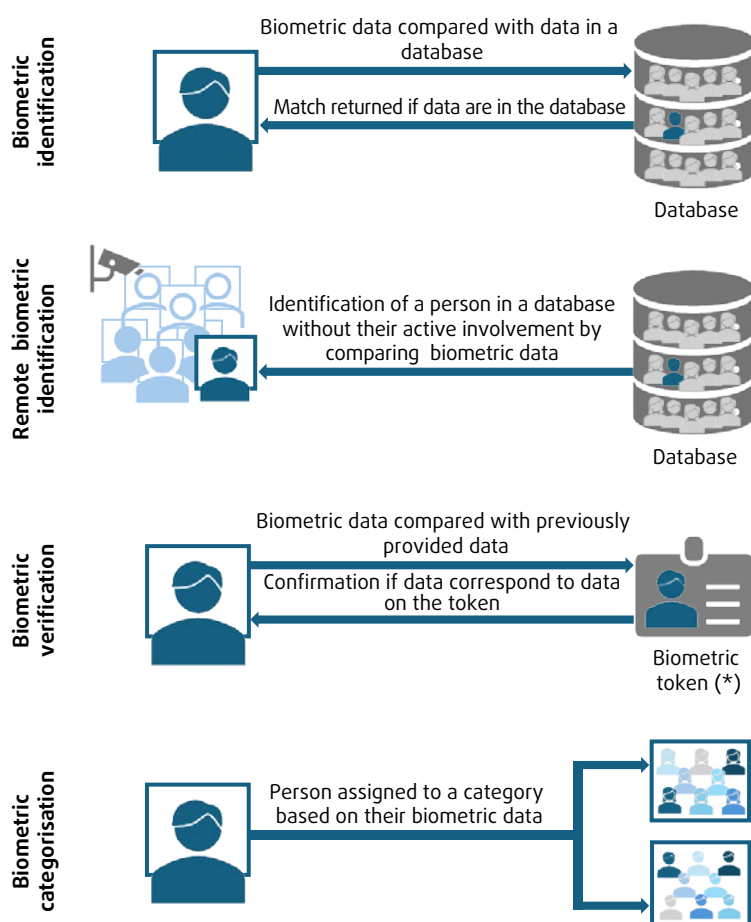
Law enforcement agencies are constantly seeking new technologies to improve the successful prevention, detection and investigation of serious crime to keep people safe ⁽²⁾. In the past few years, technological developments, including AI, have led to considerable advancements in biometric technologies ⁽³⁾. Today, a single camera scan can identify, from a distance, one human face among millions in seconds, a capability already tested in crowded public spaces across Europe and shown in (pilot) deployments to reach accuracy rates once reserved for forensic laboratories. All of this is capable of transforming remote biometric identification (RBI) into a law enforcement tool of unprecedented reach, and one that calls for finding the right balance between security and protecting fundamental rights.

RBI refers to technologies that are used to detect people at a distance, without their active involvement. Such technology is powered by AI and matches people against databases of individuals. It is most often based on people's faces, which are extracted from pictures or video material and then compared against databases of 'wanted' people (using facial recognition technology (FRT)). Other types of biometric data can be used for identification too. More information on how RBI systems work – including the facial recognition and voice recognition systems covered in this report – is available in **Annex I** to this report and **Figure 1**.

RBI technologies are increasingly being used in the public sector, including by law enforcement authorities. Accuracy of RBI has rapidly increased with the development of the technology. While it provides opportunities to enhance public security, protect people from crime and find victims of crime or missing people, it also brings various challenges to the protection of fundamental rights in the European Union (EU) and beyond. These fundamental rights challenges mostly stem from such technologies' increased capabilities to surveil, control and detect people, but also from their potential errors.

The growing attention paid to AI-driven RBI technologies used by law enforcement agencies, which is in part due to their express regulation in the AI Act (Regulation (EU) 2024/1689) ⁽⁴⁾, has not yet been matched by a body of evidence in the public domain – from socio-legal research, fieldwork evidence and accompanying scientific research – about how such technology can affect fundamental rights positively or negatively. Despite persistent concerns from and various initiatives by civil-society organisations ⁽⁵⁾, sporadic legal challenges ⁽⁶⁾ and actions before national data protection authorities against the use of FRTs ⁽⁷⁾, still relatively little is known about the fundamental rights risks (and opportunities) stemming from the use of RBI systems more widely. Only concrete, practical examples allow for a thorough examination of how deploying RBI technologies for law enforcement purposes interferes with various fundamental rights – and whether such interferences can be justified under EU fundamental rights law, including the Charter of Fundamental Rights of the European Union (the Charter) and the case-law of the Court of Justice of the European Union (CJEU).

FIGURE 1 ILLUSTRATION OF BIOMETRIC IDENTIFICATION, REMOTE BIOMETRIC IDENTIFICATION, BIOMETRIC VERIFICATION AND BIOMETRIC CATEGORISATION



(*) In the context of the AI Act, the European Commission has stated that biometric verification 'consists of comparing data presented at a sensor with another set of previously recorded data stored on a device, such as a smartphone, a passport, or an ID card'. Communication from the Commission – **Commission guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)**, C(2025) 5052 final of 29 July 2025, para. 303.

Sources: Based on Article 3(35)–(36), (40) and (41) of the AI Act; and FRA, *Facial Recognition Technology: Fundamental rights considerations in the context of law enforcement*, Publications Office of the European Union, Luxembourg, 2019, pp. 7–8.

This report examines the use of RBI systems for law enforcement purposes based on field research carried out in France, Germany, Greece, Hungary and the Netherlands, together with the planned use of RBI in Ireland and the partially discontinued use of RBI by law enforcement agencies in Italy. In addition, at the time of writing this report, a number of EU Member States were considering making legislative changes to provide a legal basis for RBI use ⁽⁸⁾.

This report also more specifically follows up on FRA's 2019 focus paper *Facial Recognition Technology: Fundamental rights considerations in the context of law enforcement*. That paper provides an overview of what FRT is and how law enforcement authorities (plan to) use it, and points to several fundamental rights risks related to the use of live FRT. This report also builds

on other FRA research on the fundamental rights impact of using AI in a number of areas of life (9).

The current report is grounded in a considerable body of evidence gathered from fieldwork (see [Annex II](#)). It sheds light on the practical applications of RBI technologies used for law enforcement purposes, including in ‘publicly accessible spaces’ (meaning ‘any physical space that is accessible to an undetermined number of natural persons, and irrespective of whether the space in question is privately or publicly owned’ (recital 19 to the AI Act)). It assesses the implications for fundamental rights, while also highlighting the key challenges to people’s rights. It thus fills a gap in the knowledge about the fundamental rights risks and opportunities that the use of such AI-powered technologies can entail.

This report covers use cases on RBI systems for law enforcement purposes in seven Member States: France, Germany, Greece, Hungary, Ireland, Italy and the Netherlands.

The methodology used consists of a combination of desk research and different forms of fieldwork, including 50 semi-structured qualitative interviews with law enforcement authorities, technology providers, national data protection authorities, ombuds institutions and other regulators, and representatives of academia and civil-society organisations. In addition, non-participant observations of three police operations in which AI-driven RBI tools were being tested or deployed were carried out, with the explicit agreement of the police. The findings from the interviews and non-participant observations included in this report do not refer to specific Member State authorities, to guarantee the anonymity of the respondents.

This research was complemented by a quantitative survey with members of the public in five selected Member States (France, Germany, Greece, Hungary and Ireland). In total, 1 054 members of the public who were using public places were interviewed about uses of RBI. The survey interviews were carried out in at least three locations in each Member State, including public places (e.g. squares) and places around sports stadiums and near public transport. In Germany, only two locations were covered. In France, the survey was carried out in two waves: one during the Olympics in July 2024 and the second later in autumn 2024 after the Paris Olympics. In this way different target groups and contexts were captured. The survey results are not representative of the general public in the Member States covered and cannot necessarily be generalised to the general public. They capture the views of people interviewed in these places during certain periods using a short questionnaire.

Given the challenges faced in recruiting representatives from the police and from technology providers of RBI tools to take part in fieldwork interviews, the findings do not claim to represent all RBI development and deployment across the Member States covered, let alone the EU. However, given the scarcity of fieldwork research in this area, the findings do provide valuable evidence to inform the roll-out and application of the AI Act in practice, especially its provisions on the use of RBI systems for law enforcement purposes, with respect to fundamental rights obligations in law.

Table 2 summarises the seven case studies covered in this report.

TABLE 2 CASE STUDIES COVERED IN THE REPORT

Member State	System	Purpose and description
France	FaceVACS-DBScan LE (provided by Cognitec) ⁽¹⁰⁾	Photo-matching system used by the French police and gendarmerie to compare facial images with images in the register of the judicial police, called the <i>Traitement d'antécédents judiciaires (TAJ)</i> ⁽¹¹⁾ . This database contains information about the perpetrators of, accomplices to and victims of criminal offences such as disturbing public security or peace and harming persons, property or state security (i.e. fifth-class contraventions), and suspects in cases involving death, serious injury or missing persons. It is used in judicial, administrative and intelligence investigations.
Germany	Vocalise (provided by Oxford Wave Research) ⁽¹²⁾	Automatic forensic speaker recognition software used by Germany's Federal Criminal Police Office and in several state criminal police offices ⁽¹³⁾ . It analyses and compares speech samples using various voice features, and provides likelihood scores to assess whether voices match. The system is flexible, allowing users to input their own data and customise its set-up ⁽¹⁴⁾ . It may be categorised as a form of biometric verification.
	Polizeiliche Sprecheridentifizierung (provided by Phonexia and Nuance)	A combined speaker identification suite that automates the extraction and comparison of voiceprints. The system includes Phonexia Voice Inspector ⁽¹⁵⁾ and Nuance Forensics ⁽¹⁶⁾ , voice identification tools for forensic experts. This combined system is used by some state criminal police offices to process large volumes of intercepted or recorded audio for investigative purposes ⁽¹⁷⁾ .
Greece	Smart policing system ⁽¹⁸⁾ (Facial recognition technology and fingerprint identification technology provided by Intracom Telecom ⁽¹⁹⁾)	Mobile identification system for screenings during police stops acquired by the Hellenic Police ⁽²⁰⁾ but not yet operational. Using mobile devices, police officers will be able to capture and analyse biometric data (i.e. faces and fingerprints), which can be compared with law enforcement and border control databases (e.g. the second generation Schengen information system, the European Asylum Dactyloscopy Database). The system was designed to streamline identity checks ⁽²¹⁾ . The system accepts remotely taken photos for editing, forensic enhancement and watch list searches, opening the door to RBI ⁽²²⁾ .
Hungary	Facial recognition technology (operated by the Hungarian Institute for Forensic Sciences ⁽²³⁾)	System used by Hungarian law enforcement and forensic experts to identify individuals from image-based evidence, such as CCTV footage, police photos or ID documents. The system matches faces against national databases of ID documents and mugshots, providing identification to support police procedures and investigations ⁽²⁴⁾ .
Italy	Sistema Automatico di Riconoscimento Immagini (SARI) (provided by Reco 3.26) ⁽²⁵⁾	SARI enterprise is a post-event facial recognition system used by the Italian police ⁽²⁶⁾ to identify suspects by comparing still images (e.g. from CCTV footage) against a mugshot database. It has been used in investigations involving theft, burglary and similar offences. The Italian Data Protection Authority has classified it as a tool that automates operations carried out on biometric data that are already conducted manually by police officials on the same database ⁽²⁷⁾ .
		SARI real time is a real-time facial recognition system designed to scan live video feeds in public spaces and match faces against watch lists. It has never been deployed, due to an intervention by the Italian Data Protection Authority in April 2021, which deemed its real-time use to be unlawful mass surveillance and lacking a legal basis ⁽²⁸⁾ .
Netherlands	Centrale Automatische Technologie voor Herkenning (CATCH) (provided by Idemia) ⁽²⁹⁾	Facial recognition tool used by the Dutch police to compare photos from crime scenes, such as those obtained from CCTV and bodycams, against two databases: CATCH- <i>strafrecht</i> , which consists of facial images of suspects and convicts ⁽³⁰⁾ , and CATCH- <i>vreemdelingen</i> , which contains facial images of non-EU nationals who have applied for asylum or a visa ⁽³¹⁾ .

The findings presented in this report add value by supporting a fundamental-rights-based approach to the use of RBI and are particularly timely in light of the implementation of the AI Act.

In terms of structure, **Chapter 1** discusses the legal framework applicable to RBI systems in the EU, covering both the general fundamental rights law framework in the EU and more specific and relevant EU legislation, namely the AI Act and the EU data protection *acquis*. **Chapter 2** describes various fundamental rights challenges stemming from the use of RBI for law enforcement purposes, which are informed by all strands of the fieldwork, and links them to the various fundamental rights affected. The concluding chapter (**Conclusions**) reflects on the fieldwork findings, the key safeguards for mitigating fundamental rights risks and future steps needed for hardwiring fundamental rights into the use of RBI for law enforcement purposes.



Endnotes

- (¹) European Court of Human Rights (ECtHR), *El-Masri v. 'the former Yugoslav Republic of Macedonia'*, No 39630/09, 13 December 2012, § 255; *Kudła v. Poland*, No 30210/96, 26 October 2000, § 152.
- (²) See Almeida, D., Shmarko, K. and Lomas, E., 'The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: A comparative analysis of US, EU, and UK regulatory frameworks', *AI Ethics*, Vol. 2, 2022, pp. 377–387; Hälterlein, J., 'Facial recognition in law enforcement', in: Borch, C. and Pardo-Guerra, J. P., *The Oxford handbook of the sociology of machine learning*, Oxford University Press, Oxford, 2023, pp. 343–360.
- (³) In the context of facial recognition, see, for example, National Institute of Standards and Technology (NIST), 'Face Recognition Technology Evaluation (FRTE) 1:N Identification', NIST website, 12 May 2026; and NIST, *Ongoing Face Recognition Vendor Test (FRVT) – Part 2: Identification*, Gaithersburg, MD, 2018.
- (⁴) **Regulation (EU) 2024/1689** of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>). It is to be noted that in November 2025 the European Commission brought forward the proposal for a digital omnibus on AI (**COM(2025) 836 final**), which is a legislative package designed to simplify and streamline certain provisions of the AI Act by reducing regulatory burdens, aligning overlapping rules and improving its practical implementation to support innovation and competitiveness. Negotiations were still ongoing at the time of writing.
- (⁵) See, for example, European Digital Rights (EDRI) 'Global civil society and experts statement: Stop facial recognition surveillance now', EDRI website, 26 September 2023; EDRI, Access Now, ARTICLE19, Bits of Freedom, Chaos Computer Club, et al., 'Joint civil society recommendations for an EU Artificial Intelligence Act for fundamental rights – Biometrics Part 1: Article 3(36) and Article 5(1)(d) – Prohibit all remote biometric identification (RBI) in publicly accessible spaces'; and Amnesty International, 'EU's AI Act fails to set gold standard for human rights', Amnesty International website, 3 April 2024. See also AlgorithmWatch, '50.000+! Petition gegen biometrische Überwachung an Bundestag übergeben', AlgorithmWatch website, 10 September 2025; and, for more outside Europe, Wakabi, W. and Roberts, T., *Smart City Surveillance in Africa: Mapping Chinese AI surveillance across 11 countries*, Institute of Development Studies, Brighton and Hove, 2026.
- (⁶) See, notably, in the United Kingdom: England and Wales High Court (EWHC), *R (Bridges) v. Chief Constable of South Wales Police and Secretary of State for the Home Department*, [2019] EWHC 2341 and *R (Bridges) v. Chief Constable of South Wales Police and Secretary of State for the Home Department*, [2020] EWCA Civ 1058. For an overview, see Big Brother Watch Team, 'Landmark legal challenges launched against facial recognition after policy and retailer misidentifications', Big Brother Watch website, 24 May 2024.
- (⁷) See, for example, Autoriteit Persoonsgegevens, 'Gezichtscherkenning: Antwoord op vragen over verwerkingen van persoonsgegevens bij de inzet van gezichtscherkenning', 2024; Garante per la protezione dei dati personali, 'Riconoscimento facciale: Sari real time non è conforme alla normativa sulla privacy', Garante per la protezione dei dati personali website, 16 April 2021; and Agencia Española Protección Datos, 'Resolución de terminación del procedimiento por pago voluntario', Procedimiento No PS/00120/2021, 2021.
- (⁸) Art. 5(5) of the AI Act requires a clear national legal basis for exceptional uses of real-time RBI systems. See, for example, in Sweden, Regeringskansliet: Justitiedepartementet, *Polisens användning av AI för ansiktsgenkänning i realtid*, Stockholm, 2025.
- (⁹) FRA, *#BigData – Discrimination in data-supported decision making*, Publications Office of the European Union, Luxembourg, 2018; FRA, *Data Quality and Artificial Intelligence – Mitigating bias and error to protect fundamental rights*, Publications Office of the European Union, Luxembourg, 2019; FRA, *Getting the Future Right – Artificial intelligence and fundamental rights*, Publications Office of the European Union, Luxembourg, 2020; FRA, *Bias in Algorithms – Artificial intelligence and discrimination*, Publications Office of the European Union, Luxembourg, 2022; FRA, *Digitalising Justice: A fundamental rights-based approach*, Publications Office of the European Union, Luxembourg, 2025; and FRA, *Assessing High-risk Artificial Intelligence: Fundamental rights risks*, Publications Office of the European Union, Luxembourg, 2025.
- (¹⁰) Cognitec Systems GmbH, 'FaceVACS-DBScan LE', Cognitec website, no date.
- (¹¹) Direction de l'information légale et administrative, 'Criminal history processing (Taj)', Service Public website, 30 January 2026.
- (¹²) Oxford Wave Research, 'VOCALISE – Automatic speaker recognition software', Oxford Wave Research website, no date.
- (¹³) Jessen, M., Forth, O. and Alexander, A., 'Vocalise: eine gemeinsame Plattform für die Anwendung automatischer und semiautomatischer Methoden in forensischen Stimmenvergleichen', *Polizei & Wissenschaft*, Issue 4, April 2013.
- (¹⁴) Alexander, A., Forth, O., Aryal Atreya, A. and Kelly, F., 'VOCALISE: A forensic automatic speaker recognition system supporting spectral, phonetic, and user-provided features', paper presented at Odyssey 2016: The Speaker and Language Workshop, Bilbao, Spain, 21–24 June 2016.
- (¹⁵) Phonexia, 'Phonexia Voice Inspector', Phonexia website, no date.
- (¹⁶) See, for example, Vrankulj, A., 'Nuance launches Nuance Forensics for law enforcement investigations', BiometricUpdate.com website, 18 March 2014.
- (¹⁷) Landtag Nordrhein-Westfalen, *Antwort der Landesregierung auf die Kleine Anfrage 1964 – Einsatz von Spracherkennungssoftware bei der Polizei*, Drucksache 18/1964, 2023.
- (¹⁸) Hellenic Police (Ελληνική Αστυνομία), 'Προμήθεια Συστημάτων για έξυπνη Αστυνόμευση – Smart Policing', 12 April 2018.
- (¹⁹) Intracom Telecom, 'Intracom Telecom undertakes a "smart policing" project', Intracom Telecom website, 2 July 2019.
- (²⁰) Internal Security Fund (Ταμείο Εσωτερικής Ασφάλειας), 'Σύμβαση που αφορά στην προμήθεια Συστημάτων για Έξυπνη Αστυνόμευση Σύμβαση που αφορά στην προμήθεια Συστημάτων για Έξυπνη Αστυνόμευση (Smart Policing)', 14 December 2019.
- (²¹) Hellenic Police (Ελληνική Αστυνομία), 'Προκήρυξη για την προμήθεια τεχνικού εξοπλισμού', 12 April 2018.
- (²²) Hellenic Police (Ελληνική Αστυνομία), 'Προκήρυξη για την προμήθεια τεχνικού εξοπλισμού', 12 April 2018.
- (²³) Gárdonyi, G., 'Az állóképes arcképezonosítás Magyarországon' [Still image face recognition in Hungary], *Belügyi Szemle*, Vol. 69, No 7, 2021, pp. 1133–1148.
- (²⁴) Gárdonyi, G., 'Az állóképes arcképezonosítás Magyarországon' [Still image face recognition in Hungary], *Belügyi Szemle*, Vol. 69, No 7, 2021, pp. 1133–1148.
- (²⁵) Reco 3.26, 'Public security for the Ministry of the Interior and the state police', Reco 3.26 website, no date.
- (²⁶) Ministero dell'Interno (Ministry of the Interior), *Decreto di aggiudicazione – Parsec 3.26 Lotto 1 SARI 2*, No 623, 8 August 2017.
- (²⁷) Giannini, A., 'Law enforcement and facial recognition technologies in Italy – An activist's update', Digital Freedom Fund, 3 October 2024.
- (²⁸) Garante per la protezione dei dati personali, 'Riconoscimento facciale: Sari real time non è conforme alla normativa sulla privacy', Garante per la protezione dei dati personali website, 16 April 2021; Garante per la protezione dei dati personali, 'Parere sul sistema Sari Real Time – 25 marzo 2021 [9575877]', Garante per la protezione dei dati personali website, 25 March 2021.
- (²⁹) Tweede Kamer der Staten-Generaal, 'Antwoord op vragen van het lid Verhoeven over het bericht "Gezichtendatabase van politie bevat

foto's van 1,3 miljoen mensen", Kamerstuk 2019Z15387, 11 September 2019; Politie Nederland, **Centrale Automatische Technologie voor Herkenning (CATCH) – Jaarcijfers 2023**, The Hague, 2024.

(³⁰) Politie Nederland, **'CATCH (Centrale Automatische Technologie voor Herkenning van personen)'**, Het Algoritmeregister website, last modified 17 November 2025.

(³¹) Politie Nederland (2021), *Centrale Automatische Technologie voor Herkenning (CATCH) – Jaarcijfers 2020*; Telefi project, **'Summary report of the project "Towards the European level exchange of facial images"'**, Version 1.0, 2021, pp. 26 and 108.

1

LEGAL FRAMEWORK APPLICABLE TO REMOTE BIOMETRIC IDENTIFICATION SYSTEMS USED FOR LAW ENFORCEMENT PURPOSES

The use of AI-driven remote biometric identification technologies for law enforcement purposes – as briefly presented in [Annex I](#) to this report – can affect multiple fundamental rights protected by EU law (see [Chapter 2](#)). Full compliance with the applicable rules, notably the relevant fundamental rights standards and safeguards, is a prerequisite for the use of RBI technologies by national law enforcement agencies in the EU.

This chapter introduces the general legal framework applicable in the EU, including fundamental rights law (see '[Legal corner: fundamental rights framework governing the use of RBI systems by law enforcement](#)'). This multilayered framework encompasses EU law, notably the Charter and selected secondary EU legislation such as the AI Act and EU data protection law; Council of Europe (CoE) standards; and international law ⁽³²⁾. These legal sources provide the normative basis and benchmarks for the lawful development and deployment of RBI tools. The chapter also helps determine, as a point of departure, whether or not a specific use of RBI by law enforcement is in compliance with applicable fundamental rights standards and safeguards, and what kind of measures are needed to mitigate the risk of fundamental rights violations, as provided for by applicable pieces of legislation in the EU.

Legal corner

Fundamental rights framework governing the use of RBI systems by law enforcement

The key sources of fundamental rights protection under **EU and international law** that are applicable to the use of AI-powered RBI systems in general, and to those used for law enforcement purposes in particular, are listed below.

- **Charter of Fundamental Rights of the European Union.** The Charter enshrines a wide array of fundamental rights and principles and has the same legal value as the EU treaties (Article 6(1) of the Treaty on European Union (TEU)). All EU institutions, bodies and agencies are bound by the Charter in the course of all of their actions, as are Member States when they act within the scope of EU law (Article 51(1) of the Charter) ^(a). Many Charter rights correspond to those set out in the ECHR ^(b). The meaning and scope of these rights must be the same as corresponding rights in the ECHR (Article 52(3) of the Charter), as interpreted by the European Court of Human Rights (ECtHR). Yet this required convergence cannot prevent EU law from providing more extensive protection.
- **EU treaties.** Provisions on fundamental rights protection are included in the preamble of the TEU, Article 3(3) (which covers non-discrimination, equality between men and women and the rights of the child) and Article 6(3) (which covers the sources of fundamental rights in the EU legal order) of the TEU and Title V ('Area of freedom, security and justice') of the Treaty on the Functioning of the European Union.
- **EU data protection legislation.** Central pieces of secondary EU legislation governing the protection of personal data and the use of AI, including RBI, are outlined in **Section 1.1** below.
- **European non-discrimination law.** Article 2 of the TEU stipulates that non-discrimination is one of the fundamental values of the EU, and Article 10 of the Treaty on the Functioning of the European Union requires the EU to combat discrimination on a number of grounds. Articles 20 and 21 of the Charter guarantee everyone's equality before the law and prohibit discrimination on a wide range of grounds. Several EU non-discrimination directives enshrine more specific and detailed rights. They have varying scopes of application ^(c). These include the Racial Equality Directive (Directive 2000/43/EC) ^(d), the Employment Equality Directive (Directive 2000/78/EC) ^(e), the Gender Goods and Services Directive (Directive 2004/113/EC) ^(f) and the recast Gender Equality Directive (Directive 2006/54/EC) ^(g).
- **European Convention on Human Rights** ^(h). All Member States have ratified the ECHR, and its additional protocols are also binding on the great majority of Member States ⁽ⁱ⁾.
- **Other CoE instruments.** These include the modernised Convention 108+ ^(j), which provides rules on protecting individuals with regard to the automatic processing of their personal data ^(k) and the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (which has not yet entered into force at the time of writing) ^(l).
- **Several further international human rights law instruments that are binding on Member States.** These include the 1948 Universal Declaration of Human Rights (reflecting customary international law) ^(m) and other UN human rights conventions of a universal character (e.g. the 1966 International Covenant on Civil and Political Rights) ⁽ⁿ⁾. These UN instruments, together with the ECHR and other CoE instruments, contain legally binding standards and safeguards that Member States must comply with in addition to EU fundamental rights law obligations. They apply also when Member States act in areas that do not fall within the scope of EU competence.

Sources:

- ^(a) See Judgment of the Court of Justice of 26 February 2013, *Åklagaren v Hans Åkerberg Fransson*, C-617/10, ECLI:EU:C:2013:105, paras 17 and 20.
- ^(b) Council of Europe, **Convention for the Protection of Human Rights and Fundamental Freedoms**, European Treaty Series No 5, Rome, 1950.
- ^(c) For an overview of European non-discrimination law, see FRA and CoE, **Handbook on European Non-discrimination Law – 2018 edition**, Publications Office of the EU, Luxembourg, 2018.
- ^(d) **Council Directive 2000/43/EC** of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin (OJ L 180, 19.7.2000, p. 22, ELI: <http://data.europa.eu/eli/dir/2000/43/oj>).
- ^(e) **Council Directive 2000/78/EC** of 27 November 2000 establishing a general framework for equal treatment in employment and occupation (OJ L 303, 2.12.2000, p. 16, ELI: <http://data.europa.eu/eli/dir/2000/78/oj>).
- ^(f) **Council Directive 2004/113/EC** of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services (OJ L 373, 21.12.2004, p. 37, ELI: <http://data.europa.eu/eli/dir/2004/113/oj>).
- ^(g) **Directive 2006/54/EC** of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast) (OJ L 204, 26.7.2006, ELI: <http://data.europa.eu/eli/dir/2006/54/oj>).
- ^(h) Council of Europe, **Convention for the Protection of Human Rights and Fundamental Freedoms**, European Treaty Series No 5, Rome, 1950.
- ⁽ⁱ⁾ For an overview of each Member State's rate of ratification of additional protocols to the ECHR and other CoE conventions, see <http://conventions.coe.int>.
- ^(j) Council of Europe, **Convention 108+ – Convention for the protection of individuals with regard to the processing of personal data**, Council of Europe Treaty Series (CETS) No 108, Strasbourg, 1981, as amended by the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No 223, Elsinore, 2018.
- ^(k) For further information on the modernised Convention 108+ and its interplay with EU law, see FRA and CoE, **Handbook on European Data Protection Law – 2018 edition**, Publications Office of the European Union, Luxembourg, 2018.
- ^(l) Council of Europe, **Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law**, CETS No 225, Vilnius, adopted 17 May 2024, opened for signature 5 September 2024.
- ^(m) See, for example, Chapter 1 of Schabas, W., *The Customary International Law of Human Rights*, Oxford University Press, Oxford, 2021.
- ⁽ⁿ⁾ Other international human rights conventions of a universal character include the 1965 International Convention on the Elimination of All Forms of Racial Discrimination; the 1966 International Covenant on Economic, Social and Cultural Rights; the 1979 Convention on the Elimination of All Forms of Discrimination against Women; the 1984 Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment; the 1989 Convention on the Rights of the Child; the 2006 Convention on the Rights of Persons with Disabilities; and the 2006 International Convention for the Protection of All Persons from Enforced Disappearance. For more on universal human rights law, including the mechanisms for its enforcement, see De Schutter, O., *International Human Rights Law: Cases, materials, commentary*, 3rd edition, Cambridge University Press, Cambridge, 2019.

1.1. EU AI ACT AND THE EU DATA PROTECTION *ACQUIS* – SPECIAL RULES ON WHAT IS BANNED AND WHAT IS PERMITTED

On top of the EU and international fundamental rights law framework, at the EU level the development and use of RBI systems is specifically regulated by the AI Act. The overarching aim of the AI Act is ‘to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of ... fundamental rights’ (Article 1(1)). It prohibits, in principle, the use of ‘real-time’ RBI systems for law enforcement purposes in publicly accessible spaces, with strictly defined exceptions (Article 5(1)(h) and (2)–(7)). The AI Act classifies the development and permitted use of RBI systems (regardless of who the deployer is) as ‘high-risk’. The provision and deployment of such high-risk AI systems need to adhere to a number of obligations, as will be further outlined below. In addition, *ex post* RBI has to be used by law enforcement authorities in a targeted way, with supplementary reporting requirements applying to its use ⁽³³⁾.

The AI Act complements other applicable EU – and national – law governing the use of RBI systems, such as EU fundamental rights law (see ‘**Legal corner: fundamental rights framework governing the use of RBI systems by law enforcement**’) and the EU data protection *acquis* (see **Section 1.1.2**) ⁽³⁴⁾. The AI Act also does not affect prohibitions that apply under other pieces of EU law. This means that, even if an AI tool or practice is not prohibited under the AI Act, it may be still not permitted under other applicable pieces of EU law ⁽³⁵⁾. This is also relevant for RBI systems used outside the law enforcement context, where it is questionable how such use could comply with the stringent requirements for the processing of special categories of personal data, such as biometric data, established under Article 9 of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) ⁽³⁶⁾, and, more broadly, how such use could meet the requirements of necessity and proportionality.



1.1.1. EU AI Act

The EU AI Act includes three sets of rules pertaining to the development and/or use of RBI systems for law enforcement purposes.

First, the AI Act prohibits, as part of Chapter II ('Prohibited AI practices'), the use of real-time RBI systems in publicly accessible spaces ⁽³⁷⁾ for law enforcement purposes unless it is strictly necessary for specified objectives and has been authorised (Article 5(1)(h)). Real-time RBI systems, in which the capturing, comparison and identification of biometric data all occur without a significant delay ⁽³⁸⁾, can only be used by law enforcement authorities in publicly accessible spaces if authorised by national law ⁽³⁹⁾ for one or more of the following situations:

- the targeted search for missing persons and specific victims of abduction, trafficking and the sexual exploitation of human beings;
- the prevention of a specific, substantial and imminent threat to the life or physical safety of persons or of a genuine and present/foreseeable threat of a terrorist attack;
- the localisation/identification of a suspect/perpetrator involved in one of the serious crimes listed in Annex II to the AI Act, which need to be punishable in the Member State concerned by a custodial sentence / detention order with a maximum period of at least four years ⁽⁴⁰⁾.

Second, the AI Act classifies the development of RBI systems that are permitted under relevant EU or national law and their permissible use by deployers (including those other than law enforcement authorities) as 'high-risk'. This means that such systems are permitted, subject to compliance with the relevant requirements under Chapter III of the AI Act and other applicable EU and/or national law ⁽⁴¹⁾.

Last, Article 26(10) of the AI Act, which forms part of Chapter III governing the use of high-risk AI systems, sets forth additional requirements for law enforcement authorities' use of *ex post* RBI systems. As with the exceptional use of real-time RBI systems, *ex post* RBI systems can only be used in a targeted manner. There needs to be a clear link to a criminal offence, a criminal proceeding, a genuine and present/foreseeable threat of a criminal offence or a search for a specific missing person ⁽⁴²⁾. However, as the European Data Protection Supervisor (EDPS) observed, the safeguards for such *ex post* uses of RBI are slightly lower than those for real-time RBI use, despite the serious interferences with fundamental rights occurring in both scenarios ⁽⁴³⁾.

The requirements for providers and deployers of RBI systems for law enforcement purposes are outlined in **Table 3**. In February 2025, the European Commission published guidelines that help to further clarify the prohibited uses of real-time RBI systems and the exceptions allowed for in the AI Act ⁽⁴⁴⁾.

TABLE 3 KEY REQUIREMENTS FOR THE DEVELOPMENT AND USE OF REMOTE BIOMETRIC IDENTIFICATION SYSTEMS FOR LAW ENFORCEMENT PURPOSES UNDER THE AI ACT

Requirements for all RBI systems	Providers - Compliance with requirements under Article 16 of the AI Act, including having in place a risk management system that considers risks to fundamental rights (Article 9) and a quality management system (Article 17), maintaining documentation (Article 18) and ensuring that the product undergoes a conformity assessment (Article 43(1)) Deployers - Compliance with requirements under Article 26 of the AI Act, including taking appropriate technical and organisational measures to ensure that such systems are used in line with their instructions for use, assigning human oversight to persons with the necessary competence, training and authority and conducting a fundamental rights impact assessment (Articles 5(2) and 27) – see ‘Legal corner: assessing the fundamental rights impact of high-risk AI systems’
Additional requirements for real-time RBI systems in publicly accessible spaces	Deployers - Use only to confirm the identity of a specifically targeted individual (Article 5(2)) - Consideration of the nature of the situation and the consequences of the system’s use for the rights and freedoms of those concerned (Article 5(2)) - Compliance with further conditions stemming from national law authorising the use of RBI systems, in particular regarding the temporal, geographic and personal scope of their use - Prior authorisation by a judicial authority or an independent administrative authority, after duly considering the necessity and proportionality of the use of RBI (Article 5(3), with some exceptions) - No decision that produces an adverse legal effect on a person based solely on the output of the system (Article 5(3)) - Notification of each use case to the relevant market surveillance authority and the national data protection authority (Article 5(4))
Additional requirements for <i>ex post</i> RBI systems	Deployers - Prior or subsequent authorisation by a judicial authority or an administrative authority of RBI use for the targeted search for a person suspected or convicted of having committed a criminal offence, except when used for initial identification purposes based on objective and verifiable facts directly linked to the offence; each instance of such use compliant with strict necessity requirements (Article 26(10)) - No decision that produces an adverse legal effect on a person based solely on the output of the system (Article 26(10)) - Documentation of each use of an RBI system in the relevant police file, to be made available to the relevant market surveillance authority and the national data protection authority upon request (except sensitive operational data) (Article 26(10)) - Submission of annual (aggregated) reports on the use of these systems to the relevant market surveillance authority and the national data protection authority (except sensitive operational data) (Article 26(10))

Sources: AI Act and Communication from the Commission – [Commission guidelines on prohibited artificial intelligence practices established by Regulation \(EU\) 2024/1689 \(AI Act\)](#), C(2025) 5052 final of 29 July 2025.

Legal corner

Assessing the fundamental rights impact of high-risk artificial intelligence systems

A fundamental rights impact assessment (FRIA) must be conducted when RBI systems are deployed for law enforcement purposes. Article 27 of the AI Act outlines the elements of this assessment, the template for which has been developed by the European AI Office with input from FRA. Deployers have to describe the processes in which the RBI system will be used and the period and frequency of its use. They are also obliged to identify categories of people and groups likely to be affected by the system's use and the specific risks of harm to those people, as well as describe the human oversight and measures to be taken in case these risks materialise.

The assessment will be complementary to the data protection impact assessment required under the EU data protection *acquis*. The deployers of these systems may also rely on FRIAs or other assessments conducted by them previously or assessments done by the providers. The providers' assessments will have to consider the risks that their systems pose to fundamental rights under Article 9 of the AI Act and corresponding standards developed by the European Committee for Standardization and the European Committee for Electrotechnical Standardization.

The provisions of the AI Act governing prohibitions of RBI use have been applicable since 2 February 2025, and the provisions on high-risk AI systems – under which permissible uses of RBI systems also fall – will apply as of 2 December 2027. The European Commission has provided provisional guidance for FRIAs where deployers are applying RBI in cases that are exceptions to the prohibited use of real-time RBI, until guidance under Article 27 of the AI Act becomes available.

FRA's 2025 report ***Assessing High-risk Artificial Intelligence: Fundamental rights risks*** provides further guidance on the FRIA process. It outlines the main elements required for effective assessment, including a description of the system and its purpose, the identification of people and groups likely to be affected and the assessment, prevention and mitigation of any adverse impacts on fundamental rights.

Sources: Articles 9 and 27 of the AI Act; Communication from the Commission – **Commission guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)**, C(2025) 5052 final of 29 July 2025, paras 370–377; FRA (2025), ***Assessing High-risk Artificial Intelligence: Fundamental rights risks***, Publications Office of the European Union, Luxembourg, pp. 56–60; **Commission implementing decision of 22 May 2023 on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence**, C(2023) 3215 final of 22 May 2023.

1.1.2. EU data protection law

EU data protection law accords specific protections to biometric data, as their processing could create significant risks to fundamental rights. Due to the uniqueness, immutability and potential ubiquity of an individual's biometric profile, biometric data are classified as 'special category' data under EU data protection law ⁽⁴⁵⁾.

The EU data protection *acquis* defines biometric data as 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm [their] unique identification' ⁽⁴⁶⁾. Although facial images and voice recordings (and other personal data) can be converted into biometric data through the extraction and coding of their unique features, they do not constitute biometric data unless they are processed for these purposes. The increased availability and accessibility of the software and data storage capacity necessary to undertake such processing have enabled large-scale RBI systems to be developed without the knowledge or consent of the data subjects or the broader public. Relevant personal data, such as the faces of people in images and video material, can be easily extracted from the internet or other sources. This poses acute challenges for the protection of personal data and the enjoyment of other fundamental rights.

RBI systems interfere with the fundamental right to data protection in two core ways:

- in the creation of reference databases or ‘watch lists’ against which additional biometric profiles may be compared,
- in processing additional biometric profiles for this purpose.

Both interferences must respect the ‘essence’ of this fundamental right and be subject to a necessity and proportionality test (see **Section 1.2**).

In their policing activities, national law enforcement agencies operate under the Law Enforcement Directive (Directive 2016/680) (LED) ⁽⁴⁷⁾ with respect to data protection ⁽⁴⁸⁾. This applies in particular to the use of RBI systems, to which LED provisions generally apply in addition to the requirements set out in the AI Act. The only exception is Article 10 of the LED, where, according to recital 38 to the AI Act, the AI Act’s provisions on the prohibition of the use of real-time RBI apply as a *lex specialis*. This means that the use of RBI systems and related processing of biometric data are regulated in an exhaustive manner by the AI Act and authorities cannot use such systems on the grounds contained in Article 10 of the LED. Conversely, when it comes to other than ‘real-time’ RBI system use for law enforcement purposes, the conditions for their processing under Article 10 of the LED apply.

Providers and deployers of both real-time and *ex post* RBI systems for law enforcement purposes therefore need to comply with the requirements set out in the LED, particularly those outlined in **Table 4** ⁽⁴⁹⁾.

TABLE 4 KEY REQUIREMENTS FOR THE DEVELOPMENT AND USE OF REMOTE BIOMETRIC IDENTIFICATION SYSTEMS FOR LAW ENFORCEMENT PURPOSES UNDER THE LAW ENFORCEMENT DIRECTIVE

Requirements for all RBI systems	Controllers (providers and/or deployers)
	• Compliance with principles relating to the processing of personal data: lawful and fair processing; the specification and limitation of the purpose of the data collection; data minimisation; accuracy; storage limitations; integrity and confidentiality; and accountability (Article 4 of the LED) • Prohibition of automated decision-making in individual cases, with the possibility of exemptions based on EU or national law (Article 11 of the LED) • Provision of information (transparency duties) (*), with some exceptions in certain cases and under certain conditions (Article 13 of the LED) • Data protection by design and by default (Article 20 of the LED) • A data protection impact assessment and prior consultation of the supervisory authority (Articles 27 and 28 of the LED) • Upholding data subject rights (Chapters III and VIII of the LED)

(*) Article 13(2)(d) of the LED even creates a duty to notify the data subject after the use of such systems. Similarly, and more concretely, deployers of high-risk AI systems that make decisions or assist in decision-making are obliged to inform the data subjects about the use of a high-risk AI system (Article 26(11) of the AI Act). For more, see De Hert, P., Kanakakis, A. and Sajfert, J., ‘Evidence law, data protection standards and the use of AI for investigation and prosecution’, in: Ligeti, K. and Visco, N. (eds), *AI Evidence and Criminal Proceedings*, Hart Publishing, Oxford, 2025, pp. 85–105.

Sources: European Data Protection Board (EDPB), *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, Version 2.0, 26 April 2023, pp. 26–27.

While the use of RBI systems by law enforcement agencies clearly falls under the LED, unless the *lex specialis* rule mentioned above takes precedence, RBI system providers may also develop systems used in the private sector, or by non-policing public authorities, which are governed by the GDPR and the data protection regulation for EU institutions, bodies, offices and agencies ⁽⁵⁰⁾. Providers may have also constructed and trained their systems using data obtained in non-law enforcement contexts; activities that would again fall under the GDPR. These scenarios may blur the distinction between policing and non-policing activities established by EU data protection law, with important implications for fundamental rights protection when developing and using RBI systems.

1.2. REQUIREMENTS FOR INTERFERENCES WITH FUNDAMENTAL RIGHTS TO BE JUSTIFIED

Full compliance with fundamental rights is a prerequisite for any law enforcement activity, irrespective of the technology used. Most of the fundamental rights affected by RBI technologies used for law enforcement purposes are not absolute but derogable rights ⁽⁵¹⁾ and hence can be subject to limitations in line with the requirements pursuant to Article 52(1) of the Charter.

Analysing to what extent various fundamental rights are impacted by the use of RBI technologies for law enforcement purposes is a complex and multifaceted process. State activities that bring a protected fundamental right into question are called ‘interferences’, and further tests are required to determine whether an interference constitutes a violation of that right ⁽⁵²⁾. This section outlines the steps to be followed and the tests to be applied to determine whether or not a Charter right can be lawfully limited. Interferences with non-absolute, derogable rights can only be justified if they respect the requirements of the Charter and of the ECHR as interpreted by the ECtHR, in the case of Charter rights that correspond to those guaranteed in the ECHR (Article 52(3) of the Charter). Requirements that are specific to an individual right (in particular those relating to interferences with the rights to respect for private life and the protection of personal data) are analysed in **Chapter 2**.

Pursuant to Article 52(1) of the Charter, as also repeatedly reiterated by the CJEU ⁽⁵³⁾, any limitation on fundamental rights must:

- be provided for by law;
- genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others;
- respect the essence of the right;
- be necessary;
- be proportionate.

As one respondent from a data protection authority interviewed during the fieldwork stated, a necessity and proportionality test always has to be conducted (see quote).

The CJEU has underlined that all of the above requirements must be complied with. The court has also emphasised that any limitation on the exercise of the rights and freedoms recognised by the Charter must respect ‘the essence’ of those rights and freedoms ⁽⁵⁴⁾. This means that fundamental rights can be limited to a certain extent but not completely disregarded. Once it has been established that the inalienable, essential core of a right is not violated or emptied of substance by a measure, the next step is to conduct the necessity and proportionality test outlined in Article 52(1) of the Charter in respect of non-core aspects of that right ⁽⁵⁵⁾. An objective of general interest – such as crime prevention, fighting serious crime and maintaining public security – is

We always have the test of proportionality and necessity, which must be examined in this case and in every application of the system, along with the system’s specifications, the legal safeguards, means of redress, etc.

Respondent from a data protection authority

—

not, in itself, sufficient to justify an interference. Any interference with a Charter right needs to be examined as to whether the given legitimate aim could not be obtained by other means that interfere less with the right ⁽⁵⁶⁾. If this test reveals that it is not possible to use 'other means' and the case meets the five conditions outlined above, then there may be grounds for the legitimate use of RBI.

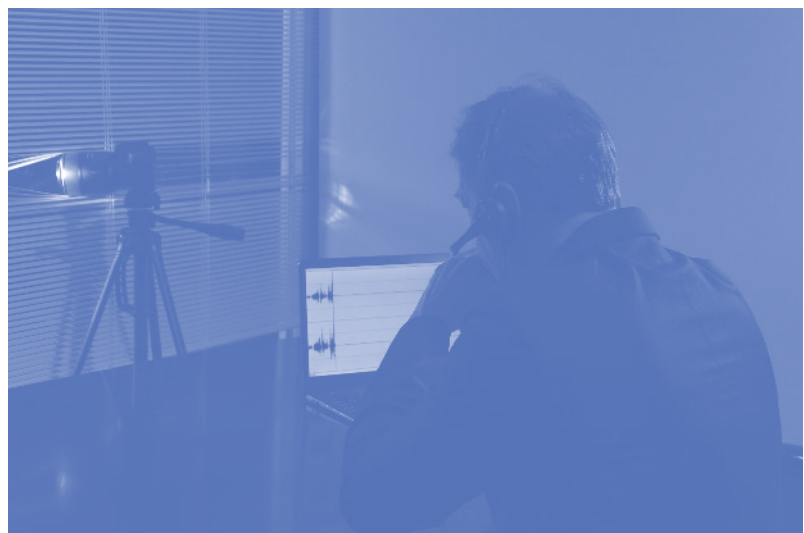
Similar requirements are also imposed by the ECHR, as interpreted by the ECtHR ⁽⁵⁷⁾. A three-pronged test developed by the ECtHR requires that any rights interference has to pursue a legitimate aim; be in accordance with the law, which necessitates an appropriate legal basis meeting qualitative requirements (public, precise and foreseeable) ⁽⁵⁸⁾; and be necessary in a democratic society (the necessity and proportionality test) ⁽⁵⁹⁾. As a fourth test, the ECtHR also uses the concept of the 'essence of a right', which can be derived from the object and purpose of the ECHR as a whole ⁽⁶⁰⁾. The case-law of the ECtHR has identified the following elements when determining whether a measure is 'necessary in a democratic society': the interference needs to correspond to a pressing social need, it must be proportionate and the reasons given to justify it must be relevant and sufficient ⁽⁶¹⁾. With respect to the use of new technologies, the ECtHR observed in *S. and Marper v. the United Kingdom*, a ruling concerning fingerprints, facial images and DNA profiles, that states should 'stri[k]e the right balance' between protecting fundamental rights and developing new technologies ⁽⁶²⁾. This also applies when national authorities use RBI technologies for law enforcement purposes. The ECtHR's jurisprudence on publicly used FRT requires a high level of justification for such mass surveillance to be considered 'necessary in a democratic society' ⁽⁶³⁾. As another data protection authority interviewed during the fieldwork stated, strict necessity considerations are needed when introducing new technologies into police work (see quote).

You can't just, in our view, replace old-fashioned police work because it's convenient with a technology that is highly intrusive and indiscriminate in its application, that doesn't meet the thresholds ... of balancing the rights of individuals, on the basis of strict necessity.

Respondent from a data protection authority

The RBI systems used for law enforcement purposes vary in their functionality, real-time or *ex post* application, location of deployment (i.e. in publicly accessible spaces or not) and the scale at which they are deployed. As a result, a wide range of fundamental rights may have to be assessed, taking into account a variety of elements, including the context in which the RBI system is used and the purpose of using it.

The assessment of the impact on fundamental rights has to be carried out for each way of using RBI technology for law enforcement purposes. It must cover all relevant fundamental rights and take into account all elements, from the legal basis, the legitimate purpose the technology is intended to help



achieve and the way the biometric data are captured (e.g. by CCTV cameras, mobile phone applications or voice recordings) to its real-time or *ex post* application, the location of deployment (in publicly accessible spaces or in private settings) and the degree of errors it entails (its accuracy). All this enables an informed assessment of the interference with the essence of a given right and of the necessity and proportionality of the system's use ⁽⁶⁴⁾. The more intrusive a specific use of an RBI technology is, the stricter the applicable test must be. According to the AI Act, the use of AI systems for real-time RBI in publicly accessible spaces for the purposes of law enforcement is 'particularly intrusive to the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights' ⁽⁶⁵⁾.

During the negotiation of the AI Act, both the EDPB and the EDPS called for the prohibition of the use of RBI systems in publicly accessible spaces in any context, and in online spaces for large-scale remote identification ⁽⁶⁶⁾. The EDPB underlined in its subsequent guidelines on the use of FRT in law enforcement that such technologies should be used 'only in cases when they satisfy the requirements of necessity and proportionality, as laid down in Article 52(1) of the Charter' ⁽⁶⁷⁾. It reiterated that the use of RBI to identify individuals in publicly accessible spaces has no place in a democratic society ⁽⁶⁸⁾. On the other hand, for example, the French Council of State considered, in a 2022 case, that facial recognition can be used by competent authorities as a support tool to identify people when absolutely necessary, acknowledging the difficulty of carrying out such comparisons manually when a database contains several million images ⁽⁶⁹⁾.

Endnotes

- ⁽³²⁾ For more details on the human rights framework within the EU, see FRA, *Bringing Rights to Life: The fundamental rights landscape of the European Union*, Publications Office of the European Union, Luxembourg, 2012.
- ⁽³³⁾ For concise analyses of the AI Act's framework for RBI, see Giannini, A. and Tas, S., 'AI Act and the prohibition of real-time biometric identification', Verfassungsblog website, 10 December 2024; and Jones, C. and Lanneau, R., 'Automating authority: Artificial intelligence in European police and border regimes', Statewatch, London, 2025, Section 2.3.2 '(Un)prohibited practices'.
- ⁽³⁴⁾ See recitals 9, 45 and 63 to and Arts 2(7), (9) and 5(8) of the AI Act. See also Commission Staff Working Document – **Impact assessment accompanying the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts**, SWD(2021) 84 final of 21 April 2021, pp. 5–6.
- ⁽³⁵⁾ Art. 5(8) of the AI Act.
- ⁽³⁶⁾ **Regulation (EU) 2016/679** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: <http://data.europa.eu/eli/reg/2016/679/oj>).
- ⁽³⁷⁾ For further information and concrete examples on what constitutes 'publicly accessible spaces', see recital 19 to the AI Act ('any physical space that is accessible to an undetermined number of natural persons, and irrespective of whether the space in question is privately or publicly owned, irrespective of the activity for which the space may be used'); and Communication from the Commission – **Commission guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)**, C(2025) 5052 final of 29 July 2025, paras 313–318.
- ⁽³⁸⁾ Art. 3(42) of and recital 17 to the AI Act. See **Annex I** for more information on real-time RBI systems.
- ⁽³⁹⁾ Art. 5(5) of the AI Act. See also Communication from the Commission – **Commission guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)**, C(2025) 5052 final of 29 July 2025, para. 289.
- ⁽⁴⁰⁾ These criminal offences are 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 or 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; and participation in a criminal organisation involved in one or more of the offences listed above.
- ⁽⁴¹⁾ Art. 6(2) of and Annex III(1)(a) to the AI Act. See also Communication from the Commission – **Commission guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)**, C(2025) 5052 final of 29 July 2025, para. 291.
- ⁽⁴²⁾ Art. 26(10) of and recital 95 to the AI Act. See also Art. 5(1)(h) of the AI Act.
- ⁽⁴³⁾ EDPS, 'EDPS comments to the AI Office's consultation on the application of the definition of an AI system and the prohibited AI practices established in the AI Act launched by the European AI Office', WW/AP/nc/D(2024)4345 C 2024-0279, 19 December 2024, p. 11.
- ⁽⁴⁴⁾ Communication from the Commission – **Commission guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)**, C(2025) 5052 final of 29 July 2025.
- ⁽⁴⁵⁾ See recital 37 to and Art. 10 of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89, ELI: <http://data.europa.eu/eli/dir/2016/680/oj>) (LED); recital 51 to and Art. 9 of the GDPR; and recital 29 to and Art. 10 of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>) (EUDPR). The ECtHR has, for example, also stated in *López Ribalda and Others*, with reference to its previous case-law on the matter, that 'a person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers.' ECtHR, *López Ribalda and Others v. Spain* [GC], Nos 1874/13 and 8567/13, 17 October 2019, § 89.
- ⁽⁴⁶⁾ Art. 3(13) of the LED, Art. 4(14) of the GDPR and Art. 3(18) of the EUDPR.
- ⁽⁴⁷⁾ **Directive (EU) 2016/680** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89, ELI: <http://data.europa.eu/eli/dir/2016/680/oj>).
- ⁽⁴⁸⁾ For a comprehensive, article-by-article, legal commentary on the LED, see Kosta, E. and Boehm, F. (eds), *The EU Law Enforcement Directive (LED) – A commentary*, Oxford University Press, Oxford, 2024. See also FRA, *The Law Enforcement Directive – Data protection challenges in practice*, Publications Office of the European Union, Luxembourg, 2026.
- ⁽⁴⁹⁾ See FRA and CoE, *Handbook on European Data Protection Law – 2018 edition*, Publications Office of the European Union, Luxembourg, 2018.
- ⁽⁵⁰⁾ **Regulation (EU) 2018/1725** of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).
- ⁽⁵¹⁾ See, for example, Fussey, P. and Murray, D., 'Human rights law considerations brought into play by public surveillance', in: Fussey, P. and Murray, D., *Facial Recognition Surveillance – Policing and human rights in the age of artificial intelligence*, Oxford University Press, Oxford, 2025; and Scheinin, M. and Sorell, T., 'Surveillance deliverable D4.10 – Synthesis report from WP4, merging the ethics and law analysis and discussing their outcomes', FP7 – SEC-2011-284725, 7 April 2015, p. 8.
- ⁽⁵²⁾ See similarly Fussey, P. and Murray, D., *Facial Recognition Surveillance – Policing and human rights in the age of artificial intelligence*, Oxford University Press, Oxford, 2025, p. 75.
- ⁽⁵³⁾ See, for example, Judgment of the Court of Justice of 16 December 2008, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*, C-73/07, ECLI:EU:C:2008:727, § 56; Judgment of the Court of Justice of 9 November 2010, *Volker und Markus Schecke and Eifert*, Joined Cases C-92/09 and C-93/09, ECLI:EU:C:2010:662, § 77; Judgment of the Court of Justice of 8 April 2014, *Digital Rights Ireland and Others*, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, § 52; Judgment of the Court of Justice of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, § 92; and Judgment of the Court of Justice of 17 December 2015, *WebMindLicenses*, C-419/14, ECLI:EU:C:2015:832, §§ 69 and 80–82.
- ⁽⁵⁴⁾ See Judgment of Court of Justice of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, §§ 94–95, which refer to Art. 52(3) of the Charter; Judgment of the Court of Justice of 8 April 2014, *Digital Rights Ireland and Others*, Joined Cases C-293/12 and C-594/12,

- ECLI:EU:C:2015:650, § 39, on the protection of the essence of Arts 7 and 8 of the Charter; Judgment of the Court of Justice of 15 February 2016, *J. N.*, C-601/15 PPU, ECLI:EU:C:2016:84, §§ 45–47, concerning the essence of the right to liberty under Art. 6 of the Charter.
- (⁵⁵) See, for example, Brkan, M., ‘The essence of the fundamental rights to privacy and data protection: Finding the way through the maze of the CJEU’s constitutional reasoning’, *German Law Journal*, Vol. 20, No 6, 2019, pp. 864–883, p. 867; Lenaerts, K., ‘Limits on limitations: The essence of fundamental rights in the EU’, *German Law Journal*, Vol. 20, No 6, 2019, pp. 779–794; and González Fuster, G., ‘**Study on the essence of the fundamental rights to privacy and to protection of personal data**’, EDPS, Brussels, 2022.
- (⁵⁶) Judgment of the Court of Justice of 8 April 2014, *Digital Rights Ireland and Others*, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2015:650.
- (⁵⁷) See, for instance, ECtHR, *Khelili v. Switzerland*, No 16188/07, 18 October 2011; *S. and Marper v. the United Kingdom* [GC], Nos 30562/04 and 30566/04, 4 December 2008; *K & T v. Finland*, No 25702/94, 12 July 2001; *Z v. Finland*, No 22009/93, 25 February 1997; *Huvig v. France*, No 11105/84, 24 April 1990; *Leander v. Sweden*, No 9248/81, 26 March 1987.
- (⁵⁸) On the requirements of ‘quality of law’, see ECtHR, *Gorlov and Others v. Russia*, Nos 27057/06, 56443/09 and 25147/14, 2 July 2019, § 97.
- (⁵⁹) See, for example, ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos 30562/04 and 30566/04, 4 December 2008, §§ 95–104; *Big Brother Watch and Others v. the United Kingdom* [GC], Nos 58170/13, 62322/14 and 24960/15, 25 May 2021, §§ 332–334.
- (⁶⁰) Scheinin, M. and Sorell, T., ‘Surveillance deliverable D4.10 – Synthesis report from WP4, merging the ethics and law analysis and discussing their outcomes’, FP7 – SEC-2011-284725, 7 April 2015, p. 9.
- (⁶¹) See, for instance, ECtHR, *Khelili v. Switzerland*, No 16188/07, 18 October 2011; *S. and Marper v. the United Kingdom* [GC], Nos 30562/04 and 30566/04, 4 December 2008; *K & T v. Finland*, No 25702/94, 12 July 2001; *Z v. Finland*, No 22009/93, 25 February 1997; *Huvig v. France*, No 11105/84, 24 April 1990; *Leander v. Sweden*, No 9248/81, 26 March 1987.
- (⁶²) ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos 30562/04 and 30566/04, 4 December 2008, § 112. See also ECtHR, *Gaughran v. the United Kingdom*, No 45245/15, 13 February 2020; *Ekimdzhev and Others v. Bulgaria*, No 70078/12, 11 January 2022; *Glukhin v. Russia*, No 11519/20, 4 July 2023.
- (⁶³) ECtHR, *Glukhin v. Russia*, No 11519/20, 4 July 2023.
- (⁶⁴) See Biometrics Institute, ‘**Facial recognition technology (FRT) in public places: Key questions before you start**’, Biometrics Institute website, 15 April 2026.
- (⁶⁵) Recital 32 to the AI Act.
- (⁶⁶) EDPB and EDPS, **EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)**, 18 June 2021, para. 32. See also EDPS, ‘**EDPS comments to the AI Office’s consultation on the application of the definition of an AI system and the prohibited AI practices established in the AI Act launched by the European AI Office**’, WW/AP/nc/D(2024)4345 C 2024-0279, 19 December 2024, p. 10.
- (⁶⁷) EDPB, **Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement**, Version 2.0, 26 April 2023, p. 29.
- (⁶⁸) Ibid.
- (⁶⁹) French Council of State (*Conseil d’État*), **Decision No 442364**, 26 March 2022, paras 5 and 7.

2

FUNDAMENTAL RIGHTS CHALLENGES WHEN USING REMOTE BIOMETRIC IDENTIFICATION – SELECTED KEY ISSUES

This chapter analyses relevant fundamental rights challenges stemming from the use of RBI, informed by all strands of the fieldwork, and links them to various fundamental rights affected by using RBI for law enforcement purposes. More specifically, the chapter dives into the questions of the legal basis of using RBI in national law; the provision of information and transparency around the use of RBI by law enforcement agencies; the accuracy and data quality of such RBI systems; risks of abuse, surveillance and social harm; and external oversight and effective (judicial) remedies.

2.1. LEGALITY OF USING REMOTE BIOMETRIC IDENTIFICATION – THE NEED FOR A CLEAR LEGAL BASIS IN NATIONAL LAW

Any use of RBI technologies by law enforcement must be set out in law (see [Section 1.2](#)). This requirement of being in accordance with the law protects against the arbitrary exercise of public power by national authorities. Thus, any measure interfering with fundamental rights must have a clear legal basis, which must be of sufficient quality to protect against arbitrariness ⁽⁷⁰⁾. In addition, Article 10 of the LED permits the processing of biometric data only (1) where strictly necessary and subject to appropriate safeguards; and (2) if authorised by EU or national law, if the processing is to protect the vital interests of a person or if the data subject makes the data manifestly public. The Article 29 Working Party – the EDPB’s predecessor under Directive 95/46/EC – clarified that the provision should be read together with Article 8 of the LED, meaning that a specific legal basis is always required for the processing of personal data ⁽⁷¹⁾. In line with the above, the CJEU reaffirmed that systematic biometric data collection without a sufficiently specific legal basis, case-by-case necessity assessment and adequate reasoning is unlawful ⁽⁷²⁾. It did so against the backdrop of a national database that had accumulated over 6.5 million fingerprints ⁽⁷³⁾. In this context, the AI Act further restricts the creation of facial recognition databases (see ‘[Legal corner: the prohibition of facial recognition databases based on untargeted scraping](#)’).

The AI Act also makes it clear that Member States must lay down in their national legislation ‘the necessary detailed rules for the request, issuance and exercise of, as well as supervision and reporting relating to, the authorisations [for real-time RBI technologies for law enforcement purposes]’ (Article 5(5)). These national rules must also specify the permitted objectives for their use (see [Section 1.1](#) above) in respect of which the competent authorities may be authorised to use those systems for the purposes of law enforcement (Article 5(5)). Member States are obliged to notify the European Commission of such

national legislation – which can be even stricter (more protective) than the requirements under the AI Act – within 30 days following its adoption (Article 5(5)). The same obligation to establish the legal basis in national law applies to the use of *ex post* (not real-time) RBI technologies for law enforcement purposes – (see recitals 54 and 59 of the AI Act). Provisions of the AI Act applicable to the use of RBI by police authorities, either with respect to the prohibitions/exceptions or when such use qualifies as high risk, complement the indispensable national legal basis as directly applicable and directly effective EU law. In the case of EU agencies, their founding regulations provide for the legal basis to use RBI, such as facial recognition technology, to assist the fulfilment of their tasks set forth in EU law. This is the case with Europol ⁽⁷⁴⁾. In addition, Article 26(10) of the AI Act sets out additional requirements for law enforcement authorities' use of *ex post* RBI systems for criminal investigation purposes, implying the need for clear legal rules governing the authorisation of such use. Also in this case, Member States can introduce stricter rules (more protective for the individual) for the use of *ex post* RBI ⁽⁷⁵⁾.

Legal corner

The prohibition of facial recognition databases based on untargeted scraping

The AI Act prohibits the placing on the market, putting into service, or use of AI systems that create or expand facial recognition databases through the untargeted scraping of images from the internet or CCTV footage. This seeks to prevent the building of a large-scale database with billions of facial images scraped from the internet. This was done, for example, by a company called Clearview, which created a law enforcement database of several billion images. The company has been subjected to enforcement action by data protection authorities across Europe. The use of data 'manifestly made public by the data subject' as a legal basis for processing biometric data has been misinterpreted by some RBI technology providers as permitting the scraping of facial images from the internet for the purposes of constructing biometric databases against which other facial images may be compared. The EDPB has, however, clarified that '[t]he fact that a photograph has been manifestly made public by the data subject does not entail that the related biometric data, which can be retrieved from the photograph by specific technical means, is considered as having been manifestly made public.'

The AI Act's prohibition has, however, some limitations. First, the AI Act prohibits only the 'untargeted scraping' of images, meaning that targeted scraping could still entail the accrual of facial images of persons with potential links to criminal offences (a potentially broad category of individuals) or criminal proceedings, and also missing persons. Second, the prohibition does not apply to the untargeted scraping of other biometric data, such as voice samples. It also does not apply where no AI system is involved in the scraping. A significant risk to fundamental rights can arise in all these scenarios. It is also possible that national law enforcement agencies have already constructed facial recognition databases from facial images collected through untargeted scraping from the internet or CCTV; the use of such databases would, however, be unlawful under EU data protection law.

Sources: Art. 5(1)(e) of the AI Act; Communication from the Commission – **Commission guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)**, C(2025) 5052 final of 29 July 2025, paras. 225, 229, 230, 232, 234, 236, 238; EDPB, **Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement**, Version 2.0, 26 April 2023, p. 4. See also, for example, Liu, T., 'How we store and search 30 billion faces', Clearview AI website, 18 April 2023; Italy, Garante per la protezione dei dati personali, 'Riconoscimento facciale: Il Garante privacy sanziona Clearview per 20 milioni di euro. Vietato l'uso dei dati biometrici e il monitoraggio degli italiani', Garante per la protezione dei dati personali website, 9 March 2023; Information Commissioner's Office, 'ICO fines facial recognition database company Clearview AI Inc more than £7.5m and orders UK data to be deleted', Information Commissioner's Office website, 23 May 2022; Hellenic Data Protection Authority, 'Imposition of fine on Clearview AI, Inc', Decision No 35/2022, 13 July 2022; Commission Nationale de l'Informatique et des Libertés, 'Délibération de la formation restreinte n° SAN-2022-019 du 17 octobre 2022 concernant la société x', 20 October 2022; Autoriteit Persoonsgegevens, 'Dutch DPA imposes a fine on Clearview because of illegal data collection for facial recognition', 3 September 2024.

We need to look into the main problems that arise and relate to the legality of the use of this system, namely the absence of a legal framework that would describe in detail and clearly the purpose of its use, how it operates and the data that are processed, as well as the rights of the data subjects and of the authorities enforcing the system.

Civil-society respondent

FRA research findings reveal various shortcomings concerning the sufficient legal basis for using RBI systems by law enforcement agencies.

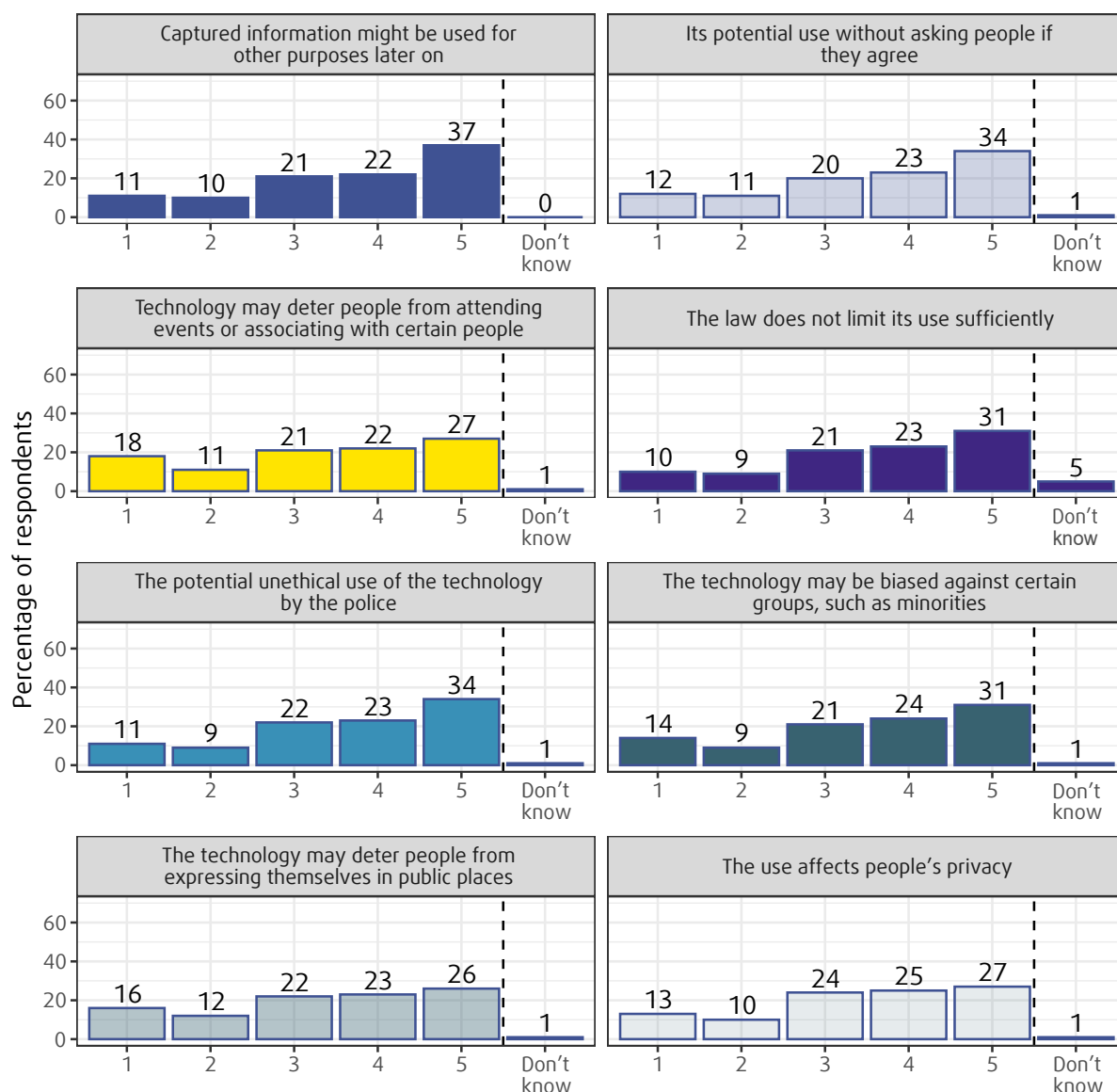
A national data protection authority, statutory human rights bodies and civil-society organisations interviewed underscored the need for a sufficient, specific and proper legal basis, which is not the case with each RBI system in the Member States covered by the fieldwork. The legal basis was lacking according to some interviewees in a discontinued application of a facial recognition tool for law enforcement purposes in Italy ⁽⁷⁶⁾, in the case of a soon-to-be deployed smart policing tool in one Member State and also in the case of another RBI tool used for criminal investigations in another Member State. For a number of respondents, the absence of a clear legal basis contributed to concerns over a risk of the abuse of RBI systems ([Section 2.4](#)).

Respondents pointed to the need for a specific legal framework to be in place, rather than to apply general legislation that regulates law enforcement activities. National rules implementing the LED, for example, are not enough in themselves to fulfil the requirements of such a national legal basis, which a national data protection authority in a Member State covered by the fieldwork highlighted. In another Member State, respondents pointed out that, in practice, tools were already extensively piloted while legislation providing a clear legal basis and safeguards was still pending.

Law enforcement deployers generally acknowledged the need for a robust legal basis. Some emphasised that the rules for deploying the RBI systems that they worked with clearly outline the conditions for their use and applicable safeguards. In one Member State, law enforcement deployers expressed the view that legislation was too restrictive and imposed impractical bureaucratic obligations on the use of the system. However, they did not elaborate further on what obligations and requirements are impractical.

FRA's survey of 1 054 people in selected public places asked respondents about whether or not they are concerned about certain issues relating to the use of FRT in public places. It shows that people are concerned about several issues. Most notably, respondents are concerned that information captured through facial recognition might be used for other purposes later on. On a scale from 1 to 5, where 1 means 'not concerned at all' and 5 means 'very concerned', 37 % of respondents indicated that they were very concerned about this. Another 22 % are concerned (selecting 4 on the scale) and only 11 % indicate not being concerned at all (see [Figure 2](#)). This is seen as the most pressing issue in the surveys carried out in France (second wave) and in Germany (see [Figure 3](#)).

FIGURE 2 CONCERNS ABOUT POLICE USE OF FACIAL RECOGNITION TECHNOLOGY



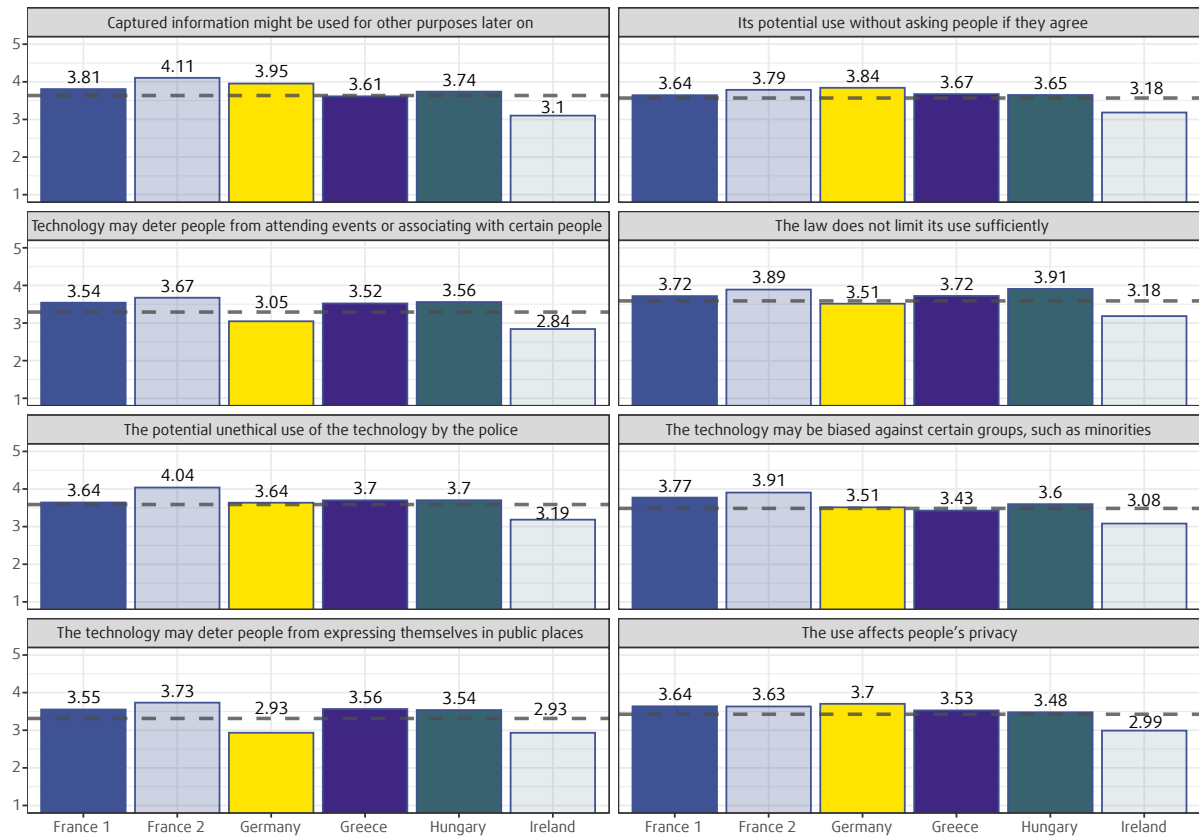
Notes: $N = 1\,054$. Question: How concerned are you about the following issues relating to law enforcement uses of facial recognition technology in public places in [Member State]? 1 = not at all concerned; 5 = very concerned.

Source: FRA, 2026.

The second most concerning issues are equally (on average) that the law does not sufficiently limit its use and the potential unethical use of the technology by the police. The concern that the law does not sufficiently limit its use was expressed most often in Hungary and in the second survey wave in France (see [Figure 3](#), showing the average values by issue and Member State).

On average, of the questions asked about in the survey, a considerable share of respondents indicated they were concerned about all of the issues asked about, including that that the use of RBI technology may deter people from attending events or expressing their opinions, with an average score of 3.3 on a scale from 1 to 5 across all respondents.

FIGURE 3 CONCERNS ABOUT POLICE USE OF FACIAL RECOGNITION TECHNOLOGY, BY MEMBER STATE (%)



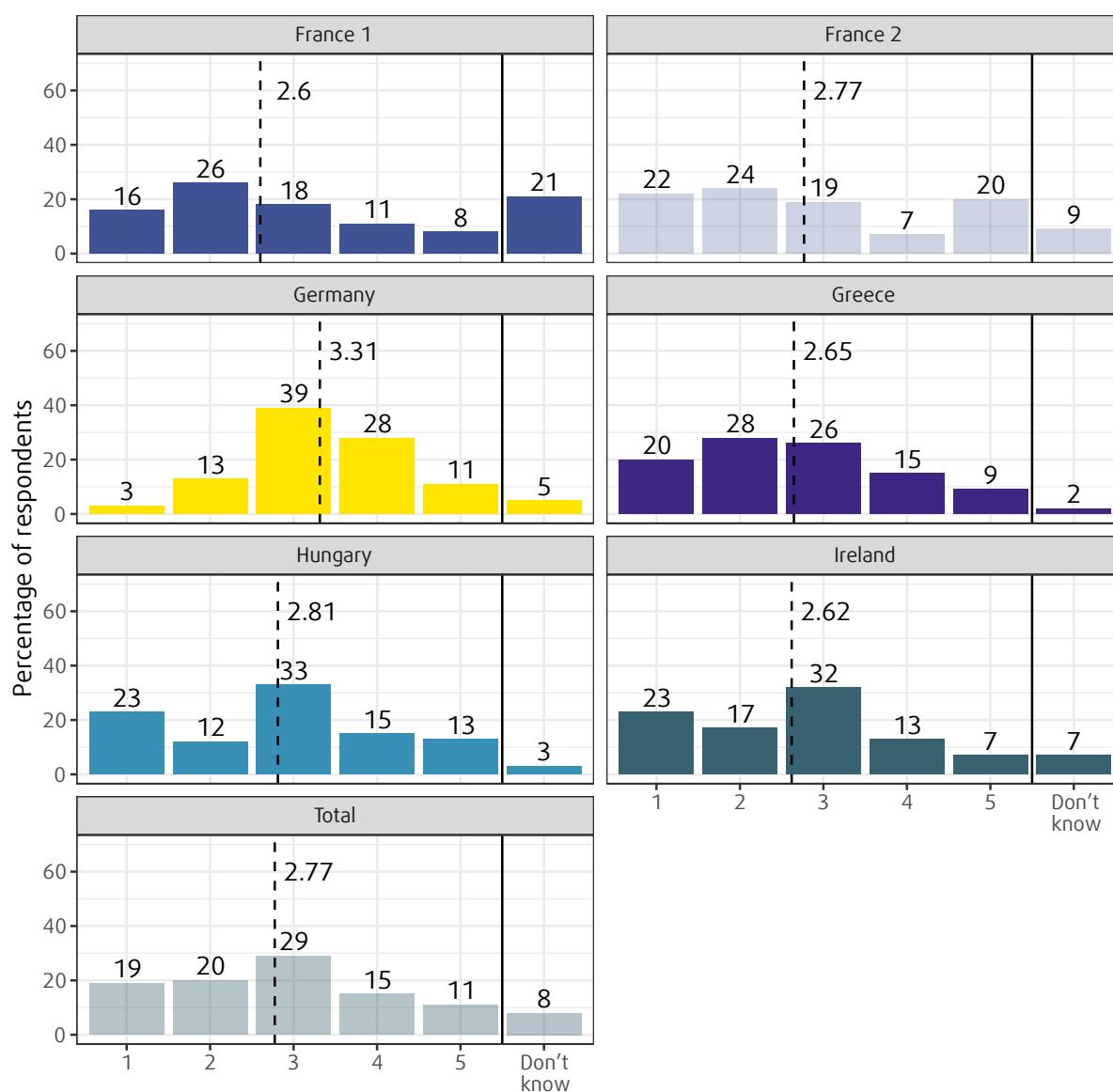
Notes: $N = 1\,054$. Question: How concerned are you about the following issues relating to law enforcement uses of facial recognition technology in public places in [Member State]? 1 = not at all concerned; 5 = very concerned.

In France, the survey was carried out in two waves, one during the 2024 Olympics and another afterwards, denoted as France 1 and France 2 respectively. The dashed horizontal line gives the average value.

Source: FRA, 2026.

Finally, having a legal basis whenever using RBI for law enforcement purposes is also important for building trust. The small-scale survey showed that people in publicly accessible spaces tend not to agree that the law in their Member State is strong enough to ensure these technologies are used ethically and responsibly. On a scale from 1 to 5, where 1 means 'completely disagree' and 5 means 'completely agree', 39 % selected 1 or 2, whereas only 26 % selected 4 or 5, with 29 % selecting the middle value of 3, while 8 % indicated that they do not know. People in Germany have most trust that the law is strong enough, with an average value of 3.3 on the five-point scale. One in five in the first wave of the survey in France during the Olympics chose 'don't know' (see Figure 4).

FIGURE 4 PEOPLE'S VIEW ON WHETHER THE LEGAL FRAMEWORK IN A MEMBER STATE IS STRONG ENOUGH FOR ITS ETHICAL AND RESPONSIBLE USE (%)



Notes: $N = 1\,054$. Question: On a scale of 1 to 5, where 1 means completely disagree and 5 means completely agree, to what extent do you agree or disagree that the law in [Member State] is strong enough to ensure these technologies are used ethically and responsibly?

In France, the survey was carried out in two waves, one during the 2024 Olympics and another afterwards, denoted as France 1 and France 2 respectively. The vertical dashed line indicates the average response on the five-point scale, excluding those saying that they don't know.

Source: FRA, 2026.

2.2. LACK OF INFORMATION AND TRANSPARENCY ABOUT THE USE OF REMOTE BIOMETRIC IDENTIFICATION

AI-powered tools are often seen as ‘black boxes’ due to their high complexity, only partially explainable decision-making process and/or self-learning character. Being transparent about the use of AI-driven RBI for law enforcement purposes and informing the general public about them is of crucial importance for reasons of legality, but also for exercising the right to an effective judicial remedy (Article 47 of the Charter). It also enables affected individuals to turn to other oversight mechanisms such as national data protection authorities or ombuds institutions. However, according to fieldwork interviews, there still remains considerable secrecy about the operation of RBI technologies used by law enforcement authorities, which is underlined by other research findings independent of FRA’s work ⁽⁷⁷⁾.

Article 13 of the LED requires Member States’ relevant authorities to provide certain information about data processing to data subjects, including information on the controller, the purpose of processing and data subject rights. The provision of information can, however, be limited to avoid obstructing or prejudicing law enforcement work or to protect public security and national security ⁽⁷⁸⁾. The EDPB also recommended publishing results of data protection impact assessments concerning the use of FRT in law enforcement, or at least their main findings and conclusions, to increase trust and transparency ⁽⁷⁹⁾.

The AI Act lays down that the general public is to receive statistics on law enforcement use of real-time RBI tools in publicly accessible spaces, aggregated to the Member State level and published annually by the European Commission (Article 5(7)). These must not include sensitive operational data, such as information about locations or cameras used ⁽⁸⁰⁾. It remains, however, unclear, due to the built-in vagueness of the provisions, whether key metrics on the nature of deployments, the types of criminal offences concerned, the number of individuals impacted and the performance of the given RBI tool will be available for public scrutiny under the new EU rules.

In addition, providers and law enforcement deployers of RBI are required to register themselves and their systems in a secure non-public section of the EU database for high-risk AI systems (Article 49(1), (3) and (4) and Article 71 of the AI Act). Only the European Commission and the competent national data protection supervisory authorities (as market surveillance authorities) will have access to this section of the EU database (Article 49(4) and Article 74(8) of the AI Act). Despite the limited access, and contrary to the obligations of some other deployers of high-risk AI systems, law enforcement deployers of RBI systems do not need to register the summary of their FRIA findings (which is an important transparency and accountability tool) in the EU database (Article 49(4)(c) of the AI Act).

In several Member States covered by the fieldwork, including where voice recognition is in use, no dedicated transparency mechanism is in place to inform the public about the RBI system’s use or to provide public reports on the system’s operation and effectiveness. Elsewhere, information is shared with the affected person only when the use of the facial recognition tool leads to a criminal case.

A civil-society respondent expressed concerns about the limited understanding and knowledge of AI technologies among judges, which illustrates how the lack of transparency can considerably hamper the administration of justice, from the courts’ perspective. However, this point concerning judges’ lack of knowledge was not picked up by other interviewees.

As regards the need for enhanced transparency, some law enforcement agencies interviewed that deploy such technology, and some statutory human rights bodies, cited the need to maintain the confidentiality of police operations and any potential use of RBI tools. Similar arguments on confidentiality have also been made by some RBI providers (tech companies), invoking the arrangements they have in place with law enforcement agencies and the need for express permission from relevant authorities to share information about the functioning of the RBI tool concerned.

Lack of first-hand information from those producing, deploying and using RBI technologies in the context of law enforcement can hinder the accurate and comprehensive understanding of the AI-supported technologies and how they are used for law enforcement purposes. It also makes it more difficult to assess the fundamental rights risks of the different use cases, including the credibility and robustness of the necessity and proportionality calculations as well as the appropriate use of such tools by deployers. Moreover, such limited transparency is unlikely to be useful, on its own, for the individuals concerned and the broader public to be able to sufficiently understand how RBI systems are used in practice for law enforcement purposes and their impact on fundamental rights. Clearly, the lack of such information limits opportunities to access an effective legal remedy.

Public perception points to similar concerns. While at the time of the survey FRT was used in all Member States covered, except for Ireland ⁽⁸¹⁾, the public's perceptions did not always align with this, as shown in **Figure 5**. Overall, the majority of the small-scale survey respondents (62 %) believe that FRT is used by police in their Member State, 24 % do not think it is used and 13 % replied that they do not know if it is used. In particular, respondents interviewed during the second wave in France (after and not during the Olympic Games) believed that it is used, with 81 % of respondents indicating this. In addition, in Hungary, a relatively high proportion of respondents believe that RBI is already used by the police (73 %).

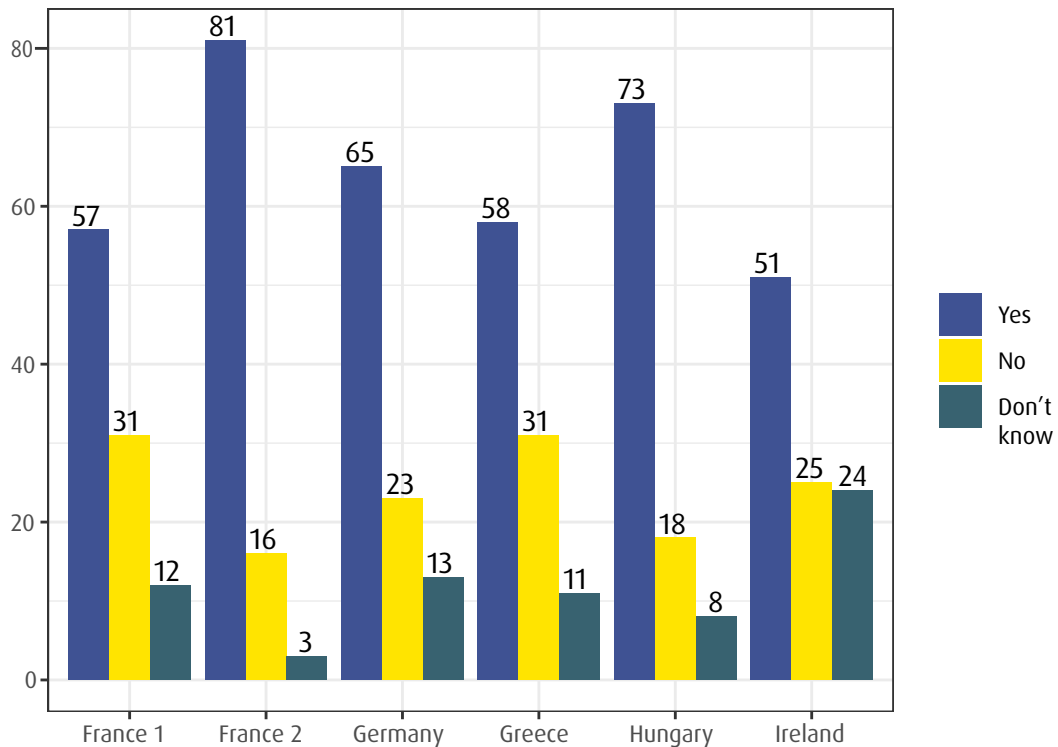
Of those who do not think that RBI is used, more than half (54 %) think it is not used because it is not in line with fundamental rights. In addition, 42 % of those who do not think it is used assume that it is not used because it is not ready to be used. 9 % think there are other reasons why such technology is not used ⁽⁸²⁾.

Finally, among those who think that the technology is not used, 64 % think that it may be used in the near future, 27 % do not think it will be used in the near future and 9 % do not know.

There could be transparency in terms of providing information on the use and the results of the system, for example, by publishing some public reports on its operation by the ... police, so that people know more about its effectiveness, and possibly some statistics, or something similar about the added value of using this [RBI] system.

Respondent from a statutory public human rights body

FIGURE 5 PEOPLE BELIEVING THAT FACIAL RECOGNITION TECHNOLOGY IS USED BY LAW ENFORCEMENT AGENCIES, BY MEMBER STATE



Notes: $N = 1\,054$. Question: Do you believe facial recognition technology is used by the police in [Member State]? In France, the survey was carried out in two waves, one during the 2024 Olympics and another afterwards, denoted as France 1 and France 2 respectively.

Source: FRA, 2026.

2.3. ACCURACY AND DATA QUALITY

Recent technological developments have led to considerable advancements in the performance of biometric technologies, notably FRTs ⁽⁸³⁾. Determining the necessary level of accuracy for various RBI technologies is, however, challenging, and RBI systems' accuracy rates can be difficult to compare across technologies in the absence of standardised test methodologies and datasets. For example, when it comes to FRT, different ways to evaluate and assess accuracy exist, which depend also on the task, purpose and context of use of a system ⁽⁸⁴⁾. Circumstances like low or variable lighting and whether the person is wearing headgear can influence accuracy rates ⁽⁸⁵⁾. FRA stated in its 2019 focus paper on FRTs that accuracy assessments need to be made for different population groups due to potentially misleading general accuracy rates ⁽⁸⁶⁾. Besides issues related to varying performance of FRT depending on people's sex, age (children and older persons) and ethnic group ⁽⁸⁷⁾, such technologies' accuracy when applied to people with disabilities is another important aspect to consider ⁽⁸⁸⁾.

Notwithstanding accuracy gains, inaccuracies remain that can lead to biased results and discriminatory outcomes ⁽⁸⁹⁾. The AI Act acknowledges the related challenges, including from a fundamental rights point of view. Its recital 32 makes it clear that '[t]echnical inaccuracies of AI systems intended for the remote biometric identification of natural persons can lead to biased results and entail discriminatory effects. Such possible biased results and

discriminatory effects are particularly relevant with regard to age, ethnicity, race, sex or disabilities.’ The potential fundamental rights impact of inaccurate systems is, however, not limited to non-discrimination (Article 21 of the Charter). Other rights could be impacted too, such as human dignity (Article 1), the right to liberty (Article 6) and the rights of the child (Article 24) ⁽⁹⁰⁾.

Permitted RBI systems are classified as ‘high-risk’ by the AI Act in view of the significant risks that they pose ⁽⁹¹⁾. These risks are amplified in a law enforcement context. The AI Act places the responsibility for accuracy and testing on technology providers, who must declare levels of accuracy and the relevant accuracy metrics of high-risk AI systems, such as permitted RBI tools, in the instructions for use ⁽⁹²⁾.

The accuracy of RBI technologies is strongly influenced by the quality of data used to create, train, validate and test the system, alongside the quality of the data fed into the system once deployed. Algorithms used in AI-powered tools can only be as good as the data used for their development ⁽⁹³⁾. High-quality data are thus essential for high-quality RBI systems. Under the principle of data accuracy – reflected in Article 5(1)(d) of the GDPR and Article 4(1)(d) of the LED – national authorities must use information and data that are accurate and up to date. RBI systems used for law enforcement purposes that are based on incomplete or biased data, and lower quality of biometric source data and biometric templates, can lead to inaccurate outcomes that infringe on people’s fundamental rights ⁽⁹⁴⁾. At the same time, ensuring high levels of accuracy may require access to large and representative datasets, which raises questions under the principles of purpose limitation and data minimisation in EU data protection law. The EDPB has clarified that the (re)use of biometric data for training FRTs constitutes a distinct processing purpose requiring its own assessment of necessity and proportionality, while even the processing of non-matched biometric data amounts to a serious interference in itself ⁽⁹⁵⁾. In this context, synthetic data may offer a ‘data protection by design’ approach by reducing reliance on real personal data for training purposes ⁽⁹⁶⁾. Although such approaches are increasingly explored in scholarly literature, ensuring that synthetic datasets are sufficiently representative and reliable for operational deployment remains challenging ⁽⁹⁷⁾. The bottom line is to ensure fairness no matter what kind of training data processing is undertaken ⁽⁹⁸⁾.

During the fieldwork, the accuracy rates (statistics) of a given RBI tool were not easily available or shared in interviews, except in the case of voice recognition software used to complement criminal investigations. From the two providers interviewed, representatives of one clarified that their company explains to the users of their technology how matching scores between images, which indicate their similarity, are created, as well as the factors that can impact them, including the quality of images. The customers set the thresholds for the matching scores they will consider. Concerning false positives and false negatives, only estimates can be given, and the provider uses different benchmarks for different use cases. It also looks at external tests, and its largest government customers run their own tests as well to assess performance. They also mentioned that there is no easy way to scientifically measure the quality of the data on the customer side, which is the most decisive factor impacting performance. The other provider declined to answer questions pertaining to accuracy assessments and expected error rates.

The majority of deployers interviewed were not familiar with details about the accuracy of the systems. Some emphasised that the matching score in facial recognition is a probability rate used as an investigative lead, so the outcome will depend on further steps taken by officers. Approaches vary when it comes to the verification of the match; while, for example, in one Member State

covered, two operators carry out two checks to verify the result, this might not always be the practice in another Member State of deployment, according to an interviewee. Two interviewees explained that it is difficult to know if a match they provided to the investigative teams is correct if these teams do not inform them of the final outcome of the investigation. Interviewees from civil society and oversight bodies, including those working for data protection authorities and other statutory human rights institutions or bodies, often expressed concerns about facial recognition systems working less accurately for certain groups, and system biases that could lead to discrimination. A civil-society respondent pointed out that seemingly very low error rates (e.g. less than 1 %) could still impact unacceptably large numbers of people in widely deployed systems or across large databases. Some respondents from various groups interviewed acknowledged the importance of data quality for facial recognition.

Voice recognition experts within law enforcement authorities were the most familiar with and transparent about the accuracy rates and related statistics of the technology used. This may be explained by the nature of the teams: they were dedicated technology specialists within the authorities, as opposed to the other, rather generalist, law enforcement officers interviewed, who worked regularly across a variety of technologies. According to various respondents, voice recognition technologies covered by this research had an error rate of 2 % or under. Two law enforcement interviewees, for example, mentioned that by enlarging their reference database they managed to reduce the 'equal error rate' (which is a performance metric for biometric systems indicating their accuracy, showing the point where the system makes the same percentage of false positives and false negatives ⁽⁹⁹⁾) from around 5 % to a range between 1.3 % and 1.7 % for phone recordings (and 0.2 % for audio chat messages, due to their higher quality). They explained that different accuracy rates across different groups are not applicable, as they use the tool only for a specific reference group (male native speakers who have completed puberty and whose voices have changed). Another law enforcement interviewee explained that they believe the error rate was intended to be, based on the tender specifications, around 2 %. The reason for this error rate is, among other things, the fact that the biometric characteristics of a voice are not as unique and individual as DNA or fingerprints. The respondent acknowledged that the error rate can be reduced by increasing the recognition threshold, which would then lead to fewer false positives (i.e. fewer false matches), but also more false rejections (i.e. the right match is more likely to be missed). Positive results are always initially re-evaluated acoustically and subsequently reviewed by expert assessment.

Overall, several voice recognition experts interviewed, both within and outside law enforcement, underlined the importance of test conditions and individual circumstances, given that real-life conditions, including the suitability and quality of the voice recording input data, impact on the performance of the technology. One expert on phonetics pointed out that neural networks are getting better at analysing voice dimensions that humans cannot analyse systematically, which poses verification challenges, as these are presented in an abstract way as numbers. On the other hand, they pointed out the issue of human bias. They added that subjective acoustic assessments by a human cannot be challenged as easily and lead to much easier violation of fundamental rights than an automated tool that has been thoroughly tested and relies on acknowledged standards and science. A voice recognition tool deployer agreed that the tool can prevent bias by providing output that cannot be influenced by the nature of the crime – unlike a human, who might be biased if they hear what the crime is about. Two other interviewees from another voice recognition tool deployer considered, however, that an automated tool does not prevent bias better than a manual/human assessment would, as

all elements in the latter assessment need to be intersubjectively verifiable, meaning that a second and a third expert verify the results to prevent bias.

The research remained inconclusive as regards any specific accuracy statistics in relation to bias. One technology provider mentioned that image quality can especially impact FRT performance on individuals with darker skin. They described internal processes for bias testing and external tests, such as testing by the US National Institute of Standards and Technology (NIST), which evaluate how different facial recognition algorithms perform on different ethnicities.

Two law enforcement officers expressed unease that they had to rely on voluntary disclosure of statistics from technology providers and on evaluation by NIST, including for bias testing. This also indicates a culture of limited voluntary disclosure from technology providers to the deploying law enforcement agencies. A respondent from academia likewise critiqued the invoking of industrial secrets. Another academic expert interviewed noted that, while the NIST testing regime is viewed as robust because it has access to large amounts of biometric data, including on different groups and demographics, there is a big difference between a lab setting and an operational setting, where one sees deployments in different situations and contexts (including different lighting conditions), which can massively affect image quality, and in turn system outputs.

A law enforcement respondent added that they look forward to the EU AI Act's transparency obligations around the development of AI systems, implying that they would benefit from increased transparency on the part of technology providers.

In general, a number of interviewees mentioned the practice of submitting technologies for standardised external assessment to gain technical credibility. Multiple providers within this study have submitted their algorithms to NIST for independent vendor test assessments, which are widely considered to be an industry benchmark for FRT. Law enforcement agencies also rely on NIST statistics. In one Member State covered, the law enforcement authority requested that the algorithm used for facial recognition be selected from those that had been evaluated by NIST ⁽¹⁰⁰⁾, and another law enforcement respondent also referenced the NIST process. NIST evaluates the submitted facial recognition-related AI tools by using large datasets collected through US public administration databases, which include mugshots, facial images for visa applications and photos taken at border-crossing points ⁽¹⁰¹⁾. While corresponding services are absent from the EU, relying on NIST could mean that the RBI systems deployed in a given Member State may have been tested on members of (vulnerable) populations who have not consented to the use of their biometric data for such purposes ⁽¹⁰²⁾. Two respondents from a deployer and a respondent from civil society noted that there is often a tension between data needs for creating accurate RBI systems and the limitations under data protection law. According to the civil-society respondent, this could be why many systems are developed and tested outside Europe.

While Article 15 of the AI Act lays down that providers have to ensure appropriate levels of system accuracy, to be declared in the instructions for use for deployers, RBI systems' accuracy rates may be ill suited for fundamental rights analysis. For example, there are different ways to measure false positives, and some of them rely on human adjudication, which can be unreliable. The measurement of false positives by means of technical standards could, therefore, conceal fundamental rights risks ⁽¹⁰³⁾.

[T]here is a good use for these automatic [voice recognition] systems, but they should never be used on their own.

Law enforcement officer

I think that [real-time voice recognition use] is very worrying given the current state of technology because the verification provided by experts, which can still be present in systems that do not run in real time, is completely lacking and this can lead to errors.

Law enforcement officer

The problem, of course, is twofold. That you (a) have to take that supplier at face value. That this is how he delivered it. And (b) our data will always differ in practice from NIST's data.

Law enforcement officer

How can we set up a system of accountability for usage when industry secrecy is protected?

Expert from academia

More importantly, even if RBI systems were fully accurate, several fundamental rights issues connected to their development and use would remain. For example, as some respondents pointed out, the risk of discrimination can arise not only through bias in the systems but also through their use, if it principally targets certain groups; that also relates to the issue of reference databases used for such systems (see [Section 2.4](#)). Risks also persist concerning several other fundamental rights, such as the rights to privacy, data protection and freedom of expression, as referred to in the preceding sections of this report. Error rates and bias are therefore only two sources of fundamental rights concern.

2.4. RISKS OF ABUSE

RBI technologies offer law enforcement agencies a powerful tool to combat terrorism and other forms of serious crime, which is a legitimate aim allowing the restriction of certain fundamental rights in some cases ⁽¹⁰⁴⁾. However, such limitations need to be construed narrowly, clearly setting out the rules and conditions for the use of such technologies, and providing effective safeguards against potential abuse.

As outlined above in the section concerning legality ([Section 2.1](#)), a clear and foreseeable legal framework for the use of remote biometric technologies is missing in some of the Member States covered by this research. In some cases, tools are extensively piloted while legislation providing a clear legal basis and safeguards is pending. According to civil-society respondents in most Member States, this carries an inherent risk that such tools are used disproportionately and beyond the intended purpose, either at present or in the future.

Once an RBI system is implemented, there is always a risk of misuse, regardless of legal safeguards. This poses a danger in itself, even under a government that respects human rights, as there is always the possibility that a future government may not.

Civil-society respondent

The AI Act limits law enforcement authorities' use of real-time RBI in publicly accessible spaces to specific objectives, as set out in [Section 1.1](#). In this regard, there appear to be significant differences among Member States when it comes to the purposes for which RBI tools can be deployed. Two RBI technologies within this study, Italy's Sistema Automatico di Riconoscimento Immagini (SARI) real time and, potentially, Hungary's facial recognition system, appear to be used for wider purposes. According to two respondents, one from an oversight body and one from academia, Hungary's system may be used for crowd control, public unrest or nuisance behaviour ⁽¹⁰⁵⁾, while SARI real time was – prior to its ban – intended for use in public spaces and events, according to a respondent from an oversight body. Furthermore, interviews in Greece indicated plans to deploy FRT in portable devices to be used during routine police stops in urban areas. All these examples might be incompatible with the limits and requirements set out in the AI Act.

The other RBI systems within this study – in their current or planned scopes of application – appear to be limited to investigations of criminal offences by law enforcement agencies. However, as some respondents flag, the use of some of these tools is not necessarily limited to serious crime; in some cases it also covers relatively minor offences such as violent public disorder or theft. This raises concerns about the necessity and proportionality of the deployment of such tools and, once more, compatibility with the requirements of the AI Act and, more generally, EU fundamental rights law.

Some civil-society respondents also point to the fact that in some Member States the RBI tools can be used for public security or national security purposes. The opaque nature of national security, together with the blurred line between such purposes and law enforcement work, prevents the scope of use of RBI from being transparent and makes it challenging to exert

effective oversight over the deployment of such technologies in line with the permitted purposes, these respondents say.

Even where national legislation limits the use of RBI systems, respondents are concerned over the relative ease with which the systems could be used beyond the currently permitted purposes and the resulting risk of function creep. Once an RBI system is in place, some civil-society respondents note, its existence encourages the introduction of additional purposes, whether the initiative comes from practitioners based on law enforcement utility, from policymakers responding to perceived and sometimes quickly shifting public security needs or from private sector entities offering such technologies. This makes it important to observe the principle of purpose limitation and ensure that a distinct legal basis is introduced for any new purpose, one respondent highlights.

The small-scale survey among people in public places also confirmed that survey respondents are mainly concerned about the abuse of the system by police for other purposes. As reported in [Section 2.1](#), most often people were concerned that the data captured are used for other purposes.

Some law enforcement deployers explicitly warned against extending the use of technologies they work with, stating that their deployment under different conditions or use in combination with different datasets could significantly impact their performance and compromise their accuracy.

Some of the tools deployed offer functionalities that go beyond what is expected and authorised in a given context. For example, the facial recognition module of the system used in one Member State can be used on mobile devices, allowing police officers to use the system directly in the field. While officers of one police force were authorised to use this functionality, another police force blocked the use of the system on mobile devices to prevent misuse during patrols. At the same time, officers of the latter police force could send photos to colleagues, who could run the photo through the FRT system immediately, as long as the comparison took place in the context of ongoing judicial investigations. This difference between what is technically feasible and what is legally permitted can potentially leave more room for irregular consultations of the system, some respondents say. Furthermore, while such use might also be permitted under the AI Act (e.g. to identify a person suspected of having committed a serious criminal offence), such ‘near-real-time’ cases – in which RBI is used within a very short time after, for example, taking a picture of a person – illustrate the challenge posed by the categorisation of real-time and retrospective RBI. Similar questions about the interpretation of the requirement of a ‘significant delay’ under the AI Act to avoid the categorisation of real-time RBI ⁽¹⁰⁶⁾, were shared by some interviewees in relation to the Centrale Automatische Technologie voor Herkenning (CATCH) system in the Netherlands, for example in cases of urgency such as an ongoing terrorist attack, when the comparison with data in the system might need to be made as soon as possible. Some civil-society respondents and law enforcement deployers consider that this lack of clarity undermines the effectiveness of legal safeguards applicable to the use of RBI systems.

A distinct area of concern relates to the risk that RBI systems could be abused by individual users. Here, law enforcement respondents highlight the existence of safeguards to prevent such cases, including limiting the use of the system only to selected staff, the requirement of a separate authorisation for each use, or the monitoring and traceability of each use (see also [Section 2.6](#)). Furthermore, as underlined by one law enforcement respondent, police generally exercise self-restraint when using available tools, aware of both the sensitivity surrounding their use and the limitations of the tools.

The police apply political choices: just because people are not happy does not mean we should stop police from using or developing certain tools.

Law enforcement officer

It is very important to be very aware and to monitor the purpose limitation in any system, because, once there is an infrastructure available, the temptation to use the infrastructure for other reasons is there, and the use of that system could be extended to, for example, wanted persons or missing persons. All these purposes, however, would have to have different grounds.

Civil-society respondent

The question to ask is therefore what is the difference between processing data in real time and processing it 10 minutes later?

Civil-society respondent

There's a certain reality to policing: when there isn't enough control or training for officers, there are risks for fundamental freedoms, because biases aren't corrected, and most operators aren't in a position to see that there's an error.

Civil-society respondent

It is impossible to limit technologies to legal and technical guarantees: the abuse of power is intrinsic. This technology is bound to be abused. These risks are very real when it comes to databases.

Civil-society respondent

Transparency and control safeguards ... are essential to prevent the system from being misused ... The system could be easily exploited for unintended purposes without leaving evidence.

Civil-society respondent

At the same time, both law enforcement and civil-society respondents acknowledge that some cases of abuse occur. Some respondents in France referred to the scrutiny by data protection bodies, courts and the media of the use of the Briefcam algorithmic video analysis software by law enforcement agencies (¹⁰⁷). In a 2024 report, law enforcement oversight bodies established that, while the use of the system was limited to criminal investigations and subject to authorisation, this could not fully prevent abuse (¹⁰⁸). Other respondents offered practical examples of when facial recognition software has been used either by unauthorised officers or against persons not involved in criminal investigations. For example, in a French immigration case, naturalisation was rejected based on the illegal consultation of a *Traitement d'antécédents judiciaires* (TAJ) file (¹⁰⁹). Even though such cases of abuse – which can range from using the systems beyond their authorised purposes to consultation of files for personal gain – are not unique to RBI systems and could be committed even through 'traditional' means, the question of to what extent technology can facilitate and amplify the impact of such abuse on fundamental rights should be considered.

In this context, some civil-society and oversight respondents also note that law enforcement officers do not always rely on officially approved tools but also experiment with publicly available facial recognition tools or use unauthorised channels for sharing images, bypassing any applicable safeguards. Such cases also risk negatively affecting public trust, some respondents highlight.

Besides the purposes for which they can be consulted, the scope of use of RBI systems is determined by the data used for consultation or contained in reference databases. In general terms, the impact on fundamental rights and the risk of going beyond permitted purposes is lower in the case of clearly determined reference databases that are limited in their scope to the objective for which the system is used, such as criminal databases in the case of combating serious crime.

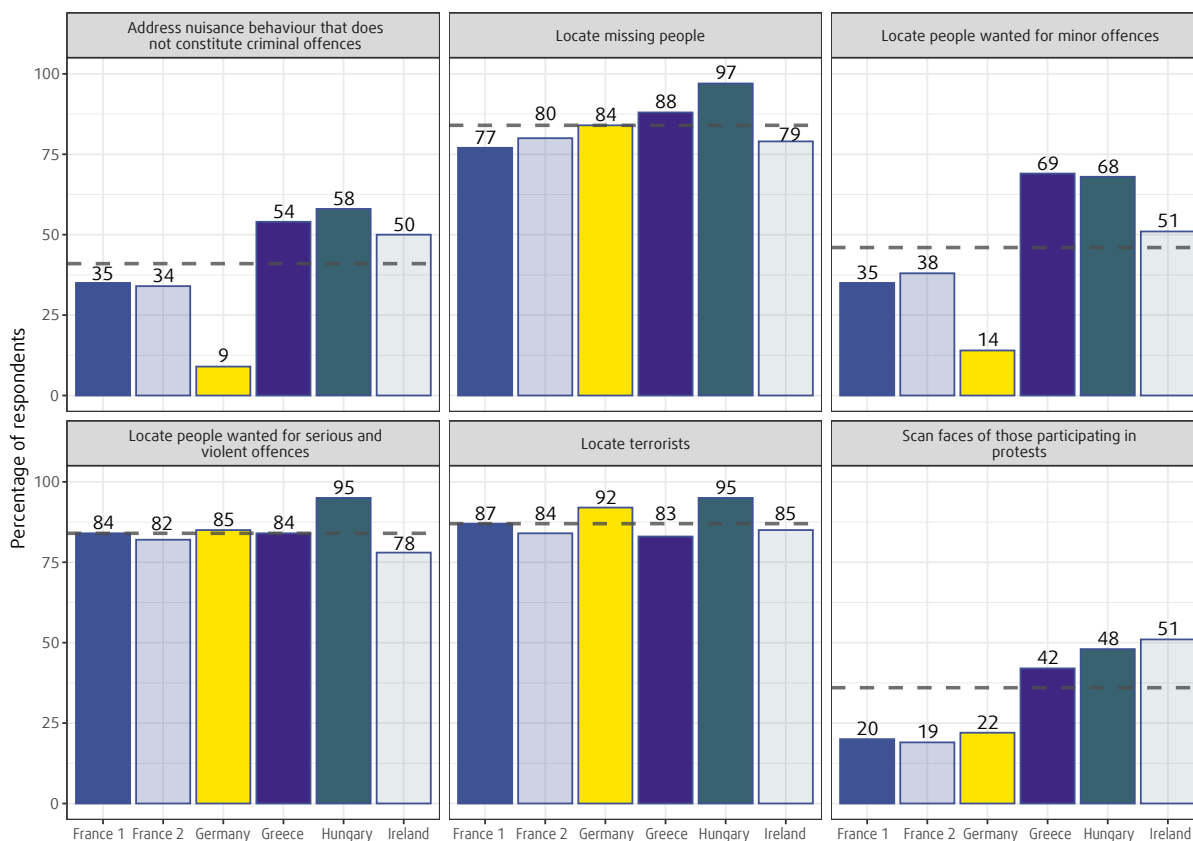
In this context, respondents particularly from civil society and oversight bodies raised several concerns. One relates to the use of broad or insufficiently clearly defined reference databases against which collected biometric data are compared. Respondents in the Netherlands, for example, highlight that CATCH works not only with a database of suspects and convicted perpetrators but also with a large database of facial images of third-country nationals (although the use of the latter is subject to stricter purpose limitation and accompanying safeguards). Respondents across the Member States covered mentioned the lack of clarity as to which databases or watch lists may be consulted or which persons can be included in them and on what basis, with one civil-society respondent expressing concerns over the increasing interoperability of police and other security databases and the 'sneak deployment' of FRT through these interconnected files. In this regard, another respondent recalled that law enforcement agencies in some Member States have expressed interest in including social media images in reference databases.

Findings also show concerns relating to the grey area of using privately held data, such as recordings from CCTV cameras, smart doorbells and similar devices, in the context of RBI. This, according to respondents, raises not only privacy issues but potentially also data quality and accountability issues.

Finally, there appears to be a degree of correlation between transparency in the use of RBI systems and concerns over its potential abuse. Here, some respondents say that the unwillingness of authorities to provide information about how and when the systems are deployed does not give a guarantee that they are used as envisaged in the law and that all safeguards are respected.

The small-scale survey also confirms that people have varying levels of acceptance of the use of RBI technology for different purposes. When asked about purposes for which the police should be able to use FRT in public places, the majority of respondents agreed with respect to locating terrorists (87 %), closely followed by locating people wanted for serious and violent offences (84 %) and locating missing persons (84 %). Far fewer respondents agreed to such use for the purposes of locating people wanted for minor offences (46 %) and addressing nuisance behaviour (41 %). The greatest opposition is to the use of FRT to scan the faces of people participating in protests, with which 36 % of respondents would agree. **Figure 6** shows these results, including the variation across Member States covered. The largest variation in the results across Member States is about using the technology for minor offences and nuisance behaviour.

FIGURE 6 PEOPLE AGREEING WITH THE USE OF FACIAL RECOGNITION TECHNOLOGY IN PUBLIC PLACES, BY PURPOSE OF USE AND MEMBER STATE (%)



Notes: N = 1 054. Question: Do you think that the police should be able to use facial recognition technology in public places to ... ?

In France, the survey was carried out in two waves, one during the 2024 Olympics and another afterwards, denoted as France 1 and France 2 respectively.

Source: FRA, 2026.

Furthermore, people see differences in the permissibility of RBI use according to its place of use. When being asked about places at which FRT should be allowed, most respondents agreed with its use at public transport stations (73 %), followed by banks and financial institutions (68 %), large sports venues, such as stadiums (68 %), and public roads and squares (65 %). People would least often agree with its use at leisure places, such as cinemas, theatres,

museums, concerts and conference halls (41 %) and shops, restaurants or cafés (39 %).

2.5. RISK OF SURVEILLANCE AND SOCIAL HARM

A key concern arising from the fieldwork is that deploying remote biometric technologies in public spaces amounts to general and indiscriminate surveillance. Such arguments are not new and have been voiced repeatedly by civil society⁽¹¹⁰⁾. Besides a direct impact on a wide range of rights, a sense of being under surveillance can have a less direct but potentially broader impact by dissuading individuals from exercising their rights, known as the ‘chilling effect’⁽¹¹¹⁾.

Numerous civil-society and oversight respondents emphasised the impact on the right to private life in this context. As outlined in the FRA paper on FRTs⁽¹¹²⁾, the rights to respect for private life and data protection are central in this regard. Granting individuals a personal sphere in which they can freely develop their personalities, think and shape their opinions is an essential prerequisite for the exercise of other rights. Importantly in this context, a reasonable expectation of privacy applies even in public spaces, referring to the extent to which people can expect privacy without being subjected to surveillance⁽¹¹³⁾.

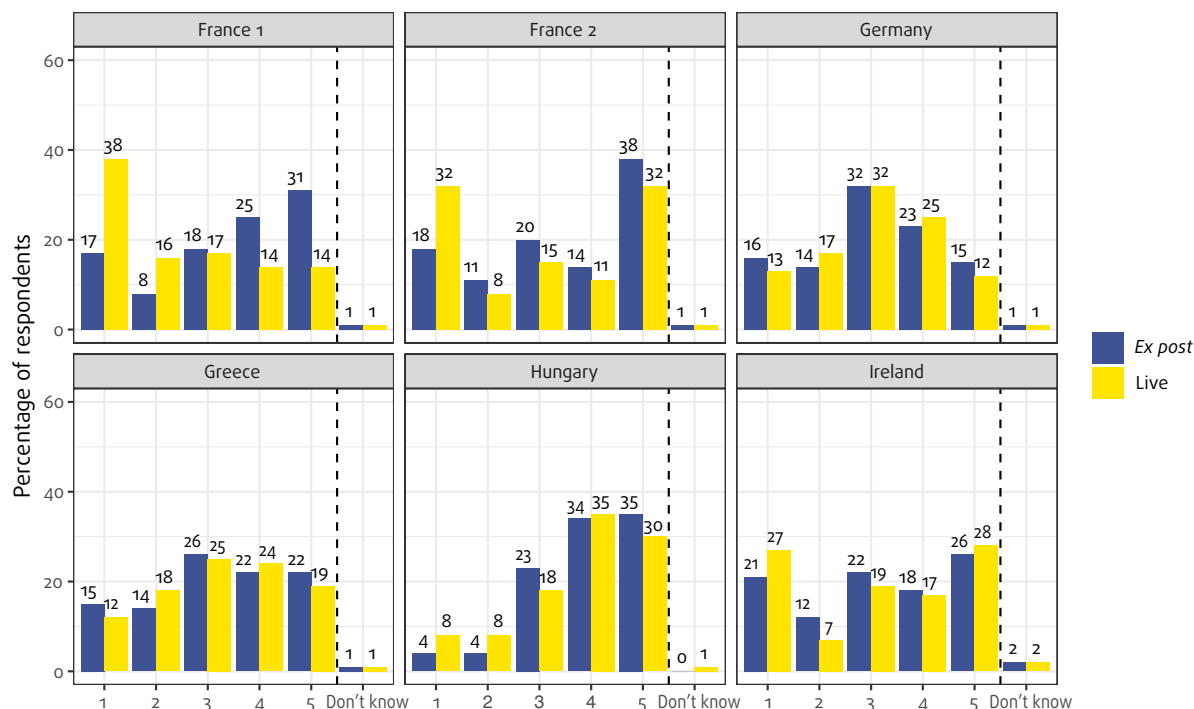
Respondents confirm this, stating that public anonymity is a precondition for the enjoyment of rights in public spaces, ranging from the freedom of expression and information, freedom of assembly and of association, freedom of thought, conscience and religion, and freedom of movement. In some Member States, frameworks are in place to safeguard these rights and freedoms, such as the Hellenic Data Protection Authority’s prohibition on using cameras in places of assembly, like restaurants or theatre foyers, unless there is a security reason for doing so⁽¹¹⁴⁾. Some civil-society respondents highlighted the importance of considering the aggregate effect of the entire surveillance infrastructure, especially in urban areas, and its transformative impact on policing and society. In this context, one respondent notes that the term ‘mass surveillance’ is appropriate, given also that the use of FRTs goes hand in hand with reliance on large reference databases.

The survey carried out with people in public places shows how comfortable people are with the use of FRT on a scale from 1 to 5, where 1 means ‘not at all comfortable’ and 5 means ‘comfortable’. Respondents were asked about their level of comfort with live (real-time) and *ex post* FRT. **Figure 7** shows the results by Member State. Overall, people tend to feel rather comfortable with the use of FRT. They feel slightly more comfortable with *ex post* FRT but there is no great difference from levels of comfort with live FRT.

France is the only Member State where respondents draw a real distinction between live and *ex post* FRT, with respondents feeling considerably less comfortable with live FRT. Respondents in Hungary, overall, tend to feel most comfortable with the use of both live and *ex post* FRT.

Overall, there is no gender difference in the level of feeling comfortable with live or *ex post* FRT, and no marked difference by minority status was observed either. Older respondents feel more comfortable with the use of FRT, as do those who believe it is already used in the Member State where they were surveyed. People interviewed in public spaces felt on average less comfortable with the use of FRT and people interviewed close to sports stadiums felt more comfortable. This may be linked to the context of use; it may be more acceptable in the context of large sports events than in public spaces as such.

FIGURE 7 FEELING COMFORTABLE WITH THE USE OF LIVE AND EX POST FACIAL RECOGNITION TECHNOLOGY, BY MEMBER STATE (%)



Notes: $N = 1\,054$. Question: How comfortable are you with the police using facial recognition technologies in public places in the following two different ways?

- Live identification, through real-time detection using camera surveillance in public places.
- Scanning recorded images or videos to identify people in public places at a later time.

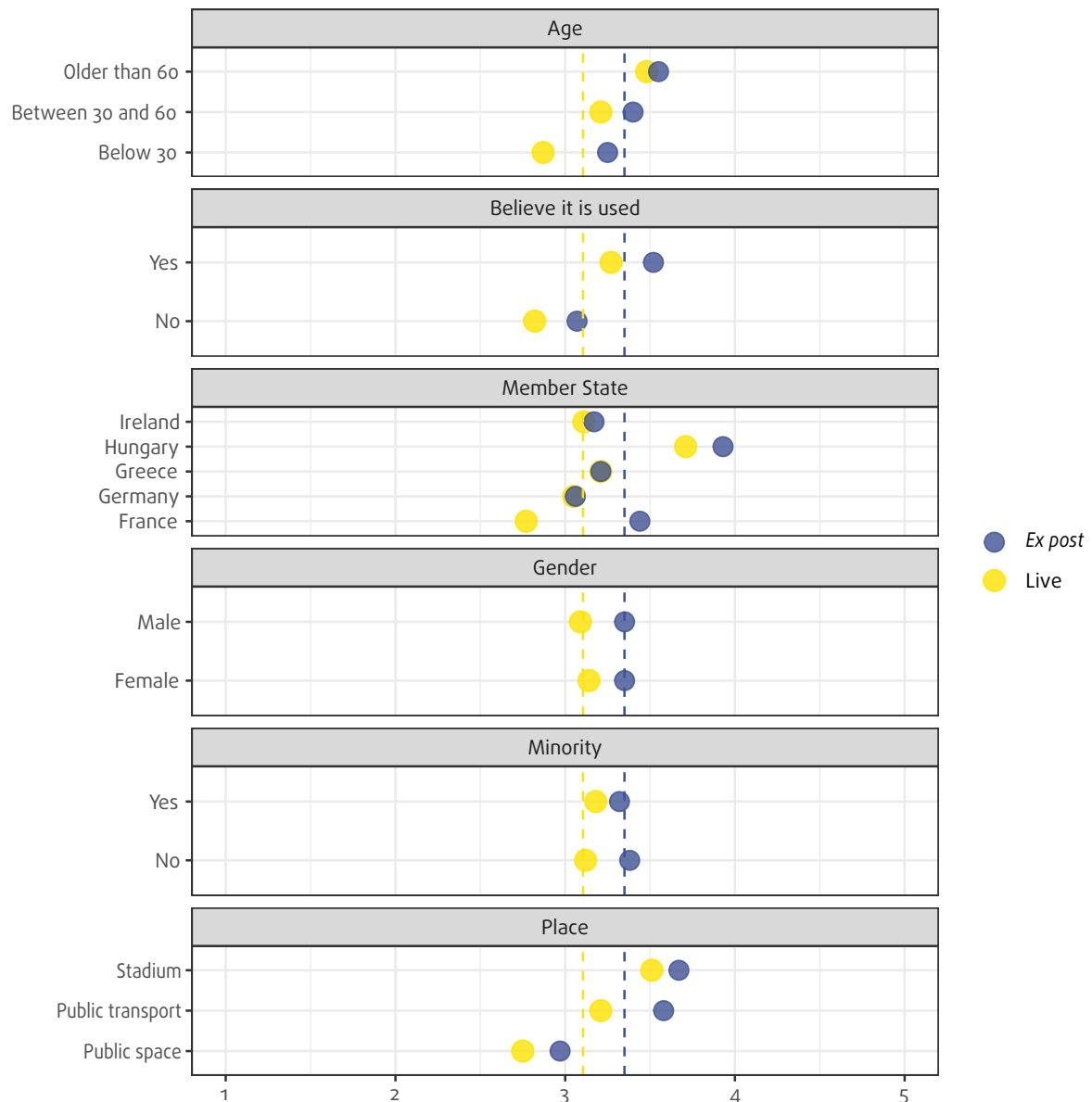
1 = not at all comfortable; 5 = comfortable.

In France, the survey was carried out in two waves, one during the Olympics 2024 and another afterwards, denoted as France 1 and France 2.

Source: FRA, 2026.

While a considerable share of respondents tend to feel comfortable with the use of FRT in public spaces, it is very important to highlight that there is always a share of respondents who do not feel comfortable at all with the use of FRT (see [Figure 7](#)). This is more than one third of respondents in France with respect to live FRT. Across all respondents, 22 % (i.e. more than one in five) are not at all comfortable with live FRT, and 16 % are not at all comfortable with *ex post* FRT.

FIGURE 8 SURVEY RESPONDENTS FEELING COMFORTABLE WITH THE USE OF LIVE AND EX POST FACIAL RECOGNITION TECHNOLOGY



Notes: $N = 1\,054$. Question: How comfortable are you with the police using facial recognition technologies in public places in the following two different ways?

- Live identification, through real-time detection using camera surveillance in public places.
- Scanning recorded images or videos to identify people in public places at a later time.

1 = not at all comfortable; 5 = comfortable.

In France, the survey was carried out in two waves, one during the Olympics 2024 and another afterwards, denoted as France 1 and France 2.

Source: FRA, 2026.

Specific concerns arise when it comes to the use of RBI systems during mass events, research findings show.

Articles 11 and 12 of the Charter – and the corresponding provisions of the ECHR (Articles 10 and 11) ⁽¹¹⁵⁾ – guarantee everyone the freedom of expression and the freedom of peaceful assembly. Risks to the freedoms of expression and assembly are considered especially high when it comes to

demonstrations and protests, a concern also reflected in ECtHR case-law ⁽¹¹⁶⁾, national jurisprudence ⁽¹¹⁷⁾, international standards for police use of technology at protests ⁽¹¹⁸⁾ and recent academic research ⁽¹¹⁹⁾, as well as work done by oversight bodies in some Member States on this topic ⁽¹²⁰⁾. In the context of the AI Act, questions arise over the compatibility of using RBI systems during demonstrations and similar mass events. While such use to identify peaceful participants per se is arguably allowed neither under the AI Act nor under EU data protection and fundamental rights law, permitted exceptions under the AI Act's Article 5(1)(h) and (2) from the prohibition of using real-time RBI can occur in this context. The same applies to *ex post* RBI use for law enforcement purposes.

Respondents from civil society and oversight bodies noted that use during demonstrations opens up a significant risk of the abuse of RBI systems against political opponents or, more generally, against people expressing critical views of the government.

In this respect, an oversight body respondent noted that, where activists, demonstrators or journalists are already under enhanced law enforcement scrutiny, RBI systems can magnify the degree of such misuse. In another example, a respondent described a case where photos taken during a demonstration were subsequently matched by law enforcement agencies with profile photos from social media accounts associated with an environmental movement to identify the participants. This illustrates a point raised by some respondents, namely that the fundamental rights implications of *ex post* RBI systems should not be automatically seen as less than those of real-time RBI, given that they make it possible to identify individuals – such as participants at protests – even years later, causing a lasting impact on their rights.

Another related yet distinct concern is the potential disproportionate impact on certain communities, in conflict with the prohibition of discrimination (Article 21 of the Charter). In this regard, civil-society respondents across the Member States covered in the fieldwork research highlighted that marginalised communities that are already at a higher risk of being subject to police checks will be affected more where these checks involve the use of RBI systems. People with an uncertain legal status or individuals with political opinions that are considered unfavourably by the government are likely to be affected more by such technology during demonstrations. Oversight respondents warned of the potential conflict with the prohibition of racial profiling and the aggregate effect of the use of RBI together with the overall changing political climate in some Member States.

The long-term chilling effect of the use of RBI systems – particularly FRT in public spaces – was mentioned as a serious concern by a number of respondents, which goes hand in hand with the more immediate impact of its use ⁽¹²¹⁾. In relation to freedom of assembly and freedom of expression, the awareness of being monitored can translate into hesitation to participate in demonstrations and political protests, and more general self-censorship and modifying one's behaviour in public for fear of potential repercussions. This effect can be greater not only among people who already distrust authorities, but also among those already singled out in national security, migration and policing discourses, and communities already impacted by counterterrorism legislation and other measures, a topic also explored in earlier FRA research ⁽¹²²⁾.

Importantly, such an effect does not necessarily require that the RBI tools are actually deployed, if people believe that this might be the case and their images may be captured and processed, for example due to the presence of police with technology such as cameras and drones during events.

It is the combination of all these developments. You may have facial recognition. You cannot cover yourself up. The demonstration might be considered illegitimate. We worry that demonstrators are not treated equally, dependent on the nature of the protest. You should look at these developments together. It is probably easier for me to go and demonstrate as a white person with a [local] passport than others with different profiles.

Respondent from an ombudsperson

When surveillance methods are not transparent, individuals may view them as a deterrent due to the mere possibility of being watched, similar to how people react to non-functional CCTV cameras.

Civil-society respondent

Once a real-time RBI system is installed in public, there are virtually no measures that can mitigate the harm to freedom of assembly and expression, as people will avoid expressing their opinions publicly once they know that the police are using the RBI system.

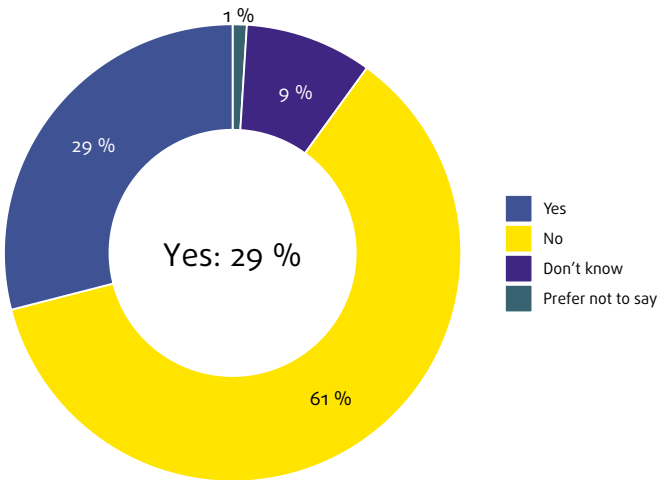
Respondent from a data protection authority

According to civil-society respondents, this underlines the need for greater transparency about the use of RBI systems and serves as an important argument that the conditions for using such technologies should be clearly stipulated by law and individual deployments should always be subject to authorisation.

One civil-society respondent and one law enforcement deployer expressed doubts about the presence of a chilling effect because of the use of RBI systems, noting that people are already used to the presence of different camera systems, and thought that the effect should rather be a sense of enhanced security. As outlined above in **Section 2.1** with respect to the small-scale survey results, 29 % of survey respondents indicated that the use of RBI technologies, such as FRT, by the police would negatively affect their decision to attend public events or protests. **Figure 9** visualises this result.

There are important differences in the survey results with respect to who is mainly negatively affected. Most notably, people who identify themselves as ethnic minorities in the Member State where they were interviewed said more often that they would not attend public events or protests. Although ethnic minority respondents would not feel less comfortable overall with the use of RBI, the percentage of those who indicated that it negatively affects their decision to attend public events or protests is considerably higher, at 40 %. In Hungary, the percentage of those for whom the use of RBI would negatively affect their decision to attend public events or protests is considerably higher than in other Member States where the fieldwork took place: 47 % of respondents indicated that the use of such technology would negatively impact their decision to attend events or protests. Moreover, across all Member States surveyed, those who are politically more active would be more often deterred from attending events or protests, as would those who have less trust in the police.

FIGURE 9 CHILLING EFFECT OF REMOTE BIOMETRIC IDENTIFICATION ON ATTENDING PROTESTS (%)



Notes: *N* = 1 054. Question: Would police use of remote biometric identification technologies, such as facial recognition technology, negatively affect your decision to attend public events or protests?

Source: FRA, 2026.

2.6. EXTERNAL OVERSIGHT AND EFFECTIVE REMEDIES

Oversight is a means of ensuring public accountability for the decisions and actions of security agencies ⁽¹²³⁾. It is aimed at (1) avoiding abuse of power, (2) legitimising the exercise of intrusive powers and (3) achieving better outcomes after an evaluation of specific actions ⁽¹²⁴⁾. Oversight mechanisms help ensure that RBI tools used for law enforcement purposes have a basis in law, are strictly necessary to achieve the well-circumscribed legitimate aims and are not excessive in relation to the objective pursued (are proportionate). They also contribute to holding law enforcement agencies using RBI tools accountable for their actions, increase public trust and encourage the development of effective internal safeguards within investigating authorities.

Under EU law, however, Member States continue to hold considerable autonomy in organising their oversight schemes of domestic law enforcement (and surveillance – see **'FRA activity: focus on surveillance by intelligence services'**) activities as per Article 4(2) of the TEU, which recognises that the Union must 'respect [Member States'] essential ... functions, including ... maintaining law and order and safeguarding national security[, which] remains the sole responsibility of each Member State'. Still, the ECtHR has expressed a preference for judicial oversight of surveillance, but it is not (yet) a requirement if appropriate safeguards are in place ⁽¹²⁵⁾.

FRA ACTIVITY

Focus on surveillance by intelligence services

The impact of surveillance by intelligence services on fundamental rights was the subject of FRA research requested by the European Parliament, which resulted in two reports, the second of which was updated after six years. The first provided a legal analysis of the situation across the EU (2015) ^(a), whereas the second focused on fundamental rights safeguards, oversight and remedies (2017) ^(b) and was updated by way of a third report in 2023 ^(c). The FRA surveillance reports focused on the activities of intelligence services in the context of large-scale surveillance (or 'general surveillance of communications'). They did not address law enforcement authorities' investigation of concrete criminal offences. The present report, on the other hand, looks at how national law enforcement authorities use RBI systems for the prevention, detection and investigation of (serious) criminal offences. The analysis of issues related to remedies and oversight (**Section 2.6**) does not cover the activities of intelligence services. However, some issues arise in both contexts, for example the effectiveness of remedies against measures that have not been communicated to the individual, or the capacity of oversight bodies to effectively scrutinise certain measures.

^(a) FRA, *Surveillance by Intelligence Services: Fundamental rights safeguards and remedies in the EU – Volume I: Member States' legal frameworks*, Publications Office of the European Union, Luxembourg, 2015.

^(b) FRA, *Surveillance by Intelligence Services: Fundamental rights safeguards and remedies in the EU – Volume II: Field perspectives and legal update*, Publications Office of the European Union, Luxembourg, 2017.

^(c) FRA, *Surveillance by Intelligence Services – Fundamental rights safeguards and remedies in the EU – 2023 update*, Publications Office of the European Union, Luxembourg, 2023.

The oversight of AI-powered tools such as RBI systems is now reinforced under EU law. The AI Act obliges Member States to designate market surveillance authorities, which are the competent national data protection supervisory authorities for such AI systems (see also **Section 1.1.1**). Their responsibilities will extend to prohibited uses of AI as per Article 5(1) of the AI Act, including prohibited forms of RBI, and the authorisation of permitted real-time RBI surveillance in accordance with the joint reading of Article 5(1)(h) of and Annex II (list of criminal offences) to the AI Act.

As concerns the practice of oversight of the use of RBI tools by law enforcement authorities, interviewees from various law enforcement authorities confirmed that some structures and processes are already in place. One example is where particular attention is paid internally, within the national police force, to the permitted use of the RBI technology to support criminal investigations, including by means of unannounced checks. Another example showcases a well-defined chain of control and a training scheme, coupled with the monitoring power of disciplinary bodies involved, whereby authorised users might be asked to justify any individual prompting of the facial recognition system and prove it took place in the context of an ongoing criminal investigation. As a third example in place in another Member State, a report is drawn up each time the facial recognition system connected to the large national reference database is used, which is then reviewed by an internal committee. Interviewed data protection authorities and civil-society organisations described limitations in providing consistent oversight, as dedicated oversight bodies are often constrained in resources and technical and legal expertise and by their mandate. A law enforcement respondent noted that more human resources in the police oversight body would enable better systematic detection of misuse and breaches of law while using the face recognition tool. As a civil-society respondent put it, '[t]here is a gap between what is at stake and what is needed.'

A further issue is the lack of visibility and/or transparency of a law-enforcement-related RBI operation to oversight bodies, which undermines the rationale of oversight. Restricted access for oversight bodies limits a full understanding of the RBI systems and consequently restricts their assessment from a fundamental rights perspective ⁽¹²⁶⁾. This also means that many other forms of investigations, such as those initiated by civil society and the media, occur outside official oversight arrangements (e.g. in the case of the SARI real time RBI system in Italy). In addition, law enforcement respondents in



one Member State noted that conducting oversight becomes cumbersome in practice if, due to administrative convenience, managers assign the same rights of access to the facial recognition tool to every officer, hence extending access very widely. This can also be a source of abuse (for more, see [Section 2.5](#) above). Although supervisors should oversee the use of the face recognition tool within the police, systematically doing so is practically impossible due to the very large number of queries using the mobile device with built-in facial recognition functionalities. The same law enforcement respondents added that a potential future improvement to prevent misuse would be a tool detecting unusually large numbers of queries in the facial recognition system. Further possible improvements in oversight include systematically conducting data protection impact assessments and periodically reassessing the risks identified initially (e.g. through monitoring), an interviewed national data protection authority underlined. Inactivity can be another hurdle to overcome. While some civil-society respondents found existing frameworks sufficient for effective oversight, they recommended more proactive approaches by national data protection authorities and other oversight bodies.

The foregoing also elevates the importance of effective access to remedies in cases of wrongful conduct and breaches of (substantive) fundamental rights by law enforcement authorities deploying RBI systems. Article 47 of the Charter and Articles 6 and 13 of the ECHR guarantee the right to an effective remedy and to a fair trial. Article 47 of the Charter extends beyond criminal procedures and covers all types of procedures, together with the requirement that the remedy sought must be before a judge. This fundamental right, which applies horizontally, empowers individuals to challenge a measure affecting any right conferred on them by EU law before a court of law and not only in respect of the fundamental rights guaranteed in the Charter ⁽¹²⁷⁾. Access to effective judicial remedies must also cover decisions taken with the support of RBI technologies used for law enforcement purposes, for example when a measure (e.g. a police stop or treating someone as a suspect) has significantly been informed by the use of an RBI system ⁽¹²⁸⁾.

With respect to the specific context of this study, the LED confirms that the right to an effective judicial remedy must be provided in relation to decisions made by the controller or the processor as well as the supervisory authority ⁽¹²⁹⁾. Data processed by RBI tools for law enforcement purposes are no exception. For instance, people may want to challenge why their facial images have been included in reference databases or watch lists; to know why RBI has taken place in a non-transparent way and even without their consent; or to seek redress for a false positive match that entailed negative consequences for them (e.g. in the form of an unlawful police stop, search or arrest), including seeking compensation for any damage suffered ⁽¹³⁰⁾.

The use of AI-powered RBI tools by law enforcement agencies can challenge the right to an effective remedy in various ways.

Given the remote nature of identifying an individual by means of their biometric characteristics, it may not be obvious to people that their fundamental rights may have been breached if they do not know that the technology has been used. A precondition for exercising the right to an effective (judicial) remedy is that the person must be aware that their biometric identifiers (e.g. facial image, voice) are processed. Therefore, one particular issue relates to the notification of the RBI system's use, its (potential) harm and the role of adjudicators in identifying and remedying such harm. The CJEU has already noted, in the context of security measures affecting the right to private life and the right to the protection of personal data, that national law enforcement authorities must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer capable of jeopardising

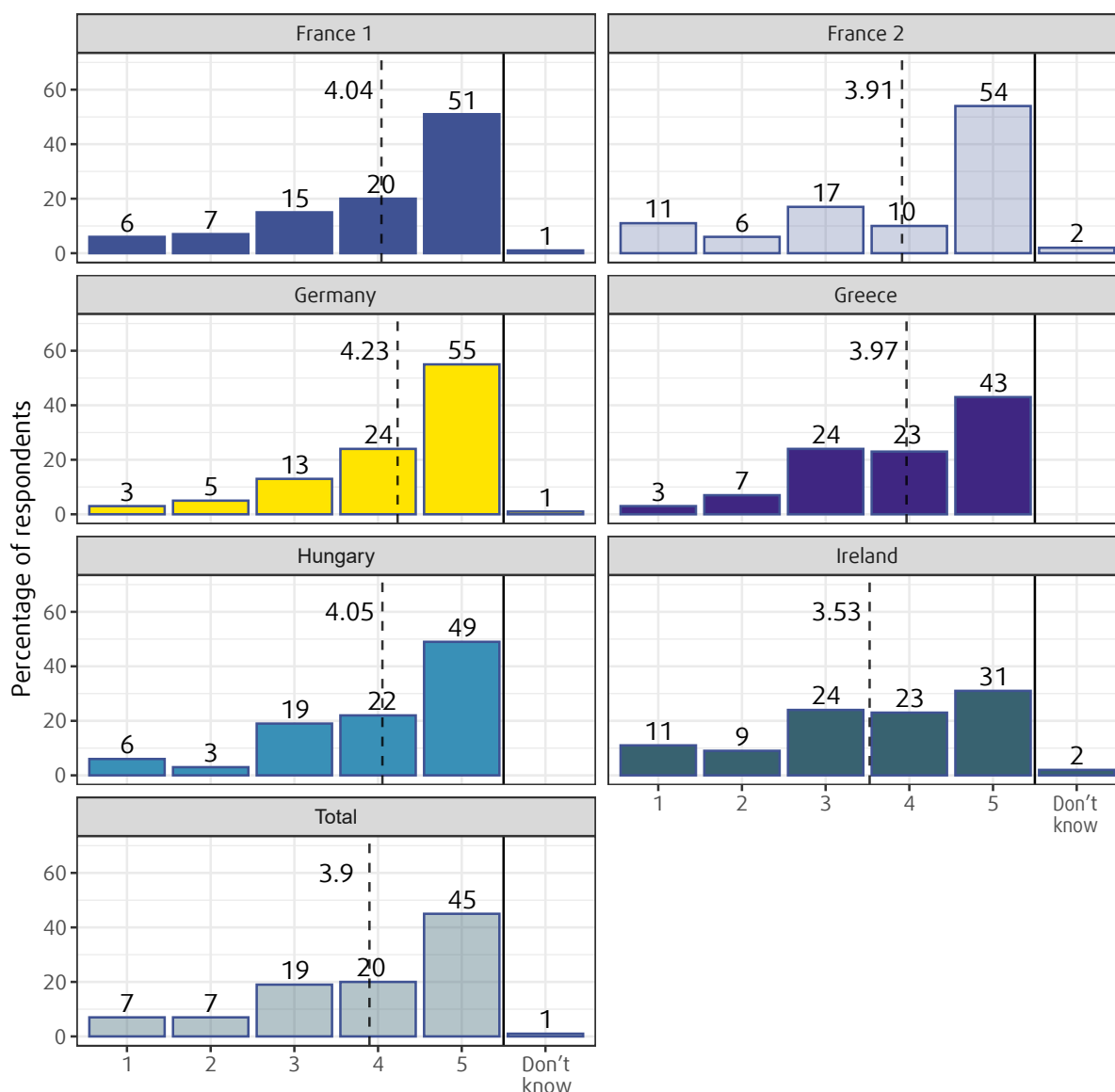
the investigations undertaken by those authorities ⁽¹³¹⁾. This notification is necessary to enable those affected by such measures to exercise their right to a legal remedy guaranteed in Article 47 of the Charter ⁽¹³²⁾.

Another prominent concern for statutory human rights bodies, civil society and academia is the lack of transparency in the use and operation of such AI-driven technologies. Algorithmic and AI-driven decision-making is often opaque: collecting biometric data, training algorithms, and the effectiveness and error rates of the algorithm, among other aspects, are often not transparently reported. Without access to this information, affected individuals may not be able to defend themselves, assign responsibility for the decisions affecting them ⁽¹³³⁾, appeal against any decision negatively affecting them or have a fair trial, which includes the principle of equality of arms and adversarial proceedings as established by the ECtHR ⁽¹³⁴⁾. These requirements also form part of the corresponding Charter right (Article 47) in view of Article 52(3) of the Charter. The CJEU has already warned of the potential of AI-driven law enforcement tools (e.g. the ones in air passenger name record systems to prevent and detect terrorist attacks and other forms of serious crime) to deprive individuals of the right to an effective judicial remedy. In *Ligue des droits humains*, the CJEU found that the ‘opacity’ of AI technology might make it ‘impossible to understand the reason why a given program arrived at a positive match’ ⁽¹³⁵⁾. People affected by such AI-powered tools must be thus able to understand ‘how ... those programs work’ to allow them to decide ‘with full knowledge of the relevant facts’ ⁽¹³⁶⁾ whether or not to challenge the unlawful outcome or decision reached by the law enforcement agency.

Additional challenges are that it is difficult for affected persons to rebut a result that is significantly informed by an RBI tool and that courts might not be in a position to provide an effective remedy in such cases at present, given that judges currently lack knowledge of and expertise in these matters, among other factors ⁽¹³⁷⁾.

The relevance of the right to an effective (judicial) remedy is also supported by the results of the small-scale survey. The majority of respondents completely agree with the statement that ‘facial recognition technology should only be used in public places where people are informed of its use and purpose’. On a scale from 1 to 5, where 1 means completely disagree and 5 means completely agree, about two thirds (65 %) selected 4 or 5. Agreement is particularly high among respondents in Germany and Hungary, as shown in **Figure 10**.

FIGURE 10 INFORMING PEOPLE OF THE USE AND PURPOSE OF FACIAL RECOGNITION TECHNOLOGY, BY MEMBER STATE (%)



Notes: $N = 1\,054$. Question: To what extent do you agree or disagree that if facial recognition technology is used, it should only be used in public places where people are informed of its use and purpose? 1 = completely disagree; 5 = completely agree.

In France, the survey was carried out in two waves, one during the 2024 Olympics and another afterwards, denoted as France 1 and France 2 respectively. The vertical dashed line indicates the average response on the five-point scale, excluding those saying that they don't know.

Source: FRA, 2026.

The AI Act aims to some extent to address the above challenges by introducing a right to obtain a clear and meaningful explanation of the role of AI in individual decision-making from deployers (Article 86). The right can be invoked when the decision of the deployer is based on the output of the AI system and produces legal effects or similarly significantly affects the individual. This right, however, applies with exceptions: notably, it is waived when other pieces of EU or national law provide for exceptions from it or restrict it (Article 86(2)–(3) of the AI Act) ⁽¹³⁸⁾. It is unclear, though, whether

only already existing exceptions or restrictions are permitted (a 'stand-still' clause) or this provision is laying the ground for future carve-outs too, thus permitting further exceptions ⁽¹³⁹⁾. At the same time, the AI Act only provides for limited possibilities of complaint. Under its Article 85, any person can complain about the infringement of the AI Act to market surveillance authorities, which have to handle the complaint in line with their relevant procedures. These complaints may not lead to individual forms of redress. The right to lodge a complaint with market surveillance authorities applies, however, without prejudice to other administrative or judicial remedies. The right to an explanation can, therefore, be used as a basis for exercising remedies afforded under other applicable law, such as EU data protection law ⁽¹⁴⁰⁾.

Some respondents interviewed raised concerns that, although necessary legal avenues are in place, this right is not effectively guaranteed in practice, and that it is often hard to mobilise non-judicial avenues to submit complaints to data protection authorities or ombudspersons about an alleged unlawful use or outcome of RBI tools for law enforcement purposes. It is crucial to note that the possibility of lodging an administrative complaint before a supervisory authority (typically a national data protection authority) as provided for in the EU data protection *acquis*, including the LED (Article 52), is not considered an effective remedy under Article 47 of the Charter. This is because no court is involved in such a review. Such complaint mechanisms can be complementary but cannot replace judicial review with all the guarantees it involves ⁽¹⁴¹⁾.

FRA research revealed that actual recourse to judicial or non-judicial remedies (e.g. by lodging a complaint with the ombudsperson) is scarce. Law enforcement respondents from one Member State reported no complaint against the facial recognition tool used by the police, before either the internal oversight body or the ombudsperson. Similarly, in the case of a discontinued live facial recognition tool used for law enforcement purposes in another Member State, no individual complaint regarding its allegedly non-rights-compliant use was lodged at the national statutory human rights body while the tool was operational. Civil-society respondents from the same Member State considered that, although many tools are legally available to monitor such RBI systems, these structures do not seem to work in practice. In a similar vein, capacity constraints of the data protection authority in another Member State have contributed to there being no closed and publicly available complaints thus far.

The very low number of initiated cases for redress can be attributed to several reasons. One is that the use of RBI systems for law enforcement purposes is not widespread yet. Added to this, some civil-society respondents pointed out that the general public is unaware of how to obtain information about whether they have been subjected to an RBI system used for law enforcement purposes, and is also unaware of the availability of redress mechanisms. In another Member State, the reasons why an ombudsperson has not received any complaint yet about the wrongful use of an RBI tool are that the general public is not informed about it and that potential complainants need to go first through the police complaint mechanism. Similar concerns were raised by civil-society respondents, stressing that it is only at the judicial phase, after indictment, that a person can find out about the evidence collected against them by the police using the facial recognition tool. To tackle this, police authorities should first of all ensure better transparency by communicating about their activities relating to the use of RBI tools, such as FRT ⁽¹⁴²⁾.

Endnotes

- (70) ECtHR, *Gorlov and Others v. Russia*, Nos 27057/06, 56443/09 and 25147/14, 2 July 2019, § 97; *Big Brother Watch and Others v. the United Kingdom* [GC], Nos 58170/13, 62322/14 and 24960/15, 25 May 2021, § 333.
- (71) Article 29 Working Party, '**Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)**', European Commission website, 7 December 2017, p. 7. See also: EDPS, '**EDPS comments to the AI Office's consultation on the application of the definition of an AI system and the prohibited AI practices established in the AI Act launched by the European AI Office**', WW/AP/nc/D(2024)4345 C 2024-0279, 19 December 2024, p. 10.
- (72) Judgment of the Court of Justice of 19 March 2026, *Comdribus*, C-371/24, ECLI:EU:C:2026:219.
- (73) Commission Nationale de l'Informatique et des Libertés (CNIL), **Délibération n° 2024-006**, 18 January 2024, Section I.A.
- (74) **Regulation (EU) 2016/794** of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53, ELI: <http://data.europa.eu/eli/reg/2016/794/oj>).
- (75) Art. 26(10) of the AI Act.
- (76) See also Garante per la protezione dei dati personali, '**Riconoscimento facciale: Sari real time non è conforme alla normativa sulla privacy**', Garante per la protezione dei dati personali website, 16 April 2021; Garante per la protezione dei dati personali, '**Parere sul sistema Sari Real Time – 25 marzo 2021 [9575877]**', Garante per la protezione dei dati personali website, 16 April 2021.
- (77) See, for example, Tracol, X., 'The use of facial recognition technologies by law enforcement authorities in the US and the EU: Towards a convergence on regulation?', *Technology and Regulation*, Vol. 2025, pp. 289–315; Matulionyte, R., 'Transparency of facial recognition technology and trade secrets', in: Matulionyte, R. and Zalnieriute, M. (eds), *The Cambridge handbook of facial recognition in the modern state*, Cambridge University Press, Cambridge, 2024, pp. 60–73.
- (78) See FRA, **Facial Recognition Technology: Fundamental rights considerations in the context of law enforcement**, Publications Office of the European Union, Luxembourg, 2019, pp. 24–25.
- (79) EDPB, **Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement**, Version 2.0, 26 April 2023, p. 27.
- (80) Communication from the Commission – **Commission guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)**, C(2025) 5052 final of 29 July 2025, paras 423 and 424.
- (81) Telefi project, '**Summary report of the project "Towards the European level exchange of facial images"**', Version 1.0, 2021, p. 22. See also the introduction to the present report.
- (82) The percentages add up to over 100 % because multiple answers were allowed, meaning that some respondents thought it is not used because it is not in line with fundamental rights and not ready to be used.
- (83) See, for example, Madiega, T. and Mildebrath, H., **Regulating Facial Recognition in the EU**, PE 698.021, European Parliamentary Research Service, September 2021, p. 2; Minaee, S., Abdolrashidi, A., Su, H., Bannamoun, M. and Zhang, D., '**Biometrics recognition using deep learning: A survey**', *Artificial Intelligence Review*, Vol. 56, 2023, pp. 8647–8695. See also NIST, '**Face recognition technology evaluation (FRTE) 1:N identification**', NIST website, last updated 12 May 2026; NIST, **Ongoing Face Recognition Vendor Test (FRVT) Part 2. Identification**, NIST Interagency/Internal Report (NISTIR), NIST, Gaithersburg, MD, 2018. Improvements of (specific) facial and voice recognition technologies were also mentioned by some FRA interviewees.
- (84) FRA, **Facial Recognition Technology: Fundamental rights considerations in the context of law enforcement**, Publications Office of the European Union, Luxembourg, 2019, p. 9.
- (85) Lynch, N., '**Facial recognition technology in policing and security – Case studies in regulation**', *Laws*, Vol. 13, Issue 3, 2024, 35, p. 6.
- (86) FRA, **Facial Recognition Technology: Fundamental rights considerations in the context of law enforcement**, Publications Office of the European Union, Luxembourg, 2019.
- (87) See also NIST, **Face Recognition Vendor Test (FRVT) Part 3: Demographic effects**, NISTIR, NIST, Gaithersburg, MD, 2019.
- (88) FRA, **Facial Recognition Technology: Fundamental rights considerations in the context of law enforcement**, Publications Office of the European Union, Luxembourg, 2019, p. 10.
- (89) See also Lohr, S., 'Facial recognition is accurate, if you're a white guy', in: Martin, K. (ed.), *Ethics of Data and Analytics*, Auerbach Publications, Boca Raton, 2022, pp. 143–147; and Limanté, A., 'Bias in facial recognition technologies used by law enforcement: Understanding the causes and searching for a way out', *Nordic Journal of Human Rights*, Vol. 42, No 2, 2023, pp. 1–20.
- (90) For a similar list of implicated fundamental rights, see also Commission staff working document – **Impact assessment – Annexes accompanying the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts**, SWD(2021) 84 final, Brussels, 21 April 2021, Annex 5, point 5.5 'Analyses of impacts on fundamental rights specifically impacted by the intervention'.
- (91) See recital 54 to the AI Act.
- (92) Art. 15(3) of the AI Act.
- (93) For more, see FRA, **Data Quality and Artificial Intelligence – Mitigating bias and error to protect fundamental rights**, Publications Office of the European Union, Luxembourg, 2019.
- (94) See also Council of Europe, **Guidelines on Facial Recognition**, Strasbourg, 2021, p. 22; EDPB, **Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement**, Version 2.0, 26 April 2023, p. 51.
- (95) See also EDPB, **Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement**, Version 2.0, 26 April 2023, pp. 14 and 33.
- (96) See also European Data Protection Supervisor, '**Synthetic data**', European Data Protection Supervisor website, 2023.
- (97) Boutros, F., Struc, V., Fierrez, J. and Damer, N., 'Synthetic data for face recognition: Current state and future prospects', *Image and Vision Computing*, Vol. 135, 2023, 104688; Sáez Trigueros, D., Meng, L. and Hartnett, M., 'Generating photo-realistic training data to improve face recognition accuracy', *Neural Networks*, Vol. 134, 2021, pp. 86–94; Qiu, H., Yu, B., Gong, D., Li, Z., Liu, W. and Tao, D., 'SynFace: Face recognition with synthetic data', in: *Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV)*, 2021, pp. 10880–10890.
- (98) Similarly, in the computer science literature, see Makhlof, K., Zhioua, S. and Palamidessi, C., '**When causality meets fairness: A survey**', *Journal of Logical and Algebraic Methods in Programming*, Vol. 141, 2024, 101000.
- (99) See, for example, European Union Agency for Cybersecurity, **ENISA Briefing: Behavioural biometrics**, 18 February 2010, p. 3.
- (100) See Hermes Center for Transparency and Digital Human Rights, '**3. Il riconoscimento facciale su migranti e persone straniere in Italia**', Hermes Center for Transparency and Digital Human Rights website.
- (101) See NIST, '**Face recognition technology evaluation (FRTE) – Part 1: Verification**', 2026.
- (102) See, for example, Stevens, N. and Keyes, O., '**Seeing infrastructure: Race, facial recognition and the politics of data**', *Cultural Studies*, Vol. 35, Issue 4–5, 2021, pp. 833–853.

- (103) Fussey, P. and Murray, D., *Independent report on the London Metropolitan Police Service's trial of live facial recognition technology*, Human Rights Centre, University of Essex, Colchester, 2019, pp. 73–75.
- (104) See, for example, CJEU, Judgment of the Court (GC) of 3 September 2008, *Kadi and Al Barakat International Foundation v Council and Commission of the European Communities*, Joined Cases C-402/05 P and C-415/05 P, ECLI:EU:C:2008:461, para. 363; CJEU, Judgment of the Court (Third Chamber) of 15 November 2012, *Al-Aqsa v Council and Pays-Bas v Al-Aqsa*, C-539/10 P, ECLI:EU:C:2012:711, para. 130; and CJEU, Judgment of the Court (GC) of 8 April 2014, *Digital Rights Ireland and Seitlinger and Others*, C-293/12, ECLI:EU:C:2014:238, para. 42.
- (105) See also the April 2025 amendments (**Act No III of 2025**) to the Hungarian legislation on misdemeanours (**Act No II of 2012**), inserting a new Art. 56(5) into the latter, allowing for broader use of FRT technology by the police. In legal scholarship, the legality of the use of RBI in Hungary has been discussed with another conclusion, see Kis Kelemen, B. and Szijártó, I., *The Hungarian Face Recognition Technology In Light of EU Law*, *Maastricht Journal of European and Comparative Law*, OnlineFirst, 2026.
- (106) Art. 3(42) of the AI Act.
- (107) CNIL, *'Utilisation de BriefCam et d'autres logiciels d'analyse vidéo par l'État et des communes: La CNIL prononce plusieurs mises en demeure'*, CNIL website, 5 December 2024; Disclose, *'The French National Police is unlawfully using an Israeli facial recognition software'*, Disclose website, 14 November 2023; Administrative Tribunal of Grenoble, *Decision of 24 January 2025*, No 2105328.
- (108) France, Ministry of the Interior, *'Usage de logiciels d'analyse vidéo par les services de la police et de la gendarmerie nationales (Briefcam)'*, Ministry of the Interior website, 28 October 2024.
- (109) See Conseil d'État, *'Analyses du Conseil d'État du 16 au 30 avril 2023'*, Conseil d'État website, 9 May 2023.
- (110) See EDRi, *'Global civil society and experts statement: Stop facial recognition surveillance now'*, EDRi website, 26 September 2023.
- (111) For a thorough and meticulous – and theoretical – account of this phenomenon, see Penney, J. W., 'Understanding chilling effects', *Minnesota Law Review*, Vol. 106, No. 2, 2022, pp. 1451–1530.
- (112) FRA, *Facial Recognition Technology: Fundamental rights considerations in the context of law enforcement*, Publications Office of the European Union, Luxembourg, 2019.
- (113) For more details, see FRA, *Facial Recognition Technology: Fundamental rights considerations in the context of law enforcement*, Publications Office of the European Union, Luxembourg, 2019, p. 23. See also Vlaamse Radio- en Televisieomroeporganisatie (VRT), *'Privacy en ik: Documentaire van Tim Verheyden'*, VRT website, 11 March 2021.
- (114) Hellenic Data Protection Authority, Opinion 1/2009 on the operation of CCTV systems in public areas, 24 July 2009.
- (115) On the ECtHR case-law concerning protests from the perspective of the implicated fundamental rights, in particular the freedoms of expression and peaceful assembly, see ECtHR, *Guide on the case-law of the European Convention on Human Rights. Mass protests*, Strasbourg, updated on 28 February 2026, Sections I and II.
- (116) ECtHR, *Glukhin v. Russia*, No 11519/20, 4 July 2023 – applicant arrested for engaging in a protest, first identified by the police using retrospective facial recognition and then arrested after being detected using live facial recognition (case also mentions but does not further engage with chilling effect).
- (117) In this regard, a court in Germany declared illegal the publication on social media of pictures taken at demonstrations, due to its negative effect on the freedom of association (FRA, *Facial Recognition Technology: Fundamental rights considerations in the context of law enforcement*, Publications Office of the European Union, Luxembourg, 2019, p. 30).
- (118) UN Human Rights Council, *'Model protocol for law enforcement officials to promote and protect human rights in the context of peaceful protests'*, A/HRC/55/60, 31 January 2024, para. 71(d); UN Human Rights Council, *'Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests'*, A/HRC/44/24, 24 June 2020.
- (119) Fussey, P. and Murray, D., *Facial Recognition Surveillance – Policing and human rights in the age of artificial intelligence*, Oxford University Press, Oxford, 2025.
- (120) National Ombudsman of the Netherlands, *Protesting, an abrasive fundamental right?*, 2018/015, 14 March 2018.
- (121) See Pech, L., *The Concept of Chilling Effect – Its untapped potential to better protect democracy, the rule of law, and fundamental rights in the EU*, Open Society European Policy Institute, 2021. The precise contours of any chilling effect in surveillance contexts are contested, but research points to its existence. See Penney, J., 'Chilling effects: Online surveillance and Wikipedia use', *Berkeley Technology Law Journal*, Vol. 31, No 1, 2016, pp. 117–182; Stoycheff, E., 'Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring', *Journalism and Mass Communication Quarterly*, Vol. 93, Issue 2, 2016, pp. 296–311; and for a general discussion Murray, D. and Fussey, P., 'Bulk surveillance in the digital age: Rethinking the human rights law approach to bulk monitoring of communications data', *Israel Law Review*, Vol. 52, Issue 1, 2019, pp. 31–60. For a discussion of the chilling effect as applicable to journalists, see ECtHR, *Centro Europa 7 S. R. L. and Di Stefano v. Italy*, No 38433/09, 7 June 2012, § 129. See also Inghilterra, R., 'L'instaurazione d'une «technopolice» administrative en milieu urbain: Les droits et libertés sur un fil', *Revue des droits de l'homme*, No 26, 2024, paras 16 and 17.
- (122) See FRA, *Directive (EU) 2017/541 on Combating Terrorism – Impact on fundamental rights and freedoms*, Publications Office of the European Union, Luxembourg, 2021, p. 9. For other research on this topic, see for example European Network against Racism, *Suspicion, Discrimination and Surveillance: The impact of counter-terrorism law and policy on racialised groups at risk of racism in Europe*, European Network against Racism, 2021.
- (123) Born, H. and Leigh, I., *Making Intelligence Accountable: Legal standards and best practice for oversight of intelligence agencies*, Publishing House of the Parliament of Norway, Oslo, 2005, p. 7.
- (124) Chesterman, S., *One Nation under Surveillance: The new social contract to defend freedom without sacrificing liberty*, Oxford University Press, Oxford, 2011, pp. 208 and 222.
- (125) ECtHR, *Klass and others v. Germany*, No 5029/71, 6 September 1978; ECtHR, *Zakharov v. Russia*, No 47143/06, 4 December 2015; ECtHR, *Big Brother Watch and Others v. United Kingdom*, Nos 58170/13, 62322/14 and 24960/15, 25 May 2021. For more, with various oversight models, see also FRA, *Surveillance by Intelligence Services – Fundamental rights safeguards and remedies in the EU – 2023 update*, Publications Office of the European Union, Luxembourg, 2023.
- (126) Inghilterra, R., 'L'instaurazione d'une «technopolice» administrative en milieu urbain: Les droits et libertés sur un fil', *Revue des droits de l'homme*, No 26, 2024, para. 60.
- (127) EU Network of Independent Experts on Fundamental Rights, *Commentary of the Charter of Fundamental Rights of the European Union*, 2006, p. 360. See also FRA and CoE, *Handbook on European law relating to access to justice*, Publications Office of the European Union, Luxembourg, 2016, p. 92.
- (128) See similarly Council of Europe Commissioner for Human Rights, *Unboxing Artificial Intelligence: 10 steps to protect human rights – Recommendation*, Council of Europe, Strasbourg, 2019, p. 13.
- (129) LED, Arts 53–54.
- (130) LED, recital 88 and Art. 56.
- (131) CJEU, Judgment of the Court (GC) of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, Joined Cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, para. 12. See also, *mutatis mutandis*, Judgment of the Court (GC) of 19 January 2010, *Seda Küçükdeveci v Swedex GmbH & Co. KG*, C-555/07, ECLI:EU:C:2010:21, para. 52;

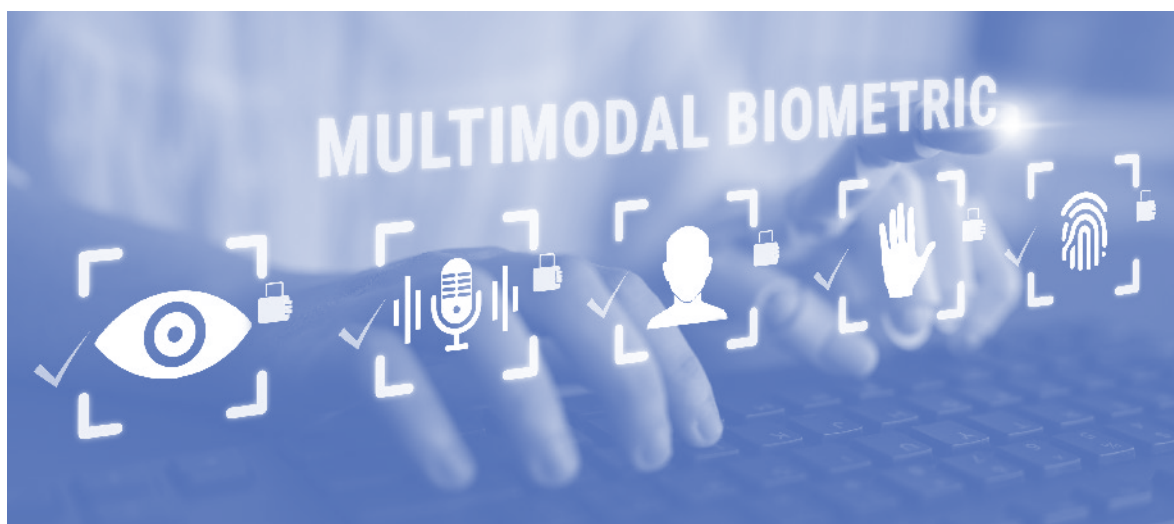
- Judgment of the Court (GC) of 6 October 2015, *Maximillian Schrems v Data Protection Commissioner*, **C-362/14**, ECLI:EU:C:2015:650, para. 95.
- (¹³²) CJEU, Judgment of the Court (GC) of 21 December 2016, *Telez Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, Joined Cases **C-203/15 and C-698/15**, ECLI:EU:C:2016:970, para. 12.
- (¹³³) Yeung, K., ***A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework***, Council of Europe, Strasbourg, 2019.
- (¹³⁴) See ECtHR, *Jespers v. Belgium*, No 8404/78, 15 October 1980; ECtHR, *Saldut v. Turkey*, No 36391/02, 17 November 2008; ECtHR, *Blokhin v. Russia*, No 47152/06, 23 March 2016.
- (¹³⁵) CJEU, Judgment of the Court (GC) of 21 June 2022, *Ligue des droits humains ASBL v Conseil des ministres*, **Case C-817/19**, ECLI:EU:C:2022:491, para. 195.
- (¹³⁶) *Ibid.*, para. 210.
- (¹³⁷) Molnár, T., 'Algorithmic decision-making in migration and security in the EU: Challenges in ensuring effective legal remedies', in: Varju, M. and Mezei, K. (eds), 'The challenges of artificial intelligence for law in Europe', *Data Science, Machine Intelligence, and Law*, Vol. 6, Springer, Cham, 2025, pp. 147–172. See also Inghilterra, R., 'L'instauration d'une «technopolice» administrative en milieu urbain: Les droits et libertés sur un fil', *Revue des droits de l'homme*, No 26, 2024, para. 22.
- (¹³⁸) For an insightful analysis of the right to explanation of individual decision-making under Art. 86 of the AI Act, see for example Kaminski, M. E. and Maltieri, G., '**The right to explanation in the AI Act**', *University of Colorado Law Legal Studies Research Papers*, No 25-9, 2025.
- (¹³⁹) See similarly Jones, C. and Lanneau, R., '**Automating authority: Artificial intelligence in European police border regimes**', Statewatch website, 9 April 2025, Section 2.3.4 'A "silicon curtain" of secrecy'.
- (¹⁴⁰) On the latter point, see Kaminski, M. E. and Maltieri, G., '**The right to explanation in the AI Act**', *University of Colorado Law Legal Studies Research Papers*, No 25-9, 2025, p. 20.
- (¹⁴¹) Molnár, T., 'Algorithmic decision-making in migration and security in the EU: Challenges in ensuring effective legal remedies', in: Varju, M. and Mezei, K. (eds), 'The challenges of artificial intelligence for law in Europe', *Data Science, Machine Intelligence and Law*, Vol. 6, Springer, Cham, 2025, pp. 147–172.
- (¹⁴²) See, for example, the short video prepared by the Swiss Federal Police informing the general public of the use of FRT for law enforcement purposes: Swiss Federal Police fedpol, '**AFIS2026 und Gesichtsbildabgleich**', YouTube, 6 April 2023.

Conclusions: Hard-wiring fundamental rights when considering remote biometric identification for law enforcement purposes

A growing number of Member States are exploring the use of RBI for law enforcement purposes. As such technologies continue to evolve and the European Commission advances its digital and security agendas, law enforcement agencies face critical decisions about their adoption, regulation, deployment and oversight. RBI technologies used for law enforcement purposes are intended to serve beneficial objectives in the public interest, such as preventing crime, apprehending offenders and protecting potential victims. When deployed within robust legal frameworks underpinned by fundamental rights safeguards and subject to effective, independent oversight, their justified use can contribute to maintaining public security in democratic societies grounded in respect for fundamental rights and the rule of law.

The fundamental rights implications of using RBI technologies vary considerably depending on the purpose, context and scope of use. Some of the fundamental rights implications are connected to the technology's accuracy. Despite technological advancements, built-in bias and risks of erroneous outputs remain, which can negatively impact fundamental rights. While errors overall can be a challenge, biased error rates – which mean that errors affecting certain groups of the population (e.g. women, people of colour, older people) are more common – are another complex challenge to duly address. Robust data, thorough assessments and evidence of such errors and biases (or of their absence) are generally lacking.

Moreover, importantly, several fundamental rights concerns would remain even if there were no errors at all in the operation of RBI tools. Effectively and adequately protecting fundamental rights in the context of using RBI for law enforcement purposes is a legal requirement under EU law that cannot be circumvented. This not only stems from the Charter as interpreted by the CJEU but is also expressly and more specifically enshrined in the AI Act. A rights-compliant approach warrants a clear, specific and proper legal basis



that defines the purpose(s) for, scope of and preconditions for the use of RBI, always to be guided by the legally enforceable principles of necessity and proportionality.

Still, the AI Act has limitations on its own scope. For instance, online spaces are not considered a ‘publicly accessible space’ within the meaning of the AI Act, so no prohibitions apply to using RBI for law enforcement purposes in online spaces. The necessity and proportionality of such systems need, however, to be considered under EU fundamental rights law and the EU data protection *acquis*. Similarly, even though regulatory attention to the law enforcement use of new technologies mostly focuses on biometric identification, non-biometric policing tools may be equally intrusive and enable surveillance (with the risk of function creep) and ultimately identification, for example by tracking a vehicle’s licence plate (¹⁴³). Future research should also shed more light on the fundamental rights implications of the emergent use of these non-biometric forms of new technologies in modern policing.

To make RBI use by law enforcement fundamental-rights-proof, transparency, accountability and independent oversight mechanisms are invariably indispensable. These elements prevent the misuse of such systems and ensure that affected individuals are informed and empowered to exercise their rights, notably the right to an effective judicial remedy against wrongful outcomes. A rights-based approach to RBI must go beyond risk mitigation: it must be embedded into comprehensive *ex ante* and *ex post* fundamental rights impact assessments, too.

The evidence in this report underlines that factoring in fundamental rights implications when law enforcement authorities consider using RBI technologies should be further mainstreamed. The findings also offer general insights into what safeguards are needed to ensure fully fundamental-rights-compliant use of RBI by law enforcement agencies in practice. At the same time, there is a great need to translate abstract legal requirements into practical and actionable guidance. Law enforcement deployers – and also technology providers – indicated that they need guidance on a number of aspects covered by the research.

ANNEX I – ABOUT REMOTE BIOMETRIC IDENTIFICATION SYSTEMS

RBI systems are AI systems used to identify persons without their active involvement (participation) by comparing their biometric data with biometric data stored in a reference database, for example a criminal database or a missing persons database. This process happens typically at a distance ⁽¹⁴⁴⁾. The systems can be deployed (1) in real time, meaning that the biometric data capture, comparison and identification all occur without a significant delay (including in instantaneous and near-instantaneous manners) ⁽¹⁴⁵⁾; or (2) in a retrospective manner (*ex post*) ⁽¹⁴⁶⁾, for example by analysing previously captured CCTV footage after an event has occurred. The European Commission notes in its guidelines on the prohibitions under the AI Act that a case-by-case assessment is needed when assessing whether RBI is used ‘without a significant delay’, explaining that a delay is generally significant ‘at least when the person is likely to have left the place where the biometric data was taken’ ⁽¹⁴⁷⁾. Recital 17 to the AI Act underlines that the AI Act provisions on real-time RBI must not be circumvented through providing for minor delays. The EDPS and EDPB, as well as civil-society representatives and academics, have, however, questioned the regulatory distinction between real-time and *ex post* RBI, as the use of *ex post* RBI could similarly, if not even more significantly than real-time RBI, adversely impact fundamental rights ⁽¹⁴⁸⁾.

The process of biometric **identification** (known as one-to-many matching) should be distinguished from biometric **verification**, when a person’s identity is automatically verified by comparing their biometric data with previously provided biometric data (one-to-one matching) ⁽¹⁴⁹⁾. The sole purpose of biometric verification is to confirm that a specific person is the person they claim to be, to enable their access to a service, device or premises ⁽¹⁵⁰⁾. For example, biometric verification can be set up by a person to unlock their phone with a fingerprint or facial image.

In certain cases, biometric identification systems (performing one-to-many matching) can be used for such identity confirmation purposes too. The key consideration to establish whether such AI-driven systems are considered high risk or not under the AI Act is whether or not they are deployed remotely, that is, without the active participation of the person ⁽¹⁵¹⁾. Biometric identification also needs to be distinguished from biometric categorisation, whereby persons are assigned to specific categories based on their biometric data, for example their age or sex ⁽¹⁵²⁾.

RBI systems can compare different biometric data of a person, for example their facial image, voice, gait or keystrokes ⁽¹⁵³⁾. FRA’s research explored biometric systems that process facial images and voice. When it comes to other types of biometric data, that is, other personal data that result from specific technical processing relating to the physical, physiological or behavioural characteristics of a person ⁽¹⁵⁴⁾, their use and reliability for remotely identifying persons are limited and questionable ⁽¹⁵⁵⁾. Their limited use, as of now, was also confirmed to FRA by several representatives of Member States’ law enforcement authorities. Some acknowledged the possibilities of technological advances in the future.

FACIAL RECOGNITION TECHNOLOGY

FRT is the dominant technology used in the RBI field, in terms of both the amount of use and the degree of attention placed on these technologies ⁽¹⁵⁶⁾. Facial recognition is different from other forms of biometric identification due to ‘the intimate and cultural meaning of our face’ ⁽¹⁵⁷⁾, a feature that the ECtHR has equally stressed: a face is ‘one of the key attributes of a person’s personality’ ⁽¹⁵⁸⁾. As explained above, this technology digitally analyses facial features captured by video cameras and compares them against other images to identify an individual ⁽¹⁵⁹⁾. A captured facial image is thereby compared against a database of facial images (e.g. a watch list) ⁽¹⁶⁰⁾ to identify the individual from the image (one-to-many matching). Such technologies can be, for example, used by a law enforcement authority to identify suspects in criminal investigations. Both the legitimacy of these databases (watch lists) and the criteria for being included in one have been the source of much debate around the legitimacy and legality of FRT ⁽¹⁶¹⁾. The technologies can be also used to track individuals, for example to track an individual through a crowd ⁽¹⁶²⁾.

Face identification, which occurs in the context of RBI, needs to be distinguished from face verification (one-to-one matching) and from face analysis or categorisation. Face analysis/categorisation examines facial images to

detect specific attributes, such as age, gender and emotions, or even whether someone is wearing a mask. Face categorisation does not normally involve direct face comparison and, therefore, does not necessarily require a source database.

VOICE RECOGNITION TECHNOLOGY

Publicly available information on voice recognition and verification technologies is scarce. One of the most comprehensive early studies of these technologies – published in 2016 – was conducted on behalf of the International Criminal Police Organization (Interpol). Sixty-nine (out of 190) law enforcement agencies from Interpol member countries participated in it, sending a total of 91 responses to the study's questionnaire ⁽¹⁶³⁾. Overall, 44 respondents indicated that their authorities had the capabilities for voice-recording analysis, of whom 26 respondents indicated that their agencies held an underpinning database for the purposes of matching recordings. Additionally, two respondents indicated they had databases, despite not having the capabilities for analysing voice recordings. Most of these 28 respondents indicated that their databases contained voice prints of 'suspects', while almost half of the respondents (46 %) held databases with voice recordings of people without any clear connection to any particular crime ⁽¹⁶⁴⁾. This reflects a similar debate concerning the use of images of those not convicted of any crime for facial recognition databases ⁽¹⁶⁵⁾. Voice recordings are drawn from a range of sources. These include crime scene recordings, telephone intercepts (fixed line and mobile), police interviewing and open sources ⁽¹⁶⁶⁾.

Like FRT, voice recognition and verification take many different forms. According to the above Interpol study, the most common approaches to speaker identification in Europe were expert-based, whereby forensic practitioners examined recordings by listening to them and making acoustic measurements of sound and used algorithms, under their expert supervision, for analysis. Only a few respondents mentioned the use of fully automatic approaches by non-forensic practitioners ⁽¹⁶⁷⁾. The emphasis on non-automated approaches can be observed in this 2016 study. While more recent data are yet to emerge, it is highly likely that these trends have shifted significantly towards computational and heavily automated processing.



ANNEX II – METHODOLOGY

The methodology applied for this report consists of a combination of desk research and different forms of fieldwork (interviews, non-participant observations) focusing on seven country case studies in selected Member States (France, Germany, Greece, Hungary, Ireland, Italy and the Netherlands). The findings are complemented by a small-scale quantitative survey with members of the public in five selected Member States (France, Germany, Greece, Hungary and Ireland).

FIELDWORK

To collect up-to-date information on the use of RBI systems by law enforcement authorities, the fieldwork for this study included both qualitative and quantitative data collection activities that encompassed semi-structured qualitative interviews, non-participant observations and small-scale surveys.

Semi-structured interviews

The core of the fieldwork summarises the findings of 50 semi-structured interviews, aimed at collecting data across the selected Member States. The overall aim of the interviews was to understand the perspectives of stakeholders on the development, deployment and regulation of RBI systems used by law enforcement agencies and their impact on fundamental rights. Overall, 69 interviewees were involved:

- law enforcement authorities (30 % of the interviews), including technical experts and criminal investigators, who covered both the operational use of RBI systems and their impact on fundamental rights from a law enforcement perspective;
- technology providers of RBI systems (4 %), who addressed the technicalities of the RBI systems, including how they are developed and trained;
- national data protection authorities, ombuds institutions and other regulators (20 %), who provided information about investigations, existing national legislation and the expected impact of the AI Act;
- academia and civil-society organisations (46 %), who brought relevant insights into the regulatory developments and the shortcomings and fundamental rights risks of the use of RBI for law enforcement purposes.

All interviews were conducted respecting the full anonymity of the interviewees and EU data protection requirements. The interview questionnaires were based on a standardised interview guide consisting of 36 open and closed questions, designed for the different types and profiles of interviewees.

While semi-structured interviews allowed FRA to gain relevant information on practices that are hard to access and observe, they were subject to several limitations intrinsic to qualitative social science research, including the snowball sampling approach and the fact that data were inevitably weighted towards the perspectives of available interviewees.

Non-participant observations

Three non-participant observations were conducted to gain an understanding of the life cycle of the given RBI system's use, including the planning, operational and post-operational phases. The observations were carried out in person with law enforcement authorities in France, Germany and the Netherlands. These exercises made it possible to engage with the authorities' personnel on-site, during a specific time frame, while gaining experimental knowledge of the use of the systems through direct observation. This included gaining visual access to the equipment used and observing the tasks carried out and the procedures and protocols in place.

While providing the most detailed examination of law enforcement agencies' activity, the observations also faced challenges and limitations. They were highly contingent on access to research sites, while several national authorities showed reluctance to allow the direct observation of their systems. The observations were also limited by the availability of data, only reflecting those authorities and activities that were allowed to be accessed, and heavily conditioned by response and non-response biases. In addition, some operational uses of RBI are rare and episodic, a factor that made their investigation more challenging. To mitigate biases and limitations, researchers involved in the non-participant observation received targeted training on applicable methodologies. Moreover, to enhance the robustness of data, the observations were complemented and validated by qualitative interviewing and documents' analysis. Despite such efforts, however, the limited engagement of selected law enforcement agencies necessarily limited the scope and depth of this aspect of the research.

Quantitative survey in public places

The aim of the quantitative survey was to add another dimension to the information and analysis of the report through collecting the views and concerns of rights holders on the use of RBI technologies in specified public locations. The surveys were conducted by Ipsos, a leading global market research agency, in five of the selected Member States, namely France, Germany, Greece, Hungary and Ireland. A total of 1 054 interviews were conducted, with a minimum of 150 per Member State (see [Table 5](#)). These were broadly split across three location types: public places, public transport hubs and sports stadiums. People who passed through these locations were approached by interviewers in a systematic way, for example every tenth person entering the place. If they agreed, respondents had to answer 14 questions that addressed people's awareness of cameras and the potential use of RBI, their views on the legitimate use of these systems and their knowledge of complaint mechanisms for challenging RBI's decisions.

TABLE 5 NUMBER OF PEOPLE INTERVIEWED PER LOCATION IN THE FIVE MEMBER STATES COVERED

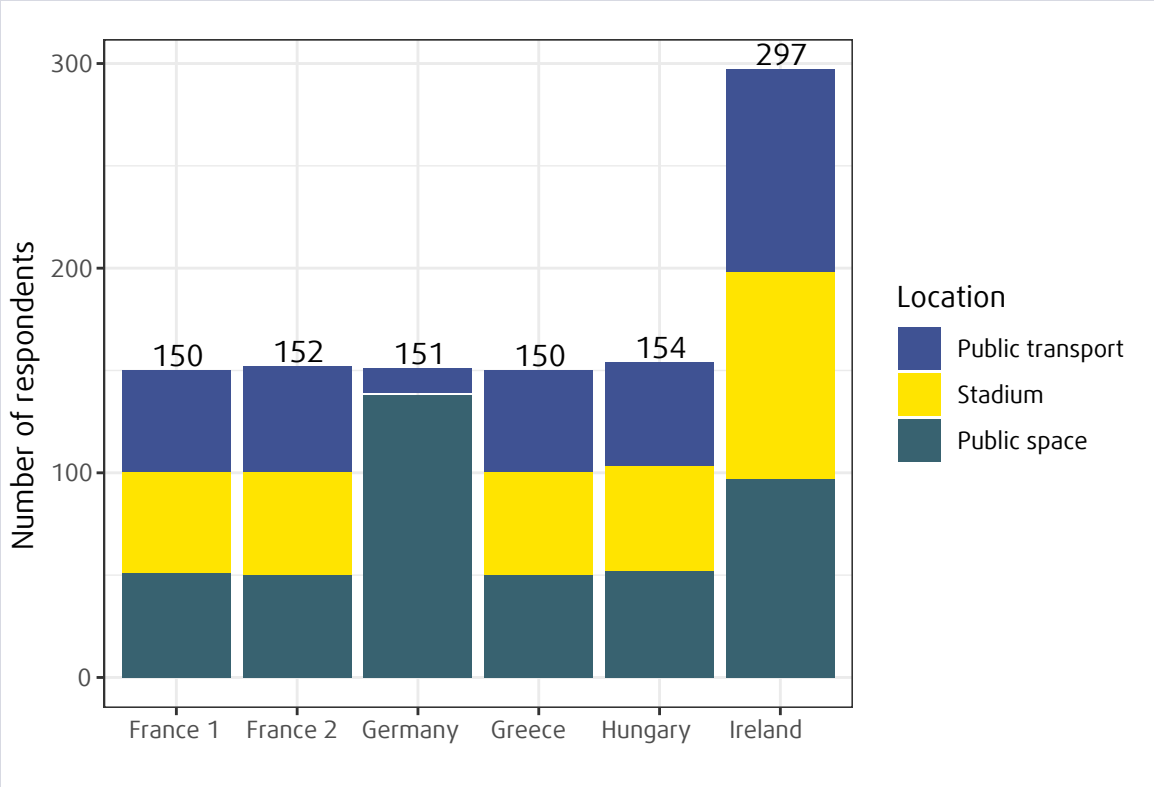
Member State	Locations	Number of surveys completed
France (wave 1)	Public transport (Gare du Nord and Gare de Lyon)	50
	Stadium (Bercy Arena)	49
	Public place (Place de la République)	51
France (wave 2)	Public transport (Gare du Nord and Gare de Lyon)	52
	Stadium (Bercy Arena)	50
	Public place (Place de la République)	50
Germany	Research locations close to public transport (Berlin, Hamburg, Leipzig)	12
	Stadium	0
	Research locations close to public spaces (Berlin, Hamburg, Leipzig)	139
Greece	Public transport (Larissa railway station)	50
	Stadium (G. Karaiskakis Stadium in Faliro)	50
	Public space (Athens Syntagma Square)	50
Hungary	Public transport (Nyugati pályaudvar)	51
	Stadium (Puskás Ferenc stadion)	51
	Public place (Széll Kálmán square)	52
Ireland	Public transport (Galway train station)	99
	Stadium (Aviva Stadium)	101
	Public place (Limerick)	97

Source: FRA, 2026.

Such a survey is subject to several limitations: participants were recruited in open streets without full control over how they were selected. This means that the results are not representative of the population in the Member States covered and cannot necessarily be generalised to the general public. Nonetheless, the analysis provides a snapshot of what people think in selected public spaces at certain time points. In order to showcase and understand differences in situation and context, the survey was carried out twice in France: once during the Olympic Games in summer 2024 and then again at the same places afterwards in autumn 2024. In Germany, it was not possible to obtain authorisation to conduct the survey at the locations directly, and research was carried out at test sites available to the survey company that are close to public spaces and public transport stations. However, no sites close to stadiums could be covered in Germany. The results capture quick feedback from people to short questions about the use of RBI technology in public places and are only reflections of people's views on very general questions at a given time. However, they still measure well how people tend to feel if asked about important topics related to RBI technology, and are an established methodological approach used in survey research to capture public opinion.

Figure 11 shows the numbers of respondents by Member State and location. Gender balance was achieved: 530 of the 1 054 respondents are men, which is roughly equal to 50 %. The average age is 39 years, ranging from 16 to 89. 12 % of respondents indicated that they consider themselves to belong to an ethnic minority in the Member State where the survey was conducted.

FIGURE 11 NUMBER OF RESPONDENTS TO THE SMALL-SCALE SURVEY, BY MEMBER STATE AND LOCATION



Note: N = 1 054.
Source: FRA, 2026.

Endnotes

- ⁽¹⁴³⁾ For more on that aspect, see for example Mahdawi, A., ‘**A dystopian surveillance fear has become reality in Texas**’, *The Guardian*, 31 May 2025.
- ⁽¹⁴⁴⁾ Art. 3(41) of the AI Act. See also Communication from the Commission – **Commission guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)**, C(2025) 5052 final of 29 July 2025, paras 299 and 306.
- ⁽¹⁴⁵⁾ Art. 3(42) of and recital 17 to the AI Act.
- ⁽¹⁴⁶⁾ Art. 3(43) of the AI Act.
- ⁽¹⁴⁷⁾ Communication from the Commission – **Commission guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)**, C(2025) 5052 final of 29 July 2025, para. 310.
- ⁽¹⁴⁸⁾ EDPB and EDPS, **EDPB-EDPS Joint Opinion 5/2021 on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)**, 18 June 2021, para. 31; EDRI, Access Now, **ARTICLE19, Bits of Freedom, Chaos Computer Club, et al., ‘Joint civil society recommendations for an EU Artificial Intelligence Act for fundamental rights – Biometrics Part 1: Article 3(36) and Article 5(1)(d) – Prohibit all remote biometric identification (RBI) in publicly accessible spaces’**, p. 1. See also, for example, González Fuster, G. and Nadolna Peeters, M., **Person Identification, Human Rights and Ethical Principles. Rethinking biometrics in the era of artificial intelligence**, PE 697.191, European Parliamentary Research Service, December 2021, pp. IV and 55–58; and Giannini, A. and Tas, S., ‘**AI Act and the prohibition of real-time biometric identification**’, Verfassungsblog website, 10 December 2024.
- ⁽¹⁴⁹⁾ Art. 3(36) of the AI Act. For a definition of ‘biometric identification’, see Art. 3(35) of the AI Act. See also International Organization for Standardization and International Electrotechnical Commission, **ISO/IEC 2382-37:2022 – Information technology – Vocabulary – Part 37: Biometrics**, points 37.08.02 and 37.08.03.
- ⁽¹⁵⁰⁾ Recital 15 to the AI Act.
- ⁽¹⁵¹⁾ See also recital 54 to the AI Act.
- ⁽¹⁵²⁾ Recital 16 and Art. 3(40) of the AI Act.
- ⁽¹⁵³⁾ See also Communication from the Commission – **Commission guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)**, C(2025) 5052 final of 29 July 2025, para. 307.
- ⁽¹⁵⁴⁾ Art. 3(34) of the AI Act. The definition of ‘biometric data’ under the AI Act is broader than under the LED, which requires that such personal data in addition ‘allow or confirm the unique identification of [a] natural person’. However, in the case of RBI systems, it is in any case implied that the data processed allow for the identification of a person.
- ⁽¹⁵⁵⁾ For example, while there were significant advancements relating to gait recognition in past years, challenges remain, especially in real-world environments; Shen, C., Yu, S., Wang, J., Huang, G. Q. and Wang, L., ‘A comprehensive survey on deep gait recognition: Algorithms, datasets and challenges’, **arXiv:2206.13732**, 2023, pp. 14 and 17–19. Another survey, for example, noted that iris recognition from long distances remains a possibility for biometric recognition. The main challenge in this regard lies in the data acquisition; Nguyen, K., Proença, H. and Alonso-Fernandez, F., ‘**Deep learning for iris recognition: A survey**’, *ACM Computing Surveys*, Vol. 56, No 9, 2024, 223, Section 9.7.
- ⁽¹⁵⁶⁾ See for example the summary report of the Telefi project, which looked into Member States’ use of facial recognition in criminal investigations; Telefi project, ‘**Summary report of the project “Towards the European level exchange of facial images”**’, Version 1.0, 2021. See also Kindt, E. J. and Jasserand, C., ‘Article 5: Prohibited AI practices’, in: Pehlivan, C. N., Forgó, N. and Valcke, P. (eds), *The EU Artificial Intelligence (AI) Act: A commentary*, Wolters Kluwer, Alphen aan den Rijn, 2025, p. 173.
- ⁽¹⁵⁷⁾ Fussey, P. and Murray, D., *Facial Recognition Surveillance – Policing and human rights in the age of artificial intelligence*, Oxford University Press, Oxford, 2025, p. 20.
- ⁽¹⁵⁸⁾ ECtHR, *Glukhin v. Russia*, No 11519/20, 4 July 2023, § 66.
- ⁽¹⁵⁹⁾ For more information on facial recognition technology, see FRA, **Facial Recognition Technology: Fundamental rights considerations in the context of law enforcement**, Publications Office of the European Union, Luxembourg, 2019.
- ⁽¹⁶⁰⁾ Face recognition watch lists are databases of known individuals used to identify people of interest in real time or through stored video footage. For more on watch lists, see for example Guo, Z. and Kennedy, L., ‘**Policing based on automatic facial recognition**’, *Artificial Intelligence and Law*, Vol. 31, 2023, pp. 397–443.
- ⁽¹⁶¹⁾ See for example Fussey, P., ‘**Facial recognition**’, in: Kaufmann, M. and Lomell, H. M. (eds), *De Gruyter Handbook of Digital Criminology*, De Gruyter, Berlin/Boston, 2025, pp. 233–241.
- ⁽¹⁶²⁾ The European Commission guidelines on the prohibitions under the AI Act acknowledge that ‘AI systems used for following natural persons can also be included in the definition of biometric identification, for example to see in which direction a suspect escapes.’ Communication from the Commission – **Commission guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)**, C(2025) 5052 final of 29 July 2025, para. 302.
- ⁽¹⁶³⁾ Morrison, G. S., Sahito, F. H., Jardine, G., Djokic, D., Clavet, S., Berghs, S. and Goemans Dorny, C., ‘INTERPOL survey of the use of speaker identification by law enforcement agencies’, *Forensic Science International*, Vol. 263, 2016, pp. 92–100.
- ⁽¹⁶⁴⁾ *Ibid.*, p. 93.
- ⁽¹⁶⁵⁾ Murray, D., ‘**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*, Vol. 87, Issue 4, 2024, pp. 833–863.
- ⁽¹⁶⁶⁾ Morrison, G. S., Sahito, F. H., Jardine, G., Djokic, D., Clavet, S., Berghs, S. and Goemans Dorny, C., ‘INTERPOL survey of the use of speaker identification by law enforcement agencies’, *Forensic Science International*, Vol. 263, 2016, p. 93.
- ⁽¹⁶⁷⁾ *Ibid.*, p. 94.

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls);
- at the following standard number: +32 22999696;
- via the following form: european-union.europa.eu/contact-eu/write-us_en.

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local information centre (european-union.europa.eu/contact-eu/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

EU open data

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.



PROMOTING AND PROTECTING YOUR FUNDAMENTAL RIGHTS ACROSS THE EU

Today, a single camera scan from a distance can identify one person in a crowd. Law enforcement authorities in a growing number of EU Member States use or are considering using this AI-driven technique, known as remote biometric identification. While it can support public security and protect people from crime, it also poses serious risks to fundamental rights. FRA's report draws on legal analysis, interviews with law enforcement practitioners and other experts, observations of police work and a public survey across selected EU Member States. FRA points to the need for a comprehensive legal basis for RBI use for law enforcement, including defined purposes, limits on identifying participants in peaceful assemblies or political gatherings, independent oversight and fundamental rights impact assessments, all of which should be in place before RBI is deployed.



FRA – EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

Rennweg 12 – 1030 Vienna – Austria

Tel +43 158030-0 – Fax +43 158030-699

fra.europa.eu

 [linkedin.com/company/eu-fundamental-rights-agency](https://www.linkedin.com/company/eu-fundamental-rights-agency)
 [instagram.com/fundamental.rights](https://www.instagram.com/fundamental.rights)
 [facebook.com/fundamentalrights](https://www.facebook.com/fundamentalrights)
 [youtube.com/EUAgencyFRA](https://www.youtube.com/EUAgencyFRA)
 [x.com/EURightsAgency](https://www.x.com/EURightsAgency)



Publications Office
of the European Union