Guidance Study on

Article 5(1)(h) prohibition and its three exceptions (Article 5(1)(h)(i)-(iii)),

the procedural requirements laid down in Article 5(2),

and the prohibition of Article 5(1)(e) of the AI Act

Final study report

Written by Catherine Jasserand

EUROPEAN COMMISSION

Directorate-General for Communications Networks, Content and Technology (CNECT)

Artificial Intelligence Office

Contact: Yordanka Ivanova

E-mail: Yordanka.ivanova@ec.europa.eu

European Commission

B-1049 Brussels

LEGAL NOTICE

The information and views set out in this document are those of the authors and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this document. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

More information on the European Union is available on the Internet (http://www.europa.eu).

Luxembourg: Publications Office of the European Union, **2026**

KK-01-25-096-EN-N

ISBN 978-92-68-29184-9

DOI 10.2759/8486644

Table of Contents

Execut ve Summary

Based on a request made by the European Commission, this study analyses two of the eight prohibitions provided by Article 5 of the AI Act. It details the prohibition of real-time use of Remote Biometric Identification systems in publicly accessible spaces for law enforcement purposes, with the three situations in which such use may be allowed by national legislation and the conditions and safeguards under which such use is possible.[1] The first prohibition is described in Article 5(1)(h) of the AI Act, together with the three cases for which such a use might be permitted under Article 5(1)(h)(i)-(iii), and the conditions and safeguards in Article 5(2) of the AI Act.[2] The second prohibition analysed relates to AI systems used to indiscriminately scrape facial images from the Internet or CCTV to creatw or expand facial recognition databases. This prohibition is detailed in Article 5(1)(e) of the AI Act. The study aims to provide input on these two prohibitions to support the European Commission in drafting the Guidelines on the prohibited AI practices. On 2 February 2025, the rules on prohibited practices will apply.[3] This report is composed of a legal analysis illustrated by practical examples and several use cases of application.

The AI Act lays down harmonised rules for the placing on the market, putting into service and use of AI systems in the EU in compliance with EU values, and the protection of safety, health, and fundamental rights. It distinguishes three levels of risks: first, AI systems posing unacceptable risks to fundamental rights (prohibited practices); second, AI systems having 'a significant harmful impact' on fundamental rights, safety and health (high-risk systems), and third, AI systems posing only limited risks (*limited* risk systems). The first category of AI systems is prohibited due to the unacceptable level of risks that they pose to fundamental rights. Exception to these prohibitions must comply with the limitations set out in Article 52(1) of the Charter of fundamental rights.

The first prohibition relates to the real-time use of remote biometric identification (RBI) systems in publicly accessible spaces for a law enforcement purpose. These technologies only cover those aimed at identifying an individual, excluding verification systems from their scope. Although the most known RBI technology is facial recognition, more types of RBI exist. The notion of publicly accessible spaces is broad and includes spaces such as shopping centres, sports arenas, airports, and many more. Finally, the prohibition is linked to the purpose (law enforcement) and not to the actors. The AI Act provides three cases in which Member States can authorise the real-time use of RBI. Member States have a choice as they can also decide not to allow any use in their national legislation. These three cases cover the real-time use of RBI to search for the victims of three crimes and for missing persons (1), to prevent imminent threats to life and genuine threats of terrorist attacks (2) and to locate and identify suspects and perpetrators of serious crimes listed in Annex II of the AI Act. The aim is to provide new investigative tools for law enforcement purposes. Yet, as these tools can seriously impede the exercise

[1] Contract LC-03096758.
[2] The other condit ons and safeguards, i.e. Art cle 5(2)-(7) of the AI Act, are analysed in Dr. Els Kindt's report.
[3] Art.113 (a) AI Act.

of fundamental rights, their use in the situations where authorised is subject to conditions and safeguards. The deployment must be strictly necessary and targeted to a specific individual as the live use of these technologies should not lead to mass surveillance. From a fundamental rights perspective, the most important tool the deployers will have to draft and update is the Fundamental Rights Impact Assessment.

The second prohibition under review is the untargeted scraping of facial images from the Internet or CCTV to create or build facial recognition databases. This prohibition echoes the Clearview AI's practices where Clearview AI scraped billions of images without any legal basis to create a facial database mainly for law enforcement purposes. If the practices of the company have been sanctioned for infringing the EU data protection rules, the AI Act tackles a specific issue. It prohibits the AI tool used to indiscriminately scrape facial images, whether this is done for law enforcement or non-law enforcement purposes.

The report ends with a list of recommendations for deployers and Member States.

1. Introduct on

1.1 Background

On 21 April 2021, the European Commission published a proposal for a 'Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence Act to harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.[4] After three years of negotiations between the EU co-legislators, the regulation was adopted and the text officially published.[5]

The Artificial Intelligence Act (AI Act) lays down harmonised rules for the placing on the market, putting into service and use of AI systems in the EU in compliance with EU values, and the protection of safety, health, and fundamental rights.[6] It is, therefore, a general framework of AI systems, which follows a risk-based approach, depending on the risks these systems pose to fundamental rights, safety, and health.[7] In the European Declaration on Digital Rights and Principles for the Digital Decade, the EU institutions acknowledged that while individuals could benefit from AI systems, they should also be 'protected against risks and harm to one's health, safety and fundamental rights.'[8] This declaration and the Ethics Guidelines for Trustworthy AI of the High-Level Expert Group on Artificial Intelligence should be taken into account to establish the common rules for AI systems.[9]

In this context, the AI Act distinguishes three levels of risks: first, AI systems posing unacceptable risks to fundamental rights (prohibited practices);[10] second, AI systems having 'a significant harmful impact' on fundamental rights, safety and health (high-risk systems), [11] and third, AI systems posing only limited risks (*limited* risk systems).[12] While the first category is prohibited, save for some exceptions,[13] the second is subject to mandatory regulatory requirements,[14] and the third to transparency obligations for their providers and deployers.[15] The current study focuses on two prohibited practices, excluding the regimes applicable to high-risk systems and AI limited risk systems from its scope. The rationale and objective of the prohibited practices are further developed in Section 2.

[4] COM (2021) 206 f nal, 21 April 2021.
[5] Regulat on (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on art f cial intelligence and amending Regulat ons (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Direct ves 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Art f cial Intelligence Act), OJ L2024/1689, 12 July 2024.
[6] Art. 1 AI Act.
[7] Rec. 26 AI Act.
[8] COM (2022) 28 f nal, p. 4.
[9] Rec. 7 AI Act.
[10] Art. 5 AI Act.
[11] Rec. 46, Art. 6, and Annex III AI Act.
[12] Rec.132 and Art. 50 AI Act
[13] Art. 5 AI Act.
[14] Art. 6 AI Act.
[15] Art. 50 AI Act.

The AI Act has two legal bases: Article 114 TFEU (internal market) and Article 16 TFEU (data protection) for the processing of personal data linked to the restrictions to the use of remote biometric identification systems for law enforcement purposes, the use of biometric categorisation systems for law enforcement purposes and the risk assessments of individuals for law enforcement purposes.[16] Therefore, the legal basis for the three cases is not Article 114 TFEU.

Article 16 TFEU establishes the right to the protection of personal data, also recognised in Article 8 of the Charter of Fundamental Rights. It gives competence to the European Parliament and the Council to adopt legislative measures relating to the processing of personal data. Article 16 TFEU is the legal basis for the General Data Protection Regulation (known as GDPR or Regulation 2016/679), the Law Enforcement Directive, laying down the rules on the processing of personal data by law enforcement authorities in the area of police and criminal justice (LED or Directive 2016/680) and the EU Data Protection Regulation applicable to EU institutions, agencies and bodies (EUDPR or Regulation 2018/1725). The rules that prohibit the real-time use of RBI in publicly accessible spaces for law enforcement purposes should apply as *lex specialis* to Article 10 of the LED on the processing of biometric data. The meaning of this lex specialis is further explained in relation to the prohibition of real-time use of RBI in Section 3 of the report.

1.2 Purpose of the study and scope

Within six months of the entry into force of the AI Act, rules relating to the prohibited practices, i.e. Article 5 of the AI Act, will be applicable. Following Article 96(1)(b) of the AI Act, the European Commission should issue guidelines to help providers and deployers comply with their respective obligations and understand the scope of the prohibited practices, along with the exceptions expressly mentioned and their practical implementation. This study provides some background, legal analysis, and practical examples of the application of the two prohibited practices covered by this study including their explicit exceptions and cases falling outside the scope of the prohibitions.

The scope of this study is the analysis of Article 5(1)(h), i.e. the prohibition of the use of remote biometric identification systems in real-time and in publicly accessible spaces for a law enforcement purpose. Besides, the analysis will include the three exceptions to this prohibition as laid down in:

- Art cle 5(1)(i), the targeted search for certain vict ms of specif c crimes and the search for missing persons;
- Art cle 5(1)(ii), the prevent on of a specif c, substant al and imminent threat to the life or physical safety of natural persons, or a genuine and present or genuine and foreseeable threat of a terrorist at ack; and
- Art cle 5(1)(iii), ident f cat on and localisat on of suspects of serious crimes as listed in Annex II.

[16] Rec. 3 AI Act.

Specific conditions and safeguards have been added in Articles 5(2) to 5(7) of the AI Act before deploying RBI systems. This study will only cover the requirements set out in Article 5(2) of the AI Act.[17]

In addition, the study covers the prohibition outlined in Article 5(1)(e). This provision prohibits placing on the market, putting into service, or using AI systems to create or expand facial recognition databases through untargeted scraping of facial images from the Internet or CCTV footage.

1.3 Methodology

This study is a desk-research analysis based on the primary sources of EU law, i.e., the Treaty on European Union (TEU), the Treaty on the Functioning of the European Union (TFEU), the EU Charter of ('the Charter'), and the case law of the Court of Justice of the EU (ECJ) completed by that of the European Court of Human Rights (ECtHR).

Besides, the study analyses the application of relevant secondary EU law, and in particular, the data protection framework composed of the General Data Protection Regulation (GDPR or Regulation 2016/679) and the Law Enforcement Directive (LED or Directive 2016/680) for the processing of personal data for a law enforcement purpose by national competent authorities (i.e. law enforcement authorities or on their behalf). This analysis is completed by examples from national legislation, when relevant, and in particular, criminal law and criminal procedure laws.

The study is based on case law, a literature review of academic articles, positions expressed and reports by NGOs on the topics of the study, newspapers articles, policy papers, reports of different EU and national bodies, including national data protection authorities (DPAs), the European Parliament (EP), including its Research Service (EPRS), the European Commission (EC), the European Union Agency for Fundamental Rights (FRA). Due to time constraints, the analysis and interpretation focused on key issues, such as the content and scope of prohibitions, including exceptions applicable to the case of real-time use of remote biometric identification systems.[18]

2. General Provision on the Prohibited Pract ces

Article 5 of the AI Act prohibits placing on the EU market, putting into service, or using AI systems that violate the EU values, as defined in Article 2 TEU, and fundamental rights, as recognised by the Charter of Fundamental Rights. The list of prohibited practices proposed by the European Commission contains exceptions to certain prohibitions. These exceptions were intensively debated during the

[17] The remaining condit ons applicable to the except ons are analysed in Dr Els Kindt's report. The analysis was split between two reports due to t me management.

[18] Input and comments from NGOs, DG Home, DG Just, and DG CNECT, were provided during the draf ing period of the report. Some use cases were also added at the request of the European Commission; however, their analysis remains the author's.

trilogue negotiations, in particular, the exceptions to the RBI systems' use in public spaces, including for non-law enforcement purposes.[19]

2.1 Unacceptable risks to fundamental rights

AI systems that pose unacceptable risks to fundamental rights are prohibited practices. The fundamental rights impacted by these systems are listed in a non-exhaustive manner as:

- The right to the protect on of personal data ('right to data protect on')[20]
- The right to respect for private and family life ('right to privacy')[21]
- Freedom of expression and informat on[22]
- Freedom of assembly and of associat on[23]
- Freedom of thought, conscience and religion[24]
- The right to non-discriminat on[25] and equality[26]
- The right to human dignity[27]
- The right to an ef ect ve remedy and to a fair trial[28]
- Presumpt on of innocence and right of defence[29]

Among the fundamental rights, those that are absolute, such as the right to human dignity and the right not to be directly discriminated against as far as it is based on racial and ethnic origin, [30] cannot be restricted. The other fundamental rights, which are called qualified rights or non-absolute rights, can be restricted following the conditions of Article 52(1) of the Charter. Most fundamental rights fall in that category.

2.2 Restrict ons to fundamental rights

To the extent that the fundamental rights are not absolute, their exercise can be limited if it meets the requirements of Article 52(1) of the Charter. Limitations on the exercise of fundamental rights **must be provided by law**, **respect the essence of the right(s)** at stake, pursue a **legitimate aim** (either an objective of general interest as recognised by the Union or the protection of the rights and freedoms of others), and comply with the **necessity and proportionality** tests.

Article 52(1) Charter reads as follows:

---

[19] E.g. Bertuzzi, L. 'AI Act: MEPs mull narrow facial technology uses in exchange of other bans' Euract v, 6 November 2023 ht ps://www.euract v.com/sect on/art f cial-intelligence/news/ai-act-meps-mull-narrow-facial-recognit on-technology-uses-in-exchange-for-other-bans/

[20] Art. 8 of the Charter.

[21] Art. 7 of the Charter.

[22] Art. 11 of the Charter.

[23] Art. 12 of the Charter.

[24] Art. 10 of the Charter.

[25] Art. 21 of the Charter.

[26] Art. 20 of the Charter.

[27] Art. 1 of the Charter.

[28] Art. 47 of the Charter.

[29] Art. 48 of the Charter.

[30] as protected by Direct ve 2000/43/EC; Council Direct ve 2000/43/EC of 29 June 2000 implement ng the principle of equal treatment between persons irrespect ve of racial or ethnic origin, OJ L180, 19 February 2000.

> *Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.*

The requirements of legality, proportionality, and necessity derive from the case law of the ECtHR, whereas the requirement of 'respect for the essence of the right' can find its roots in the constitutions of several Member States.[31] ***Legality*** implies the existence of a legal basis, which is clear and precise in its terms and foreseeable in its application.[32] ***Necessity*** refers to the least restrictive but equally efficient means to achieve a legitimate aim.[33] Regarding the exceptions to the prohibition of real-time RBI use in publicly accessible spaces, the requirement is heightened to that of strict necessity.[34] The meaning of *strict necessity* is further explained in Section 3 on RBIs. ***Proportionality*** calls for balancing competing interests or rights (such as public security and data subjects' rights) and checking the existence of safeguards that accompany a measure.[35] The CJEU found, for example, that data retention measures lacked safeguards concerning the persons affected by the measures. Those included the lack of objective criterion to limit law enforcement access to the retained data, the lack of substantive and procedural conditions on access and further use of the retained data,[36] and the obligation to notify concerned individuals. [37]

As noted by the EDPS, these safeguards aim at reducing the impact of a measure on fundamental rights.[38]

For example, In the context of automated systems, the EDPS proposed introducing safeguards such as 'human verification', 'meaningful explanation', and 'reporting'.[39]

[31] Brkan M., 'The Concept of Essence of EU Fundamental Rights in the EU Legal Order: Peeling the Onion to Its Core' (2018) 14(2) European Const tut onal Law Review.
[32] Concerning interference with the rights to data protect on and privacy, see AG opinion Case C-203/15 and C-698/15 *Tele2 Sverige and Watson*, 19 July 2016, paras 138-140, referring to the ECtHR's case law.
[33] Tridimas T., 'The Principle of Proport onality' in Schütze R. and Tridimas T.(eds) *Oxford Principles of European Union Law* (vol I, OUP 2018); AG opinion Case C-203/15 and C-698/15 *Tele2 Sverige and Watson*, 19 July 2016, paras 207 et seqs.
[34] Art cle 5(1)(h) of the AI Act.
[35] See Kindt's report for a general presentat on on necessity and proport onality.
[36] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, paras, 54, 60-62; joined Cases C-203/15 and C-698/15, *Tele2 Sverige and Watson*, 21 December 2016, paras 117-119.
[37] Joined Cases C-203/15 and C-698/15, *Tele2 Sverige and Watson*, 21 December 2016, para. 121.
[38] EDPS Guidelines on Assessing the Proport onality of Measures that Limit the Fundamental Rights to Privacy and to the Protect on of Personal Data, 25 February 2019, ht ps://www.edps.europa.eu/data-protect on/our-work/publicat ons/guidelines/edps-guidelines-assessing-proport onality-measures_en
[39] Ibid, p. 32.

The ***essence of the right*** represents 'core', 'minimum content' of a right, which cannot be infringed, although it is difficult to define what this essence represents.[40] In several decisions, the CJEU assessed whether the essence of the rights to privacy and data protection was infringed. In *Schrems*, the Court considered that 'legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life.'[41] In *Digital Rights Ireland*, the Court considered that the essence of the right to data protection was not adversely affected by data retention measures as some principles existed to ensure that 'appropriate technical and organisational measures [were] adopted against accidental or unlawful destruction, accidental loss or alteration of the data.' [42]

Although Article 52(1) of the Charter is not mentioned in the recitals of the AI Act, **exceptions to the prohibited practices must comply with the requirements outlined in Article 52(1) of the Charter.**

2.3. Actors and AI pract ces

2.3.1 Actors [43]

The AI Act distinguishes different categories of actors: providers, deployers, importers, distributors and product manufacturers.

Providers are natural and legal persons, whether public authorities, agencies or other bodies that develop AI systems, place them on the EU market, or put them into service.[44] According to Article 3 of the AI Act, they either make available the AI systems for the first time ('place on the market,' which refers to introducing the AI systems to the EU market for the first time) or supply the AI systems for first use directly to the deployer or for their own use ('putting into service,' under its own name or trademark, which means using the AI systems for the first time).[45] Providers established or located outside the EU are subject to the AI Act rules if they place them on the EU market or put them into service in the EU. [46] This is linked to the extra-territorial scope of the AI Act.[47]

For example, A **provider** of a remote biometric identification system is the manufacturer or the seller of the system.

Deployers, distributors and importers are considered providers if 1) they put their name or trademark on a high-risk AI system already in the market or put it into service, or 2) they make a substantial modification to a high-risk system already on the market or put it into service, or 3) they

[40] Tridimas T. and Gent le G., 'The Essence of Rights: An Unreliable Boundary?' (2019) 20 German Law Journal 794. On the scope of the essence of the rights, see Els Kindt's report for further developments.
[41] Case C-362/14*, Schrems v. Data Protect on Commissioner*, 6 October 2015, para. 94.
[42] Joined cases C-293/12 and C-594/12, *Digital Rights Ireland*, 8 April 2014, para. 40
See Kindt's report for a general descript on of the essence of fundamental rights.
[43] This sect on gives an overview of the dif erent actors; however, the focus for this study is mainly on providers and deployers.
[44] Art.3(3) AI Act.
[45] Art.3(9) and Art. 3(11) AI Act.
[46] Art. 2(1)(a) AI Act.
[47] ibid.

modify the intended purpose of an AI system not classified as high-risk in such a way that, as a result, it becomes a high-risk system.[48]

For example,
Actors can have different roles:

- If they develop their own AI tools that they use af erwards, they are both providers and deployers.
- If they develop their own AI tools used by other actors, they will be providers.

Deployers are natural or legal persons, public authorities, agencies or other bodies using the AI systems unless the use is for a 'personal non-professional activity.'[49] Deployers are the users of the systems.

For example,
The **deployer** of a remote biometric identification system is the user, i.e. a law enforcement authority (police, prosecutor), an entity or body or individual acting on their behalf, or a private company.

Importers are natural or legal persons located or established in the EU that places on the market an AI system bearing the name or trademark of a natural or legal person established in a third country.[50]

Distributors are natural or legal persons in the supply chain, other than the provider or the importer, that make an AI system available on the Union market. [51]

Product manufacturers are not defined in the AI Act but are understood as defined in the New Legislative Framework.[52]

The AI Act does not provide harmonised rules for the 'end-users', i.e. the persons impacted by the use of the AI system, the persons against whom the AI system is used.[53]

2.3.2 AI pract ces

The AI practices covered by Article 5 of the AI Act are the placing on the EU market, putting into services or using AI systems. According to Article 3(9) of the AI Act, **placing on the market** is 'the first making available of an AI system or general-purpose AI model on the Union market.' As for making

[48] Art. 25(1)(a)-(c) AI Act and Rec. 84 AI Act.
[49] Art. 3(4) AI Act.
[50] Art. 3(6) AI Act.
[51] Art. 3(7) AI Act.
[52] Composed of Regulat on (EC) No 765/2008, Decision No 768/2008/EC and Regulat on (EU) 2019/1020; Rec. 87 AI Act.
[53] The term 'end-users' does not imply that the individuals are using the system or have an act ve role. But it ref ects the fact that the system is deployed for or against them. In her policy brief ng delivered to Ada Lovelace, Edwards uses the expression 'af ected individuals'. See Policing Brief ng, 'People, Risk and the Unique Requirements of AI: 18 Recommendat ons to Strengthen the EU AI Act,' Ada Lovelace, 31 March 2022.

available, it is defined as the supply of the system 'for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge.'[54]

For example, A remote identification biometric system developed outside the EU by a foreign manufacturer is placed on the EU market for the first time when it is first sold in one of the EU countries.

Article 3(11) of the AI Act defines **putting into service** as 'the supply of an AI system for first use to the deployer or for own use in the Union for its intended purpose.' The intended purpose is the 'use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions of use, promotional or sales materials and statements, as well as in the technical documentation.'[55]

For example, A company that bought a remote biometric identification system built outside the EU supplies it to a law enforcement authority or a private company to be used for the first time.

Although the **use** of an AI system is not defined in the AI Act, it should be understood that it covers deployment under normal conditions, i.e., as specified by the provider of the system and the technical documentation accompanying the system.

For example, A remote identification system, such as facial recognition software, used by a shop owner, according to the technical specifications provided by the seller of the system.

2.4 Interplay with exist ng legislat on

As acknowledged in Recital 9, the AI Act is a horizontal Regulation that applies across sectors but without prejudicing existing EU law, in particular on the protection of personal data, consumer protection, fundamental rights, employment, protection of workers, and product safety. The AI Act complements existing legislation. Concerning the restrictions on the use of RBI systems for law enforcement purposes, the AI Act applies as a *lex specialis* of Article 10 of the LED.[56] The AI Act does not overlap with the LED but should apply in addition to and comply with the LED. See section 3 for detailed explanations on the *lex specialis* and the data protection rules.

Finally, the prohibitions outlined in Article 5 of the AI Act and the explicit exceptions to these prohibitions cannot be used to circumvent obligations derived from other EU laws or infringe on other EU laws.[57]

[54] Art. 3(10) AI Act.
[55] Art. 3(12) AI Act.
[56] Rec.38 AI Act.
[57] Art. 5(8) AI Act.

2.5 Enforcement aspects

2.5.1 National Competent Authorities

Member States must designate competent authorities to supervise and enforce the AI Act. These competent authorities should include, at least, one **notifying authority** and **one market surveillance authority**.[58] According to Article 3(26) of the AI Act, market surveillance authorities (MSA) are the 'national authority[ies] carrying out the activities and taking the measures pursuant to Regulation (EU) 2019/1020.' MSAs enforce the AI Act rules, investigate complaints and impose penalties for violations of the AI Act rules, while notifying authorities are responsible for 'setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring.'[59]

According to Article 74(2) of the AI Act, market surveillance authorities must 'annually report to the European Commission about the use of prohibited practices that occurred during that year and about the measures taken.' The European Data Protection Board (EDPB) issued a statement, statement 3/2024, concerning the role that DPAs could play in the enforcement and implementation of the AI Act and their designation as Market Surveillance Authorities in several cases, including for 'high-risk AI systems used for law enforcement, border management, administration of justice and democratic processes.'[60]

Designation of Market Surveillance Authorities and the role of national DPAs: the case of the Netherlands[61]

Concerning the supervision of the AI Act rules, the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), together with the Dutch Authority for Digital Infrastructure (*Rijksinspectie Digitale Infrastructuur*), has provided an opinion to the Dutch government on the supervisory structure in the Netherlands. A part relates to the supervision of the prohibited practices. In their advice, the authorities recommend designating the Dutch DPA as a market surveillance authority for the prohibited AI systems concerning real-time use of RBIs, biometric categorisation, emotion recognition, untargeted facial image scraping and predictive policing. Relating to the real-time use of RBIs and predictive policing systems, the Dutch DPA will be the market surveillance authority, while the Inspectorate of Justice and Security (*Inspectie Justitie en Veiligheid*) will be involved in the supervision as the sector-specific supervisory authority. A follow-up opinion will explain how the cooperation between the market surveillance authority (the Dutch DPA) and the sector or domain-specific supervisory authorities will be implemented.

[58] Rec. 153 AI Act and Art. 3(48) AI Act.
[59] Article 3(19) AI Act and Article 28 AI Act.
[60] EDPB, Press release on the EDPB's statement on DPAs role in AI Act framework https://www.edpb.europa.eu/news/news/2024/edpb-adopts-statement-dpas-role-ai-act-framework-eu-us-data-privacy-framework-faq_en
EDPB, 'Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework', 16 July 2024, https://www.edpb.europa.eu/system/files/2024-07/edpb_statement_202403_dpasroleaiact_en.pdf
[61] https://autoriteitpersoonsgegevens.nl/en/current/ap-and-rdi-supervision-of-ai-systems-requires-collaboration-and-must-be-arranged-quickly

2.5.2 Fines for non-compliance

According to Article 99 of the AI Act, Member States will have to establish rules on penalties and other enforcement measures (including warnings addressed to operators or non-monetary measures) for infringements of the AI Act. The AI Act follows a tiered approach to impose penalties for non-compliance with the AI Act rules, linking the seriousness and severity of the infringement to the level of the fine.

Non-compliance with the prohibitions of the AI practices provided in Article 5 of the AI Act are the most severe infringements. Therefore, they are subject to administrative fines of up to 35 million euros or, in case of an undertaking, 7% of the total worldwide annual turnover for the preceding financial year, whichever is higher.[62] Member States should notify the European Commission of the rules on penalties and other enforcement measures they have adopted, at the latest by the date of entry into application of the AI Act. [63]

Date of Application of the penalties provision for prohibited AI practices
Following Article 113 of the AI Act, chapter XII on penalties, which includes Article 99, will apply on 2 August 2025. Consequently, the **provision on penalties for non-compliance with the prohibition of the AI practices** of Article 5 will not apply before **2 August 2025** while the **rules on the prohibited practices** will apply from **2 February 2025**.

2.6 Exclusions of Member States

In application of protocols annexed to the TFEU, two Member States have a special status and a discretion in applying or not the rules prohibiting the real-time use of RBIs for law enforcement purposes, the conditions applicable to the exceptions, and the rules on retrospective use of RBI for law enforcement purposes.[64]

Ireland[65]
With the discretion granted to Ireland under Protocol No. 21 on the position of the United Kingdom and Ireland in the area of freedom, security and justice (AFSJ) annexed to the TEU and TFEU, Ireland can decide not to apply the rules concerning the prohibition of real-time use of RBIs in public spaces for a law enforcement purpose as well as the procedural rules linked to that article (Article 5(2) to Article 5(6) of the AI Act). Similarly, Ireland is not bound by the rules on retrospective RBI for law enforcement outlined in Article 26(10) of the AI Act. The discretion is linked to the fact that Ireland is not bound by obligations on judicial cooperation in criminal matters or police cooperation. This results from the opt-outs given to Ireland (and the UK) in the AFSJ.

[62] Art cle 99(4) AI Act.
[63] Art cle 99(2) AI Act.
[64] And the prohibit on concerning biometric categorisat on for law enforcement purposes and AI systems used for predict ve policing, which are not covered by the scope of this study, see recitals 40 and 41 of the AI Act;
For more informat on on these opts-out, see Chevallier-Govers C., 'Art cle 67 TFEU [Establishing the AFSJ]' in Blanke H-J and Mangiameli S. (eds) *Treaty on the Funct oning of the European Union – A Commentary* (Springer)
[65] Rec.40 AI Act.

Denmark[66]
Denmark benefits from opt-out agreements when applying Protocol No. 22 to the TEU and TFEU and can decide not to fully apply the prohibitions of Article 5 of the AI Act.

3 Real-t me Remote Biometric Ident f cat on Systems

Article 5(1)(h) of the AI Act prohibits:

> *the use of 'real-t me' remote biometric ident f cat on systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as such use is strictly necessary for one of the following object ves […]*

This section analyses the ban on real-time use of RBIs for law enforcement purposes and the three cases for which Member States can choose to allow, through their national legislation, the real-time use of RBI systems. Member States are free to allow the three exceptions, some of them, or not to allow any of them. In the absence of national legislation allowing the real-time use of RBI in publicly accessible areas for one of the three cases, law enforcement authorities and entities acting on their behalf will not be allowed to deploy the technologies. Thus, the existence of a national legislation that complies with the requirements of Article 5(2) of the AI Act is a pre-requisite.

Each component of the prohibition will be explained together with the rationale of the ban and the exceptions.

3.3 Rat onale of the prohibit on

The rationale for the prohibition of the real-time use of RBIs in publicly accessible spaces for law enforcement purposes can be found in Recital 32 AI Act. In that recital, the AI Act acknowledges the 'intrusive nature' of RBIs on the right to privacy (their use 'may affect a large part of the population' and 'evoke a feeling of constant surveillance'), on the 'freedom of assembly and on other fundamental rights.'

As identified among others by the FRA and the EDPB,[67] those fundamental rights include:

- The right to data protect on as RBIs rely on the processing of biometric data and other personal data (e.g. names, ID numbers, as well as sensit ve data such as ethnicity) to ident fy specif c individuals.
- Freedom of expression in public spaces, as if individuals know they are monitored, they might change their behaviour.[68]
- The right to an ef ect ve remedy and a fair trial.
- The right to non-discriminat on and the right to human dignity.

[66] Rec.41 AI Act.
[67] FRA's Report on Facial Recognition in the Context of Law Enforcement and EDPB's Opinion 05/2022.
[68] van der Sloot B. and Lanzing M., 'The Continued Transformation of the Public Sphere: On the Road to Smart Cities, Living Labs and a New Understanding of Society' in Nagenborg M. and others (eds) Technology and the City: Towards a Philosophy of Urban Technologies (Springer 2021).

Due to the serious interferences that their use poses to fundamental rights, their deployment is, in principle, not allowed. However, as most of these fundamental rights are not absolute,[69] interferences, such as in the context of public security, justify restrictions on exercising these rights as provided by Article 52(1) of the Charter. Any limitation must comply with the requirements of legality, necessity, proportionality and respect for the essence of fundamental rights, as already described.

Until the adoption of the AI Act, no legal rules applied to the deployment and use of RBIs. Those systems were only regulated by data protection rules as they process personal and biometric data for their functioning. Personal data are defined as information relating to *an identified or identifiable* individual,[70] whereas biometric data are a category of personal data, which result 'from *specific technical processing* relating to the physical, physiological or behavioural characteristics of a natural person, which *allow or confirm the unique identification* of that natural person, such as facial images or dactyloscopic data'.[71] Biometric data that are processed for the purpose of *uniquely identifying* an individual fall into the category of sensitive data. The regime applicable to the processing of sensitive data under the GDPR and the LED, and the different concepts of biometric data, are explained in the next section.

3.4 Background

3.4.1 Biometric recognit on technologies

Biometric recognition technologies detect, capture, and transform measurable physical characteristics (such as eye distance and size, nose length, etc.) or behavioural characteristics into machine-readable biometric data.[72] These data are available in different forms: images or templates, which are a mathematical representation of the salient features used for recognition purposes. Biometric recognition technologies are used for two purposes: **verification** and **identification** purposes. [73] Verification consists in comparing data presented at a sensor with another set of previously recorded data stored on a device, such as a smartphone, a passport, an ID card, or in a single database. This is known as a one-to-one comparison. The purpose of the verification modality, often called authentication, is to check if the person is who they claim to be and not to establish who they are. This modality is used in access control, identity checks, or as a password replacement.[74]

For example, [75]

[69] The right of human dignity is an absolute fundamental right; as such it cannot be limited under any condit ons, as already ment oned.
[70] Art.4(1) GDPR and Art. 3(1) LED.
[71] Art. 4(14) GDPR and Art.3(13) LED.
[72] eg Hamsici O.C. and Mart nez A.M., 'Face Recognit on, Component-Based', in Li S.Z., Jain A.K. (eds) Encyclopedia of Biometrics (1st ed. Springer Science, 2015).
[73] As def ned by the biometrics community in ISO/IEC Standard 2382-37:2022 Informat on Technology - Vocabulary, Biometric recognit on, Term 37.01.03.
[74] eg Ross A., Jain A.K. (2015) 'Biometrics, Overview' in Li S.Z. and Jain A.K. (eds) Encyclopedia of Biometrics, (1st ed. Springer Science, New York), pp. 289-294.
[75] E.g. Factsheet, Entry-Exit System for non-EU cit zens, ht ps://home-af airs.ec.europa.eu/document/download/3bcec877-43b6-4de4-b440-300ab47462be_en?f lename=factsheet_-_entryexit_system_en.pdf

The capture of a traveller's facial images and fingerprints, as a pre-enrolment stage for automated border control checks, is a processing operation that enables identity verification at the borders. When the traveller crosses the borders, their recorded data in a border control system (such as the Entry-Exit System) will be compared with their live biometric data. This is a **one-to-one comparison**.

The second modality, **biometric identification**, compares captured data with multiple sets of data to find who the person is, i.e. whether there is a match between the data presented at the sensor and any other data contained in databases used for comparison purposes. This is the one-to-many comparison. **From a technical perspective, identifying someone is not establishing the identity of a person** or **knowing the name** but determining if the person is known in any of the databases checked during the identification process. Identification is often used in criminal investigations. As explained in this study, the biometric recognition technologies that are covered by the notion of **RBI** in the AI Act **are biometric technologies used for identification purposes only**.[76]

Beyond identification and verification, biometric recognition technologies can be used for purposes other than biometric recognition. For instance, they **can be used for biometric categorisation** (linked to gender classification or age estimation for example) or **emotion detection**. But in these cases, although the technologies are called biometric recognition technologies, they technically do not perform biometric recognition. [77]

Functioning of a facial recognition system used for identification purposes

Several technical steps can be distinguished from the capture of the biometric characteristics to their transformation into biometric data.[78] These steps can be defined, for example, as follows:[79]

1) Images are captured through CCTV cameras or other video devices ('**image acquisition'**)
2) Within the frame captured, human faces are detected ('**face detection'**)
3) Those facial images are then enhanced, i.e. their quality is improved, to extract the physical features that will be used to perform the identification ('**facial extraction**')
4) The extracted features are then transformed into a biometric template, which is a mathematical representation of the facial features ('**template generation'**)
5) The template is then compared with other biometric data to measure the percentage of similarity between them ('**face comparison'**)

[76] Rec. 17 AI Act.
[77] Since biometric recognit on only covers ident f cat on and verif cat on, Term 37.01.03, ISO/IEC Standard 2382-37:2022.
[78] See Jasserand C. ''Biometric Data, Within and Beyond Data Protect on' in van der Sloot and van Schendel (eds) The Boundaries of Data (AUP 2024); A29WP, Opinion 3/2012 on developments in biometric technologies, 27 April 2012, WP193; A29WP, Opinion 02/2012 on facial recognit on in online and mobile services, 22 March 2012, WP192.
[79] It should be noted there is no standardised way to present these steps. Inspiration for the description was taken in part from the functioning of the live automated facial recognition system (called AFR) used by the South Wales Police, in *Bridges v. South Wales Police*, see [2019] EWHC 2341 (Admin), paras 23-25.

For comparison purposes, a **reference database** needs to be established, i.e. a database containing other facial images or facial templates against which the generated image or template will be compared.

3.4.2 Not on(s) of biometric data

Biometric recognition systems rely on the measurement of identifiable features, such as measurable facial characteristics, to perform biometric recognition. The systems collect and process biometric data for their functioning. Biometric data is both a technical notion and a legal notion.

Definition of biometric data in the data protection framework

While a legal definition of biometric data has been introduced in EU the data protection framework, a more inclusive definition of biometric data has been introduced in 3(34) of the AI Act. From a data protection perspective, biometric data aredefined as:

> 'personal data resulting from technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data'[80]

The definition is composed of four elements:

1) their qualif cat on as personal data (i.e. they relate to an ident f ed or ident f able individual),
2) the technical processing through which biometric data are generated (which should include the transformat on of biometric characterist cs into a biometric template),
3) the biometric characterist cs from which the data are generated (physical and physiological characterist cs,[81] such as an individual's biological characterist cs, e.g. facial features, f ngerprint ridges, and behavioural characterist cs, relat ng to how a person moves, speaks, types, etc., e.g. gait recognit on).
4) the purpose of the processing: allowing or conf rming the unique ident f cat on.

There is uncertainty concerning the meaning of *unique identification*, whether it relates to the biometric identification function[82] or whether it should be interpreted as a threshold of identification from a data protection perspective (where individuals are *uniquely* singled out or identified thanks to the *unique* characteristics of their biometric data) or whether the processing is carried out for identity verification purposes or biometric identification purposes). Beyond a terminological discussion, the criterion of 'unique identification' is used to classify biometric data as sensitive data. According to Article 9(1) GDPR and Article 10 LED, biometric data fall into the special category of data (i.e. sensitive data) if they are processed to *uniquely identify* an individual. Although the debate is not settled, biometric data that are processed for purposes other than biometric recognition (i.e. identification or verification) do not fall into the legal definition of biometric data under EU data protection law. Thus,

[80] Art. 9(1) of the GDPR, Art. 10 of the LED, and Art. 10(1) of the EUDPR.

[81] Physical and physiological characterist cs are not necessarily dist nguished in technical papers, see also the def nit on of biometric recognit on by the UK DPA, ICO, ht ps://ico.org.uk/for-organisat ons/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognit on/biometric-recognit on/

[82] e.g. See Tosoni L. and Bygrave L.A., 'Art cle 3, Def nit ons' in the EU Law Enforcement Direct ve (LED), A Commentary

biometric data processed for categorisation purposes and emotion recognition, whose purpose is not to identify an individual, are excluded from this GDPR/LED/EUDPR definition.

Definition of biometric data in the AI Act

Article 3(34) of the AI Act defines 'biometric data' as:

> personal data resulting from technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, such as facial images or dactyloscopic data.

The AI Act provides a broader definition of biometric data than that in the EU data protection instruments as '[b]iometric data [under the AI Act] can allow for the authentication, identification or categorisation of natural persons and for the recognition of emotions of natural persons.'[83] Yet, from a data protection perspective, it is understood that personal data relating to biometric characteristics and processed for emotion or categorisation purposes do not fall under the definition of biometric data.[84] Although the notion of biometric data in the AI Act should be interpreted in light of the definitions provided in Article 4(14) of the GDPR, Article 3(13) of the LED, and Article 3(18) of the EUDPR, the definition builds on the constitutive elements of biometric data from a data protection perspective to the exception of the purpose of processing (i.e. 'to allow or confirm the unique identification').

Biometric data as sensitive data

From a data protection perspective, biometric data processed to u*niquely identify* an individual fall into the special categories of personal data. The rules applicable to their processing are different in the GDPR and the LED.

GDPR rules

The processing of the special categories of personal data (also referred to as sensitive data) is prohibited under the GDPR unless an exception applies.[85]

Article 9(2) of the GDPR provides ten legal grounds:

- Explicit consent of the data subject (Art.9(2)(a) GDPR)
- In the f eld of employment, social security and social protect on law (Art.9(2)(b) GDPR)
- Protect on of vital interests (Art. 9(2)(c) GDPR)
- Legit mate act vit es of a foundat on, associat on or not-for-prof t body with a polit cal, philosophical, religious or trade union aim (Art. 9(2)(d) GDPR)
- Data manifestly made public by the data subject (Art. 9(2)(e) GDPR)
- Establishment, exercise or defence of legal claims (Art. 9(2)(f) GDPR)
- Substant al public interest (Art. 9(2)(g) GDPR)
- Prevent ve or occupat onal medicine (Art. 9(2)(h) GDPR)
- Public interest in the area of public health (Art. 9(2)(i) GDPR)
- Archiving purposes in the public interest, scient f c or historical research purposes or stat st cal purposes (Art. 9(2)(j) GDPR)

[83] Rec. 14 AI Act.

[84] Due to their purpose of processing, which is to *uniquely ident fy*.

[85] Art. 9(2) GDPR.

In addition, Member States can introduce further conditions or restrictions concerning the processing of biometric data.[86]

GDPR and legal bases to process biometric data through facial recognition technologies

- The **French DPA** considered that **only three exceptions** could justify the processing of biometric data: the data subject's explicit consent, substantial public interest, and the protection of vital interests.[87]

- On the occasion of an official warning against a Dutch supermarket that used FRT for security and shoplifting prevention, the **Dutch DPA** considered that **only two legal bases** could be invoked for the deployment of FRTs: explicit consent and substantive public interest.[88] In the case of the supermarket, customers did not explicitly consent to the use of FRT. Conducting a strict necessity and proportionality test, the Dutch DPA found that ensuring the security of the supermarket by scanning the faces of everyone was not justified, as there were other means to ensure the protection of the property, staff and customers. For instance, the supermarket could use surveillance cameras without facial recognition. Thus, no substantive public interest justified the use of FRT and the processing of biometric data.[89]

LED rules

By contrast**, Article 10 of the LED allows the processing** of sensitive data only **when strictly necessary**, **subject to appropriate safeguards**, and in **three cases**: when authorised by Union or Member State law, to protect the vital interests of an individual, and when the data have been manifestly made public by the data subject.[90]

Yet, **several Member States experimented with facial recognition technologies in public spaces, including for policing purposes, without a clear legal framework**.[91] In France, the municipality of Nice trialled live facial recognition technologies on volunteers during the Carnival in 2019, relying on the explicit consent of the participants. However, as observed by the French DPA, there was no other legal basis was available for deploying the technologies for policing purposes.[92] In the UK, when it was still part of the EU, more than ten police forces trialled the technologies on different occasions, which led to some arrests.[93] In Italy, the Italian DPA stopped the deployment of the SARI Real-Time System (live

[86] As well as genet c data and data concerning health; Art. 9(4) GDPR.
[87] CNIL, 'Facial Recognit on: For A Debate Living Up to the Challenges' (2019), p.6
[88] ht ps://www.edpb.europa.eu/news/nat onal-news/2021/dutch-dpa-issues-formal-warning-supermarket-its-use-facial-recognit on_en
See also ht ps://autoriteitpersoonsgegevens.nl/documenten/juridisch-kader-gezichtsherkenning
[89] ht ps://autoriteitpersoonsgegevens.nl/documenten/juridisch-kader-gezichtsherkenning
[90] Art. 10 (a)-(c) LED.
[91] For an overview of Member States' experiments and deployments of FRTs, see Algorithmic Watch, 'Automat ng Society, Report 2020'; Montag L. et al. 'The rise and rise of biometric mass surveillance in the EU'(2021) ht ps://edri.org/wp-content/uploads/2021/11/EDRI_RISE_REPORT.pdf
[92] No specif c law existed in France to allow police authorit es to deploy live FRTs in public spaces in applicat on of Art cle 10 of the LED.
[93] In France, the municipality of Nice experimented FRTs on volunteers during the Carnival of 2019; while in the UK more than ten police forces across the country trialled FRTs for test ng and operat onal purposes, for more

facial recognition technologies) that the Italian Ministry of Interiors had planned to deploy, while there was no adequate legal basis for such a system.[94]

As observed by the EDPB, **a mere transposition of Article 10 of the LED into national laws does not constitute the legal basis** for processing biometric data since such a law would not be specific enough and lack foreseeability.[95] In particular, such a general clause 'would **lack specific requirements** indicating the **circumstances** in and **conditions** under which **law enforcement authorities** would be **empowered to resort to using facial recognition technology**.' [96]

The AI Act has introduced a general prohibition for the real-time use of RBI systems for law enforcement purposes, subject to limited exceptions, as explained in this section. This prohibition is conceived as a *lex specialis* to Article 10 of the LED, preventing a Member State from adopting national legislation to allow their use based on the implementation of Article 10 of the LED.[97]

Lex specialis

The rules that prohibit the real-time use of RBI, subject to certain exceptions, should apply as *lex specialis* to Article 10 of the LED.[98] Article 5 of the AI Act provides a framework of rules and does not provide the legal basis to process biometric data for any of the exceptions permitted under Article 5(1)(h)(i)to(iii). Member States need to adopt a national law to allow these exceptions, should they decide to allow them.[99] As specified in Recital 94 of the AI Act, the processing of biometric data linked to RBI for law enforcement purposes must comply with the conditions outlined in Article 10 of the LED, i.e. strict necessity, the existence of safeguards, and a legal basis. Thus, the rules of the AI Act must comply with Article 10 of the LED and the requirements laid down in Article 5 of the AI Act.

Other cases

The processing of biometric data involved in the use of RBI, in cases other than real-time RBI for a law enforcement purpose in publicly accessible spaces, is subject to Article 10 of the LED for **a law enforcement purpose**.

For example, The processing of biometric data that results from the retrospective use of a voice recognition system for a criminal investigation remains subject to Article 10 of the LED. Such processing needs, therefore, to be allowed by clear and specific provisions at national level.

informat on, see Jasserand C. 'Experiments with Facial Recognit on Technologies in Public Spaces: in Search of an EU Governance Framework' in Zwit er A. and Gstrein O.J. (eds) *Handbook on the Polit cs and Governance of Big Data and Art f cial Intelligence* (EE 2023).

[94] Il Garante, Opinion on the Sari Real Time System, 25 March 2021, No.9575877 (*Parere sul sistema Sari Real Time - 25 marzo 2021 [9575877]*) ht ps://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877

[95] EDPB, 'Guidelines 05/2022 on the use of facial recognit on technology in the area of law enforcement', version 2.0, 26 April 2023, p.21.

[96] ibid.

[97] Art. 10(a) of the LED.

[98] Rec. 38 AI Act.

[99] Rec. 37 and Art. 5(5) AI Act.

For **purposes other than law enforcement**, the rules provided by Article 9(1) of the GDPR and Article 10(1) of the EUDPR remain applicable, prohibiting the processing of biometric data unless an exception applies.[100] The rules of the AI Act will not allow the circumvention of existing rules and prohibitions or decisions taken by national DPAs.

3.5 Scope of the prohibit on

Different elements composed the prohibition: the notion of RBIs, the definition of use, the meaning of real-time, the definition of publicly accessible spaces, and the scope of law enforcement purposes. These elements are defined below.

3.5.1 Not on of RBI

According to Article 3(41) of the AI Act, a remote biometric identification system is:

> *An AI system for the **purpose of ident fying** natural persons, **without their act ve involvement**, **typically at a distance** through the **comparison** of a person's **biometric data** with the **biometric data contained in a reference database**.*

The definition is linked to the identification functionality of biometric systems, where the systems are deployed in a 'one-to-many comparisons', which implies the absence of active involvement (i.e. no participation, contrary to the capture of fingerprints) that results in the capture of the characteristics at a distance most of the time. For identification performance, the captured biometric data are compared with biometric data already stored in a reference database (such as a repository, e.g. a criminal database containing facial images or templates of suspects).

Identification purposes only

The notion of 'biometric identification' in the AI Act is defined as

> 'the automated recognition of physical, physiological and behavioural human features such as the face, eye movement, body shape, voice, prosody, gait, posture, heart rate, blood pressure, odour, keystroke characteristics'
>
> 'for the purpose of establishing an individual's identity'.[101] Thus, **AI systems that are intended to be used for biometric verification are excluded from the scope of RBI**. [102]

Examples of those systems used for verification purposes are, for instance, systems deployed for **access control purposes**

For example, A face verification system could be deployed to enter a restricted area (e.g. power plant premises) through face scanning; the system compares the face of the individual presented at the entrance camera with a reference image contained in a reference database of persons allowed to enter the building.

[100] Rec. 39 AI Act.
[101] Rec. 15 AI Act; Art cle 3(35) AI Act adds 'psychological human features' to the list of characterist cs.
[102] Rec. 17 and Art. 5(5) AI Act.

or **identity verification at the borders**

For example, Through the comparison of a traveller's face scanned at an e-gate with the facial image contained in their passport.

The **exclusion of identity verification systems** from the scope of RBI is justified, in the AI Act, by their 'minor impact on fundamental rights' by comparison with that of 'remote identification systems' involving 'a large number of persons without their active involvement.'[103]

It should be noted that these systems are not part of the list of high-risk AI systems in Annex III of the AI Act and are not subject to transparency obligations imposed on *limited* risk AI systems.[104] Unless they are linked to a high-risk AI system as listed in Annex III (for instance, using a biometric verification system in the context of access to educational training ,as provided in Annex III, 3(a)), they are excluded from the scope of the AI Act. However, they are subject to other rules, and, in particular, the GDPR rules on the processing of personal data for biometric verification purposes (such as the existence of a legal basis, a data protection impact assessment, and envisaged alternative solutions).

For example, The Dutch DPA considered that using a facial verification system to access the repair shop of a garage would not be justified, i.e. not proportionate and necessary, based on the GDPR rules applicable to the processing of biometric data.[105]

Remoteness

The particularity of these biometric systems is their ability to identify individuals without their active involvement, which can imply a distance but not necessarily. Fall into the definition of RBI any AI tools that allow 'automated recognition of human features in public spaces.'[106]

For example, Typical RBI systems are facial recognition, voice recognition or gait recognition systems.[107] Biometric recognition systems that process fingerprints, DNA, keystrokes and other biometric and behavioural signals also fall into the category of RBI systems.[108]

⚠ In their joint opinion on the proposal for the AI Act, the EDPS-EDPB described these technologies as 'frictionless'. [109] It could be questioned whether the notion of RBI includes frictionless or contactless biometric systems in case individuals actively provide their biometric

[103] Rec. 17 AI Act.
[104] Art. 50(4) AI Act.
[105] See AP, 'Voorlicht ng -regels voor gezichtsherkenning in supermarkten' (Explanat ons – rules concerning facial recognit on technologies in supermarkets), 1 May 2020, p. 4; as well as ht ps://autoriteitpersoonsgegevens.nl/themas/ident f cat e/biometrie/regels-voor-gebruik-biometrie#afweging-gebruik-biometrie-voor-authent cat e-of-beveiliging
[106] EDPB-EDPS, Joint Opinion 5/2021, pp. 12-13; Council of the European Union, 'Opinion of the Legal Service', 12302/22, 12 September 2022, para. 33, and Recital 15 of the AI Act.
[107] Impact Assessment, SWD (2021) 84 f nal, p.18.
[108] fn 106.
[109] EDPB-EDPS, Joint Opinion 5/2021, p12.

data, such as for some types of fingerprint systems, and are, thus, not passive in the collection of their data.

Reference database

Identification is not possible without a reference database containing biometric data for comparison purposes. Thus, the existence of a reference database is **indispensable** to perform the comparison for identification purposes. The reference database needs to be appropriate for each use of the real-time RBI system.[110]

For example,
In the case of missing persons, the SIS II database could be used as the reference database for facial recognition purposes (once operational).

3.5.2 Use only

As mentioned, the AI Act does not define the term 'use'; only 'reasonably foreseeable misuse' is defined in relation to high-risk AI systems as part of their risk management.[111] By use, one could understand deployment.

The prohibition only covers the use of the technologies; it does not cover all the other practices, whether their development, placing on the EU market or putting into service. Only real-time use of RBI for a law enforcement purpose is considered to infringe fundamental rights, so it must be prohibited (except in three situations). Ex-post use of the same technologies for a law enforcement purpose falls into the category of high-risk systems. This results from the political negotiations between the EU institutions. The European Parliament was in favour of a more extensive ban on RBI systems deployed in publicly accessible spaces by all actors (public and private), with the limited exception of retrospective use to prosecute specific serious crimes after judicial authorisation.[112] The European Commission and Council supported a more restricted ban of real-time RBI for a law enforcement purpose.[113] As a result of the negotiations, the AI Act lays down:

- A **ban** for real-t me use of RBI systems in publicly accessible areas for a law enforcement purpose (Art cle 5(1)(h) of the AI act), **except in three situat ons** (Art cle 5(1)(h)(i)-(iii) that must be authorised by nat onal legislat on and comply with certain condit ons and safeguards (Art cle 5(2)-(7) of the AI Act).

- **A classif cat on of all the other uses of RBI systems**, as well as **their placing on the market and put ng into service**, in the category of **high-risk systems** as ident f ed in Annex III (Art cle 6(2) of the AI Act).

[110] Rec. 34 AI Act.
[111] Art. 3(13) AI Act and Art. 9 AI Act.
[112] EP, 'Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulat on of the European Parliament and of the Council laying down harmonized rules on art f cial intelligence (Art f cial Intelligence Act) and amending certain Union legislat ve acts,' Amendment 227.
[113] Council's General Approach on the Art f cial Intelligence Act, 6 December 2022, 14954/22.

- In addition, **specific rules are applicable to the retrospective use of RBI systems for law enforcement purposes** (Article 26(10) of the AI Act). Due to the intrusive nature of ex-post use of RBI systems, they should be subject to safeguards, be used in a way that is proportionate, legitimate, strictly necessary, and targeted. Article 26(10) of the AI Act refers to the *targeted search* of a suspect or perpetrator of a criminal offence but also to the use of the technologies in a *targeted way*.

Although this study is limited to the prohibited practices, it will also mention the rules applicable to retrospective use of RBI for law enforcement purposes (see section 3.7).

3.5.3 Real-time

Real-time means that the systems capture and further process biometric data 'instantaneously, near-instantaneously or in any event without any significant delay.' [114] All the processing steps, i.e. the capture of biometric data, comparison, and identification, occur at the same time or almost simultaneously, which can include a 'limited short delay' to avoid the prohibition being circumvented through retrospective use of RBI systems.[115] The notion of 'without a significant delay' is not defined; it will be appreciated on a case-by-case, based on the state-of-the-art of real-time RBI systems.

For example,
The live automated facial recognition system deployed by the South Wales Police authorities during the Champions League could process up to 5 images per frame and 10 frames per second, enabling the system to scan up to 50 faces per second.[116]

⚠ Based on the technical papers consulted, there is no consensus about what **real-time** means as it is **not a performance metric**. Technical papers refer to the **image processing speed** or the number of frames a system can process per second (known as **fps**, i.e. **frame per second**).
Technical experts working on the ongoing *ISO/IEC DIS 9868 Standard on Biometric Identification Systems Involving Passive Capture Subjects* might have specific technical references to provide on their understanding of real-time.

As there is no consensus in scientific papers on what real-time means,[117] one could argue that a system generating a match or non-match within a few seconds (or fraction of seconds) is real-time, while a system generating the same result after one hour might not be.

[114] Rec. 17 AI Act.
[115] Art. 3(42) AI Act.
[116] As described on the website of the UK College of Policing, https://www.college.police.uk/app/live-facial-recognition/live-facial-recognition; see also Davies B. et al. 'An Evaluation of South Wales Police's Use of Automated Facial Recognition' (2018), p.17.
[117] e.g. the following papers do not provide a definition of real-time but illustrate the speed of the different steps of the facial recognition process through the frame per second (fps) speed; e.g. Adhikari B. et al., 'Towards a Real-Time Facial Analysis System' (2021) IEEE 23rd International Workshop on Multimedia Signal Processing; Álvarez Casado C. and Bordallo López M., 'Real-Time Face Alignment: Evaluation Methods, Training Strategies and Implementation Optimization,' (2021) 18 Journal of Real-Time Image Processing, pp. 2239-2267.

Thus, the prohibition does not cover the retrospective use of RBIs for law enforcement purposes in publicly accessible spaces, such as police forces using facial recognition technologies on recorded video feeds from CCTV cameras to identify a suspect.[118] This case falls into the high-risk category of AI systems, as listed in Annex III of the AI Act,[119] the study of which falls outside the scope of this study on Article 5 of the AI Act.

3.5.4 Publicly accessible spaces

Following Article 3(44) of the AI Act, **publicly accessible spaces** are defined as:

> 'any publicly or privately owned physical space accessible to an undetermined number of natural persons, regardless of whether certain conditions for access may apply, and regardless of the potential capacity restrictions.'

Several elements characterised these spaces: [120]

- **Accessibility to an undetermined number of persons**, independently of the potent al capacity or security restrict ons, such as purchasing a t cket or t tle of transport, prior registrat on or having a certain age. However, the possibility of get ng access to a space through an unlocked door does not mean that the space is publicly accessible if indicat ons or circumstances are suggest ng the contrary (such as a sign restrict ng access). Besides, access to a space can be limited to certain persons, as def ned by law, linked to public safety or security, or to the decision of the person having the relevant authority over the space.

For example, are publicly accessible spaces:

- a concert arena for which part cipants pay an entrance fee.
- an event locat on with a trade fair is organised target ng part cipants over 50.

A space closed by a gate, even if the gate is unlocked, such as the gated entrance of a fenced residential area of several houses, will not be considered a publicly accessible space. By contrast, a park in a gated residence with public opening hours without any access restriction during those hours will be a publicly accessible space during the opening hours and a closed space outside these opening hours.

- **Irrelevance of their ownership**, i.e. they do not need to be owned by public authorit es to be considered publicly accessible spaces.

For example, the space can be owned by a private entity, a public entity, or a public entity and managed by a private party, without impacting the nature of the space.

- **No specif c act vity for which the space is used;** a publicly accessible area is **not** a space **linked to a public service.** It can be linked to a public service, but it does not have to be.

For example, these spaces can be used for **commerce**, such as shops, restaurants, cafés; for **services**, such as banks, professional activities (a doctor's office as well as an accountant's office),

[118] Rec. 95 and Art cle 26(10) AI Act.
[119] Art. 1(a) of Annex III.
[120] Rec. 19 AI Act.

hospitality (e.g. a hotel); for **sport**, such as swimming pools, gyms, stadiums; for **transport**, such as bus, metro and railway stations, airports, means of transport; for entertainment, such as cinemas, theatres, museums, concert and conference halls; or for **leisure** or otherwise, public roads and squares, parks, forests, playgrounds.[121]

The following spaces are **excluded from the definition**:

- **online spaces** as they do not const tute a physical space

For example, chat rooms, social media, online platforms, etc. are, therefore, excluded from the scope of publicly accessible spaces.

- **spaces meant to be accessed by a limited number of persons**, such as factories, companies and workplaces with entry control or limitat ons to relevant employees or service providers.

For example, a workplace accessible with a badge is not considered a publicly accessible space, whereas an office without entry control falls into the category of publicly accessible spaces.

- **prisons and border control**.

Some spaces can have a dual function. For example, an airport is considered a publicly accessible area for the common areas, but the area dedicated to border control (where the customs stand and check passports or ID documents) is excluded from the scope of a publicly accessible space.

As specified in recital 19 of the AI Act, assessing whether a space is accessible to the public should be done case-by-case based on the specificities of the individual situation at hand.

3.5.5 Law enforcement purposes

The prohibition of Article 5(1)(h) applies to law enforcement purposes, irrespective of the entity, authority, or body carrying out the activities.

Law enforcement is defined in Article 3(46) of the AI Act as the '**activities** carried out by **law enforcement authorities** or on their **behalf** for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security.' These activities are also those that constitute the subject matters of the LED in Article 1.[122]

Thus, any interpretation relating to the LED can be used by analogy in the context of the definition of law enforcement in the AI Act.

[121] Rec. 19 AI Act.

[122] Some activities of law enforcement authorities are excluded from the scope of the LED, such as when competent authorities perform administrative tasks (such as human resources). These activities are carried outside the law enforcement framework and fall under the GDPR rules. See Recital 19 GDPR.

First, investigation, detection, and prosecution of criminal offences are 'commonly distinguished stages of the criminal justice process, which precede the criminal trial and the executive phase.'[123] In his opinion in Case C-180/21, AG Campos Sánchez interpreted the scope of Article 1 of the LED. He considered that investigation in the broad sense should be understood as covering both the detection and investigation of criminal offences.[124] Brewczyńska explains that the purpose of these activities is to determine 'whether a crime has taken place, finding a suspect and collecting information, which eventually translates into evidence that can either confirm or deny the assumption that a certain person has committed a crime.' [125] These activities are distinguished from the prosecution of the criminal offence, performed by the prosecutor who formulates the charges.[126] **Second,** the **prevention of criminal offences, including safeguarding against and the prevention of threats to public security** happen before any crimes have been committed. This stage has 'an anticipatory nature.'[127] For instance, police can take 'coercive measures at demonstrations, major sporting events or riots' in the context of crime prevention.[128] Third, the **execution of penalties** is the execution of sentences. The LED does not specify which types of penalties are covered.

According to Article 3(46) of the AI Act, **these activities** are **performed by law enforcement authorities or on their behalf**. Law enforcement authorities are further defined in Article 3(45) of the AI Act in the same way as the national competent authorities of the LED.[129] The definition covers law enforcement authorities and entrusted bodies or entities (which can be private parties).

> *(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or*

For example, These authorities are public authorities, such as police authorities and criminal justice authorities (such as prosecutors) when they carry out a law enforcement task.

> *(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.*

The second type of law enforcement authorities are entities entrusted by national legislation with public authority and powers for criminal justice and police purposes. These entities must be identified at national level by law and vary from one Member State to another.

---

[123] See Brewczyńska M. 'Article 1, Subject Matter and Objectives', Commentary of the LED, p.60.
[124] AG Opinion, Case C-180/21, para. 52.
[125] fn 123.
[126] In Sweden, the 'prosecutors have three main tasks: to lead the investigations, to bring prosecutions, and to appear in Court'. See https://www.aklagare.se/en/the-role-of-a-prosecutor/#:~:text=Swedish%20prosecutors%20have%20three%20main%20tasks%3A%20to%20lead,to%20bring%20prosecutions%2C%20and%20to%20appear%20in%20court.
[127] fn 123, p.61.
[128] Rec. 12 LED, as cited in Brewczyńska, M. 'Article 1, Subject Matter and Objectives', Commentary of the LED.
[129] Art. 3(7) LED.

Based on the implementation of the LED, entities entrusted to exercise public authority and prerogatives of public power for a law enforcement purpose are, for example:[130]

- The Paris metro company or the Dublin Bus company when they are issuing transport t cket of ences or ensuring the internal security of public transport networks, as explained by the French DPA and the Irish DPA in their respect ve guidance on the scope of the LED.[131] These ent t es are not public authorit es but are entrusted by nat onal law to exercise public power and process personal data for law enforcement purposes.
- Local authorit es when they prosecute lit ering f nes, as ment oned by the Irish DPA in its guidance on the LED. [132]
- Sports federat ons approved to provide security at sport ng events, as ment oned by the French DPA in its guidance on the LED. [133]

Finally, other entities, bodies, or persons, can exercise law enforcement activities on behalf of law enforcement authorities. ***'On behalf'*** means that a law enforcement authority has delegated the task to another entity, including private parties.

⚠ **Interpretation of 'on behalf of' and private entities**

In his analysis of the AI Act, Korff notes an uncertainty concerning private entities to determine when their activities can be considered law enforcement. Taking the example of banks, he explains that when those entities 'detect and counter crimes (such as fraud), they act on their 'own behalf', and are, therefore, excluded from the scope of law enforcement activities. However, when those same banks are requested by law enforcement authorities to conduct certain actions to 'counter certain crimes (such as money laundering)', these activities could fall within the definition of law enforcement as they act 'on behalf' of these law enforcement authorities.

Reference: Korff, D. 'Note, On the Rules in the AI Act on the Use of "Real Time" Remote Biometric Identification in Publicly Accessible Places by Law Enforcement Agencies' https://www.ianbrown.tech/2024/02/01/police-real-time-remote-biometric-id-in-the-ai-act/

Therefore, Article 5(1)(h) prohibits the real-time use of RBI in publicly accessible spaces for a law enforcement purpose, which can be carried out by law enforcement authorities (either public authorities or entrusted entities or bodies) or on their behalf.

[130] These examples are provided by the French DPA and the Irish DPA in their interpretat on of the LED to illustrate who the nat onal competent authorit es are.
[131] As explained by the Irish Data Protect on Authority in its explanat on about the ent t es that are considered competent authorit es under the LED, see the 'Law Enforcement Direct ve', see ht ps://www.dataprotect on.ie/en/organisat ons/resources-organisat ons/law-enforcement-direct ve
[132] Ibid.
[133] Example provided by the French Data Protect on Authority (CNIL), see 'Law Enforcement Direct ve: What are We Talking About?' ht ps://www.cnil.fr/en/law-enforcement-direct ve-what-are-we-talking-about

3.5.6 Examples of prohibited pract ces

Scenario 1 –Real-time crime with RBI systems in publicly accessible spaces to arrest wanted individuals

The police install mobile CCTV cameras equipped with facial recognition technologies on a police van at the main entrance of a football stadium during a European Championship match to secure the area and identify individuals whose faces are recorded in an ad hoc watchlist database of wanted individuals. This watchlist includes persons suspected of having committed a crime (ranging from serious crimes to frauds and burglaries), persons of possible interests for intelligence purposes, and vulnerable persons with mental issues. The police's use of live facial recognition technologies is not linked to information concerning the presence of a specific person at the event. They want to secure the area by identifying individuals whose faces match the facial data recorded in their watchlist.

Concerning the functioning of the real-time FRT, the faces of individuals who pass in front of the van are captured and processed in real-time to extract their biometric features and transform them into a facial biometric template for real-time comparison with the biometric information contained in the watchlist.

Does such use of FRT fall under the prohibition of Article 5(1)(h)?

1) Law enforcement purposes carried out by a law enforcement authority or on their behalf: the purpose is to ident fy wanted individuals who might enter the football arena and possibly arrest them. Several of the individuals whose facial images are on the ad hoc watchlist are not criminal suspects.
2) Public spaces: a sports arena is considered as such.
3) Purpose of use of FRTs: ident fying wanted individuals
   The police use live FRT for a mix of purposes: possibly crime prevent on concerning the ident f cat on of individuals with mental issues if those represent a danger to others; crime invest gat on concerning the ident f cat on of individuals suspected of crimes, and intelligence gathering concerning the ident f cat on of persons of interest.
4) Real-t me: all the operat ons, i.e. the capture, processing, and comparison of facial informat on, occur in real-t me.
5) Reference database: the police included facial images of suspects of crimes, irrespect ve of the seriousness of the of ences, and facial images of persons who did not commit a crime (persons of possible interest, vulnerable individuals with mental issues).

Conclusion: the use of FRT in that **scenario** is **covered by the prohibition**. The use of RBI results in constant monitoring and surveillance. As it is prohibited, no national law can authorise such a deployment.

This use case is based on the *Bridges versus South Wales Police* case, in which the Court of Appeals considered that the use of live FRT by SWP was not in accordance with the law due to the discretion

left to the police concerning the constitution of the ad hoc watchlists and the locations for deployment.

[2019] EWHC 2341 (Admin)
[2020] EWCA Civ 1058

Scenario 2 – Deployment of 'biometric-ready' CCTV cameras with live facial recognition capabilities across a city to monitor public areas

The police authorities of a busy city decide to deploy 25 AI-empowered CCTV cameras, which can perform live facial recognition technologies. They place these cameras at multiple locations, including places of worship, a number of places frequented by the LGBT + community, as well as doctors' offices, pharmacies, and various restaurants and bars. They use these cameras for preventive purposes without links to specific serious crimes, allowing them to switch on the live facial recognition function on demand should they detect a crime in real-time.

Does such use of FRT fall under the prohibition of Article 5(1)(h)?

1) Law enforcement purpose carried out by a law enforcement authority or on their behalf: yes, securing public spaces carried out by the police
2) Public spaces: mult ple spaces are targeted
3) Purpose of use of FRTs/ law enforcement purpose: for security and crime prevent on with the possibility of ident fying individuals.
   The cameras are 'biometric-ready', meaning that they can ident fy individuals and should be considered like remote biometric ident f cat on systems.
4) Real-t me: yes, if act vated.

Issue to consider: The term 'use' in the AI Act is not defined. It is understood as the deployment. But, it could be argued that if a live facial recognition functionality is integrated into a CCTV camera and can be activated or deactivated on demand or is added as a filter if the user has paid a separate licence to activate live FRT, then the integration of such functionality falls into the scope of use.[134] Activating by a click on a computer or using a filter to select live facial recognition functionality should not be allowed.

In conclusion: Based on the functionality and design of the systems, biometric-ready cameras, and the conditions of use (without targeting any individual and with no link to any serious crime), the system should fall under the prohibition of Article 5(1)(h) of the AI Act.

Possible variations:

[134] This is, for instance, the way the Briefcam surveillance cameras are designed. See User Manual, ht ps://s3.documentcloud.org/documents/24165059/manuel_de_l_ut lisateur_briefcam_en_version_francaise_clean.pdf; and the invest gat on conducted by Disclose on the use of Briefcam by the French police, ht ps://disclose.ngo/fr/art cle/la-police-nat onale-ut lise-illegalement-un-logiciel-israelien-de-reconnaissance-faciale

Deployers of the biometric-ready cameras can add different functionalities to their camera systems. They can integrate third party systems to add 'object detection', 'crowd movement' on top of facial recognition. These additional functionalities are not covered by the prohibition or by the definition of remote biometric identification systems.

Concerning the use of the systems for purposes other than biometric identification, the rules on the use of video surveillance in public spaces as well as data protection rules (should personal data be processed) should be checked.

[Case based on Cologne case study]
See EDRi's report, 'The rise and rise of biometric surveillance in the EU', p.20 et seqs.

Scenario 3 – Real-time use of RBIs by police to identify a burglar

Several burglaries occurred in a residential neighbourhood during the summer break. Thanks to eyewitnesses, the police got a description of the suspect, who was seen at different occurrences in the neighbourhood ahead of the burglaries. To try to identify him and arrest him, the police decided to deploy a live FRT at various locations in the neighbourhood during a weekend. Based on the indications of eyewitnesses, the police created a facial composite of the suspect and extracted several pictures of individuals resembling the facial composite from a custody database.

To determine whether this scenario falls within the scope of Article 5(1)(h) of the AI Act, several questions need to be answered:

1) Is the purpose a law enforcement purpose? A burglary is a criminal of ence.
2) Publicly accessible spaces: streets are considered as such.
3) Purpose of use: the use of a live FRT to ident fy a suspect in burglaries
4) Real-t me: yes
5) Reference database: ad hoc watchlist of potent al suspects.

Conclusion: Even if the police use live FRT against a targeted suspect and have defined a perimeter and time of use, the use is not allowed to be deployed in case of an offence, which is not listed in Annex II of the AI Act.

Variation: Instead of the police, **a group of neighbours** decides to deploy a real-time FRT system to identify the suspect of the burglaries and possibly transmit the images to the police for further investigation. As these private parties are neither entrusted to exercise public authority for a law enforcement purpose nor acting on behalf of the police, the real-time use of RBI will not fall under the prohibition of Article 5(1)(h) of the AI Act. Other rules will apply (e.g. data protection rules) and compliance with fundamental rights must be assessed.

The retrospective use of RBI for criminal investigation by the police is also not covered by the prohibition of Article 5(1)(h) of the AI Act. Other rules apply as outlined in Article 26(10) of the AI Act.

Scenario 4 – Police's use of FRT to identify and locate a demonstrator

The police rely on the CCTV network installed in the city and underground to spot a political demonstrator who organised a collective protest in the streets. If demonstrating is a fundamental right in the country where he lives, the organiser of a collective protest held on public roads and areas such as streets must notify the municipality three days ahead of the event to prevent public disorder and violence. The absence of notification is a criminal offence punishable by up to six months imprisonment and a maximum fine of 8.000 euros. To identify him, the police extracted the video feeds from the CCTV cameras installed in the streets and performed retrospective facial recognition by comparing the extracted images with photographs posted on social media.

Once they have identified him, they try to locate him by enabling live facial recognition software on the CCTV surveillance network. They see him walking in the underground and arrest him a few days after the protest.

Does this scenario fall under the prohibition of Article 5(1)(h) of the AI Act?

1) Law enforcement purpose: In this case, the police tried to locate and ident fy a demonstrator who failed to not fy a collect ve protest to local authorit es. The absence of not f cat on of a collect ve protest is a criminal of ence in the country where he lives.

2) Publicly accessible areas: Streets and underground stat ons are considered as such.

3) Purpose and modalit es of use of FRTs: in this situat on, the police used two modalit es of facial recognit on technologies.
    - First, the police used FRT retrospect vely to ident fy the individual: they extracted images from the cameras installed in the underground and compared them with images found on social media.
    - Second, af er ident fying him, they tried to locate him to arrest him. To do so, they used live facial recognit on cameras.

Two different regimes of rules apply in this case:

- First, the **retrospect ve use of FRT** is not prohibited under the AI Act. It is considered high-risk. The processing of biometric data for a law enforcement purpose remains subject to Art cle 10 of the LED, which needs to be implemented at nat onal level. The processing of biometric data to perform the retrospect ve use of FRT should only be allowed if it is strictly necessary and subject to appropriate safeguards. Whether the retrospect ve use of FRT is strictly necessary to ident fy the demonstrator is quest onable.

  The retrospect ve use of FRT cannot meet the necessity and proport onality tests, even if based on an exist ng law. It results in mass surveillance and constant monitoring of the city, which is not allowed under the AI Act but also infringes several fundamental rights. It undermines the rights to privacy and data protect on, as well as the right to assembly and the freedom of expression. Such a use has a chilling ef ect on exercising individuals' rights and freedoms in public spaces, while it cannot be just f ed by any 'substant al public interest.'

- Second, **the real-t me use of FRT for a law enforcement purpose is subject to Art cle 5 of the AI Act**. The use of real-t me ident f cat on for the purpose described in this case is not covered by the except ons of Art cle 5(1)(h)(i)-(iii) and should be prohibited.

N.B. In the case that serves as a basis for this scenario, *Glukhin v Russia*, the ECtHR ruled that while crime detection can be a legitimate aim, the use of FRT, both retrospective and live, was disproportionate as there were no risks to public order or transport safety. The Court emphasised the 'highly intrusive' nature of FRTs and concluded that, in that case, using FRTs did not answer a pressing social need, nor was it necessary in a democratic society.

Based on ECtHR, *Glukhin v Russia*, No 11519/20, 4 July 2023

3.6 Except ons to the prohibit on

The AI Act has introduced three exceptions to the general prohibition of real-time use of RBIS in public spaces for a law enforcement purpose. Article 5(1)(h)(i) to (iii) defines which law enforcement purposes (referred to as 'objectives') can justify the real-time use of RBIS, completed by conditions and safeguards in Articles 5(2) to 5(7). The three exceptions are described in this section together with the conditions of Article 5(2).[135]

In compliance with the conditions to restrict the exercise of fundamental rights, as interpreted by the CJEU, the real-time use of RBI must be legitimate, necessary, and proportionate (i.e. subject to safeguards). Concerning the necessity requirement, Article 5(1)(h) requires that the deployment of real-time RBI systems for one of the permitted objectives should be ***strictly necessary*** to achieve the purpose. As noted in a commentary on Article 10 of the LED, '[s]trict necessity implies balancing the public interest objective with the limitations to the right to data protection [and other fundamental rights] and checking whether these limitations can be justified in a democratic society. The result of the test should determine whether a less intrusive measure is possible to achieve the same goal, i.e. whether or not it is required to process sensitive data to safeguard the public interest.'[136] The CJEU interpreted the condition of ***strict necessity*** in its case law on Article 10 of the LED (Case C-205/21), which links that requirement with the principle of purpose specification, lawfulness, and data minimisation.[137] The Court provided **factors to carry out** the **strict necessity assessment**, which includes the **nature and gravity of the offence**, **the criminal record of the person**, and the **particular circumstances of the offence**. [138]

The conditions for the real-time use of RBI must be laid down in national legislation, based on the criteria defined in the AI Act and the identified safeguards. However, Member States remain free to allow all the exceptions, only some of them or none of them. Member States can also adopt stricter rules on the real-time use of RBI.[139]

[135] The other condit ons and safeguards, Art. 5(3)-(7) AI Act, are described in Dr. Els Kindt's report.
[136] See Jasserand C, 'Art cle 10, Processing of Special Categories of Personal Data' in Kosta E and Boehm F (eds) *The EU Law Enforcement Direct ve (LED), A Commentary* (OUP 2024), p.225.
[137] Case C-205/21, *Ministerstvo na vatreshnite rabot* , paras 122 et seqs.
[138] Ibid, para. 132.
[139] Art. 5(5) and Rec.37 AI Act.

⚠ **Article 5(1)(h)(i)-(iii)** does **not constitute a legal basis** for the real-time use of RBI systems in public spaces. It lists three cases for which the technologies can be **allowed through national legislation.** As prescribed by Article 5(2) of the AI Act, **only a domestic law that fulfills the requirements in Article 5(2) to Article 5(7) can allow the real-time use of RBI**.

The real-time use of RBI systems for one of the exceptions is 'only possible where and in as far as the Member State concerned has decided to expressly provide for the possibility to authorise such use in its detailed rules of national law. Consequently, Member States remain free under this Regulation not to provide for such a possibility at all or to only provide for such a possibility with respect to some of the objectives capable of justifying authorised use identified in this Regulation. Such national rules should be notified to the Commission within 30 days of their adoption.' (Recital 37 of the AI Act). Thus, Member states are not obliged to allow the use of real-time RBI systems. It is up to them to decide if and what they allow.

3.6.1 Rat onale

Due to their adverse effects on fundamental rights, their intrusive nature, the risk of constant surveillance and their impact on other fundamental rights, real-time RBI in publicly accessible spaces should be prohibited (Recital 32 of the AI Act). However, when their use is *strictly necessary* to achieve a *substantial public interest,* and when the exceptions are exhaustively listed and narrowly defined, their use *outweighs the risks* to fundamental rights (Recital 33 of the AI Act). To ensure that these systems are used in a 'responsible and proportionate manner', their use is subject to safeguards, specific obligations and requirements, as detailed in Article 5(2)-(7) of the AI Act. **Any other real-time use of RBI systems in public spaces for a law enforcement purpose, which is not allowed under Article 5(1)(i)-(iii), must be prohibited.**

The exceptions defined in Article 5(1)(h)(i)-(iii) aim to provide new AI and investigative tools to law enforcement authorities and entities acting on their behalf. However, due to the serious risks of interference with fundamental rights that RBI systems pose, the cases in which their use is allowed must be **strictly defined** and **narrowly interpreted**. The 'substantial public interests' justifying the real-time use of RBI systems are the following:

(1) the targeted search of victims of three specific serious crimes and missing persons [protection];

(2) the prevention of imminent threats to life or public security or a genuine threat of terrorist attacks [prevention], and

(3) localisation and identification of suspects of certain serious crimes as listed in Annex II [prosecution/investigation].

For instance,
The real-time use of a biometric identification system (which could include facial recognition mobile devices) by police authorities to identify undocumented or improperly documented migrants living a country and compare their facial images against criminal databases is prohibited as it does not fall under any of the exceptions of Article 5(1)(h)(i)-(iii). It would also constitute a serious infringement of the rights to privacy and data protection, as well as the right to non-discrimination.

The **Italian** DPA found in 2021 that the 'Sari Real Time System' that the Ministry of the Interiors wanted to deploy to 'monitor disembarkation operations in Italy by the police authorities' lacked an appropriate legal basis for processing biometric data and its use resulted in mass surveillance.[140]

As reported by Human Rights Watch,[141] the **Greek** police signed a several million contract for a smart policing project. This project would enable the police to deploy live facial recognition technologies and automated fingerprint identification, targeting migrants and asylum seekers. To this date, the Hellenic police have not established a clear legal basis to process biometric data through biometric identification tools.

3.6.2 Targeted search for the vict ms of three serious crimes and missing persons

According to Article 5(1)(h)(i), subject to strict necessity and the conditions established in Article 5(2)-(7), the real-time use of RBIs in publicly accessible spaces for law enforcement is allowed for the **targeted search of victims** of abduction, trafficking in human beings or sexual exploitation of human beings, as well as for the **search for missing persons**.

3.6.2.1 Targeted search for the vict ms

Notion of victims

Article 5(1)(h)(i) does not relate to potential victims but to **actual victims** of three serious crimes for which real-time RBI systems can be deployed for a **targeted search**. Although the notion of targeted search is not defined, it could involve the identification and localisation of victims. A victim is defined at the EU level as 'a natural person who has suffered harm, including physical, mental or emotional harm or economic loss which was directly caused by a criminal offence.'[142]

Three types of crimes

The victims of three serious crimes are covered: abduction, trafficking in human beings and sexual exploitation. Kidnapping, trafficking in human beings, and sexual exploitation of children are three crimes that can trigger a European Arrest Warrant (EAW) to arrest and transfer a criminal suspect or a sentenced person to the country that issued the EAW.

The three crimes relate, mostly but not exclusively, to women and children. According to the European Commission's DG Migration and Home Affairs, almost 40 percent of the victims are EU citizens, and most of them are women and children trafficked for sexual exploitation. The number of men victims

[140] E.g. Il Garante (Italian DPA), 'Facial Recognit on : the SARI Real Time system is not compliant with privacy laws' ; see also EDPB, 'Response to MEP Sophie in't Veld regarding the use of Automat c Image Recognit on Systems on Migrants in Italy' 10 August 2021, ht ps://www.edpb.europa.eu/our-work-tools/our-documents/let ers/edpb-response-mep-sophie-int-veld-regarding-use-automat c_en

[141] Human Rights Watch, 'Greece: New Biometrics Policing Program Undermines Rights, Risks of Illegal Racial Prof ling and Other Abuses.' 18 January 2022, ht ps://www.hrw.org/news/2022/01/18/greece-new-biometrics-policing-program-undermines-rights

[142] Art. 2(1)(a) of Direct ve 2012/29/EU.

has nearly doubled in ten years. They are trafficked for forced labour and forced begging, while most of the women and children are trafficked for sexual exploitation. [143]

Trafficking in human beings and sexual exploitation belong to the ten euro-crimes, as listed in Article 83 (1) TFEU, for which 'a common Union approach due to their particularly serious nature and their typical cross-border dimension' is necessary.[144] They are a priority of the European Multidisciplinary Platform Against Criminal Threats (EMPACT), which is 'a permanent and key EU instrument for structured multidisciplinary cooperation to fight organised and serious international crime driven by the Member States and supported by EU institutions, bodies and agencies'[145] For the period January 2022 to December 2025, human trafficking and child sexual exploitation are EMPACT's priorities. [146]

Abduction is not identified as one of the euro-crimes, but it constitutes a priority for Amber Alert Europe, a foundation created in 2013 to provide support in cases of abductions or disappearances of children.[147] Abduction includes parental abduction, but not only. As stated in the Amber Alert Europe's report of 2020, '[t]he decision to launch an AMBER Alert is country specific. In the Netherlands, for example, the National Police is responsible for issuing AMBER Alerts. In other countries the Public Prosecutor has the final say.'[148] An AMBER Alert relates to minors (i.e. under 18 years old). In its report on 'Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement,' FRA considered that facial recognition technology 'could be used to identify missing persons and victims of crime, including children.'[149]

As the exception covers victims and not potential victims of the three serious crimes, it can be argued that the RBI cannot be deployed in real-time and publicly accessible spaces to locate and identify children who are at risk of being abducted or going missing. This exception does not support using real-time RBI systems for prevention purposes.

Scenario 5 – Targeted search for an abducted child

The police are informed that a child was abducted by his caretaker, who plans to cross the borders between the Netherlands and Germany. An Amber Alert has been issued with the photograph of the child. They will set up police roadblocks and checkpoints between the Netherlands and Germany at different locations. Under which conditions could they deploy a live FRT to locate and identify the child?

[143] ht ps://home-af airs.ec.europa.eu/policies/internal-security/organised-crime-and-human-traf cking/together-against-traf cking-human-beings_en

[144] Bogensberger W., 'Art cle 83 TFEU' in Kellerbauer M. et al. (eds) *The EU Treat es and the Charter of Fundamental Rights* (OUP 2019).

[145] ht ps://www.europol.europa.eu/crime-areas-and-stat st cs/empact.

[146] Council conclusions set ng the EU's priorit es for the f ght against serious and organised crime for EMPACT 2022-2025, 9 March 2023, 7101/23.

[147] Amber Alert EU also supported to extend the except on to missing persons (including missing children), see ht ps://www.amberalert.eu/news/the-art f cial-intelligence-ai-act-and-the-search-for-missing-children-at-immediate-risk-of-life-an-open-let er-to-the-european-parliament

[148] Amber Alert, Annual Report 2020, p.20

[149] FRA's report (2019), p. 25.

1) Deployment in public spaces
2) Law enforcement purpose of the deployment: f nding the vict m of an abduct on as allowed under Art cle 5(1)(h)(i) of the AI Act provided:
    - A nat onal law authorises the use of live FRT in this case.
    - The use of live FRT is proport onate and strictly necessary, i.e. no other less intrusive alternat ves can achieve the same result to locate and ident fy the child. For instance, performing live FRT on every child found in the cars stopped at the borders would not be just f ed, unless the caretaker changed cars af er abduct ng the child and the police authorit es have no other evidence regarding the vehicle type in which he travels.
    - Before deploying live FRT, the police have conducted a Fundamental Rights Impact Assessment on their system.
    - Other condit ons and safeguards contained in Art cle 5(3) to Art cle 5(7) of the AI Act should be fulf lled.
    - The police must def ne a perimeter of deployment and durat on of use and ident fy the targeted vict m. As the vict m is travelling in a car, the police have def ned several geographic perimeters where they deployed live FRT. As indicated, the police chose dif erent locat ons between the Netherlands and Germany where they established roadblocks and checkpoints.

Conclusion: the use of FRT in that **scenario** is **covered by the exception** provided that the national law and the use by the police comply with the conditions and safeguards of Article 5(2) et seqs of the AI Act. Such use must also comply with other rules (e.g. data protection rules) and the conditions to restrict the exercise of fundamental rights.

3.6.2.2 Searching for missing persons

The second situation is covered by the exception of the search for a missing person. A 'missing person' is not defined at EU level. But in a Council Conclusions of December 2021 on 'Stepping Up Cross-Border Police Cooperation in the area of Missing Persons', the Council takes as reference both the definition of a missing person in the Council of Europe's Recommendation CM/Rec (2009) 12 and in national regulations.[150] In the Recommendation of the Council of Europe on missing persons, Recommendation CM/Rec (2009) 12, a missing person is defined as 'a natural person whose existence has become uncertain, because he or she has disappeared without trace and there are no signs that he or she is alive.'[151]

A distinction can be made between missing children and missing adults. The applicable rules regarding missing children vary considerably from one Member State to another;[152] however, since the exception applies to missing individuals, it can be assumed that the deployment of a real-time RBI

[150] Council Conclusions (2021) 14808/21, para 11, page 4.
[151] Principle 1, Recommendat on CM/Rec (2009) 12; the Recommendat on was elaborated in the af ermath of the terrorist at acks of 2001 and the tsunami of 26 December 2004, see explanatory memorandum.
[152] European Commission, European Migrat on Network, 'How do EU Member States treat cases of missing unaccompanied minors?' EMN Inform, 2020.

system is only possible once the disappearance has been officially acknowledged (through a police's report, for instance).

The disappearance of an adult does not always lead to a police investigation, as adults have the right to disappear. In France, like in Belgium, for instance,[153] a police investigation can only be open if the disappearance is concerning ('*disparition inquiétante'*) due to the circumstances of the disappearance. This could be linked to the legal status of the person ('under curatorship'), their health condition (a mental illness), the existence of a suicidal note, but also their departure without personal belongings. If the circumstances of the disappearance are a cause for concern, the disappearance can be filed with the police so that an investigation can start.[154]

Point of attention: The criminal invest gat on for the search of a missing person whose disappearance is a cause for concern, is a separate process from that establishing the legal status of a missing person. For instance, in Belgium, when the circumstances are a cause for concern, the disappearance will be not f ed to the police. Three months af er the disappearance, and in case the person has not reappeared at their place of residence or no one heard from that person, and it results in uncertainty whether the person is dead or alive, a judge can establish a 'presumpt on of absence.'[155] The judge can designate an administrator to manage the missing person's assets.[156] The Court can declare the person absent f ve years af er this 'presumpt on of absence' or seven years in the absence of such judgment.[157] The 'declarat on of absence' is inscribed in the civil register and produces the same legal consequences as death (such as succession or dissolut on of the marriage). [158]

Once operational the Schengen Information System, SIS II, could serve as a reference database as it contains alerts on missing and wanted persons.[159]

Scenario 6 – Searching for a missing vulnerable person
Police officers are informed that an eldery person who has Alzheimer's disease disappeared from his retirement house. Under which circumstances could they deploy live FRT to locate and identify that person?

1) Depending on the age of the person, their health and mental condit on, and the other circumstances of the disappearance, the police authorit es will have to assess whether the

[153] ht ps://www.belgium.be/fr/famille/deces/disparus
[154] Art cles 112 et seqs. of French Civil Code and Art cles 1062 e seqs. of French Civil Procedure Code; ht ps://www.legifrance.gouv.fr/loda/id/JORFTEXT000000369046/ - Art cle 26 of Law 95-73 of 21 January 1995, as amended by Law No. 2002-1138 of 9 September 2002.
ht ps://www.116000enfantsdisparus.fr/agir-en-cas-de-disparit on/disparit on-inquietante/
see also ht ps://www.belgium.be/fr/famille/deces/disparus
[155] Art cles 112 of the Belgian Civil Code.
[156] Art cle 113 et seqs. of the Belgian Civil Code.
[157] Art cles 118 -124 of the Belgian Civil Code.
[158] Ibid.
[159] ht ps://home-af airs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-informat on-system/alerts-and-data-sis_en

missing person is in danger, or the disappearance is a cause for concern (worrying nature of the disappearance) to trigger the search.

2) The missing person is known, and the search can be targeted.
3) They must rely on a nat onal law allowing them to deploy live RBI (including FRT) in case of worrying disappearance.
4) They need to determine a geographic perimeter and durat on of use of the technology to deploy it.
5) Their system must have undergone a Fundamental Rights Impact Assessment before their use and comply with the requirements laid down in Art cles 5(3) to 5(7).

Conclusion: the use of FRT in that **scenario** is **covered by the exception** provided that the national law and the use by the police comply with the conditions and safeguards of Article 5(2) et seqs. of the AI Act. Such use must also comply with other rules (e.g. data protection rules) and the conditions to restrict the exercise of fundamental rights.

Food for thought for a variation of the scenario:
The police in the UK are testing a live facial recognition mobile app, which allows them to take photographs of wanted persons (including missing persons) that they can compare in real-time with a police database of wanted persons. The app aims at 'making the work of police officers easier and faster' by 'assist[ing] an officer to identify a subject.' See https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/

The way the app is designed and intended to be used does not fulfil the conditions specified in the AI Act:

- First, the app is described as 'an *on-street* intelligence tool to assist the of cers in ident fying an unknown person.' According to Art cle 5(2) of the AI Act and Recital 54 of the AI Act, real-t me RBI can only be deployed to 'conf rm the ident ty of a targeted individual.' So, it **cannot be used as an intelligence tool**.

- Second, the **reference database** is linked to custody images, whereas for the cases permit ed in the AI Act, the reference database should not only be **appropriate to each deployment** but also **only contain images** of either vict ms of crimes as described in Art cle 5(1)(h)(i) or persons (suspects, perpetrators) involved in one of the situat ons described in Art cle 5(1)(h)(ii) and Art cle 5(1)(h)(iii).

- Third, such a use would **not be strictly necessary** as for each use of the live RBI, the specif c object ves pursued by the deployment must be specif ed before the deployment. The object ves of the deployment cannot be just f ed af er the deployment.

- **Such a tool would increase the feeling of constant surveillance** as it will not answer any object ve other than being able to ident fy an individual, af er an interact on with that individual, to determine whether they are known in a custody database. Thus, the

deployment would not necessarily be linked to a specif c crime, and in part cular, to one of the serious crimes listed in Annex II of the AI Act.

3.6.3 Prevent on of imminent threats to life or terrorist at acks

According to Article 5(1)(h)(ii), subject to strict necessity and the conditions established in Article 5(2)-(7), the use of RBI in publicly accessible spaces is allowed for:

> '[T]he prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack.'

This exception covers **two situations**: first, **the prevention of a threat to individuals' life or physical safety** and second, **threats of a terrorist attack**. It should be observed that a terrorist attack can include a threat to life, whereas a threat to life does not necessarily qualify as a terrorist attack.[160] For instance, when threats to life are motivated by racism or resulting from mental issues, they are not necessarily linked to a terrorist motive, which is explained later in this section.

3.6.3.1 Interplay between law enforcement and nat onal security

While the first situation (threats to life or physical safety) resorts mainly to law enforcement except if it can be linked to a terrorist motivation, the second situation concerning a terrorist threat is at the interplay between law enforcement and national security.

National security

Following Article 2(3) of the AI Act, the AI Act 'does **not apply to areas outside the scope of Union law, and shall not, in any event, affect the competences of the Member States concerning national security**, regardless of the type of entity entrusted by the Member States with carrying out tasks in relation to those competences.' Consequently, the AI Act expressly **excludes** AI systems that are '**placed on the market**, **put into service**, or **used with or without modification exclusively** for military, defence or **national security purposes**, **regardless of the type of entity carrying out those activities**.' Therefore, it is the purposes of use of the systems and not the entities carrying out the activities that define the exclusion.

This exclusion is based on Article 4(2) TEU, which provides that 'national security remains the sole responsibility of each Member State', as reminded in Recital 24 of the AI Act. In addition, Recital 24 specifies that this exclusion is also justified by the 'specific nature and operational needs of national security activities and specific national rules applicable to those activities.'

The concept of 'national security' has not been defined in EU law, but in *La Quadrature du Net*, the Court of Justice suggested that the term refers to 'the primary interest in protecting the **essential functions of the State and the fundamental interests of society** and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the

[160] According to Recital 8 of Direct ve 2017/541, 'at acks against a person's life…can qualify as terrorist of ences when and insofar as commit ed with a specif c terrorist aim.'

population or the State itself, such as terrorist activities.[161] According to Article 4(2) TEU, essential State functions include 'ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security.'

As interpreted by the CJEU, the notion of '**essential State functions and the fundamental interests of society' excludes, for instance**:

- 'act vit es relat ng to road safety' [Case C-439/19, para 68, concerning the registrat on of penalty points in the nat onal register for vehicles and their drivers];
- 'act vit es relat ng to the organisat on of elect ons' [Case C-306/21, para. 41, concerning the processing of personal data through video recording in the context of elect ons];
- 'organisat on or administrat on of just ce.' [Case C-204/21]

In *La Quadrature du Net*, the Court delimited the application of the national security exemption, specifying that: 'although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law.' [162]

The concept(s) of national security at national level

For example,

In the **Netherlands**, the term 'national security' is not defined, as explained on the website of the General Intelligence and Security Service as 'it is not set in stone what falls under the umbrella of national security. It is a difficult concept. It encompasses values, rules, laws that we believe are important in our country. Generally, *national security* is best approached by describing things that are a threat to it. The explanatory memorandum of the Wiv 2017 does enable us to infer that national security refers to a safe country in which people may live in freedom and in which democratic legal order is safeguarded.'[163]

In **France**, national security is defined in Article L1111-1 of the French Code of Defence (c*ode de la défense*) as follows:
'The national security strategy aims to identify all the threats and risks likely to affect the Nation's life, particularly concerning the protection of the population, the integrity of the territory, the permanence of the institutions of the Republic, and the answers [to the threats and risks] from the public authorities. All public policies contribute to national security.' [*own translation*]

Examples of threats to national security can include threats to critical infrastructures (such as power plants, hospitals, water treatment facilities), terrorism, military threats, cyber threats, environmental

[161] Joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others*, judgment of 6 October 2020, para. 135; Case C-204/21, Commission v Poland, paras 318-319, referring to Case C-439/19, paras 67-68 and Case C-306/21, para. 40

[162] *La Quadrature du Net and Others*, para. 99, as well as case para 44 of case C-623/17, *Privacy Internat onal*, Judgement of 6 October 2020.

[163] ht ps://english.aivd.nl/about-aivd/quest on-and-answer/is-there-a-law-that-def nes-nat onal-security

threats.[164] In Luxembourg, Article 3(2)(a)-(b) of Law of 5 July 2016 on the reorganisation of the State Intelligence Services explicitly identifies what constitutes a threat to national security as:
'any activity, individual or collective, within the country or from abroad, which

- may be linked to espionage, interference, terrorism, extremism of a violent nature, the proliferat on of weapons of mass destruct on or products and technologies related to defense, organised crime or cyber threat, provided those two last act vit es are linked to the previous ones, and
- may endanger the State independence and sovereignty, the security and funct oning of the inst tut ons, fundamental rights and civil libert es, the safety of persons and propert es, the scient f c and technical potent al or the economic interests of the Grand Duchy of Luxembourg' [*own translat on*]

The ECtHR has recognised the following activities as 'acts endangering national security':[165] espionage,[166] terrorism, [167] provocation to commit a terrorist attack, [168] political subversion, [169] separatist extremist organisations threatening the unity of a state territory, [170] and undermining military discipline.[171]

Delimitation of the national security exemption and the applicability of EU law
As analysed by Korff, '[i]t follows from the PNR judgment [Case C-817/19] of the CJEU that even when Member States hold exclusive competence in some areas (such as, in particular, national security), if the exercise of that competence affects an area where the EU has competence and that is covered by EU law (e.g., data protection, internal market), the exercise of that exclusive Member State competence may not impinge on the EU legal order or undermine the relevant EU legal rules…Therefore, whenever an EU Member State exercises its exclusive competence in relation to national security to impose obligations on entities that are subject to EU law in their relevant activities, whether these are those telecommunication service providers, airlines, or providers or users of AI – those obligations must be compatible with the relevant EU law such as the GDPR, the LED, or the Europol Regulation (all read in line with the PNR judgment). This compatibility also needs to extend to future regulations such as the AI Act (also read in that way), and more generally with the EU Charter of Fundamental Rights – and the Court of Justice is competent to assess that compatibility.' [172]

Counterterrorism

[164] ht ps://english.nctv.nl/topics/nat onal-security-strategy
[165] As listed in the FRA's report on Surveillance by Intelligence Services, volume II FRA's report, 2017, p.53.
[166] e.g. *Zakharov v Russia*, App. No 47143/06, 4 December 2015.
[167] e.g. *Klass v Germany*, App. No 5029/71, 6 September 1978, para. 48.
[168] e.g. *Dicle v Turkey*, App. No 53915/11, 08 May 2022, para. 87
[169] e.g. *Leander v. Sweden*, App. No. 92248/81, 26 March 1987.
[170] e.g. *United Communist Party of Turkey v Turkey*, App. No. 133/1996/752/951, 30 January 1998.
[171] e.g. *Arrowsmith v United Kingdom*, App. No. 7050/75, 5 December 1978.
[172] Korf , Opinion (2022), p.27.

Counterterrorism is mainly a national security issue for Member States and an 'internal security' issue for the EU since terrorism has a cross-border dimension and is also a serious crime.[173] If national security issues are the exclusive competence of Member States (Article 4(2) TEU), internal security issues, through the area of justice, security, and justice, are a shared competence area of Member States and the EU (Article 4(2)(j) TFEU).

In application of Article 83 TFEU, the EU can 'establish common rules for serious crimes with a cross-border dimension, such as terrorism.'[174] In that context and to align EU law with international standards,[175] the EU adopted Directive 2017/541 on combating terrorism as 'the cornerstone of the EU countries' criminal justice response to counter-terrorism.'[176] Replacing Council Framework Decision 2002/475/JHA,[177] Directive 2017/541 establishes minimum common rules on the definition of terrorist offences and sanctions linked to them.[178] See section 3.6.3.3 for further details.

⚠ **The national security exclusion applies independently of the entities pursuing the activities**. Thus, if law enforcement authorities use real-time RBI for national security purposes (such as to gather intelligence), these entities are excluded from the scope of the AI Act. See Article 2(3) of the AI Act.

As observed by Galli, traditionally '**the police**, in the framework of their judicial function, have the **task of gathering information in relation to specific offences for prosecution purposes**; **intelligence services** do not have the objective of investigating offences but instead to **recognise threats** and to **provide intelligence assessments** to policymakers.'[179] But as she acknowledges, the role of intelligence agencies and law enforcement authorities in the prevention and fight of terrorism has evolved and the distinction of their 'tasks and competences have become blurred.'[180] FRA had already observed the lack of clear boundaries between the tasks of law enforcement and intelligence services in its 2015 report on 'Surveillance by Intelligence Services.'[181]

Same system used for national security and law enforcement purposes

An RBI system could have been developed for intelligence service purposes, such as intelligence gathering on the threats to terrorism deployed online (e.g. publicly available websites, platforms, and social media) to identify violent extremists or potential members of terrorist groups. The same system could then be used by law enforcement authorities to pursue one of the law enforcement purposes allowed by Article 5(1)(i)-(iii) of the AI Act. For instance, based on the intelligence collection carried out by the national intelligence services, the police could receive factual indications of an imminent

[173] e.g. A Counter-terrorism Agenda for the EU (COM(2020) 795 f nal).
[174] Art cle 83 TFEU.
[175] In part cular, the UN Security Council Resolut on 2178 (2014) and the Addit onal Protocol of the Council of Europe Convent on on the Prevent on of Terrorism, see rec 6 Direct ve 2017/541.
[176] See Summary of Direct ve (EU) 2017/541, ht ps://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A4322328
[177] Council Framework Decision 2002/475/JHA.
[178] Art cle 1 of Direct ve 2017/541.
[179] Galli F., 'Interoperable Law Enforcement: Cooperat on Challenges in the Area of Freedom, Security, and Just ce' 15 EUI Working Paper RSCAS 2019/15, Robert Schuman Centre for Advanced Studies (2019), p.11
[180] Ibid.
[181] FRA, 'Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU: Mapping Member States' Legal Frameworks' 2015, pp.13-14.

terrorist attack. The RBI use for intelligence service purposes, i.e. to protect national security, is excluded from the scope of the AI Act.[182] However, if the same system is used for law enforcement purposes, this use is then subject to the AI rules, and in particular, to the prohibition of Article 5(1)(h) and its explicit exceptions.

3.6.3.2 Specif c, substant al and imminent threat to life or physical safety of natural persons

In application of Article 2 of the Charter, which guarantees the right to life, the EU and Member States must safeguard and, thus, protect the lives of individuals. According to the ECtHR case law, the protection of individuals' life can require further specific actions from the police when 'a real and immediate risk to the life of an identified individual or individuals' exists.[183] Such a real and imminent risk to life can be linked to the need for an urgent medical intervention[184] or to life-threatening injuries.[185] The appreciation of such a risk is based on the facts. The criteria set out in Article 5(1)(h)(ii) concerning the threat to life to allow for the use of RBI are slightly different. They require the existence of (1) a specific, (2) substantial and (3) imminent threat to the life or physical safety of (4) natural persons. Besides, the threat does not need to be limited to identified individuals or a group, as it relates to natural persons in general.

References to a **significant** and **imminent risk to the life** and **safety of natural persons** can be found in the Second Additional Protocol to the Budapest Convention on Cybersecurity on enhanced cooperation and disclosure of electronic evidence. In that protocol, an ***emergency*** is defined as 'a situation in which there is a **significant and imminent risk** to **the life or safety** of **any natural person**.'[186] Examples of these risks are provided in the Explanatory Report accompanying the Second Additional Protocol to the Budapest Convention.

For instance,[187]
'Situations involving 'a significant and imminent risk to the life or safety of any natural person' may involve, for example, **hostage situations** in which there is a **credible risk of imminent loss of life**, **serious injury** or **other comparable harm to the victim**; **ongoing sexual abuse of a child**; **immediate post-terrorist attack scenarios** in which authorities seek to determine with whom the attackers communicated in order to determine if further attacks are imminent; and **threats to the security of critical infrastructure** in which there is **a significant and imminent risk to the life** or **safety of a natural person**.'

[182] Rec. 14 and Art. 2(3) AI Act.
[183] By the ECtHR on Art cle 2 of the European Convent on on Human Rights, see *Osman v. United Kingdom* No 87/1997/871/1083, 28 October 1998, para 116.
Art cle 2 of the Charter corresponds to Art cle 2 of the European Convent on on Human Rights and should be interpreted similarly. See Art cle 52(3) of the Charter of Fundamental Rights.
[184] e.g. *Lapshin v. Azerbaijan*, App. No. 13527/18, judgment of 11 October 2021, paras 71-72.
[185] e.g. *Tërshana v Albania*, App. No. 48756/14, judgment of 04 November 2020, paras 131-132.
[186] Art cle 3.2.c of the Second Addit onal Protocol to the Budapest Convent on on Cybercrime on enhanced cooperat on and disclosure of electronic evidence (CETS No. 224).
[187] Explanatory Report, Second Addit onal Protocol, para. 42.

The EU Regulation on European Production Orders and European Preservation Orders for e-evidence also refers to **emergency cases**, where the **threat to the life or physical integrity or safety of a person** is '**so imminent that immediate action has to be taken'**.[188] Emergency cases also include an imminent threat to a critical infrastructure. This threat is defined as described in Article 2(a) of Directive 2008/114/EC, i.e. 'where the disruption or destruction of such critical infrastructure would result in an imminent threat to the life, physical integrity or safety of a person, including through serious harm to the provision of basic supplies to the population or to the exercise of the core functions of the State.'[189] **Recital 33** of **the AI Act cross-refers** to the imminent threat to life and the physical safety of persons resulting from a serious disruption of critical infrastructure as defined in Article 2(4) of **Directive 2022/2557**.[190]

For example,[191]
A serious disruption and destruction of critical infrastructure (e.g., a power plant, water supply, or a hospital) can result in an imminent threat to the life or the physical safety of a person when there is serious harm to the basic supplies to the population (deprivation of electricity or drinkable water for a long period, in particularly warm or cold weather, etc.).

⚠ One question is whether the threat needs to be **intentional** or whether it also includes **non-intentional** actions, such as the reckless behaviour of an individual in violation of mandatory security rules for instance (such as driving at 200 km/hour on a road limited to 50 km/hour) that would result in a threat to life or physical safety.

In a nutshell, an **imminent** threat to life or physical safety is a threat that can occur at any moment and requires '**immediate action to be taken.**'[192] A **substantial** threat means that the threat to life or physical safety is **significant**[193] or **real**. [194] A **specific** threat means that the threat is **clearly defined**.

Scenario 7 – real-time use of RBI to prevent school's shooting
The police are informed that a former student plans a deadly attack at his previous University as he seeks revenge on several former classmates. The police received information from the national security intelligence services about the imminence of the attack, the targeted school, and the weapons he plans to use to execute his plans. Under which conditions could the police rely on real-time RBI (such as facial recognition technologies) to locate and identify the criminal suspect?

1- Constitution of the threat to life or physical security:
Based on the information received, the attack is imminent. The suspect also plans to attack his school to kill or harm students. The appreciation of the case is made at national level.

[188] Rec. 37 of Regulat on 2023/1543.
[189] Rec. 37 and Art. 3(18) of Regulat on 2023/1543.
[190] Direct ve 2022/2257 has repealed Direct ve 2008/114/EC.
[191] Rec. 33 AI Act.
[192] Rec. 37 of Regulat on 2023/1543.
[193] Explanatory Report, Second Addit onal Protocol, para. 42.
[194] See ECtHR's case law on Art cle 2 of the ECHR that refers to real and imminent risks to life, e.g. *Lapshin v. Azerbaijan*, *Tërshana v Albania;* or *Osman v United Kingdom*.

2- Legal basis:
The police cannot deploy the technologies without national law allowing the real-time use of RBI in publicly accessible areas in this case .
3- Strict necessity:
The police should demonstrate they have no other means (and tools) available to locate and identify the suspect and prevent the school's attack.
4- Temporal, geographical, and personal scope of RBI use:
The police will have to define a perimeter (such as around the University), a duration (such as 24 hours, which could be extended if duly justified), and the targeted individual (the suspect). To identify the suspect, the police might incidentally scan the faces of passers-by, impacting their rights to privacy and data protection. However, the objective of saving lives will prevail over the privacy of passers-by. In addition, their processed images will not be recorded as they should be automatically discarded in case of non-match.
5- Compliance with the conditions of prior authorisation (except emergency), a Fundamental Rights Impact Assessment (prior to the use), notification to the relevant market surveillance authority and data protection authority, and compliance with all the conditions of Art. 5(2) to Art. 5(7) of the AI Act. The circumstances of the case, i.e. the life-threatening situation, justify the emergency procedure, which allows deploying RBI in real-time without prior judicial or administrative authorisation. However, such authorisation will have to be obtained within 24 hours.

Critical issues:
- Without a national law authorising this exception, the police cannot deploy the technologies.
- The police must comply with the limitations set in Article 5(2)-5(7). Therefore, they are not allowed to deploy the technologies in the wild (i.e. across the whole city) to locate and identify the suspect. Such a use would not meet the necessity and proportionality tests.

3.6.3.3. A genuine and present or genuine and foreseeable threat of a terrorist at ack

Several elements compose this exception: the existence of a **threat of a terrorist attack** and the characteristics of the threat, which must be **genuine and present** or **genuine and foreseeable**.

Threat of a terrorist attack

Terrorist offences are defined at EU level in Directive 2017/541 on combatting terrorism. According to Article 3(1), terrorist offences are 'intentional acts, as defined as **offences under national law**, which, given their nature or context, may seriously damage a country or an international organisation… where committed with one of the aims listed in paragraph 2'. Article 3(1) provides a list of ten terrorist offences, which includes nine intentional acts plus the threat to commit any of those acts.

The terrorist offences listed in Article 3(1) are:

(a) at acks upon a person's life which may cause death
(b) at acks upon the physical integrity of a person
(c) kidnapping or hostage-taking

(d) causing extensive destruct on to a government or public facility, a transport system, an infrastructure facility, including an informat on system, a f xed plat orm located on the cont nental shelf, a public place or private property likely to endanger human life or result in major economic loss
(e) seizure of aircraf , ships or other means of public or goods transport
(f) manufacture, possession, acquisit on, transport, supply or use of explosives or weapons, including chemical, biological, radiological or nuclear weapons, as well as research into, and development of, chemical, biological, radiological or nuclear weapons
(g) release of dangerous substances, or causing f res, f oods or explosions, the ef ect of which is to endanger human life
(h) interfering with or disrupt ng the supply of water, power or any other fundamental natural resource, the ef ect of which is to endanger human life
(i) illegal system interference, as referred to in Art cle 4 of Direct ve 2013/40/EU of the European Parliament and of the Council in cases where Art cle 9(3) or point (b) or (c) of Art cle 9(4) of that Direct ve applies, and illegal data interference, as referred to in Art cle 5 of that Direct ve in cases where point (c) of Art cle 9(4) of that Direct ve applies
(j) threatening to commit any of the acts listed in points (a) to (i).

In addition, Directive 2017/541 has introduced **several 'preparatory offences'**, as noted by FRA[195]. Those offences include 'public provocation to commit a terrorist offence',[196] 'receiving training for terrorism', [197] or 'travelling for the purpose of terrorism.' [198] Article 20(1) of the Directive allows for the use of '**investigative tools'** to **investigate or prosecute terrorist offences**. As illustrated in Recital 21, these tools 'should, where appropriate, include, for example, the search of any personal property, the interception of communications, covert surveillance including electronic surveillance, **the taking and keeping of audio recordings**, in private or public vehicles and places, and of **visual images of persons** in public vehicles and places, and financial investigations.'

The exception introduced in Article 5(1)(h)(ii) provides **a new investigative tool** that **can be used in the prevention phase of a terrorist attack**, i.e. in the detection of a serious threat, which needs to reach the level of a genuine and present or genuine and foreseeable threat of a terrorist attack, as defined by the CJEU (and explained later in this section).

[195] FRA, 'Direct ve (EU) 2017/541 on Combat ng Terrorism, Impact on Fundamental Rights and Freedoms'
[196] Art.5 of Direct ve 2017/541
[197] Art.8 of Direct ve 2017/541
[198] Art.9 of Direct ve 2017/541

The **terrorist threat level is**, however**, defined at national level** and varies from one Member to another. For example, the Netherlands have established five levels of threats,[199] Belgium four,[200] France three, [201] and Sweden five.[202]

☞ **Levels of threats** with the example of the **Netherlands**: the Dutch Government has established five 'ascending threat levels.' The first level is *minimal*, i.e. 'it is unlikely that a terrorist attack will occur in the Netherlands'; the second level is *limited*, i.e. 'there is a slight chance of a terrorist attack'; the third level is *significant*, i.e. 'a terrorist attack is conceivable'; the fourth level is *substantial,* i.e. 'there is a real chance of a terrorist attack', and the last level is *critical*, i.e. 'a terrorist attack in the Netherlands is imminent.' The last level of threats is the one that will represent a genuine and present or genuine and foreseeable threat.

Characteristics of the threat: genuine and present or genuine and foreseeable

The threshold of seriousness that a threat needs to reach to allow for the real-time use of RBI in publicly accessible areas derives from the CJEU's case law on data retention and Passenger Name Record measures aimed at safeguarding national security, in particular, against terrorist attacks. According to the CJEU, 'a threat to national security must be genuine and present, or at the very least, foreseeable, which presupposes that sufficiently concrete circumstances have arisen.'[203] The Court added that '[s]uch a threat is therefore distinguishable, by its nature, seriousness, and the specific nature of the circumstances of which it is constituted, from the general and permanent risk of the occurrence of tensions or disturbances, even a serious nature, that affect public security, or from that of serious criminal offences being committed.'[204] The assessment concerning the existence and seriousness of the threats is made by the courts at national level when they review the actual circumstances of a measure taken to safeguard national security, and more specifically, in case of threats to terrorist attacks.

Examples of genuine and present threats

☞ In its Decision, *French Data Network and Others*, which followed up the CJEU's judgment in the joined cases *La Quadrature du Net* [C-511/18, C-512/18, and C-520/18], the **French Council of State** assessed the level of terrorist threat based on a **persistent high terrorist risk** linked to the number of attacks that occurred in 2020 and foiled attacks in 2021, the **highest threat level** of the French threat level system ('Vigipirate') at that time, the **high exposure to the risk of espionage** and **foreign interferences** due to its military involvements, and malicious actions against French companies linked

[199] ht ps://www.government.nl/topics/counterterrorism-and-nat onal-security/risk-of-an-at ack-threat-level
[200] https://cuta.belgium.be
https://crisiscenter.be/en/risks-belgium/security-risks/terrorism-and-extremism
[201] https://www.sgdsn.gouv.fr/vigipirate#
ht ps://www.sgdsn.gouv.fr/f les/f les/Vigipirate/20160130-np-sgdsn-pse-tackling-terrorism-together.pdf
[202] https://www.krisinformation.se/en/hazards-and-risks/terrorism
[203] Joined Cases C-793/19 and C-794/19, *BundesRepublik Deutschland v. Space Net AG and Others* (20 September 2022), para. 93.
[204] Case -140/20, *Commissioner of An Garda Síochána and Others*, para. 62.

to **industrial and scientific espionage**, among others. [Conseil d'Etat, Decision No. 393099, 21 April 2021, para.44].

☞ In its Decision following up on the CJEU's judgment in *La Ligue des droits humains* [C-817/19], the **Belgian Constitutional Court** relied on terrorist attacks committed between 2014 and 2016, the **threat level of terrorist attacks still genuine and present at the time of assessment** (with a threat level at 2 out of 4), and the **geographic position** of the country at the center of Europe, increasing the risk of using all transport modes via Belgium to commit terrorist offences. [Cour Constitutionnelle, Decision 131/2023, 12 October 2023, paras B.40.2.1 and B.40.2.2]

Prevention

Contrary to Article 5(1)(h)(i) and Article 5(1)(h)(iii), this exception does not specify whether the deployment of real-time RBI would be allowed to locate and/or identify the suspect(s). The broad wording of the exception calls for several remarks.

First, Article 5(1)(ii) must be read together with the conditions and safeguards provided by Article 5(2) et seqs. Yet, Article 5(2) requires deploying the technologies 'to confirm the identity of the specifically targeted individual', hence, to target one person. Yet, terrorist attacks are not systematically carried out by a single individual. But in the case of terrorist groups, deployers should be allowed to target several individuals who are linked to the same group.

Second, as the deployment must also be restricted temporally and geographically, this exception does not allow the use of real-time RBI to detect and follow 'terrorists on the move.'[205]

For example,
The geographic limitation safeguard would not allow to deploy drones equipped with live FRT to follow moving targets (fugitives) to identify them **whenever** and **wherever** they stop. However, if **justified by the circumstances of the case**, such as in a situation where a terrorist suspect is running in a public park to randomly attack people he crosses paths with; police authorities could be allowed to follow his moves within a certain perimeter, beyond the public park.

Third, at national level, national legislators will have an important role in further specifying this exception for the national law to meet the 'quality of the law' criteria, i.e. it should be clear, accessible, and foreseeable in its application. This will require specifying whether the technologies can be used to locate or identify an individual, or both.

Scenario 8 – Real-time RBI to prevent a terrorist attack in a park
The police are informed that a terrorist suspect is running around a park looking for people to attack with a knife while he is screaming violent extremist slogans, which are usually associated with terrorist attacks and terrorist groups. The government of that country has been facing several terrorist attacks and has raised the level of threats to its maximum.

[205] As proposed in the EU counter-terrorism agenda (2020), p. 4

Law enforcement authorities want to deploy real-time RBIs to identify and locate him to prevent the attack. Does such a use of FRT fall under the exception of Article 5(1)(h)(ii)?

1) Public spaces: a park is considered as such.
2) Purpose of use of FRTs: to ident fy and locate a suspect of terrorist at ack
3) Real-t me: yes
4) The use of real-t me RBI for this except on needs to be authorised by nat onal law
5) Law enforcement purpose: the prevent on of a terrorist threat
   a- Is it a terrorist threat? The suspect is threatening the lives of people; his at ack has a terrorist mot ve.
   b- Is the threat genuine and present or foreseeable? Based on the current situat on in the country where several terrorist at acks have occurred, the armed suspect screaming extremist slogans and threatening people around him with his knife, the threat is genuine and present.
   The threat would not be genuine and reasonably foreseeable if his act ons were considered int midat on, such as the suspect would only scream violent extremist slogans without trying to harm anyone.

Identification and localisation of the suspect: the police should define a perimeter of deployment (the park and the near surroundings as the individual is running with his knife), a target (the suspect), and a duration (which could be extended). If the suspect leaves the park, the police are not authorised, on the basis of this exception, to follow the move of the suspect with real-time RBI (such as via a drone), should he run away. However, as the suspect is running around the park, the police should be authorised to cover a perimeter, which includes the park and its near surroundings.

Conclusion: The use of FRT in that **scenario falls under the exception** of Article 5(1)(h)(ii) of the AI Act. To deploy the technologies, the police will have to comply with the requirements set forth in Article 5(2) et seqs. of the AI Act, other rules and comply with the conditions applicable to the restrictions of fundamental rights.

3.6.4 Localisat on and ident f cat on of suspects of certain crimes

Article 5(1)(h)(iii) allows the real-time use of RBI in publicly accessible spaces for 'the localisation and identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member States concerned by a custodial sentence or a detention order for a maximum period of at least four years.'

3.6.4.1 Localisat on and ident f cat on

The use of real-time RBI is authorised to locate and identify a suspect of a criminal offence to conduct a criminal investigation, prosecute them for the committed crime or execute an existing sentence. Article 5(1)(h)(iii) mentions the localisation and identification of a suspect or a perpetrator for one of the crimes listed in Annex II.

Suspects and Perpetrators

Article 5(1)(h)(iii) covers **two categories of individuals**: **suspects** and **perpetrators**.[206] A suspect is defined in EU law as a person 'with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence.'[207] In Case C-205/21, the CJEU specified that the existence of 'serious grounds for believing that the person in issue has committed a criminal offence... presupposes that sufficient evidence of that person's involvement in the offence has already been gathered.'[208] Strictly speaking, a perpetrator is the person who has committed a crime and is convicted.[209] It is not specified whether RBI could also be used to locate or identify the accomplice of the crimes listed in Annex II to the AI Act.[210]

Suspects or accused persons have different rights protected at EU level.[211] These rights are:

- The right to informat on (Direct ve 2012/13)
- The right to interpretat on and translat on (Direct ve 2010/64)
- The right to have a lawyer (Direct ve 2013/48)
- The right to be presumed innocent and be present at a trial (Direct ve 2016/343)
- The right to legal aid (Direct ve 2016/1919)
- And concerning children (persons under 18 years old), special safeguards when they are suspected and accused in criminal proceedings (Direct ve 2016/800)

These rights are enshrined in Articles 47 to 49 of the Charter, which cover respectively the right to an effective remedy and to a fair trial, the presumption of innocence and the right of defence, and the principles of legality and proportionality of criminal offences and penalties.

3.6.4.2 List of serious crimes

Only serious crimes could justify the use of real-time RBI systems. In the proposal for the AI Act, the European Commission referred to the list of criminal offences that can trigger a European Arrest Warrant (EAW), i.e. 32 offences.[212] But, as not all the crimes in the list are equivalent in terms of 'seriousness, probability and scale of the harm or possible negative consequences' for the criminal suspects,[213] the AI Act has limited the list to the most serious crimes which are punished with a custodial sentence or detention order of a maximum of at least four years.

Annex II of the AI Act provides an exhaustive list of serious crimes for which the real-time use of RBI can be authorised. These criminal offences are:
– terrorism,

[206] Rec. 33 AI Act.
[207] Art cle 6 of the LED, read together with Rec. 31 of the LED.
[208] Case C-205/21, para. 131.
[209] In the LED, the perpetrator is referred to as a 'person convicted of a criminal of ence' (Art. 6(b) LED); see also Quintel, T. and Mitsilegas, V., 'Art cle 6: Dist nct on Between Dif erent Categories of Data Subject', Commentary of the LED, p. 177.
[210] Recital 33 of the AI Act mentions persons 'involved in a crime', which could include accomplices, but the mention is made in link with the ability of law enforcement, border control, immigration or asylum authorities to perform identity checks.
[211] See European Commission, 'Rights of Suspects and Accused'; and the Commission Recommendat on (EU) 2023/681 of 8 December 2022 on procedural rights of suspects and accused persons subject to pre-trial detent on and on material detent on condit ons.
[212] Art. 5 of the Proposal for the AI Act.
[213] Rec. 33 AI Act.

– trafficking in human beings,
– sexual exploitation of children, and child pornography,
– illicit trafficking in narcotic drugs or psychotropic substances,
– illicit trafficking in weapons, munitions or explosives,
– murder, grievous bodily injury,
– illicit trade in human organs or tissue,
– illicit trafficking in nuclear or radioactive materials,
– kidnapping, illegal restraint or hostage-taking,
– crimes within the jurisdiction of the International Criminal Court,
– unlawful seizure of aircraft or ships,
– rape,
– environmental crime,
– organised or armed robbery,
– sabotage,
– participation in a criminal organisation involved in one or more of the offences listed above.

The first five offences are identified as euro crimes in Article 83 TFEU, while the others constitute priorities for law enforcement cooperation.[214] Some of them (e.g. kidnapping, illicit trafficking in nuclear or radioactive materials) can be linked to terrorism.[215]

Although the list of criminal offences is those that can trigger the issuance of a European Arrest Warrant against a suspect or perpetrator, it is not required that an EAW has been issued to deploy a real-time RBI system for locating or identifying a suspect or perpetrator of one of these serious criminal offences.

Scenario 9 - Real-time biometric surveillance in public spaces to locate and identify individuals with an outstanding arrest warrant

During a busy festival in a city, police authorities deploy live facial recognition technologies to monitor the area around the festival and identify wanted individuals with outstanding arrest warrants for illegal drug trafficking and sexual offences. At different entrances to the festival, the police use live video footage of people passing in front of a mobile camera to compare their faces with a watchlist of faces of wanted individuals. Does this case fall under the exception of Article 5(1)(h) (iii)?

1) Law enforcement purpose carried out by a law enforcement authority: monitoring of public spaces to ident fy wanted individuals with an outstanding arrest warrant for two types of crimes.
2) Public Spaces: areas around the fest val
3) Live use of FRT

[214] Europol priorit es.
[215] See def nit on of terrorist of ences in Art.3 of Direct ve 2017/541.

4) Existence of a reference database (specif c watchlist database of wanted individuals with an outstanding arrest warrant for illegal drug traf cking and sexual of ences)

Are the conditions of Article 5(1)(h)(iii) met?
Live FRT cannot be used for the surveillance of public spaces in general, but it could be used to identify and locate a suspect of one of the criminal offences of Annex II of the AI Act under strict conditions.

First, concerning the offence types, illegal drug trafficking is one of them. However sexual offences are not unless they relate to the sexual exploitation of children, child pornography, or a rape. The police are not allowed to deploy live FRT in the wild, i.e. in the hope of finding wanted criminal and taking them off the streets.

Variation:
The case is different if the police have received a physical description with a photograph of a wanted individual, who is subject to an EAW for drug trafficking. They have gathered information about his whereabouts and reasons to believe he will be present at the festival (for instance, the presence of acquaintances who are performing at the festival). In those circumstances, deploying real-time facial recognition technologies to identify the targeted individual could be covered by Article 5(1)(h)(iii) of the AI Act. As the live use of FRT must be proportionate and strictly necessary, the police will have to show that no other less intrusive alternatives (such as the use of traditional CCTVs or police officers present at the festival for visual surveillance) can achieve the same result to locate and identify the suspect of a drug trafficking.
In conclusion, depending on the circumstances of the case (initial case or variation), the case could fall under Article 5(1)(h)(iii) of the AI Act. However, the live use of FRT will only be allowed if it complies with the conditions and safeguards of Article 5(2) et seqs. of the AI Act, in addition to the application of other rules.

A link between Article 5(1)(h)(i) and Article 5(1)(h)(iii) can be made for the crimes covered in Article 5(1)(h)(i). While real-time RBI systems could be deployed to find the victim or a missing person, the technologies could also be used to locate and identify the perpetrator or suspect of trafficking in human beings, sexual exploitation as far as it concerns children (as listed in Annex II), and kidnapping (as far as the abduction mentioned in Article 5(1)(h) (i) qualifies as kidnapping as listed in Annex II of the AI Act).

Scenario 10 – Algorithmic video surveillance

New AI video surveillance systems are deployed in a city to secure the Olympic Games. Although the public authorit es do not have the authorisat on to deploy live facial recognit on systems, they have put in place a new generat on of AI systems, which can detect crowd movements, abnormal behaviours, crowd emot on detect on, dumping bags, in various publicly accessible areas (in the streets, the stadiums, and the metro stat ons). The tools do not ident fy any individuals. Instead,

they alert law enforcement and other competent authorit es of an issue so that they can react appropriately to stop a major incident.

It may also be possible to add further funct onality to the AI system to:

- Capture a facial image of the individual/s who dumped a suspicious bag, started an altercat on or any act on that could result in an incident. This can later, if required, and based on prior authorisat on, be run through a post-remote AI system to compare the captured facial image with databases of threat actors (hooligans, terrorist suspects) (variat on 1) or
- Capture a facial image of the individual/s who dumped a suspicious bag, started an altercat on or any act on that could result in an incident, and use real-t me remote RBI immediately to compare the captured facial image with databases of threat actors (hooligans, terrorist suspects) (variat on 2).

Analysis:

1) Algorithmic video-surveillance systems do not process biometric data for ident f cat on purposes as their aim is to alert about incidents and abnormal behaviours and crowd emot ons. However, they could st ll be used for mass surveillance and adversely af ect the fundamental rights of the part cipants in the event. But these systems do not fall under the prohibit on of Art cle 5(1)(h).

2) In variat on 1, if images are extracted from these systems and further analysed for ident f cat on purposes, the police perform retrospect ve facial recognit on on the images collected. This retrospect ve use of FRT is not prohibited by Art cle 5(1)(h). However, it must comply with the requirement of Art cle 26 (10) of the AI Act, which includes a targeted use of the technology (for instance, in link with a criminal of ence), the existence of safeguards and a prior authorisat on.

3) In variat on 2, images are compared in real-t me. This type of use falls under Art cle 5(1)(h) of the AI Act. Real-t me RBI cannot be switched on if the use does not fall under one of the three except ons, which must have been authorised in the nat onal legislat on of the Member State.

   Concerning the threat of a terrorist at ack, the threat cannot be potent al under Art cle 5(1)(h)(iii). It must be genuine and foreseeable or genuine and present. This means that the threat level for a terrorist at ack must be at the highest level of terrorist threats, as def ned at domest c level, and that police received concrete informat on that can relate to one or several suspects, the locat ons of the terrorist at acks, or the t ming of these at acks. Real-t me use should be targeted, based on prior knowledge and informat on, and should not be switched on due to the presence of a potent al suspect or informat on on the targeted locat ons for a terrorist at ack during the Olympic Games. The reference database is also not specif c enough.

   Based on the informat on provided, the real-t me use of RBI would not be allowed.

3.6.5 Condit ons and Safeguards (Art cle 5(2) AI Act)

The deployment of real-time RBI systems for one of the objectives covered by Article 5(1)(h)(i) to (iii) is subject to conditions and safeguards, which are detailed in Article 5(2) to Article 5(7) of the AI Act. This study is limited to the conditions provided by Article 5(2) of the AI Act.

Article 5(2) provides that:
'The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement for any of the objectives referred to in paragraph 1, first subparagraph, point (h), shall be deployed for the purposes set out in that point only to confirm the identity of the specifically targeted individual, and it shall take into account the following elements:

(a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm that would be caused if the system were not used;

(b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences.

In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement for any of the objectives referred to in paragraph 1, first subparagraph, point (h), of this Article shall comply with necessary and proportionate safeguards and conditions in relation to the use in accordance with the national law authorising the use thereof, in particular as regards the temporal, geographic and personal limitations. The use of the 'real-time' remote biometric identification system in publicly accessible spaces shall be authorised only if the law enforcement authority has completed a fundamental rights impact assessment as provided for in Article 27 and has registered the system in the EU database according to Article 49. However, in duly justified cases of urgency, the use of such systems may be commenced without the registration in the EU database, provided that such registration is completed without undue delay.'

3.6.5.1 Targeted individual and Safeguards

First, real-time use of RBI systems should only be deployed to **'confirm the identity of the specifically targeted individual'**, balancing the seriousness of the situation and the harm resulting from not using the system with the impact of the technologies' use on individuals' rights and freedoms. The first condition aims to avoid mass surveillance by targeting an individual for the deployment of real-time RBI. As a consequence, the deployment of a RBI in real-time should only be authorised for a targeted individual or individuals (in case of terrorist groups). By 'confirming the identity', one should understand that the purpose of the real-time use of RBI can only be initiated for specific individuals for which the law enforcement authorities have reasons to believe or are informed that the individuals are victims of the crimes listed in Article 5(1)(h)(i) or are involved in one of the situations described in Article 5(1)(h)(ii) or Article 5(1)(h)(iii). Concerning the application of Article 5(1)(h)(ii), law enforcement authorities might not necessarily know the identity of the individuals they are searching for in the context of a genuine threat of a terrorist attack. But, if they have factual indications and information about a planned terrorist attack by a terrorist group (without knowing who will execute the plan) on a specific day at a defined place, it could be envisaged that the RBI system is deployed to identify the members of a terrorist group. However, the scope of who (and what) is targeted in that case will depend on what the national law authorises explicitly in the context of the prevention of a genuine threat of a terrorist attack.

Law enforcement authorities will also have to constitute a reference database containing the biometric data of these individuals. In the situation covered by Article 5(1)(h)(iii), law enforcement authorities need information about the suspect or perpetrator of one of the offences covered by Annex II as they are looking for a specific person.

Confirming the identity in relation to identification

Prima facie, the expression 'to confirm the identity of the specifically targeted individual' appears confusing. Real-time biometric identification contributes to the identification of persons. Yet identification and confirmation of identity are two different notions, as set out in Article 3(35) and (36) and explained in recitals 15, 17 and 54. However, that phrase should be interpreted as an additional safeguard for fundamental rights to limit the risk of indiscriminate surveillance. To this end, the identification of individuals in a publicly accessible space or without cause for a relevant individual is not allowed. Only the deployment of the technologies to confirm their identity is allowed.

Second, before using the system, the risk of not using the system and the resulting harm should be assessed against the impact of using the system on individuals' rights and freedoms. This should include evaluating whether less intrusive alternative solutions are available to law enforcement authorities or entities acting on their behalf. In application of Article 5(2)(a) and (b), deployers must conduct a **risk assessment** for the deployment of the RBI systems, **balancing** on one side the **seriousness**, **probability** and **scale** of the **harm if the system is not used** and on the other side the **impact of using these systems on people that are concerned** (i.e. the victim, the missing person, persons involved in a terrorist attack, suspect or perpetrator of one of the crimes listed in Annex II of the AI Act). The seriousness, probability and scale of the real-time use of RBI on persons affected by the use of the technologies have to be assessed. The '**seriousness**' criterion implies a variation in degrees of interference with the fundamental rights at stake, which is linked to the principle of proportionality.[216] Concerning the interferences with fundamental rights, some interferences are viewed as more serious than others. For instance, the general and indiscriminate retention of telecommunications data cannot be justified by the objective of fighting crime, [217] even serious crime, [218] as such measures exceed the limits of what is strictly necessary and cannot be considered justified in a democratic society.[219] However, the objective of protecting national security could justify such blanket retention.[220] The '**scale**' criterion refers to the number and categories of persons affected by the interference (including children and vulnerable or marginalised persons).[221] Finally, the

[216] Case C-207/16, *Ministerio Fiscal*, Judgement of 2 October 2018, para. 55, where the Court states that 'access must be proport onate to the seriousness of the interference with the fundamental rights in quest on.'
[217] Joined Cases C- 203/15 and C-698/15, *Tele2 Sverige and Watson*, 21 December 2016, para. 107
[218] Joined Cases C- 293/12 and C-594/12, *Digital Rights Ireland*, 8 April 2014, paras. 57 et seqs, and joined Cases C- 203/15 and C-698/15, *Tele2 Sverige and Watson*, para. 119.
[219] Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Ne*t, 6 October 2020, para. 141.
[220] Ibid.,paras 134-139 and 177.
[221] See Malgieri G. and Santos C., 'Assessing the (Severity of) Impacts on Fundamental Rights', work-in-progress paper, 28 June 2024, ht ps://papers.ssrn.com/sol3/papers.cfm?abstract_id=4875937

'**probability**' is the likelihood that an event will occur. **This risk assessment should be part of the Fundamental Rights Impact Assessment.**

Third, the real-time use of RBI should be clearly delimited in terms of geographic scope, duration, and targeted person. This is to ensure that the RBI system is strictly used. These safeguards derive from the CJEU's case law on data retention measures.[222] Concerning the **geographic restriction**, the CJEU interprets this safeguard as 'the place where the offence or act adversely affecting national security was committed or prepared.'[223] The geographic limitation can cover one or several geographical areas based on 'objective and non-discriminatory factors' if the competent authorities consider that in these geographical areas, there is 'a situation characterised by a high risk of preparation or commission of serious criminal offences.' [224] Another safeguard relates to the **personal scope** of the measure, i.e. defining the **categories of persons concerned** allows, on the basis of objective evidence to target individuals 'to reveal a link, at least an indirect one, with serious criminal offences, to contribute in one way or another to combating serious crime or to preventing a serious risk to public security or a risk to national security.' [225] Finally, the **time limit** is a period limited to what is strictly necessary, but which may be extended. [226]

Fourth, before the deployment, the law enforcement authority deploying the system must have conducted a Fundamental Right Impact Assessment (FRIA) and registered the system in the EU database (except in a duly justified case).

3.6.5.2 Fundamental Rights Impact Assessment

FRIAs carried out in application of Article 5(2) of the AI Act must comply with the conditions set in Article 27 of the AI Act. This article details the requirements concerning FRIAs applicable to high-risk systems. The study is limited here to **FRIAs in the context of the permitted exceptions to real-time use of RBI in publicly accessible spaces** and explains **what the FRIA is**, who conducts it, when it should be conducted, and the elements that should be assessed according to Article 27 of the AI Act.

First, A FRIA is a new **type of impact assessment** that aims to identify the impact on fundamental rights that a RBI system may produce. A FRIA is an accountability tool. The **FRIA does not replace the existing Data Protection Impact Assessment (DPIA)** that data controllers (i.e. those in charge of processing personal data) must conduct under Article 27 of the LED or Article 35 of the GDPR. The obligation to carry out a DPIA is triggered by the existence of at least two criteria, such as the processing of sensitive data with innovative technologies, the processing on large-scale or the systematic monitoring of a publicly accessible area.

For example,

[222] Joined Cases C- 203/15 and C-698/15, *Tele2 Sverige and Watson*, para. 106; joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 165.
[223] Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 165.
[224] Ibid, para 150.
[225] ibid, para. 148.
[226] ibid, para. 168.

A DPIA must be conducted when biometric data are processed with new technologies (such as CCTV, facial recognition, and body-worn cameras) in publicly accessible spaces.

A list of **nine criteria**, established by the former advisory body, Article 29 Data Protection Working Party, and endorsed by the EDPB, serves as guidance.[227] **A DPIA focuses on the risks to the rights and freedoms of individuals resulting from the processing of their personal data; whereas the FRIA covers the possible impact of AI systems on individuals' fundamental rights, irrespective of whether personal data are processed**. The scope of a FRIA is broader. In case personal data are processed by the AI system (which is the case of RBI systems), the FRIA can complement a DPIA as long as the deployer is also the data controller.[228] The analysis of the FRIA in this study is limited to the authorised use of RBI in real-time.[229]

Second, **law enforcement authorities**, and not entities or bodies or anyone acting on their behalf, **have the obligation to carry out the FRIA**. It seems logical to impose the obligation on law enforcement authorities, as if those authorities delegate the task to another entity, body or person ('acting on their behalf'), law enforcement authorities remain responsible.

Third, a FRIA must be carried out **before the deployment** of the authorised RBI system. Although Article 5(2) of the AI Act does not specify that the law enforcement authority must complete a FRIA for each use of the system, it should be understood that the law enforcement authority updates the FRIA for each deployment if one already exists for the system.[230]

Fourth, according to **Article 27 of the AI Act**, a **FRIA should include the following information**:

- Descript on of the RBI use and deployer's processes together with the intended purpose of use:

The description should be as detailed as possible and **include**
- the name of the technology provider,
- the technical documentation of the RBI system (that should explain the functioning of the technology)
- the law enforcement purpose for which it will be used

[227] In its 'Guidelines on Data Protect on Impact Assessment (DPIA)', WP248 rev.01, the Art cle 29 WP ident f ed nine criteria of which the combinat on of two triggers the obligat on to conduct a DPIA. Although these Guidelines relate to DPIAs in the context of Art cle 35 of the GDPR, they are also relevant in the interpretat on of the applicat on of Art cle 27 of the LED.
These criteria are 1) evaluat on scoring (including prof ling and predict ng); 2) automated-decision making with legal or similar signif cant ef ect; 3) systemat c monitoring (including of a publicly accessible space); 4) sensit ve data or data of a highly personal nature; 5) data processed on a large scale; 6) matching or combining datasets; 7) data concerning vulnerable data subjects; 8) innovat ve use or applying new technological or organisat onal solut ons; and 9) when the processing prevents data subjects from exercising a right or using a service or a contract.
[228] Art. 27(4) AI Act.
[229] Thus, the analysis does not cover the case of high-risk AI systems in general.
[230] Art. 27 of the AI Act requires a FRIA for the f rst t me use of a high-risk AI system.

In this description, the **reference database** against which the biometric identification will be performed should be described, including the sources of the biometric data (facial images, voice samples, etc.) that will be used.

This description should include the **legal basis** on which the real-time RBI will be deployed, **the purpose of use**, the **entity deploying the technologies**, as well as **the temporal** (time limit of the deployment, which can be extended)**, geographic (**geographic areas of deployment, which can be multiple**), and personal limitations (which include identifying the targeted person,** and other impacted persons (i.e. those whose biometric data might be included in the specific reference database, passersby).

- Period of use and frequency of use

Concerning the real-time use of RBI, **each use for one of the permitted exceptions needs to be allowed prior to the deployment**. Hence, the law enforcement authorities will need to update the FRIA each time they deploy a given RBI system as they should identify the specific purpose and circumstances for which they will use the system.

The temporal limitation of use needs to be described, together with objective factors that could justify an extension (for instance, a victim has been abducted and travels in a car).

- Categories of persons and groups af ected by the system

The FRIA should distinguish between:

- The **targeted individual**, who can be the victim of a crime, the perpetrator or the suspect,
- The **individuals** whose biometric data are included in the reference database, and
- **People who are present in the surroundings of the targeted individual**.

The real-time use of RBI will not only affect the fundamental rights of the targeted individual, but also other individuals whose biometric data are used for comparison purposes, **passersby**, and **people incidentally presented in the frame of the cameras,** for example. The description of the geographic scope of the area(s) covered by the RBI system will impact a number of persons affected by the system.

- Specif c risks of harm to the af ected persons:

The fundamental rights that are affected by the real-time use of RBI in publicly accessible spaces are the following ones:

- The right to privacy, including people's reasonable expectat on of anonymity in public spaces.[231]
- the right to data protect on as RBIs rely on the processing of biometric data and other personal data (e.g. names, ID numbers, as well as sensit ve data such as ethnicity) to ident fy specif c individuals,

[231] See EDPB, 'Guidelines 05/2022 on the Use of Facial Recognit on Technology in the Area of Law Enforcement', p.49.

- Freedom of expression and freedom of assembly and associat on in public spaces, as if individuals know they are monitored, they might change their behaviour.[232]
- The right to an ef ect ve remedy and a fair trial includes the right to be informed about the processing of their biometric data[233] and the inclusion of their biometric data in a reference database.[234]
- The right to non-discriminat on might be adversely af ected by the performance of a system that embeds biases (such as gender, ethnic or racial biases)[235] and might lead to the misident f cat on of a suspect or perpetrator.
- The right to human dignity might be impacted by the feeling of becoming an object to the system. [236]
- The presumpt on of innocence and right of defence, which can be challenged by the outcome of the RBI system, as no decision adversely af ect ng an individual can be solely taken on the output of the real-t me RBI system.[237]
- The rights of the child in case the vict m, missing person or suspect is a minor.
- The rights of the elderly may be relevant in case of a missing person whose disappearance is a cause for concern.

To assess the risks of harm likely to impact the identified affected persons or groups**, the FRIA should identify the fundamental rights of these persons** and assess the impact on these fundamental rights, including the severity of the impact. The level of the impact could be assessed through a matrix based on the number of persons affected and the severity of the infringement, using the criteria of negligible, critical, and serious (as proposed in the **ALIGNER** project, see examples of methodologies in this section).

This part should also include the **necessity and proportionality assessment** of the deployment, including the existence or absence of less intrusive alternative measures. The FRIA should describe the **performance and accuracy** level of the system, based on the technical documentation and, if available, the training data on which the technology was tested and developed to prevent biases and discrimination.

For instance,
If the **targeted individual** is a **suspect or a perpetrator**, the FRIA should assess the impact on their right to privacy (including the risk of misidentification), their right to an effective remedy and a fair trial. If the individual is a **victim**, the FRIA should identify the fundamental rights at stake and assess,

[232] Ibid.
[233] In that context, see the obligat on of not f cat on as interpreted by the CJEU in joined Cases C-203/15 and C-698/15, *Tele2 Sverige*, para. 121.
[234] As analysed by FRA in 'Facial Recognit on Technology: Fundamental Rights Considerat ons in the Context of Law Enforcement', p. 32.
[235] Buolamwini J. and Gebru T., 'Gender Shades: Intersect onal Accuracy Disparit es in Commercial Gender Classif cat on', (2018) Proceedings of Machine Learning Research 81, 1-15.
[236] See EDPB, 'Guidelines 05/2022 on the Use of Facial Recognit on Technology in the Area of Law Enforcement', para 39, p.15.
[237] Art. 5(3) AI Act.

among others, the impact on their rights to privacy, but also children' rights in case the victim is a child.

It is essential that the FRIA identifies the impacts on the fundamental rights of **other individuals present** in the publicly accessible spaces. This is because the system will also process biometric data of these individuals, and their rights to privacy and data protection will be impacted. Depending on the context of deployment of the RBI, other fundamental rights of these individuals, such as their rights to assembly or freedom of expression, could be impacted.

The '**fundamental rights roadmap'** established by the Dutch Ministry of Interiors, together with the questions listed to assess the impact of the AI systems on individuals, could serve as a guidance for deployers (see examples of methodologies in this section).

- Human oversight measures

According to Article 5(3) of the AI Act, no decision that would adversely affect an individual can be taken solely based of the output of the real-time RBI system. As a consequence, the FRIA should describe the **procedures** that will be followed and how the output will be interpreted. The procedures should provide instructions on the deployment of the RBI system, clarify the **role of a human agent** in verifying and interpreting the output and provide **training to operate the system.** The person in charge of human oversight should have enough 'AI literacy, training and authority'[238] to understand how the system functions, when it underperforms or malfunctions. The human oversight implies a technical knowledge of the AI system.

For the real-time use of RBI, the human oversight is best assigned to a team (or at least, two persons)[239] rather than a single person.

- Risk mit gat on measures

Beyond implementing human oversight measures (including to avoid discriminatory measures), the deployer should explain redress measures in case of occurrence of the risks, including the governance procedures and complaint mechanisms (such as in case of misidentification).

Two FRIA methodologies – Examples

1. The **ALIGNER project**[240] has published an ad hoc template addressed to law enforcement authorities who deploy AI systems for law enforcement purposes, i.e. prevention, investigation,

[238] Rec. 91 AI Act.
[239] This is a suggest on made by the IAPP in their analysis of the human oversight's obligat on. See Andrews C. 'EU AI Act Shines Light on Human Oversight Needs'.
[240] ALIGNER stands for Art f cial Intelligence Roadmap for Policing and Law Enforcement; the project is an EU Horizon 2020 project.

detection or prosecution of criminal offences or execution of criminal penalties. The template focuses on four 'categories of fundamental rights:'

- Presumpt on of innocence and right to an ef ect ve remedy and a fair trial
- Right to equality and non-discriminat on
- Freedom of expression and informat on
- Right to respect for private and family life and right to the protect on of personal data.

For each category, the template identifies various challenges that law enforcement authorities might face. The document accompanying the templates provides an 'impact matrix' risk to assess the negative impact of the use of the AI systems, based on the number of individuals affected by the system and the severity of the prejudice.[241]

References: [242]

- ALIGNER: How to use the ALIGNER Fundamental Rights Impact Assessment Template.
- ALIGNER: AFRIA Templates.

2. The **Dutch Ministry of the Interior and Kingdom Relations** has elaborated a Fundamental Rights Impact Assessment template to map out the risks posed by the use of algorithms by Dutch public authorities on fundamental rights and identify mitigating measures. The methodology developed by the Dutch government is very comprehensive, although not specific to the field of law enforcement.

The FRIA is composed of four steps:
1. **Identification of the objective of the algorithm** (including its intended effects, objectives and preconditions): this includes describing the problem that the algorithm will solve and reasons to use the algorithm, the public values that support the use and the public values that might be affected, the adequate legal basis allowing the use of the algorithm.

2. **Description of the algorithm** (including the data used as input and their origin): this includes data sources and quality as well training data, the representativeness of the data, possible assumptions and biases embedded in the data, security of the data, the type of algorithm (self-learning or machine learning), accuracy of the algorithm, transparency and explainability.

3. **Explanation of the implementation, use**, and **supervision of the algorithm**: this includes human oversight, evaluation and auditing of the system, as well as decisions based on the algorithm's output.

4 **Impact on fundamental rights**. This last step comprises a 'fundamental rights roadmap' composed of seven steps: which fundamental rights are affected? Is there any specific legislation? How serious is the infringement? What are the aimed social, political, or administrative objectives? Is the

[241] Such a matrix is useful; however, the document does not explain the methodology used to build it.
[242] ht ps://aligner-h2020.eu/fundamental-rights-impact-assessment-fria/

algorithm a suitable tool for the objectives? Is the algorithm necessary to achieve these objectives or are there alternatives? Are the objectives sufficiently balanced to justify the interference with the fundamental rights.

References: [243]

- Government of the Netherlands, 'Fundamental Rights and Algorithms Impact Assessment (FRAIA)'

Points for attention:

While Article 5 of the AI Act will be applicable six months after the entry into force of the AI Act, Article 27 of the AI Act that details the obligation to carry out a FRIA will only be applicable 24 months after the entry into force of the AI Act. The European Commission will also issue a template for FRIAs at a later stage. The description and explanations for each element of a FRIA, as listed in Article 27 of the AI, are intended to provide some indications about the FRIA. As a suggestioon, a mapping of Article 27 of the AI Act, modelled after the one published by Mustać[244] but adapted to law enforcement purposes, could be added to the Guidelines.

Registration of the authorised RBI systems

Concerning the registration of the system in the EU database, as outlined in Article 49 of the AI Act, in case of a duly justified emergency (such as an imminent event), the deployment can start, provided the law enforcement authority registers the RBI system without undue delay. **Undue delay** should be understood **as soon as possible**, considering the circumstances of the emergency that prevented the registration of the system prior to its use.[245] It requires an appreciation on a case-by-case basis and cannot be defined a priori with a precise time limit. But the delay should not be caused by a deliberate action.

For example,
Requesting law enforcement authorities to register the RBI system within 24 hours of its use might be considered a reasonable delay in case the system was deployed in a situation of an imminent threat to life, such as in the shooter scenario(scenario 8).

3.7 Out-of-Scope

All the other uses of RBI systems that are **not covered by the prohibition** of Article 5(1)(h) and the explicit exceptions of Article 5(1)(h)(i)-(iii) **fall into the category of high-risks** as defined in Article 6 of the AI Act and listed in 1(a) of Annex III of the AI Act. However, the **AI Act does not create a legal basis**

[243] https://www.government.nl/documents/reports/2021/07/31/impact-assessment-fundamental-rights-and-algorithms

[244] See Mustać T. 'The AI Act Series: Fundamental Rights Impact Assessments', Medium, 9 August 2024.

[245] By analogy, the Art cle 29 Data Protect on Working Party, replaced by the EDPB, interpreted the not on of 'undue delay' in relat on to the t mely communicat on of a data breach to individuals as meaning 'as soon as possible'. See A29WP, 'Guidelines on Personal Data Breach under Regulat on 2016/679' WP250 rev.01, as endorsed by the EDPB, p.20.

to process biometric data as data protection rules still apply (either the GDPR or the LED, depending on the nature of the data processing). Besides, the AI Act does not allow to circumvent other legislation.

Although the study of high-risk systems is not part of this report, three cases can be mentioned. First, this concerns **the retrospective use of RBI systems in public spaces for law enforcement purposes**. For instance, police authorities might be authorised by national law to perform retrospective facial recognition to compare images of criminal suspects with recorded facial images in a criminal database.[246] **Another case is the use of real-time RBI systems for a law enforcement purpose in either a private space** (such as at somebody's place) or **online space** (such as the use of live FRT in a chat room or online game to identify a suspect of child pornography). The **last situation is the use of RBI systems by private actors, both in real-time and retrospective** (such as the use of live FRT by a supermarket to identify known shoplifters, the use of live FRT by a sports arena to identify individuals banned from entering the arena, or the use of live FRT in schools for security purposes and school attendance).

RBI systems that fall into the category of high-risk AI systems are subject to the following rules, briefly summarised:[247]

- Conformity assessments (pre/post market)[248]
- Fundamental Rights Impact Assessments (FRIAs) are imposed on deployers that are bodies governed by public law, private ent t es providing public services and deployers of certain high-risk AI systems, such as banking or insurance companies.[249]
- Risk-management system,[250]
- Data governance,[251]
- Technical documentat on,[252]
- Record-keeping, [253]
- Transparency obligat ons imposed on the providers (e.g. manufacturer, seller) and deployers (law enforcement authorit es, public authorit es, private ent t es, etc.). [254]
- Human oversight, [255]
- Accuracy, robustness, and cybersecurity.[256]

[246] For instance, the *Traitement des Antécédents Judiciaires* database in France, created by *Décret no. 2012-652 du 4 mai 2012 relat f au Traitement des Antécédents Judiciaires* (Decree 2012-652).
[247] This part falls outside the scope of the study.
[248] Art. 43 AI Act.
[249] Art. 27 AI Act and Rec. 96 AI Act.
[250] Art. 9 AI Act.
[251] Art. 10 AI Act.
[252] Art. 11 AI Act.
[253] Art. 12 AI Act.
[254] Art. 13 AI Act, Art. 16 AI Act (providers' obligat ons), Art. 26 AI Act (deployers' obligat ons).
[255] Art. 14 AI Act.
[256] Art. 15 AI Act.

Besides, the **retrospective use of RBI systems for law enforcement purposes** is subject to **additional rules**, which are applicable to their deployers: [257]

- **Prior authorisat on** by a judge or an administrat ve authority whose decision is binding before the deployment, or without undue delay and no later than 48 hours, except when the system is used for the init al ident f cat on of a potent al suspect based on object ve and verif able facts directly linked to the of ence. In case no authorisat on is delivered, the use should stop immediately, and the personal data processed deleted.

- Use is only allowed for a **targeted** search (i.e. the technology is used in a targeted way), whether it is in link with a criminal of ence (and the targeted search of a suspect or perpetrator), a criminal proceeding, a genuine and present or genuine and foreseeable threat of a criminal of ence, or the search for a specif c missing person.

- **No decision** with an **adverse legal ef ect** on a person should **be solely based on the output** of the system.

- **Each retrospect ve use** of RBI must be **documented** and made available to the relevant market surveillance and DPA upon request.

- **Annual reports** must be submit ed to the relevant market surveillance authorit es and DPAs.

Member States can introduce more restrictive laws in compliance with Union law. They could, therefore, decide to ban the retrospective use of RBI for law enforcement and non-law enforcement purposes.[258]

Based on national Courts' and DPA's decisions, the cases below illustrate the use of RBIs for non-law enforcement purposes (in the context of schools, a supermarket, and football stadiums). As the RBI systems process biometric data, they are subject to compliance with data protection rules and, in particular, Article 9(2) of the GDPR governing the processing of sensitive data.

For example,
A French administrative Court found that the trial of live FRT in two public schools for access control and security purposes was neither necessary nor proportionate. Alternative solutions that were less intrusive for the students were available, e.g. the use of badges. Besides, the conditions for explicit consent were not met. Therefore, consent could not be used as a valid legal basis to trial FRT in high schools. [259]

For example,
A supermarket was not allowed to use live FRT to prevent shoplifting in the Netherlands. Without explicit consent from the customer or any legal basis allowing the processing for a substantial public

[257] Art cle 26(10) and Rec. 94 AI Act.
[258] Last paragraph of Art. 26(10) AI Act.
[259] TA Marseille (Administrat ve Court in Marseille) 27 February 2020, no. 1901249.

interest (such as security purposes), the supermarket could not process biometric data and thus deploy FRTs.[260]

For example,
The use of live FRT at the entrance of a football club was banned in France to *identify supporters*[261] and was banned in Spain to *ensure the safety of spectators*.[262]

4 Untargeted Scraping of Facial Images

Art. 5(1)(e) prohibits 'the placing on the market, putting into service and use of AI systems that create of expand facial recognition databases through the untargeted scraping of facial images from the Internet or CCTV footage.'

4.1 Rat onale

Recital 43 of the AI Act justifies the prohibition of Article 5(1)(e) based on the 'feeling of mass surveillance' and the risks of 'gross violations of fundamental rights, including the right to privacy.' This prohibition was not part of the proposal for the AI Act but was added during the negotiations of the AI Act.[263] This prohibition aims at complementing the GDPR rules. While the GDPR applies to the processing of personal data, including by AI systems, the AI Act governs the use and other practices of AI systems.

The prohibition introduced in the AI Act echoes the Clearview AI case, resulting in several fines imposed by DPAs in Europe and beyond. As revealed in January 2020 by the investigative journalism of the New York Times, Clearview AI is a US start-up that scraped billions of facial images from various online platforms and social media, along with associated metadata and information, to create a large-scale facial database, whose access was sold to law enforcement authorities and private companies.[264]

4.2 Legal Background

Several DPAs fined the company in Europe for non-compliance with the General Data Protection Regulation. Despite the company's absence of establishment or representation in the EU, the DPAs applied the GDPR based on its extra-territorial scope (in particular, Article 3(2) GDPR, targeting data subjects in the EU through the monitoring of their behaviour). In their respective decisions, they found several violations of the GDPR, including the lack of legal bases to collect and process personal and

[260] ht ps://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-issues-formal-warning-to-supermarket-for-use-of-facial-recognit on-technology.

[261] ht ps://www.cnil.fr/fr/reconnaissance-faciale-et-interdict on-commerciale-de-stade-la-cnil-adresse-un-avert ssement-un-club
See also Jasserand C., 'Yellow Card to a French Football Club: No Facial Recognit on System to Monitor their Supporters', 30 March 2021, CiTiP Blogpost.

[262] ht ps://www.biometricupdate.com/202401/spanish-data-authority-opposes-facial-recognit on-for-football-stadium-access

[263] By the European Parliament.

[264] Hill K., 'The Secret ve Company that Might End Privacy as We Know It', the New York Times, 18 January 2020.

biometric data, non-respect of data subjects' rights (e.g. right of access, right to erasure, right of information), and the lack of protection for biometric sensitive data.

DPAs decisions against Clearview AI's practices on the GDPR basis and DPAs decisions against police authorities using Clearview AI's platform on the LED basis

☞ **Several DPAs issued injunction orders and decisions against Clearview AI**. They found that its practices of indiscriminately scraping facial images from publicly accessible social media and websites to create individuals' profiles infringe the GDPR. In particular, the company could not rely on explicit consent or data manifestly made available by the data subjects themselves to process their biometric data. They also found several violations of data subjects' rights.
Several ordered the company to delete the data to pay 20 million euros of fines [e.g. CNIL, Decision No. MED 2021-134; Il Garante, injunction order 9751362; Hellenic DPA, Decision 35/2022]. The French DPA, CNIL, issued an additional fine for non-execution of the original decision [CNIL, Deliberation No. SAN-2022-019], while the Hamburg Commissioner for Data Protection and Freedom issued a limited order that only requested deleting the hash value generated for the complainant's profile. [Hamburg DPA, Order 545/2020; 32.02-102]

☞ In addition, the **Swedish DPA fined the police for using Clearview AI's platform** without legal basis, while the Deputy Data Protection Ombudsman in **Finland** issued a warning to the police for testing the platform and processing biometric data without legal basis.
[Swedish IMY decision, DI-20200-2719; Office of the Data Protection Ombudsman, Decision 3394/171/21]

Despite the growing number of fines imposed on Clearview AI for infringing the GDPR, the company has not paid the penalties and could not be compelled to do so due to the difficulties of enforcing the sanctions against a company that is neither established nor represented in the EU. Similar databases, such as PimEyes, exist even if they present themselves as a 'reverse engineering image search' engine relying on publicly available images that enable users to reclaim facial images that third parties would have unlawfully published.[265]

Concerning the use of these large-scale facial databases, the EDPS considered that no specific data protection rules would allow law enforcement authorities to use such platforms, [266] while the Swedish police forces were fined for using Clearview AI without legal basis, and the Finnish police received a warning for the same reason. See above.

4.3 Legal Analysis

This prohibition was added by the European Parliament in its position on the proposal for the AI Act and kept by the EU institutions in the final text.[267]

[265] PimEyes, 'Image Search with PimEyes, How to Reverse Image Search' Blog ht ps://pimeyes.com/en/blog/image-search-with-pimeyes-how-to-reverse-image-search
[266] EDPB, Guidelines 05/2022, p.52.
[267] See EP, 'Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulat on of the European Parliament and of the Council laying down harmonized rules on art f cial intelligence (Art f cial

The components of the prohibition include:

1) the purpose of the facial database (facial recognit on, which includes both ident f cat on and verif cat on modalit es. Yet, no recital specif es that the databases should be limited to their ident f cat on funct on);

2) the means to populate the database, i.e. AI tools for untargeted scraping; and

3) the sources of the images, either online sources (internet) or CCTV footage.

Concerning **untargeted scraping**, it should be interpreted in a manner that does not allow circumvention of the prohibition. The scraping of the Internet or CCTV footage for the creation of a database step-by-step, thereby selecting specific groups of individuals or other criteria each time, should fall within the prohibition where the end-result is functionally the same as pursuing untargeted scraping from the outset.

4.3.1 Placing on the market, put ng into service or use of AI systems that create/expand facial recognit on databases

The prohibition covers all practices of the AI system used to create or expand the facial recognition database. It is addressed at both the providers of the systems and the deployers, and is not restricted to law enforcement authorities, public authorities or private companies. What the AI Act **prohibits** is **not the resulting facial recognition database**, but the **AI systems used to create or expand facial recognition databases made through online or CCTV untargeted scraping**.

In some countries, e.g., in France, the police authorities are already authorised to perform facial recognition for investigation purposes on an existing criminal record database, composed of facial images of suspects, victims, and missing persons.[268] Under Article 5(1)(e), it will not be possible to expand further this database through untargeted scraping of images.

The purpose of use of the constituted database is facial recognition, which covers both verification and identification purposes. If the resulting databases are not prohibited per se, they cannot be used as the reference databases for the real-time use of RBI as the reference database needs to be appropriate to each authorised use.[269]

Points of discussion concerning the resulting facial recognition database and the notion of 'output'
Is the resulting facial recognition database constituted with a prohibited AI tool (such as an automated image scraper) covered by the prohibition of Article 5(1)(e)?
Article 5(1)(e) prohibits the AI tool used for untargeted scraping to create or expand a facial recognition database. It is not the creation or expansion per se of the database that is prohibited. But, logically, if the results of the illegal scraping of images are gathered to create or expand a database,

Intelligence Act) and amending certain Union legislat ve acts', Amendments 51 and 225; and Art cle 5(1)(e) AI Act.

[268] The database is called TAJ, *Traitements des Antécédents Judiciaires*, created by *Décret no. 2012-652 du 4 mai 2012 relat f au Traitement des Antécédents Judiciaires* (Decree 2012-652).

[269] Rec.34 AI Act.

such a database should also be prohibited as a consequence. However, their constitution is also subject to EU data protection rules. Based on the decisions by various EU DPAs concerning Clearview AI, their constitution will not be allowed under data protection law due to the lack of an appropriate legal basis.

Is the resulting facial recognition database an output of the AI system used to scrape the images?
According to Article 1(c) of the AI Act, the AI Act applies to 'providers and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the Union.' Article 3(1) of the AI Act provides examples of outputs: 'predictions, content, recommendations, or decisions'. Beyond these examples, the AI Act does not define the concept. Following Recital 22 of the AI Act, the 'AI Act applies to providers and deployers of AI systems that are established in a third country, to the extent that the output produced by those systems is intended to be used in the Union.'
Concerning Clearview AI or providers of similar AI systems (e.g. PimeEyes), is it the facial recognition database created from the scraped images which is considered as the output of the automated image scraper or the mathematical representation of the scraped images gathered in the facial recognition database?

4.3.2 Through untargeted scraping of facial images

The prohibition is **limited to facial images** and does not cover other biometric data, such as voice samples that could be scraped from social media (through video available online) to create voice recognition databases. Concerning the **format** of the facial images, one could argue that, at the stage of their collection (i.e., when they are scraped), these images include photographs, which are not biometric data yet.[270] However, once the database is constituted, they are technically transformed to allow the biometric recognition of individuals.

Web scraping is a process that involves the use of bots to extract data or content from different sources automatically. These bots are software 'programmed to sift through databases and extract information,'[271] including facial images. The AI Act prohibits the making available, supplying, or use of these tools that are used to either create or expand facial recognition databases.

Concerning the tools used by Clearview AI, a reference is made to the '**automated image scraper'**[272] in the complaint drafted by NOYB to describe the search of publicly accessible webpages and the extraction of facial images and associated metadata. However, neither the technical functioning of this tool nor the technologies used are explained in detail. **Technical experts should be consulted** for technical input on the different tools and technologies that can extract data, and in particular facial images, from a website, webpage or a platform.

[270] Rec.51 GDPR, Art 4(14) GDPR.
[271] https://www.imperva.com/learn/application-security/web-scraping-attack/#:~:text=Web%20scraping%20is%20the%20process,replicate%20entire%20website%20content%20elsewhere.
[272] E.g. complaint drafted by NOYB https://noyb.eu/sites/default/files/2021-05/Clearview%20AI%20-%20EN%20DE%20-%20noyb%20-%20redacted.pdf and addressed to the Austrian DPA; and

Although the adjective '**untargeted**' is not defined, it relates to scraping, a technique that operates like a 'vacuum cleaner', absorbing as much data and information as possible. Scraping indiscriminately harvests data or content. Thus, the notion of 'untargeted', meaning without a specific focus on a given individual or individuals, derives from the notion and purpose of scraping. For instance, Clearview AI scraped billions of photographs indiscriminately without targeting specific individuals.

If a scraping tool can be instructed to collect a portion of data or information, then the scraping becomes **targeted**. This is not covered by the prohibition. In the context of data retention, targeted surveillance measures for the purposes of safeguarding national security and combating serious threats are allowed when 'limited, on the basis of objective and non-discriminatory factors in terms of categories of persons concerned or using a geographical criterion, for a period that is limited to what is strictly necessary, but which may be extended.'[273] However, the Court did not discuss whether and under which conditions targeted surveillance could be conducted for the investigation, detection and prosecution of offences other than serious crimes.

As a suggestion, in law enforcement, **targeted scraping** could mean that the **collection of images is connected to a class of victims or suspects linked to a serious crime**, and thus would not lead to indiscriminate surveillance as a specific crime is targeted.

For example,
The targeted collection of images focusing on a class of victims or suspects, by using crawlers to pick up on images of victims that traffickers post/advertise on social media channels (such as telegram), will not be covered by the prohibition.

Background: Clearview AI's facial recognition technology

☞ 'Clearview AI is a facial recognition software company founded in 2017 in New York. The company's face collection has grown from 3 million images to 20 billion with the promise to develop it further. The photographs held by Clearview AI have been scraped from social media (e.g. Facebook, YouTube, Twitter, Venmo) with an 'automated image scraper' as described by NOYB in its complaint to the Austrian DPA. This tool searches the Internet and detects images containing human faces. It collects these images with any associated information (such as the source of the image (URL), the geo-localisation, and sometimes the names of the individuals). Then, the facial features are extracted from the pictures and transformed into mathematical representations, which are hashed for indexation and future comparison. The hashed vectors, together with the images and associated information, are stored by Clearview AI. When a user uploads the picture of an individual, they will run the search engine to determine whether a face is known. The uploaded image will go through the same mathematical transformation as the scraped images and will be hashed to be compared with already stored hashed vectors. The results communicated to the user are not the hashed vectors but the corresponding images with associated information.'

[273] Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others*, judgment of 6 October 2020, para. 168.

Extracted from Clearview AI: Illegally Collecting and Selling Our Faces in Total Impunity, Part I, Blogpost, CiTiP, 28 April 2022.

☞ Article 5(1)(e) of the AI Act prohibits the placing on the market, putting into service, and use of the AI tool, the 'automated image scraper', which will be used to indiscriminately collect images to build up or expand a facial database. Therefore, it prohibits explicitly the means, not the database itself.

4.3.3 From the Internet and CCTV footage

The sources of the images can be both online and from a physical network of surveillance cameras. Examples of scraping facial images from CCTV footage could include footage operated in publicly accessible places, such as airports, streets, parks, etc. It should also be extended to the scraping of facial images from CCTV footage from private or semi-public places, such as CCTV footage from residence buildings.

Scenario 11- Untargeted scraping of facial images from social media to create a facial recognition database

A company outside the EU used an AI-based web scraping tool to indiscriminately extract facial images from various social media websites to develop a large-scale facial database composed of several billions of images and related identifying information. The company sells access to its platform to law enforcement authorities and private entities. In addition, it licenses its AI-based face web-scraping system to enable users to create their own facial database. Which practices are covered by the prohibition of Article 5(1)(e) of the AI Act?

The company's services can be divided into two distinct operations: first, it provides access to its end-product, which is a large-scale facial database that results from untargeted web-scraping; and second, it offers the use of its face web scraping tool, allowing users (either law enforcement authorities or private parties) to create their own facial databases.

1) Access to the large-scale facial database is not covered per se by the prohibit on as Art cle 5(1)(e) prohibits AI systems that create or expand of such databases. However, this part of the scenario is covered by data protect on rules (as analysed by various DPAs in their decisions against Clearview AI and the police authorit es using its plat orm).

2) By contrast, the use of the web-scraper tool to indiscriminately collect facial images to create or expand a facial database for biometric recognit on purposes falls within the prohibit on of Art cle 5(1)(e) of the AI Act. It does not mat er whether the facial database is created for law enforcement purposes or private sector use. The fact that the provider is located outside the EU does not prevent the applicat on of the AI Act rules as soon as the technology is provided to deployers in the Union.

In conclusion, using an AI-based web-scraping tool to indiscriminately collect images from various sources to create or expand a facial database for biometric recognition falls under the prohibition of Article 5(1)(e) of the AI Act.

[Case inspired by Clearview AI's practices]

4.3.4 Out-of-the scope of the prohibit on

The prohibition does not apply to the untargeted scraping of biometric data other than facial images (such as voice samples). The ban covers the AI systems used to create or expand facial databases, but it does not extend to the use of the databases, which should be covered by data protection rules (the GDPR and the LED). The AI Act does not apply to 'AI systems developed or put into service for the sole purpose of scientific research and development.'[274] Thus, an automated image scraper developed to create a facial database for research purposes is not subject to the prohibition of Article 5(1)(e) of the AI Act.

It does not apply to AI systems used to categorise individuals on the basis of their age, gender etc. nor to AI systems which harvest large amount of facial images from the internet to generate new images about fictitious persons because such systems would not result in the identification of real persons.

Finally, if the national security exemption applies, the prohibition will not cover the constitution or expansion of a facial recognition database through untargeted scraping for intelligence gathering.

Scenario 12– Development for training purposes of a facial database through untargeted scraping of facial images from an existing photo platform

A research team at a university needs to train their facial recognition models on non-professional facial images, i.e. with different poses, light exposures, and angles. They collect a large volume of images, around 1 million images linked to more than 300.000 persons, to have two or three pictures from the same individual. They will use a web scraper to harvest images from photo platforms, such as Flickr, to build up their gigantic database. No additional information, such as name or other identifying information, will be collected with the images. The researchers are only interested in diverse photos from a technical perspective. The database will be released in open access under the restrictions that it can only be used for research and development. Does this case fall under the prohibition of Article 5(1)(e) of the AI Act?

1) Images scraped from the Internet
2) Purpose of collect on: to create a facial database that will be used to train facial recognit on models. From a technical perspect ve, training a facial recognit on model is dif erent from performing facial recognit on as the goal is not to ident fy anyone but to train models.

Conclusion: As the purpose is to scrape images to constitute a database for AI training purpose , this practice will not be covered by the prohibition of the AI Act.

[274] Rec. 25 AI Act.

Additional issues to consider are the interplay with data protection rules (the legal basis to collect the facial images as publicly available images are not freely re-usable), copyright issues if applicable, and the terms and conditions (contractual rules) of the photo platforms that might prohibit web scraping, including for research and development purposes.

[case inspired by the constitution of MegaFace]

5. Conclusions and takeaways

The Guidelines the European Commission will publish are intended to be a living document, which should be enriched with additional examples based on the feedback of deployers, but also civil society and citizens. As the prohibited AI practices are those that pose unacceptable risks to society and individuals from a fundamental perspective, the involvement of NGOs and civil society is very important. They could also provide helpful input for the content of the Fundamental Rights Impact Assessment.

Takeaways for deployers:

Concerning the real-time use of RBI in publicly accessible spaces and the three exceptions:

- The provisions permit ng the real-t me use of RBIs in certain situat ons do not the legal basis on which law enforcement authorit es or persons or bodies act ng on their behalf can deploy the AI systems. These provisions provide a framework of rules that allow Member States to adopt rules in their nat onal legislat on to authorise real-t me use RBIs in the cases explicitly allowed by the AI Act. However, Member States are not obliged to provide these except ons in their domest c legislat on.

- The AI Act does not replace exist ng legislat on. In the case of real-t me use of RBI, the deployers must also comply with the rules of the Law Enforcement Direct ve and with the condit ons allow restrict ons to fundamental rights as outlined in Art cle 52(1) of the Charter of Fundamental Rights.

- The Fundamental Rights Impact Assessment is the most important document to just fy the real-t me use of RBI, which will also serve as an accountability and record-keeping document. The document is not a 't ck-the-box' tool. Not only does it have to describe the technical characterist cs of the system and its performance and accuracy level, but it should also explain which fundamental rights are impacted for both the targeted individual and the passersby present during the deployment of the RBI system. Law enforcement authorit es will also have to just fy, in this document, the strict necessity of deploying RBI in the case at stake. Although the AI Act does not impose the publicat on of FRIAs, deployers should consider making them available.

- Besides real-t me RBI, the AI Act has introduced specif c rules for retrospect ve use of RBI for law enforcement purposes, which are classif ed as high-risk systems and subject to addit onal rules due to their purpose of use (law enforcement), as specif ed in Art cle 26(10) of the AI Act.

Concerning untargeted scraping:

- The prohibit on relates to the AI tools used to indiscriminately scrape the Internet or CCTV footage. Even if it does not prohibit the result ng facial databases, it does not allow their const tut on. The creat on of these databases falls under data protect on rules. Likewise, the

AI Act does not allow for the use of Clearview AI, which has been f ned by several DPAs for illegally scraping facial images of individuals located in various EU Member States.

Takeaways for Member States:

- Concerning the except ons to real-t me RBIs, Member States are free to allow all of them, some of them, or none of them. If they decide to allow all or some of the except ons, they must adopt them together with specif c condit ons and safeguards detailed in Art cle 5(2) et seqs of the AI Act in their nat onal law. The AI Act is not the legal basis for the real-t me use of RBIs. According to Art cle 5(5), Member States can also introduce stricter rules for the deployment of real-t me RBI.

- Besides real-t me RBI, the AI Act introduces specif c rules for the retrospect ve use of RBIs for law enforcement purposes, member States that have already allowed such use in their nat onal laws will have to update their procedural rules in accordance with the condit ons set in Art cle 26(10) of the AI Act. Member States can also adopt stricter rules. Those can include prohibit ng the retrospect ve use of RBI at nat onal level.

- Member States are in charge of the implementat on of the AI Act, through the designat on of Market Surveillance Authorit es and the enforcement of infringements.

Bibliography

1. Legislation

EU

Charter of Fundamental Rights of the European Union

Treaty on the Functioning of the European Union

Treaty on the European Union

Commission Recommendation (EU) 2023/681 of 8 December 2022 on procedural rights of suspects and accused persons subject to pre-trial detention and on material detention conditions

Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin [Racial Equality Directive]

Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA)

Directive 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the right to interpretation and translation in criminal proceedings

Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA

Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings

Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty

Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings

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)

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 [LED]

Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings

Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings

Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on Combatting Terrorism and Replacing Council Framework Decision 2002/475/JHA and amending Council decision 2005/671/JHA

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

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC

Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings

Directive (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the Automated Search of Data for Police Cooperation, and Amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 of the of the European Parliament and of the Council (the Prüm II Regulation)

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)

Case Law

ECtHR

Arrowsmith v United Kingdom, App. No. 7050/75, 5 December 1978

Dicle v Turkey, App. No 53915/11, 08 May 2022

Gaughran v the United Kingdom, App. No. 45245/15, judgment of 13 June 2020

Glukhin v Russia, App. No 11519/20, judgment of 4 October 2023

Lapshin v Azerbaijan, App. No. 13527/18, judgment of 11 October 2021

Leander v. Sweden, App. No. 92248/81, 26 March 1987

Osman v the United Kingdom, App. No. 87/1997/871/1083, judgment of 28 October 1998

P.G. and J.H. v the United Kingdom, App. No 44787/98, judgment of 25 December 2001

Podchasov v Russia, App. No. 33696/19, judgment of 13 May 2024

S and Marper v the United Kingdom, App. Nos. 30562/04 and 30566/04, judgment of 4 December 2008

Tërshana v Albania, App. No. 48756/14, judgment of 04 November 2020

United Communist Party of Turkey v Turkey , App. No. 133/1996/752/951, 30 January 1998

Zakharov v Russia, App. No. 47143/06, judgment of 4 December 2015

CJEU

Joined Cases C-293/12 and C-594/12, Opinion of Advocate General Cruz Villalón in *Digital Rights Ireland and Seitlinger and others*, 12 December 2013 (ECLI:EU:C:2013:845)

Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, judgment of 8 April 2014 (Grand Chamber) (ECLI:EU:C:2014:238)

Case C-362/14, *Schrems* (Schrems I), judgment of 6 October 2015 (ECLI:EU:C:2015:650)

Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB and Watson*, judgment of 21 December 2016 (Grand Chamber) (ECLI:EU:C:2016:970)

Case C-207/17, Ministerio Fiscal, Judgement of 2 October 2018 (ECLI:EU:C:2018:788)

Case C-623/17, *Privacy International,* judgment of 6 October 2020 (Grand Chamber) (ECLI:EU:C:2020:790)

Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others*, judgment of 6 October 2020 (Grand Chamber) (ECLI:EU:C:220:791)

Case C-439/19, *Latvijas Republikas Saeima*, judgment of 22 June 2021 (Grand Chamber) (ECLI:EU:C:2021:504)

Joined Cases C-793/19 and C-794/19, *BundesRepublik Deutschland v. Space Net AG and Others*, judgment of 20 September 2022 (ECLI:EU:C:2022:702)

Case C-817/19, *Ligue des droits humains*, judgment of 21 June 2022 (ECLI :EU :C :2022 :491)

Case C-140/20, *Commissioner of An Garda Síochána and Others*, judgment of 5 April 2022 (Grand Chamber) (ECLI:EU:C:2022:258)

Case C-180/21, Opinion of Advocate General Campos Sánchez-Bordona in *Inspektor v Inspektorata kam Visshia sadeben savet*, judgement of 19 May 2022 (ECLI:EU:C:2022:406)

Case C-180/21, *Inspektor v Inspektorata kam Visshia sadeben savet*, judgment of 8 December 2022 (ECLI:EU:C:2022:967)

Case C-204/21, *European Commission v. Poland*, judgment of 5 June 2023 (ECLI:EU:C:2023:442)

Case C-205/21, *Ministerstvo na vatreshnite raboti*, judgment of 26 January 2023 (ECLI:EU:C:2023:49)

Case C-306/21, *Koalitsia 'Demokratichna Bulgaria – Obedinenie*, judgment of 20 October 2022 (ECLI:EU:C:2022:813)

National
Clearview AI Inc v The Information Commissioner [2023] UKFTT 00819 (GRC)

(R) Bridges v Chief Constable of South Wales Police and others [2019] EWHC 2341 (Admin), Judgment of 4 September 2019

R (on the application of Edward Bridges) v the Chief Constable of South Wales Police [2020] EWCA civ 1058, Judgment of 11 August 2020

Conseil d'Etat, *French Data Network and Others*, Decision No. 393099, 21 April 2021
https://www.legifrance.gouv.fr/ceta/id/CETATEXT000043411127?isSuggest=true

Conseil d'Etat*, La Quadrature du Net,* Decision No.442364, 26 April 2022
https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2022-04-26/442364

Cour Constitutionnelle, *La Ligue des Droits Humains*, Decision N131/2023, 12 October 2023
https://www.const-court.be/public/f/2023/2023-131f.pdf

TA Marseille (Administrative Court in Marseille) no. 1901249, 27 February 2020
https://www.laquadrature.net/wp-content/uploads/sites/8/2020/02/1090394890_1901249.pdf

2. Reports, Guidelines, Opinions, and Recommendations

EU

Article 29 Data Protection Working Party (A29WP)
Opinion 02/2012 on facial recognition in online and mobile services, WP192, 22 March 2012

Opinion 3/2012 on developments in biometric technologies, WP193, 27 April 2012

Opinion 1/2014 on the Application of Necessity and Proportionality Concepts and Data Protection within the Law Enforcement Sector, WP211, 27 February 2014

Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in High Risk" for the Purposes of Regulation 2016/679, WP248 rev.01, 4 October 2017

Guidelines on Personal Data Breach under Regulation 2016/679', WP250 rev.01, 6 February 2018

Council of the European Union
Council Conclusions on Stepping Up Cross-Border Police Cooperation in the Area of Missing Persons, 9 December 2021, 14808/21

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' [General Approach on the Artificial Intelligence Act], 14954/22, 25 November 2022, https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf

Opinion of the Legal Service, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence, Appropriateness of the legal bases of Articles 114 and 16 TFEU in relation to the provisions applicable to law enforcement and judicial authorities', 12302/22, 12 September 2022
https://data.consilium.europa.eu/doc/document/ST-12302-2022-INIT/en/pdf

Council conclusions setting the EU's priorities for the Fight against Serious and Organised Crime for EMPACT 2022-2025,' 7101/23, 9 March 2023 https://data.consilium.europa.eu/doc/document/ST-7101-2023-INIT/en/pdf

European Commission
Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Towards an EU Criminal Policy: Ensuring the Effective Implementation of EU Policies through Criminal Law', COM (2011) 573 final, 20 September 2011

Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A European Strategy for Data', COM (2020) 66 final, 19 February 2020

Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A Counter-terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond', COM (2020) 795 final, 9 December 2020

Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Fostering a European Approach to Artificial Intelligence', COM (2021) 205 final, 21 April 2021

Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'Establishing a European Declaration on Digital Rights and Principles for the Digital Decade', COM (2022) 27 final, 26 January 2022

Combatting Trafficking in Human Beings, Factsheet, 19 December 2022
https://ec.europa.eu/commission/presscorner/detail/en/fs_22_7735

DG for Communication, European Commission, 'Rights of Suspects and Accused'
https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/criminal-justice/rights-suspects-and-accused_en

DG Migration and Home Affairs, How Do EU Member States Treat Cases of Missing Unaccompanied Minors? European Migration Networks, EMN Inform, 2020
https://home-affairs.ec.europa.eu/document/download/f6aadb50-7ce2-4612-9f9b-e2e2ab5bfbbf_en?filename=inform_missing_uam_final_15042020.pdf

DG Migration and Home Affairs, 'Stronger and Smarter Borders for the European Union – The Entry-Exit System', Factsheet
https://home-affairs.ec.europa.eu/document/download/3bcec877-43b6-4de4-b440-300ab47462be_en?filename=factsheet_-_entryexit_system_en.pdf

DG Migration and Home Affairs, 'Alerts and Data in SIS'
https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/alerts-and-data-sis_en

DG Migration and Home Affairs, 'Together Against Trafficking in Human Beings', 23 April 2024
https://home-affairs.ec.europa.eu/policies/internal-security/organised-crime-and-human-trafficking/together-against-trafficking-human-beings_en

Public Consultation on the AI White Paper- Final Report, November 2020
https://digital-strategy.ec.europa.eu/en/library/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence-and

Staff Working Document, 'Executive Summary of the Impact Assessment Report', SWD (2021) 85 final, 21 April 2024

Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe, 21 April 2021
https://digital-strategy.ec.europa.eu/en/library/study-supporting-impact-assessment-ai-regulation

White Paper on Artificial Intelligence: A European Approach to Excellence and Trust, COM (2020) 65 final, 19 February 2020
https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

European Data Protection Board (EDPB)

Guidelines 3/2019 on Processing of Personal Data Through Video Devices, 30 January 2020

Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement' version 2.0, 26 April 2023
https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en

Opinion 11/2024 on the Use of Facial Recognition to Streamline Airport Passengers' Flow (Compatibility with Articles 5(1)(e) and (f), 25 and 32 GDPR), version 1.1, 23 May 2024
https://www.edpb.europa.eu/system/files/2024-05/edpb_opinion_202411_facialrecognitionairports_en.pdf

Press Release, Facial Recognition in School Renders Sweden's first GDPR fine, 22 August 2019
https://www.edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en

Press Release, Finnish SA: Police Reprimanded for Illegal Processing of Personal Data with Facial Recognition Software, 20 September 2021

https://www.edpb.europa.eu/news/national-news/2021/finnish-sa-police-reprimanded-illegal-processing-personal-data-facial_en

Press release on the EDPB's 'statement on DPAs role in the AI Act framework', 17 July 2024 https://www.edpb.europa.eu/news/news/2024/edpb-adopts-statement-dpas-role-ai-act-framework-eu-us-data-privacy-framework-faq_en

Response to MEP Sophie in't Veld regarding the use of Automatic Image Recognition Systems on Migrants in Italy, 10 August 2021, https://www.edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-mep-sophie-int-veld-regarding-use-automatic_en

Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework, 16 July 2024
https://www.edpb.europa.eu/system/files/2024-07/edpb_statement_202403_dpasroleaiact_en.pdf

EDPB-EDPS
Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 18 June 2021

European Data Protection Supervisor (EDPS)
Assessing the Necessity of Measures that Limit the Fundamental Right to the Protection of Personal Data: A Toolkit, 11 April 2017
https://www.edps.europa.eu/sites/default/files/publication/17-04-11_necessity_toolkit_en_0.pdf

Facial Recognition: A Solution in Search of a Problem? Blogpost, 28 October 2019
https://www.edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_de

Guidelines on Assessing the Proportionality of Measures that Limit the Fundamental Rights to Privacy and to the Protection of Personal Data, 19 December 2019
https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/assessing-proportionality-measures-limit_en

AI and Facial Recognition: Challenges and Opportunities, Blogpost, 21 February 2020
https://www.edps.europa.eu/press-publications/press-news/blog/ai-and-facial-recognition-challenges-and-opportunities_en

Artificial Intelligence, data and our values – on the path to the EU's digital future', Blogpost, 7 September 2020
https://www.edps.europa.eu/press-publications/press-news/blog/artificial-intelligence-data-and-our-values-path-eus-digital_en

Opinion on the Possibility to Use Clearview AI and Similar Services at Europol (Case 2020-0372)', 29 March 2021

Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the Light of Legislative Developments', 23 October 2023

Statement in View of the 10th and Last Plenary Meeting of the Committee on Artificial Intelligence (CAI) of the Council of Europe drafting the Framework Convention on Artificial Intelligence, Human Rights', Democracy and the Rule of Law, 11 March 2024

European Parliamentary Research Service (EPRS)
EPRS, EU Policies, Insight Briefing, 'Understanding EU Counter-Terrorism Policy' 2021 https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/659446/EPRS_BRI(2021)659446_EN.pdf

Madiega T. and Mildebrath H.A., 'Regulating Facial Recognition in the EU' PE 698.021, 15 September 2021

https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf

European Parliament
Resolution on a Framework of Ethical Aspects of Artificial intelligence, Robotics and Related Technologies, 2020/2012, 20 October 2020
https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html
Resolution of 6 October 2021 on Artificial Intelligence in Criminal Law and Its Use by the Police and Judicial Authorities in Criminal Matters, 2020/2016 (INI), 6 October 2021
https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.pdf

Amendments adopted by the European Parliament on 14 June 2023 on the Proposal for a Regulation of the European Parliament and of the Council laying down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and amending Certain Union Legislative Acts' https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html

Europol
'TE-SAT, European Union, Terrorism Situation and Trend Report, 19 December 2023
https://www.europol.europa.eu/cms/sites/default/files/documents/European%20Union%20Terrorism%20Situation%20and%20Trend%20report%202023.pdf

'EU Policy Cycle – Empact
https://www.europol.europa.eu/crime-areas-and-statistics/empact

European Union Agency for Fundamental Rights (FRA)
Directive (EU) 2017/541 on Combating Terrorism, Impact on Fundamental Rights and Freedoms, 18 November 2021

Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement, 27 November 2019

Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies, Volume I, Member States' Legal Frameworks, 11 July 2017

Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies, Volume II, Fields Perspectives and Legal Update,

Others
Facial Recognition Working Group of the Biometrics and Forensics Ethics Group, 'Ethical Issues Arising from the Police Use of Live Facial Recognition Technology' (February 2019)

High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI', 8 April 2019
https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Europe
Council of Europe
Additional Protocol of the Council of Europe Convention on the Prevention of Terrorism (CETS No. 217), 22 October 2015

Convention on the Prevention of Terrorism (CETS No. 196), 16 May 2005

Convention for the Protection of Individuals with regard to Automatic Processing of Personal data (CETS No. 108), 28 January 1981 [Convention 108]

Explanatory Report, Second Additional Protocol to the Budapest Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, CM(2021) 57-addfinal, 11 November 2021

Guidelines on Facial Recognition, Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108), 30 January 2021

Modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal data, Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal data 17-18 May 2018 [Convention 108+]

Recommendation No. R (87) 15 of the Committee of Ministers Regulating the Use of Personal Data in the Police Sector, 17 September 1987

Recommendation CM/Rec (2009) 12 of the Committee of Ministers to Member States on the principles concerning missing persons and the presumption of death, 9 December 2009

Recommendation, Commissioner on Human Rights, 'Unboxing Artificial Intelligence: 10 Steps to Protect Human Rights, 24 May 2019

Second Additional Protocol to the Budapest Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, CM(2021) 57-final, 11 November 2021

International

Interpol, Fact Sheet 'Facial Recognition'
https://www.interpol.int/en/How-we-work/Forensics/Facial-Recognition

United Nations High Commissioner for Human Rights, 'Impact of new Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, including peaceful protests'

United Nations, Security Council, 'Resolution 2178 (2014)', 24 September 2014

United Nations, Security Council, press release, 'Terrorist Groups Remain Significant Threat in Conflict Zones, Neighbouring States, Senior Official Tells Security Council, Noting Force Alone Can Exacerbate Matters', 9405TH Meeting, SC/15396, 25 August 2023
https://press.un.org/en/2023/sc15396.doc.htm

World Economic Forum 2022: World Economic Forum et al., 'A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations, Insight Report, Revised November 2022'

National

Belgium

Articles 112 à 124 of the Belgian Civil Code

National Crisis Center, 'Terrorism and Extremism'
https://crisiscenter.be/en/risks-belgium/security-risks/terrorism-and-extremism

Personnes Disparues (missing persons), factsheet
https://www.belgium.be/fr/famille/deces/disparus

The Coordination Unit for Threat Analysis', https://cuta.belgium.be/

Finland

Poliisi, 'Testing of Facial Recognition Software by NBI reported to Data Protection Ombudsman' 9 April 2021
https://poliisi.fi/en/-/testing-of-facial-recognition-software-by-nbi-reported-to-data-protection-ombudsman

Office of the Data Protection Ombudsman, Decision 3394/171/21, 29 September 2021 [concerning the use of the Clearview AI's platform]
https://finlex.fi/fi/viranomaiset/tsv/2021/20211023

Office of the Data Protection Ombudsman, 'Police Reprimanded for Illegal Processing of Personal Data with Facial Recognition Software', Press Release, 1 October 2021
https://tietosuoja.fi/en/-/police-reprimanded-for-illegal-processing-of-personal-data-with-facial-recognition-software

France

Assemblée Nationale, Rapport d'information sur les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité, 2023

Commission Nationale de l'Informatique et des Libertés (CNIL, French DPA)
Facial Recognition: For A Debate Living Up to the Challenges, 15 November 2019

Law Enforcement Directive: What are We Talking About? 2 June 2021
https://www.cnil.fr/en/law-enforcement-directive-what-are-we-talking-about

Decision no MED 2021-134 of 1 November 2021 issuing an order to comply to the company Clearview AI (No. MDMM211166)
https://www.cnil.fr/sites/cnil/files/atoms/files/decision_ndeg_med_2021-134.pdf

Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning Clearview AI'
https://www.cnil.fr/sites/cnil/files/atoms/files/deliberation_of_the_restricted_committee_no_san-2022-019_of_17_october_2022_concerning_clearview_ai.pdf

Commission Nationale Consultative des Droits de l'Homme (CNCDH), 'Avis sur la surveillance de l'espace public', 20 June 2024
https://www.cncdh.fr/sites/default/files/2024-06/A%20-%202024%20-%205%20-%20CNCDH%20-%20Avis%20Surveillance%20de%20l%27espace%20public%2C%20juin%202024_0.pdf

Décret no. 2012-652 du 4 mai 2012 relatif au Traitement des Antécédents Judiciaires (Decree 2012-652)

French Code of Defence, Article L1111-1

French Civil Code, Articles 112 et seqs

French Civil Procedure Code, Articles 1062 et seqs.

Law 95-73 of 21 January 1995, as amended by Law No. 2002-1138 of 9 September 2002, Article 26
https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000369046/

Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN), 'Vigipirate'
https://www.sgdsn.gouv.fr/vigipirate

Sénat, Rapport d'information sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles, 2022 [French Senate Report]

Germany

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (Hamburg DPA), Consultation Prior to an Order Pursuant to Article 58(2)(g) GDPR
https://noyb.eu/sites/default/files/2021-01/545_2020_Anhörung_CVAI_ENG_Redacted.PDF

Greece

Hellenic DPA, Decision 35/2022
https://homodigitalis.gr/wp-content/uploads/2022/07/HellenicDPA_ClearviewDecision_13.7.2022_.pdf

Ireland

An Coimisún um Chosaint Sonraí (Data Protection Commission), 'Law Enforcement Directive' https://www.dataprotection.ie/en/organisations/resources-organisations/law-enforcement-directive

Italy

Il Garante (Italian DPA)
Opinion on the Sari Real Time System, 25 March 2021, No.9575877 (*Parere sul sistema Sari Real Time - 25 marzo 2021 [9575877]*)
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877

Facial Recognition: The SARI Real Time System is not Compliant with Privacy Laws', 16 April 2021
https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9575842#english_version

Injunction Order against Clearview AI' (*Ordinanza ingiunzione nei confronti di Clearview AI*), 10 February 2022 [9751362]
https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9751362

Luxembourg

Law of 5 July 2016 on the reorganization of the State Intelligence Services [Loi du 5 juillet 2016 portant reorganisation du Service de renseignement de l'État]

Netherlands

Autoriteit Persoonsgegevens (AP, Dutch DPA)
AP and RDI: Supervision of AI Systems Requires Cooperation and Must Be Arranged Quickly', 11 June 2024, https://www.autoriteitpersoonsgegevens.nl/en/current/ap-and-rdi-supervision-of-ai-systems-requires-cooperation-and-must-be-arranged-quickly

Voorlichting -Regels voor Gezichtsherkenning in Supermarkten' [*Explanations – rules concerning facial recognition technologies in supermarkets*] 1 May 2020
https://www.autoriteitpersoonsgegevens.nl/documenten/brief-regels-voor-gezichtsherkenning-in-supermarkten

Regels voor Gebruik Biometrie' [*Rules regarding the Use of Biometrics*]
https://autoriteitpersoonsgegevens.nl/themas/identificatie/biometrie/regels-voor-gebruik-biometrie#afweging-gebruik-biometrie-voor-authenticatie-of-beveiliging

Government of the Netherlands
Fundamental Rights and Algorithms Impact Assessment' (FRAIA)
https://www.government.nl/documents/reports/2021/07/31/impact-assessment-fundamental-rights-and-algorithms

Risk of an attack (threat level)' https://www.government.nl/topics/counterterrorism-and-national-security/risk-of-an-attack-threat-level

Sweden

Åklagarmyndigheten (Swedish Prosecution Authority), 'the role of a prosecutor'
https://www.aklagare.se/en/the-role-of-a-prosecutor/#:~:text=Swedish%20prosecutors%20have%20three%20main%20tasks%3A%20to%20lead,to%20bring%20prosecutions%2C%20and%20to%20appear%20in%20court

IMY decision (Swedish DPA), DI-20200-2719 [Concerning the use of the Clearview AI's platform]
https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-polismyndigheten-cvai.pdf

Krisinformation.se (Emergency information for Swedish Authorities), 'Terrorism and Deadly Force Attacks' https://www.krisinformation.se/en/hazards-and-risks/terrorism

United Kingdom

Information Commissioner's Office (ICO, UK DPA)

Information Commissioner's Opinion: The Use of Live Facial Recognition Technology by Law Enforcement in Public Spaces, 31 October 2019, ref. 2019/01
https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf

Biometric Recognition
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/biometric-recognition/

College of Policing
'Live Facial Recognition', first published on 22 March 2022 https://www.college.police.uk/app/live-facial-recognition/live-facial-recognition

London Policing Ethics Panel, 'Final Report on Live Facial Recognition', May 2019
http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/live_facial_recognition_final_report_may_2019.pdf

NGOs

AI Now Institute, 'Regulating Biometrics: Global Approaches and Urgent Questions', 1 September 2020

Ada Lovelace, 'Countermeasures: The Need for New Legislation to Govern Biometric Technologies in the UK', June 2022

AlgorithmWatch, Kayser-Bril N., 'At least 11 Police Forces Use Face Recognition in the EU, AlgorithmWatch Reveals', 18 June 2020, https://algorithmwatch.org/en/face-recognition-police-europe/

AlgorithmicWatch, 'Automating Society Report 2020' October 2020
https://automatingsociety.algorithmwatch.org/

AlgorithmicWatch, 'EU Parliament vote on AI Act; Member States will have to plug surveillance loopholes', 13 March 2024
https://algorithmwatch.org/en/eu-parliament-votes-on-ai-act/

Amber Alert EU, 'The EU's Groundbreaking Move: Using AI to Find Missing Persons', 19 March 2024
https://www.amberalert.eu/news/using-ai-to-find-missing-persons

Article19, 'EU:AI Act passed in Parliament Fails to Ban Harmful Biometric Technologies' https://www.article19.org/resources/eu-ai-act-passed-in-parliament-fails-to-ban-harmful-biometric-technologies/

Big Brother Watch Files Legal Complaint Against Facial Recognition 'Search Engine' PimEyes, 8 November 2022
https://bigbrotherwatch.org.uk/press-releases/pimeyes-press-release/

Big Brother's Submission to the UK ICO
https://bigbrotherwatch.org.uk/wp-content/uploads/2022/11/20220912-Big-Brother-Watch-Submission-re-PimEyes-AS-SENT.pdf

Bits of Freedom, 'De AI-verondening is er, maar wij zijn sceptisch' 9 December 2023 https://www.bitsoffreedom.nl/2023/12/09/de-ai-verordening-is-er-maar-wij-zijn-sceptisch/

Center for Democracy and Technology (CDT), Jake Laperruque, 'Limiting Face Recognition Surveillance: Progress and Paths Forward' 23 August 2022 https://cdt.org/insights/limiting-face-recognition-surveillance-progress-and-paths-forward/

Center for Democracy and Technology (CDT), 'Testimony of Jake Laperruque' in hearing entitled 'Advancing Innovation (AI): Harnessing Artificial Intelligence to Defend and Secure the Homeland', 22 May 2024 https://docs.house.gov/meetings/HM/HM00/20240522/117189/HHRG-118-HM00-Wstate-LaperruqueJ-20240522.pdf

ECNL, European Center for Not-for-Profit Law, 'Packed with Loopholes: Why the AI Act Fails to Protect Civic Space and the Rule of Law', 3 April 2024 https://ecnl.org/news/packed-loopholes-why-ai-act-fails-protect-civic-space-and-rule-law

EDRi, 'The Rise and Rise of Biometric Surveillance in the EU: A Legal Analysis of Biometric Mass Surveillance Practices in Germany, the Netherlands, and Poland', 7 July 2021 https://edri.org/wp-content/uploads/2021/11/EDRI_RISE_REPORT.pdf

EDRi, 'Remote Biometric Identification: A Technical and Legal Guide', 23 January 2023

EDRi, 'EU Act will fail commitment to ban biometric mass surveillance' 18 January 2024 https://reclaimyourface.eu/eu-ai-act-will-fail-commitment-to-ban-biometric-mass-surveillance/

Homo Digitalis, 'A big Success for Homo Digitalis: The Hellenic DPA fines Clearview AI with € 20 million', 13 July 2022 https://homodigitalis.gr/en/posts/12155/

Human Rights Watch, 'Greece: New Biometrics Policing Program Undermines Rights, Risks of Illegal Racial Profiling and Other Abuses.' 18 January 2022 https://www.hrw.org/news/2022/01/18/greece-new-biometrics-policing-program-undermines-rights

NOYB, 'Complaint under Article 77(1), 80(1) GDPR filed by XXX (complainant) against Clearview AI, Inc', Case No:C043, May 2021 https://noyb.eu/sites/default/files/2021-05/Clearview%20AI%20-%20EN%20DE%20-%20noyb%20-%20redacted.pdf

Privacy International, 'How Facial Recognition is Spreading in Italy: The Case of Como', 17 September 2020 https://privacyinternational.org/case-study/4166/how-facial-recognition-spreading-italy-case-como

The Ryder Review, 'Independent Legal Review of the Governance of Biometric Data in England and Wales', Ada Lovelace Institute, 29 June 2022 https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/The-Ryder-Review-Independent-legal-review-of-the-governance-of-biometric-data-in-England-and-Wales-Ada-Lovelace-Institute-June-2022.pdf

3. Academic writings

Article, Books, Books' chapters, and Reports

Adhikari B. et al., 'Towards a Real-Time Facial Analysis System' (2021) IEEE 23rd International Workshop on Multimedia Signal Processing

Álvarez Casado C. and Bordallo López M., 'Real-Time Face Alignment: Evaluation Methods, Training Strategies and Implementation Optimization,' (2021) 18 Journal of Real-Time Image Processing 2239

Bogensberger W., 'Article 83 TFEU' in M. Kellerbauer et al. (eds) *The EU Treaties and the Charter of Fundamental Rights* (OUP 2019)

Brewczyńska M., 'Article 1, Subject Matter and Objectives' in E. Kosta and F. Boehm (eds) *The EU Law Enforcement Directive (LED), A Commentary* (OUP 2024)

Brkan M., 'The Concept of Essence of EU Fundamental Rights in the EU Legal Order: Peeling the Onion to Its Core' (2018) 14(2) European Constitutional Law Review 332

Buolamwini J. and Gebru T., 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', (2018) Proceedings of Machine Learning Research 81, 1-15 http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

Chevallier-Govers C., 'Article 67 TFEU [Establishing the AFSJ]' in H.-J. Blanke and S. Mangiameli (eds) *Treaty on the Functioning of the European Union – A Commentary*, volume I: Preamble, Articles 1-89 (Springer 2021)

Christakis T. and Lodie A., 'The Conseil d'Etat Finds the Use of Facial Recognition by Law Enforcement Agencies to Support Criminal Investigations 'Strictly Necessary' and Proportional' (2022) 3(1) ERDAL 159

Christakis T. et al., Mapping the Use of Facial Recognition in Public Spaces in Europe', series of reports (2022)

Davies B. et al. 'An Evaluation of South Wales Police's Use of Automated Facial Recognition' (2018)

Edwards L., 'People, Risk and the Unique Requirements of AI: 18 Recommendations to Strengthen the EU AI Act', Policy Briefing, Ada Lovelace, 31 March 2022 https://www.adalovelaceinstitute.org/policy-briefing/eu-ai-act/

Eirener A.V., 'Imminent Dystopia ? Media Coverage of Algorithmic Surveillance at Berlin-Südkreuz', 30 May 2020, 9(1) Internet Policy Review https://policyreview.info/articles/analysis/imminent-dystopia-media-coverage-algorithmic-surveillance-berlin-sudkreuz

Galič M. and Stevens L., 'Regulating Police Use of Facial Recognition Technology in the Netherlands: The Complex Interplay between Criminal Procedural Law and Data Protection Law' (2023) 4(14) New Journal of European 459

Garvie C. et al., 'The Perpetual Line-Up: Unregulated Police Face Recognition in America' (2016) Georgetown Law, Center on Privacy and Technology https://www.perpetuallineup.org/

Galli F. 'Interoperable Law Enforcement: Cooperation Challenges in the Area of Freedom, Security, and Justice' 15 EUI Working Paper RSCAS 2019/15, Robert Schuman Centre for Advanced Studies (2019)

González Fuster G. and Naldona Peeters M.A. 'Person Identification, Human Rights and Ethical Principles: Rethinking Biometrics in the Era of Artificial Intelligence' EPRS study, PE 697.191, December 2021 https://www.europarl.europa.eu/RegData/etudes/STUD/2021/697191/EPRS_STU(2021)697191_EN.pdf

Hamsici O.C. and Martinez A.M., 'Face Recognition, Component-Based', in Li S.Z. and Jain A.K. (eds) *Encyclopedia of Biometrics* (1st ed. Springer Science, 2015)

Janssen H., 'An Approach for a Fundamental Rights Impact Assessment to Automated Decision-Making' (2020) 10(1) International Data Privacy Law 76

Jasserand C., 'Experiments with Facial Recognition Technologies in Public Spaces: in Search of an EU Governance Framework' in A. Zwitter and O.Gstrein (eds) *Handbook on the Politics and Governance of Big Data and Artificial Intelligence* (EE 2023)

Jasserand C. 'Biometric Data, Within and Beyond Data Protection' in B. van der Sloot and S. van Schendel (eds) *The Boundaries of Data* (AUP 2024)

Jasserand C., 'Article 10, Processing of Special Categories of Personal Data' in E. Kosta and F. Boehm (eds) *The EU Law Enforcement Directive (LED), A Commentary* (OUP 2024)

Kemelmacher-Shlizerman I. et al. 'The MegaFace Benchmark: 1 Million Faces for Recognition at Scale' (2016) CVPR 4873
https://openaccess.thecvf.com/content_cvpr_2016/papers/Kemelmacher-Shlizerman_The_MegaFace_Benchmark_CVPR_2016_paper.pdf

Kindt E., Privacy and Data Protection Issues of Biometric Applications: A Comparative Analysis (Springer 2013)

Korff D., 'Opinion on the Implications of the Exclusion from New Binding European Instruments on the Use of AI in Military, National Security and Transnational Law Enforcement Contexts' European Center for Not-for-Profit Law, October 2022

Korff D., 'Police Real-Time Remote Biometric ID in the AI Act' (1 February 2024) https://www.ianbrown.tech/2024/02/01/police-real-time-remote-biometric-id-in-the-ai-act/

Leslie D., 'Understanding bias in facial recognition technologies, An explainer' The Alan Turing Institute, 6 October 2020
https://www.turing.ac.uk/sites/default/files/2020-10/understanding_bias_in_facial_recognition_technology.pdf

Lynch J., 'Face Off: Law Enforcement Use of Face Recognition Technology' EFF, 5 May 2019
https://www.eff.org/files/2019/05/28/face-off-report.pdf

Quintel T. and Mitsilegas V.,'Article 6, Distinction between Different Categories of Data Subject' in E. Kosta and F. Boehm (eds) *The EU Law Enforcement Directive (LED), A Commentary* (OUP 2024)

Ragazzi F. et al., 'Biometric and Behavioural Mass Surveillance in EU Member States', Report for the Greens/EFA in the European Parliament, 25 October 2021
https://extranet.greens-efa.eu/public/media/file/1/7297

Ross A. and Jain A.K., 'Biometrics, Overview' in Li S.Z. and Jain A.K. (eds) *Encyclopedia of Biometrics*, (1st ed. Springer Science, 2015)

Sobel B., 'A New Common Law of Web-Scraping' (2021) 25(1) Lewis and Clark Review 147

Tosoni L. and Bygrave L., 'Article 3, Definitions' in E. Kosta and F. Boehm (eds) *The EU Law Enforcement Directive (LED), A Commentary* (OUP 2024)

Tridimas T., 'The Principle of Proportionality' in Schütze R. and Tridimas T. (eds) *Oxford Principles of European Union Law*, vol I (OUP 2018)

Tridimas T. and Gentile G., 'The Essence of Rights: An Unreliable Boundary?' (2019) 20 German Law Journal 794

Turner N. and Chin-Rothman C., 'Police Surveillance and Facial Recognition: Why Data Privacy is Imperative for Communities of Color', 12 April 2022
https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/

Van der Sloot B. and Lanzing M., 'The Continued Transformation of the Public Sphere: On the Road to Smart Cities, Living Labs and a New Understanding of Society' in M. Nagenborg et al. (eds) *Technology and the City: Towards a Philosophy of Urban Technologies* (Springer 2021)

Veale M. and Zuiderveen Borgesuis F., 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 22(4) Computer Law Review International 97

Wang F. et al., 'The Devil of Face Recognition is in the Noise' in Ferrari V. et al (eds) *ECCV 2018* (Springer Nature Switzerland AG 2018)

Wendehorst C. and Duller Y., 'Biometric Recognition and Behavioural Detection: Assessing the Ethical Aspects of Biometric Recognition and Behavioural Detection Techniques with a Focus on their Current and Future Use in Public Spaces', Study requested by JURI and PETI Committees, European Parliament, 6 August 2021
https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf

Wever R., 'Unmasking Biometrics' Biases: Facing Gender, Race, Class and Ability in Biometric Data Collection' (2018) 21(2) Tijdschrift voor Mediageschiedenis 89.

Woodward J., 'Super Bowl Surveillance: Facing Up to Biometrics', RAND study, 27 June 2001
https://www.rand.org/pubs/issue_papers/IP209.html

Blogposts

Arnold L., 'How the European Union's AI Act Provides Insufficient Protection Against Police Discrimination' (2024) Journal of Law and Social Change, 14 May 2024
https://www.law.upenn.edu/live/news/16742-how-the-european-unions-ai-act-provides

Belkadi L., 'Clearview AI: the ICO's Jurisdiction under Judicial Scrutiny' CiTiP blogpost, 16 January 2024
https://www.law.kuleuven.be/citip/blog/clearviewai-the-icos-jurisdiction-under-judicial-scrutiny/

Gikay A.A., 'Should the EU Ban the Real-Time of Remote Biometric Identification Systems for Law Enforcement Purposes?' 28 October 2022, EU Law Analysis
http://eulawanalysis.blogspot.com/2022/10/should-eu-ban-real-time-use-of-remote.html

Jasserand C., 'Yellow Card to a French Football Club: No Facial Recognition System to Monitor their Supporters', CiTiP Blogpost, 30 March 2021
https://www.law.kuleuven.be/citip/blog/yellow-card-to-a-french-football-club/

Jasserand C., 'Clearview AI: Illegally Collecting and Selling Our Faces in Total Impunity, Parts I and II, Blogpost, CiTiP, 28 April 2022 and 5 May 2022
https://www.law.kuleuven.be/citip/blog/clearview-ai-illegally-collecting-and-selling-our-faces-in-total-impunity-part-i/

4. Newspaper Articles

ABC News, 'Biometrics Used to Detect Criminals at Super Bowl' 13 February 2001
https://abcnews.go.com/Technology/story?id=98871

Abdul G., 'Police to Use Live Facial Recognition in Cardiff during Beyoncé Concert' 17 May 2023
https://www.theguardian.com/technology/2023/may/17/police-to-use-facial-recognition-technology-in-cardiff-during-beyonce-concert

Attrino A.G., 'He Spent 10 Days in Jail after Facial Recognition Software Led to the Arrest of the Wrong Man, Lawsuit Says' 28 Dec. 2020, updated on 29 Dec. 2020,

https://www.nj.com/middlesex/2020/12/he-spent-10-days-in-jail-after-facial-recognition-software-led-to-the-arrest-of-the-wrong-man-lawsuit-says.html

Bertuzzi L. 'AI Act: MEPs Mull Narrow Facial Technology Uses in Exchange of Other Bans', Euractiv, 6 November 2023
https://www.euractiv.com/section/artificial-intelligence/news/ai-act-meps-mull-narrow-facial-recognition-technology-uses-in-exchange-for-other-bans/

Bogle, A. 'Australian Federal Police Tested Controversial Facial Recognition Search Engine, FOI documents reveal' The Guardian, 23 October 2023
https://www.theguardian.com/australia-news/2023/oct/24/australian-federal-police-afp-pimeyes-facial-recognition-facecheck-id-search-engine-platform

Borak M., 'Police in Germany Using Live Facial Recognition' BiometricUpdate, 8 May 2024
https://www.biometricupdate.com/202405/police-in-germany-using-live-facial-recognition

Bhuiyan J., 'TechScape: 'Are you kidding, carjacking?' The problem with Facial Recognition in Policing' The Guardian, 15 August 2023
https://www.theguardian.com/newsletters/2023/aug/15/techscape-facial-recognition-software-detroit-porcha-woodruff-black-people-ai

Butler S., 'Shoplifting Crackdown to Include £ 55M for Facial Recognition Tools in England and Wales' The Guardian, 10 April 2024
https://www.theguardian.com/business/2024/apr/10/shoplifting-crackdown-to-include-55m-for-facial-recognition-tools-in-england-and-wales

CBS Detroit, 'Protesters Demand to Discontinue Facial Recognition Technology', 15 June 2020
https://www.cbsnews.com/detroit/news/protesters-demand-to-discontinue-facial-recognition-technology/

Cecco L., 'Canadian University Vending Machine Error Reveals Use of Facial Recognition' The Guardian, 23 February 2024
https://www.theguardian.com/world/2024/feb/23/vending-machine-facial-recognition-canada-univeristy-waterloo

Clayton J., 'I was misidentified as shoplifter by facial recognition tech' BBC, 26 May 2024
https://www.bbc.com/news/technology-69055945

Croft J., 'Leisure Centres Scrap Biometric Systems to Keep Tabs on Staff Amid UK Watchdog Clampdown' The Guardian, 16 April 2024
https://www.theguardian.com/business/2024/apr/16/leisure-centres-scrap-biometric-systems-to-keep-tabs-on-staff-amid-uk-data-watchdog-clampdown

Destal M. et al., 'La Police Nationale Utilise Illégalement un Logiciel Israélien de Reconnaissance Faciale' Disclose, 14 November 2023
https://disclose.ngo/fr/article/la-police-nationale-utilise-illegalement-un-logiciel-israelien-de-reconnaissance-faciale

Euractiv, 'Sweden Wants to Let Police Use Facial Recognition Technology' 3 June 2024
https://www.euractiv.com/section/law-enforcement/news/sweden-wants-to-let-police-use-facial-recognition-technology/

Fassler E., 'South Korea is Giving Millions of Photos to Facial Recognition Researchers', MotherBoard, Tech by Vice, 16 November 2021
https://www.vice.com/en/article/xgdxqd/south-korea-is-selling-millions-of-photos-to-facial-recognition-researchers

Ferguson D., ‘Police Using Live Facial Recognition at British Grand Prix’ 8 July 2023 https://www.theguardian.com/technology/2023/jul/08/police-live-facial-recognition-british-grand-prix

Journal Record Staff, ‘Casino Uses Facial Recognition Technology to Supplement Security’ Journal Record, 25 October 2022
https://journalrecord.com/2022/10/casino-uses-facial-recognition-technology-to-supplement-security/

Hao K., ‘After Feeding Explosion of Facial Recognition, China Moves to Rein it’ Wall Street Journal, 8 August 2023
https://www.wsj.com/articles/china-drafts-rules-for-facial-recognition-use-4953506e

Hill K., ‘The Secretive Company that Might End Privacy as We Know It’, New York Times, 18 January 2020
https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

Hill K., ‘Wrongfully Accused by an Algorithm’, the New York Times, 24 June 2020/updated 3 August 2020
https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

Hill K. and Kilgannon C., ‘Madison Square Garden Uses Facial Recognition to Ban Its Owner’s Enemies,’ the New York Times, 22 December 2022, updated on 3 January 2023
https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html

Hill K., ‘Face Search Engine PimEyes Blocks Searches of Children’s Faces’, the New York Times, 23 October 2023
https://www.nytimes.com/2023/10/23/technology/pimeyes-blocks-searches-childrens-faces.html

Macdonald A., ‘Spanish Data Authority Opposes Facial Recognition for Football Stadium’, BiometricUpdate, 22 January 2024
https://www.biometricupdate.com/202401/spanish-data-authority-opposes-facial-recognition-for-football-stadium-access

Malgieri G. and Santos C., ‘Assessing the (Severity of) Impacts on Fundamental Rights’, work-in-progress paper, SSRN, 28 June 2024
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4875937

Masri L., ‘Facial Recognition is Helping Putting Curb Dissent with the Aid of U.S. Tech’ Reuters, 28 March 2023
https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/

Mustać, T. ‘The AI Act Series: Fundamental Rights Impact Assessments’, Medium, 9 August 2024
https://ai.gopubby.com/the-ai-act-series-fundamental-rights-impact-assessments-b1de3855f8cc

Singh M., ‘How Singapore Uses Facial Recognition’ CDT Europe, 29 January 2024
https://cdt.org/insights/limiting-face-recognition-surveillance-progress-and-paths-forward/

Ulmer A. and Siddiqui Z., ‘India’s Use of Facial Recognition Tech During Protests Causes Stir’ Reuters, 17 February 2020
https://www.reuters.com/article/us-india-citizenship-protests-technology/indias-use-of-facial-recognition-tech-during-protests-causes-stir-idUSKBN20B0ZQ/

Vincent J., ‘NYPD Used Facial Recognition to Track Down Black Lives Matter activist’ The Verge, 18 August 2020
https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram

5. Miscellaneous

116000 Enfants Disparus, ‘Agir en cas de disparition, disparition inquiétante’ (*acting in case of disappearance, worrying disappearance*)
https://www.116000enfantsdisparus.fr/agir-en-cas-de-disparition/disparition-inquietante/

ALIGNER (Artificial Intelligence Roadmap for Policing and Law Enforcement), Horizon 2020 project, ‘Fundamental Rights Impact Assessment’
https://aligner-h2020.eu/fundamental-rights-impact-assessment-fria/

Amber Alert, Annual Report, 2020
https://www.amberalert.eu/wp-content/uploads/2022/04/2020.pdf

Astute Analytica, ‘Facial Recognition Market – Industry Dynamics. Market Size and Opportunity Forecast to 2032’
https://www.astuteanalytica.com/industry-report/facial-recognition-market

Human-Centered Artificial Intelligence, Stanford, ‘Artificial Intelligence Index Report 2023’ https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report_2023.pdf

Imperva, ‘Web Scraping’
https://www.imperva.com/learn/application-security/web-scraping-attack/#:~:text=Web%20scraping%20is%20the%20process,replicate%20entire%20website%20content%20elsewhere

ISO/IEC Standard 2382-37:2022 Information Technology - Vocabulary

National Academies of Sciences, Engineering, and Medicine (USA), *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance* (2024)

PimEyes, ‘Image Search with PimEyes, How to Reverse Image Search’ Blog https://pimeyes.com/en/blog/image-search-with-pimeyes-how-to-reverse-image-search

TELEFI (Towards the European Level Exchange of Facial Images), EU’s ISFP project, ‘Summary Report’, version 1.0, January 2021
https://www.telefi-project.eu/sites/default/files/TELEFI_SummaryReport.pdf

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 documentation 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.

Publications Office
of the European Union