Technology and Regulation

The use of facial recognition technologies by law enforcement authorities in the US and the EU: towards a convergence on regulation?

Author(s)	Xavier Tracol
Contact	xavier.tracol@eurojust.europa.eu
Affiliation(s)	Dr. Xavier Tracol is Senior Legal Officer at EUROJUST. The views expressed herein are those of the author in his personal capacity and do not necessarily reflect those of EUROJUST or the European Union in general.

Keywords	facial recognition, US, EU, moratorium, prohibition/ban, regulation
Citation	Xavier Tracol, The use of facial recognition technologies by law enforcement authorities in the us and the EU: towards a convergence on regulation?, Technology and Regulation, 2025, 289-315 • 10.71265/nga7v921 • ISSN: 2666-139X

Abstract

Law enforcement authorities have been using facial recognition technologies for many years in both the US and the EU. Some US legislators adopted bans and/or moratoriums whilst other US legislators adopted nuanced regulations about such use. The EU legislature considered adopting a ban of the use of live or real-time facial recognition technologies by law enforcement authorities in publicly accessible spaces. The EU legislature however ended up adopting a partial ban which provides for many broad exceptions. In this context, the US and the EU share a common interest in sharing experience about regulating the use of facial recognition technologies by law enforcement authorities.

1. Introduction

Facial recognition is defined as a probabilistic technology which can automatically recognise data subjects based on their face "*to authenticate or identify them*."[1] This technology uses algorithms to extract and analyse certain facial features from images or video to match and verify identities.[2] Facial recognition technology thus processes biometric data of data subjects to authenticate or identify them.

1. Guidelines of the European Data Protection Board 05/2022 on the use of facial recognition technology in the area of law enforcement dated 12 May 2022, available at https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf, p. 7, para. 6.
2. Europol Innovation Lab, Observatory Report on the Benefits and Challenges of Artificial Intelligence for Law Enforcement, 2024, available at AI-and-policing.pdf (europa.eu), p. 24.

Facial recognition technologies are not fully accurate. Regarding their key risks, Recital 32 of the AI Regulation[3] explicitly recognises that their "[t]*echnical inaccuracies* [...] *can lead to biased results and entail discriminatory effects. Such possible biased results and discriminatory effects are particularly relevant with regard to age, ethnicity, race, sex or disabilities*." The use of facial recognition technologies thus presents a risk of bias and false positives or false negatives. In the area of law enforcement, this situation has serious consequences for data subjects who are falsely identified as suspects.[4]

Conversely, the benefits of using facial recognition technologies in law enforcement lack clear quantifiable evidence.[5] Facial recognition includes two different types of technologies, *i.e.*:

(1) Retrospective or post-remote facial recognition: this type of technology assists law enforcement authorities in comparing still images of unknown data subjects against a reference police database. For instance, such data subjects may be a suspect of a crime or a mugshot of a person arrested who are caught on footage of CCTV cameras, photos from social media or those on a victim's phone. The database may include mugshots, custody images or images collected during criminal proceedings. Retrospective or post-remote facial recognition focuses on a single data subject in pre-recorded imagery.[6] Recital 17 of the AI Regulation specifies that "*the comparison and identification occur only after a* ***significant delay"*** (emphasis added). Retrospective or post-remote facial recognition implies the capacity to look back at events such as a protest or meetings several years before its date whilst the data subject has, for instance, become a political opponent in the meantime.[7]

(2) Live or real-time facial recognition: this type of technology performs a real-time reading of all data subjects passing a camera regardless of their capacity and compares them against a pre-determined closed watch-list of persons of interest.[8] Live or real-time facial recognition is often connected to cameras in public spaces. Article 3(42) of the AI Regulation provides that "*the capturing of the biometric data, the comparison and the identification occur all* [...] ***without a significant delay***" (emphasis added; see also Recital 17 of the AI Regulation). This notion is however not defined in the AI Regulation and needs to be assessed on a case by case basis.[9] Criticism about the use of facial recognition technologies has mostly focused on these systems as involving a constant and generalised identity check.[10]

3. Artificial Intelligence Regulation (AI 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), OJ 2024 L 1689/1.
4. See US Government Accountability Office, "Biometric Identification Technologies: Considerations to Address Information Gaps and Other Stakeholder Concerns", GAO-24-106293, 22 April 2024, available at https://www.gao.gov/products/gao-24-106293
5. US Commission on Civil Rights, Annual Statutory Enforcement Report on the Civil Rights Implications of the Federal Use of Facial Recognition Technology, 19 September 2024, available at https://www.usccr.gov/files/2024-09/civil-rights-implications-of-frt_0.pdf, p. 47.
6. Europol Innovation Lab, Observatory Report on the Benefits and Challenges of Artificial Intelligence for Law Enforcement, 2024, available at AI-and-policing.pdf (europa.eu), p. 24.
7. See Daragh Murray, "Police Use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Law Framework", *Modern Law Review*, 11 December 2023, available at https://doi.org/10.1111/1468-2230.12862 For instance, the police used this technology to identify the applicant in the case of *Glukhin v. Russia*. See judgment of the ECHR, application no. 11519/20, 4 July 2023.
8. Europol Innovation Lab (n 6) 24.
9. Annex to the Communication to the Commission Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final, 4 February 2025, available at https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act, p. 100, para. 310.
10. See Asress Adimi Gikay, "Regulating Use by Law Enforcement Authorities of Live Facial Recognition Technology in Public Spaces: an Incremental Approach", *The Cambridge Law Journal*, Volume 82, Issue 3, November 2023, pp. 414 – 449, available at DOI: https://doi.org/10.1017/S0008197323000454. For instance, the police used this technology to identify the real-time location of the applicant in Moscow in the case of *Glukhin v. Russia*: see judgment of the ECHR, application no. 11519/20, 4 July 2023. In the UK, the South Wales Police Force also used an automated facial recognition technology in a pilot project which led to the judgment of the British Court of Appeal dated 11 August 2020 in the case of Edward Bridges (Case No: C1/2019/2670); [2020] EWCA Civ 1058.

The use of facial recognition technologies by law enforcement authorities in public spaces interferes with fundamental rights such as the right to the respect for private life, the protection of personal data, freedom of movement, freedom of assembly, human dignity and non-discrimination.[11] The permanent processing of everyone's biometric data implies a risk of mass surveillance.

Since Europe has not adopted any specific regulation about the use of facial recognition technologies by law enforcement authorities before 2024, applicants filed actions legally based *inter alia* on Article 8 of the European Convention about the fundamental right to the respect of private life before European Courts. On 11 August 2020, the UK Court of Appeal rendered the first judicial decision on the matter. By a unanimous landmark judgment of 59 pages, the Court found *inter alia* that the use of the Automated Facial Recognition (AFR) Locate technology by the South Wales Police Force was proportionate under Article 8(2) of the European Convention. The Court however found that there was no clear guidance on where AFR Locate could be used and who could be put on a watch-list. The Court therefore held that this was too broad a discretion to afford to the police officers to meet the standard required by Article 8(2) of the European Convention.[12] The South Wales Police did not appeal against the decision,[13] thus making it a final judgment. The South Wales Police Force however continues using facial recognition technology.[14] On 4 July 2023, the ECHR rendered the first decision on facial recognition technology by a European Court. By a unanimous landmark judgment in the case of *Glukin v. Russia* on the compatibility of the use of facial recognition technology by government with fundamental rights, the ECHR found *inter alia* a violation of Article 8 of the European Convention on the right to respect for private life.[15] The Court specifically found that the use of facial recognition technology by the law enforcement authorities in the Moscow underground to identify and later locate and arrest Glukhin had interfered with his right to respect for his private life. The Russian law enforcement authorities however continue using facial recognition technology in the Moscow underground despite this judgment.[16] These two judicial decisions which are generally aligned have therefore not been applied in practice. This situation shows the weakness of both a domestic and a European Court to ensure compliance with applicable law on the use of facial recognition technology by law enforcement authorities.

In the US, the Federal Trade Commission has taken significant actions about the use of facial recognition technology, particularly about its application in the commercial sector and in cases where it poses risks to consumer privacy and civil liberties.[17] The Commission has also taken enforcement actions against private companies making deceptive claims about their facial recognition software. For instance, the Commission prohibited IntelliVision Technologies Corp. from making false claims that its facial recognition software was free of gender and racial bias.[18]

The use of facial recognition technology by federal law enforcement agencies however falls under the purview of other governmental bodies. The Government Accountability Office has examined this issue, noting that agencies such as the Department of Homeland Security and the Department of Justice have both used facial recognition technologies for criminal investigations. The Government Accountability Office however reported that these agencies had not fully implemented recommended safeguards to protect civil rights and liberties as of September 2023.[19] In addition, the US Commission on Civil Rights has highlighted concerns

11. See Agnė Limantė, "Bias in Facial Recognition Technologies Used by Law Enforcement: Understanding the Causes and Searching for a Way Out", *Nordic Journal of Human Rights*, 17 November 2023, p. 1 to 3.
12. Case No: C1/2019/2670); [2020] EWCA Civ 1058.
13. See Response to the Court of Appeal judgment on the use of facial recognition technology, 11 August 2020, available at https://www.south-wales.police.uk/news/south-wales/news/2020/response-to-the-court-of-appeal-judgment-on-the-use-of-facial-recognition-technology/
14. See Facial Recognition Technology | South Wales Police
15. *Glukhin v. Russia*, Application no. 11519/20.
16. See Masha Borak, "Researchers spotlight Russia's opaque facial recognition surveillance system", *Biometric update.com*, 21 June 2024, available at https://www.biometricupdate.com/202406/researchers-spotlight-russias-opaque-facial-recognition-surveillance-system
17. See Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards, 19 December 2023, available at https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without
18. See in the matter of Intellivision, 13 January 2025, available at https://www.ftc.gov/legal-library/browse/cases-proceedings/232-3023-intellivision-matter
19. See Facial Recognition Technology: Federal Law Enforcement Agency Efforts Related to Civil Rights and Training, 7 March 2024, available at https://www.gao.gov/products/gao-24-107372?utm_source=chatgpt.com

about the federal use of facial recognition technologies, pointing out the absence of explicit laws regulating its use and the potential civil rights implications. Regarding transparency, the Commission specifically found that no comprehensive data is available about the accuracy of the facial recognition technology which "*is used by law enforcement*."[20] In its report, the Commission called for additional oversight and clear guidelines to prevent misuse.

Law enforcement authorities have thus been widely using facial recognition technologies for many years in both the EU and the US (2). This situation led US legislators to adopt bans and/or moratoriums about the use by law enforcement authorities of facial recognition technologies. The EU considered prohibiting the use of live or real-time facial recognition technologies by law enforcement authorities in publicly accessible spaces (3). The EU legislature however reached a compromise which partly bans it in principle whilst providing for many broad exceptions. US legislators also adopted nuanced regulations about the use of facial recognition technologies by law enforcement authorities (4).

2. Law enforcement authorities have been widely using facial recognition technologies for many years in both the EU and the US

At federal level in the **US**, the FBI has been using facial recognition technologies since at least 2018.[21] In a study about the use of facial recognition technologies by the federal government commissioned by Congress and published in August 2021, the US Government Accountability Office found that six law enforcement agencies used facial recognition technologies for law enforcement purposes and five for security purposes including live monitoring of locations. They reported that this technology assisted in identifying suspects of lawbreaking during civil unrest. The Government Accountability Office made very critical findings about this use.[22]

In addition, law enforcement authorities use facial recognition technologies in many States such as New Jersey,[23] Massachusetts,[24] Virginia,[25] Kentucky,[26] Michigan,[27] Idaho[28] and New York State.[29] Last, law enforcement authorities use facial recognition technologies in many US cities. For instance, the New York City Council enacted an ordinance on biometric privacy which went into effect on 9 July 2021. "[G]*overnment agencies, employees or agents*"[30] are however excluded from the scope of this law which does accordingly not apply to the police. New York City police reportedly used facial recognition technologies from 15,000 cameras 22,000 times to identify individuals in 4 years from 2017 to 2021.[31]

20. US Commission on Civil Rights, Annual Statutory Enforcement Report on the Civil Rights Implications of the Federal Use of Facial Recognition Technology, 19 September 2024, available at https://www.usccr.gov/files/2024-09/civil-rights-implications-of-frt_0.pdf, p. 102, para. V.a.
21. See Facial Recognition Technology: Ensuring Transparency in Government Use
22. See gao.gov
23. See https://mediacentral.princeton.edu/media/Facial+Recognition+Technology+in+the+State+of+New+JerseyA+Promoting+Resident+Privacy+through+Transparency+and+Regulation+Within+Law+Enforcement%2C+Grace+Zhuang%2C+UG+%2723+%283963609%29/1_r3ivpzey/254706753
24. See https://data.aclum.org/public-records/frt-ma/
25. Local and campus law enforcement can use facial recognition technology without a warrant if police have "reasonable suspicion" that an individual committed a crime. See https://www.dataguidance.com/news/virginia-bill-use-facial-recognition-technology-signed, § 15.2-1723.2. (Effective July 1, 2026) Facial recognition technology; approval and Document PDF · 529 ko
26. See Kentucky Bill Would Limit ALPR Data Retention, Help Block National License Plate Tracking Program
27. See Facial_Recognition_FAQ and eu.lansingstatejournal.com
28. See Document PDF · 89 ko
29. See nysba.org
30. See codelibrary.amlegal.com
31. Amnesty International, "Surveillance city: NYPD can use more than 15,000 cameras to track people using facial recognition in Manhattan, Bronx and Brooklyn", 3 June 2021, available at https://www.amnesty.org/en/latest/news/2021/06/scale-new-york-police-facial-recognition-revealed/

In the **EU**, law enforcement authorities of 16 Member States already use facial recognition technologies in their criminal investigations for *ex post* identification. Footage is checked after an incident and not in real-time in Austria, Finland, France,[32] Germany, Greece, Hungary, Italy, Latvia, Lithuania, Slovenia, Denmark, the Netherlands, Sweden,[33] Croatia, Cyprus and Czechia. Four additional Member States are expected to follow suit, *i.e.* Estonia, Portugal, Romania and Spain.[34]

For instance, the Dutch law enforcement authorities introduced a facial recognition database and software called CATCH in 2016. It allows the police to compare images taken by surveillance cameras to attempt at identifying suspects.[35]

The Austrian police has been using a facial recognition software in surveillance cameras since the end of 2019. The software compares surveillance footage with photos of suspects which are already stored in the database of the law enforcement authorities. The software does however not identify faces in real-time. Out of 581 times that the Austrian law enforcement authorities have used this software, 83 suspects have been identified.[36]

2.1 High number of face photos held in databases

In the **EU**, law enforcement agencies of Member States hold a high number of face photos in databases for facial recognition. For instance, Hungary holds 30 million photos, Italy 17 million, France 8 million[37] and Germany 5.5 million. These images can include mere suspects, persons convicted of crimes,[38] asylum seekers and "*unidentified dead bodies*". They come from multiple sources in each Member State.[39]

The law enforcement authorities are supposed to remove the photos of data subjects who are no longer considered suspects in a case or that courts have found innocent. In July 2021, the Dutch law enforcement authorities deleted 218,000 photos that they wrongly included in the facial recognition database. The database still had more than 2.65 million photographs on it at the end of 2021.[40]

32. The police and gendarmerie have both been using it since 2012. See Assemblée Nationale, Rapport d'information déposé en application de l'article 145 du Règlement par la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, en conclusion des travaux d'une mission d'information sur les fichiers mis à la disposition des forces de sécurité, 17 October 2018, available at https://www.assemblee-nationale.fr/dyn/15/rapports/cion_lois/l15b1335_rapport-information#P739_166902, section III.B; Traitement des Antécédents Judiciaires (TAJ) database in France, created by Décret no. 2012-652 du 4 mai 2012 relatif au Traitement des Antécédents Judiciaires (Decree 2012-652). The TAJ includes a facial recognition tool which enables law enforcement authorities to identify a data subject *a posteriori* by comparing an image that they hold – for instance from a CCTV camera - with images included in the database. Article R40-26 of the Code of Criminal Procedure requires photographs with technical features which allow the performance of facial recognition.

33. See European Data Protection Board, "Swedish DPA: Police unlawfully used facial recognition app", 12 February 2021, available at https://www.edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en; Joanna Mazur and Zuzanna Choińska, "European Union data protection law and the use of facial recognition technology for the purpose of fighting crime", Julia Kapelańska-Pręgowska and Michał Balcerzak (eds), *European Union data protection law and the use of facial recognition technology for the purpose of fighting crime*, Edward Elgar Publishing Limited, Cheltenham, 2024, p. 130, 132 and 137 to 144.

34. See "Biometric Behavioural Mass Surveillance in EU Member States", Report for the Greens/EFA in the European Parliament, October 2021, available at https://extranet.greens-efa.eu/public/media/file/1/7297

35. See "Dutch police likely used controversial facial recognition software despite minister's denial: Report", 26 August 2021, *nl#times*, available at Dutch police likely used controversial facial recognition software despite minister's denial: Report | NL Times; Letter of the Dutch minister of justice to the Dutch supervisory authority dated 13 June 2024, reference 5537977, available at https://open.overheid.nl/documenten/dpc-10268f0f085dccaef97bbd1e5b4451cec117a098/pdf

36. See "Austrian facial recognition database collects over 600,000 entries in a year", *Statewatch*, 8 September 2021, available at Statewatch | Austrian facial recognition database collects over 600,000 entries in a year

37. Rapport d'information déposé en application de l'article 145 du Règlement par la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, en conclusion des travaux d'une mission d'information sur les fichiers mis à la disposition des forces de sécurité, 17 octobre 2018, available at https://www.assemblee-nationale.fr/dyn/15/rapports/cion_lois/l15b1335_rapport-information.pdf, p. 64, footnote 2. See also Avis fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur le projet de loi (n° 3360) de finances pour 2021, Tome VII, Sécurités, par M. Stéphane Mazars, Député, 13 October 2020, available at https://www.assemblee-nationale.fr/dyn/opendata/AVISANR5L15B3404-tVII.html#%3Cem%3ETOC256000028, section III.

38. Rapport d'information (n 37) 12.

39. See "Europe Is Building a Huge International Facial Recognition System", *Wired*, 6 April 2022, available at Europe Is Building a Huge International Facial Recognition System | WIRED

40. See "Dutch police likely used controversial facial recognition software despite minister's denial: Report", 26 August 2021, *nl#times*, available at Dutch police likely used controversial facial recognition software despite minister's denial: Report | NL Times

The situation is similar in the **US** where law enforcement and government agencies have access to over 641 million photos for facial recognition purposes.[41] This number represents almost twice the total population of the US, *i.e.* 333.3 million of Americans. The FBI has access to all these photos through its facial recognition database.[42]

2.2 Lack of openness and transparency about the use of facial recognition technologies by law enforcement authorities

Law enforcement authorities of the **EU** are not always open or fully transparent about the use of facial recognition. Regarding "pilot projects",[43] the airport of Zaventem in Brussels deployed four cameras of automated facial recognition systems in 2017. The Belgian supervisory authority has however not been notified about this use of facial recognition technologies.[44]

In France, a 87 page report dated February 2024 was published online on 28 October 2024 found that the French *gendarmerie* unlawfully used the post-remote facial recognition software of the Israeli company Briefcam in an investigation for damages to public buildings perpetrated in Fosses in the context of riots in the summer of 2023. The investigators uploaded in the Briefcam software the pictures from a database of two persons suspected to have participated in such riots to identify the perpetrators of the damages.[45] The law enforcement authorities have not requested any member of the judiciary to authorise this use as provided for in the applicable French law. Such use has not been mentioned in the case file either. Although the software identified the two persons, the investigation subsequently showed that they had not participated in perpetrating the relevant offences. On 5 December 2024, the French supervisory authority published its own report. It did not find any use of real-time facial recognition in public space. The supervisory authority has however similarly found an unlawful use of post-remote facial recognition in a judicial investigation during riots in the summer of 2023. It therefore gave notice to the Home Secretary to either remove or de-activate this functionality by default from the software.[46] On 30 November 2023, members of the European Parliament published an open letter on the matter.[47] Last, the Administrative Tribunal of Grenoble quashed the decision of the mayor of Moirans to implement the Briefcam software on the territory of the city by decision No. 2105328 of 24 January 2025.[48]

41. See Electronic Frontier Foundation, available at Who Has Your Face?
42. See "The FBI Has Access to Over 640 Million Photos of Us Through Its Facial Recognition Database", American Civil Liberties Union, 7 June 2019, available at The FBI Has Access to Over 640 Million Photos of Us Through Its Facial Recognition Database | ACLU
43. In the UK, a pilot project took the shape of an automated facial recognition technology used by the South Wales Police Force which led to the judgment of the British Court of Appeal dated 11 August 2020 in the case of Edward Bridges. See Case No: C1/2019/2670: [2020] EWCA Civ 1058.
44. See Gabriela Galindo, "'No legal basis' for facial recognition cameras at Brussels Airport", *The Brussels Time*, 10 July 2019, available at 'No legal basis' for facial recognition cameras at Brussels Airport (brusselstimes.com); Bert Peeters, "Facial recognition at Brussels Airport: face down in the mud", 17 March 2020, available at https://www.law.kuleuven.be/citip/blog/facial-recognition-at-brussels-airport-face-down-in-the-mud/
45. Usage de logiciels d'analyse vidéo par les services de la police et la gendarmerie nationales, February 2024, available at https://www.interieur.gouv.fr/content/download/137154/1085003/file/23114R%20-%20Breifcam.pdf, p. 36.
46. See Decision MED-2024-150 of 15 November 2024, available at Décision MED-2024-150 du 15 novembre 2024 - Légifrance; see also « La police nationale utilise illégalement un logiciel israélien de reconnaissance faciale », *Disclose*, 14 November 2023, available at La police nationale utilise illégalement un logiciel israélien de reconnaissance faciale (disclose.ngo)
47. Available at Lettre ouverte de parlementaires européens à la France sur la reconnaissance faciale - DocumentCloud
48. Available at La mise en œuvre par la commune de Moirans du logiciel « Briefcam » censurée par le tribunal - Tribunal administratif de Grenoble

The situation is again similar in the **US** where experts urged Congress to increase transparency about the use of facial recognition technologies by law enforcement authorities.[49] Lawmakers have made the same point at local level.[50]

The use of facial recognition technologies by law enforcement authorities however implies experimentation at the expense of fundamental rights of data subjects including the respect of private life and the protection of personal data. This situation led lawmakers to adopt bans and/or moratoriums on the matter.

3. Bans and/or moratoriums of the use by law enforcement authorities of facial recognition technologies

Facial recognition includes various technologies. Their accuracy has already improved since 2018.[51] In all likelihood, the accuracy of facial recognition technologies will continue improving.

In this specific context, lawmakers may adopt *provisional* bans and/or moratoriums about the use of facial recognition technologies by law enforcement authorities until such time when their level of accuracy becomes socially acceptable. Whenever bans have not been characterized as provisional, it is however understood that lawmakers have both the power and authority to undo what they have done. Lawmakers may accordingly decide to put a term to any ban if they consider that the level of accuracy has become socially acceptable for the use of facial recognition technologies by law enforcement authorities.

3.1 Bans and/or moratoriums based on the flaws of facial recognition technologies by US city councils

A number of US city councils prohibited the use of facial recognition technologies by law enforcement authorities especially in California and Massachusetts. These bans and/or moratoriums are based on the flaws of facial recognition technologies, *i.e.* on their lack of accuracy and the negative consequences of their use in erroneously identifying minorities and women. Some moratoriums include sunset provisions.

3.1.1 Diverse scope of bans and moratoriums

San Francisco was the first US city to prohibit its municipal agencies from using facial recognition technologies. On 14 May 2019, the Board of Supervisors of San Francisco approved the Stop Secret Surveillance Ordinance.[52] The ordinance outlaws the use of facial recognition technologies by the city's 53 departments including the San Francisco Police Department.[53] It entered into force in June 2019.[54]

On 27 June 2019, the Boston suburb of **Somerville** in Massachusetts enacted the Face Surveillance Full Ban Ordinance.[55] Its scope also includes prohibiting the use of data or evidence produced by IT systems of facial recognition during criminal investigations and judicial proceedings.

---

49. See Benjamin S. Weiss, "Experts urge Congress to help set standards, increase transparency of AI-assisted law enforcement", *Courthouse News Services*, 24 January 2024, available at Experts urge Congress to help set standards, increase transparency of AI-assisted law enforcement | Courthouse News Service and Facial Recognition Technology: Part II, Ensuring Transparency in Government Use, Hearing before the Committee on Oversight and Reform, House of Representatives, 116th Congress, First Session, 4 June 2019, Serial No. 116-031, available at - FACIAL RECOGNITION TECHNOLOGY: PART II ENSURING TRANSPARENCY IN GOVERNMENT USE (govinfo.gov)
50. See Jim Nash, "NYC argues over increased scrutiny for police use of facial recognition", 18 December 2023, *BiometricUpdate.com*, available at NYC argues over increased scrutiny for police use of facial recognition | Biometric Update
51. See "How the accuracy of facial recognition technology has improved over time", *Innovatrics*, available at How the accuracy of facial recognition technology has improved over time - Innovatrics; Alice Towler, James D. Dunn, Sergio Castro Martínez, Reuben Moreton, Fredrick Eklöf, Arnout Ruifrok, Richard I. Kemp & David White, "Diverse types of expertise in facial recognition", *Scientific Reports* 13, 11396 (2023), available at https://www.nature. com/articles/s41598-023- 28632-x#Abs1
52. Available at 190110 - Leg Ver3 (legistar.com)
53. See City and County of San Francisco - File #: 190110
54. See 19B Surveillance Technology Policies
55. Available at library.municode.com

On 16 July 2019, the **Oakland** City Council unanimously approved an ordinance to ban the use by police of both real-time and non-real-time facial recognition technologies. The ordinance prohibits the city of Oakland from "*acquiring, obtaining, retaining, requesting, or accessing Facial Recognition Software*." The ordinance defines facial recognition technology as "*an automated or semi-automated process that assists in identifying or verifying an individual based on an individual's face*."[56]

Five other cities in Massachusetts followed suit, *i.e.* **Berkeley** (ordinance of 16 October 2019),[57] **Brookline** (ordinance of 11 December 2019),[58] **Northampton** (ordinance of 19 December 2019 prohibiting the use of face surveillance systems),[59] **Cambridge** where the City Council unanimously approved the ban about the use of facial recognition technologies on 13 January 2020)[60] and **Springfield** where the City Council adopted an ordinance on 24 February 2020 placing a moratorium on the use of facial recognition technologies by the police until 2025.[61]

On 3 August 2020, the City Council of **Portland** (Maine) similarly adopted an ordinance banning the use of facial recognition and surveillance technology software by law enforcement.[62] On 3 November 2020, it added concrete penalties, *i.e.* data subjects are entitled to a minimum of $ 1,000 in civil fees for each violation of the ordinance if they are subjected to a facial recognition scan by the police.[63]

On 1 December 2020, the Common Council of the City of **Madison** passed ordinance 62413 which prohibits its city agencies, departments and divisions including the Madison Police Department from using facial recognition technologies or "*information derived from a face surveillance system*" in the city. The ordinance however allows the use of facial recognition technologies to identify and locate "*victims of human trafficking, child sexual exploitation or missing children*."[64] It also allows the use of facial recognition to identify the user of a device and the use of evidence relating to the investigation of a specific crime which may have been generated from a face surveillance system, provided that the evidence was not generated by or at the request of any department.

On 12 February 2021, the **Minneapolis** City Council unanimously approved an ordinance which prohibits city employees including its police department and other city agencies from acquiring or using facial recognition systems and the results. It however created a formal appeals process for a city agency to request exemptions.[65] On 25 February 2021, the Township Council of **Teaneck** in Pennsylvania unanimously adopted ordinance 7-2021 which banned the use of facial recognition surveillance technologies by the police and departments.[66]

On 1 June 2021, the **King** County Council unanimously approved an ordinance which partially bans both acquiring and using facial recognition technology or information by all official county government administrative and executive offices including law enforcement, *i.e.* the Sheriff's Office, to identify suspects or potential suspects. This county in the area of Seattle thus became the first county in the US to partly prohibit the use of facial recognition software by government. Departments including the Sheriff's Office may still use facial recognition evidence provided that they do not produce it themselves or request it. They may also continue using the technology in service of the federal programme which searches for missing children. It provides for suing if facial recognition technology is used in violation of the ordinance.[67]

56. Available at https://www.eff.org/files/2019/11/12/oaklandfr.pdf
57. See 2.99.030 City Council Approval Requirement | Berkeley Municipal Code
58. See Face-Surveillance-Ban_July-2020-Committee-Report
59. See 13774 and Document PDF · 139 ko
60. See library.municode.com
61. See City of Springfield, MA: Enforcement.
62. Available at 5dc0d075-9119-49d4-baf7-348e33cbf68a
63. See Chapter 34.10 Prohibit the use of Face Recognition Technologies by Private Entities in Places of Public Accommodation in the City of Portland | Portland.gov
64. Available at 2020 Madison Ordinance 62413 Banning Facial Recognition Technology - ProGov21
65. Available at https://lims.minneapolismn.gov/Download/FileV2/23216/Facial-Recognition-Ordinance-01.21.2021.pdf
66. Available at ecode360.com
67. Available at King County - File #: 2021-0091

Last, the City Council of **Worcester** in Massachusetts unanimously passed ordinance # 923 on 14 December 2021. This ordinance bans the City of Worcester and any department or agency thereof or any official "*to knowingly obtain, retain, request, access, or use* [...] *any facial recognition system; or* [a]*ny information obtained from a facial recognition system*."[68] Regarding exceptions, the ordinance however provides that the City of Worcester or any Worcester official may lawfully use "*evidence from a non-Worcester law enforcement agency that may have been generated from a facial surveillance system for the purposes of the investigation of a specific crime*".

3.1.2 Bans and/or moratoriums based on risks of inaccuracy, unreliability and bias

In its ordinance of 16 July 2019, the **Oakland** City Council stated that "*[f]ace recognition technology runs the risk of making Oakland residents less safe as the misidentification of individuals could lead to the misuse of force, false incarceration, and minority-based persecution.*"[69] On 18 August 2020, the city council of **Jackson** ordered that the use of facial recognition technology by the Jackson Police Department be prohibited in the city of Jackson. The resolution mentioned cities across the US which have already adopted similar measures: "*San Francisco, Calif.*, *Somerville, Mass.*, and *Oakland, Calif.*, *have all passed legislation banning FRT*. [...S]*tudies have shown that facial recognition surveillance programs routinely identify the wrong person. These errors have real-world impacts, including harassment, wrongful imprisonment and deportation*." The resolution noted that one of the technology's deficiencies is that it has a higher error rate when it comes to identifying people who are not white. It states that "*facial recognition software has been shown to programmatically misidentify people of color, women, and children: thus supercharging discrimination and putting vulnerable people at greater risk of systemic abuse*." The strongly worded resolution also claims that another problematic aspect is that the tool can lend itself to abuse by law enforcement agencies: "*law enforcement officers frequently search facial recognition databases without warrants and even reasonable suspicion thus violating the Fourth Amendment and basic human rights*. [...P]*olice officers across the United States routinely abuse confidential databases to spy on exes, business partners, neighbors, and journalists.*"[70]

On 9 September 2020, the city council of **Portland** (Oregon) adopted an ordinance strictly banning the use of facial recognition technologies. It mentioned that "*the use of facial recognition technologies raises general concerns around privacy, intrusiveness, and lack of transparency*."[71] Last, in its ordinance unanimously approved on 1 June 2021, the **King** County Council based its partial ban on the technology's threat to privacy and history of bias.[72]

The sixteen above-mentioned city councils and county have been banning the use of facial recognition technologies by law enforcement authorities since 2019. These bans all remain in force to date. It would therefore be worth assessing the level of compliance with, effectiveness and results of these bans over the last five years.

3.1.3 Some city councils and States have been reconsidering their initial bans and/or moratoriums on the use of facial recognition by law enforcement authorities from the second semester of 2020

The ordinance strictly banning the use of facial recognition technologies adopted by the city council of **Portland** (Oregon) on 9 September 2020 went into effect on 1 January 2021. On 1 February 2023, the City Council however unanimously passed an overall policy resolution on the use of surveillance technologies.[73]

At the level of States, **Vermont** became the first State in October 2020 to ban the use of facial recognition technologies or information derived from such technology by law enforcement in all circumstances until otherwise approved by the legislature.[74] It then however added an exception that the police may use the technology in the investigation of certain crimes, specifically in cases involving sexual exploitation of

68. Available at REVISED ORDINANCES OF THE CITY OF WORCESTER (worcesterma.gov)
69. See https://www.eff.org/files/2019/11/12/oaklandfr.pdf
70. Available at https://www.jacksonms.gov/meetings/august-18-2020-special-council-meeting/
71. See portland.gov
72. Available at King County - File #: 2021-0091
73. See portland.gov
74. Available at Vermont S124 and Vermont S0124 | 2019-2020 | Regular Session

children, provided that the search is solely confined to locating images of an individual within electronic media legally seized by law enforcement in relation to the specific investigation.[75]

Similarly, **California** passed Assembly Bill ("AB") 1215 on 8 October 2019.[76] This law adopted a three-year moratorium on law enforcement agencies from using handheld and body-worn cameras for facial recognition. AB 1215 prohibited an automated or semi-automated process which analysed biometric data in connection with data collected by an officer camera. On 1 January 2023, the law expired and California now considers adopting new legislation on the use of facial recognition technologies by law enforcement authorities.[77]

The single reason why city councils and States reconsidered their initial bans and/or moratoriums is the rise in violent crime[78] including homicides[79] and the argument that the use of facial recognition technologies would assist law enforcement authorities in addressing it.[80]

3.2 Calls for a ban and/or moratorium leading to a compromise in the EU

Several actors have been calling for a ban and/or moratorium on the use of facial recognition technologies by law enforcement authorities. These calls focused on their use in public spaces. The legislative process however led to the compromise found in the relevant provisions of the EU Regulation.

3.2.1 Calls of the European Data Protection Supervisor and Parliament for a moratorium on the use of facial recognition technologies by law enforcement authorities in public spaces

On 29 June 2020, the European Data Protection Supervisor (hereinafter the "EDPS") released Opinion 4/2020 on the European Commission's White Paper on Artificial Intelligence calling for a temporary ban on automated recognition technologies which capture biometric data including faces in public spaces.[81] On 3 September 2020, the Commission stated that it was considering a potential ban on the use of facial recognition technologies in public places in the EU. The Commission further stated that it would look into "*whether we need additional safeguards or whether we need to go further and not to allow facial recognition in certain cases, certain areas or even temporarily*."[82]

Regarding live facial recognition, the EDPS stated that he supported the idea of a moratorium on automated recognition of faces in public spaces on 7 September 2020.[83] In its report of 4 January 2021, Parliament invited the Commission to assess the consequences of a moratorium on the use of facial recognition systems, and, depending on the results of such an assessment, to consider a moratorium on the use of facial recognition systems by law enforcement authorities in semi-public spaces such as airports, until the technical standards can be considered fully fundamental rights-compliant, the results derived are non-biased and non-discriminatory, and there are strict safeguards against misuse and that ensure the necessity and proportionality of using such technologies.[84] Last, the European Data Protection Board (hereinafter the

75. 2020 Vermont Acts and Resolves 799 Section 14. Available at VT H0195 | BillTrack50
76. Available at Bill Text: CA AB1215 | 2019-2020 | Regular Session | Chaptered | LegiScan
77. See https://www.biometricupdate.com/202401/california-facial-recognition-bill-aims-to-keep-citizens-safe-from-false-arrests
78. Paresh Dave, "Focus: U.S. cities are backing off banning facial recognition as crime rises", *Reuters*, 12 May 2022, available at Focus: U.S. cities are backing off banning facial recognition as crime rises | Reuters; Scott Ikeda, "Facial Recognition Bans Begin To Fall Around the US as Re-Funding of Law Enforcement Becomes Politically Popular", *CPO Magazine*, 18 August 2022, available at Facial Recognition Bans Begin To Fall Around the US as Re-Funding of Law Enforcement Becomes Politically Popular - CPO Magazine
79. Rachel Metz, "First, they banned facial recognition. Now they're not so sure", *CNN*, 5 August 2022, available at First, they banned facial recognition. Now they're not so sure | CNN Business
80. Jule Pattison-Gordon, "About Face: How Should Government Regulate Emerging Tech?", *Government Technology*, June 2023, available at About Face: How Should Government Regulate Emerging Tech? (govtech.com)
81. Available at 20-06-19_opinion_ai_white_paper_en.pdf (europa.eu)
82. See Samuel Stolton, "Commission will 'not exclude' potential ban on facial recognition technology", *Euractiv*, 3 September 2020, available at https://www.euractiv.com/section/data-protection/news/commission-will-not-exclude-potential-ban-on-facial-recognition-technology/
83. Available at https://edps.europa.eu/press-publications/press-news/blog/artificial-intelligence-data-and-our-values-path-eus-digital_en
84. Report on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice (2020/2013(INI)), 4 January 2021, available at https://www.europarl.europa.eu/doceo/document/A-9-2021-0001_EN.html

"EDPB") and the EDPS jointly called on 18 June 2021 "*for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces - such as of faces* [...] *- in any context*."[85]

3.2.2 The compromise found as a result of the legislative process

In its Proposal for a Regulation on a European approach for Artificial Intelligence of 21 April 2021,[86] the Commission proposed that a limited use of facial recognition technologies by law enforcement authorities would be subject to strict requirements. Real-time remote use of facial recognition technologies in publicly accessible spaces for law enforcement purposes would be prohibited "*in principle*". Exceptions would apply for fighting "*serious*" crime, *i.e.* uses to search for victims of crime or missing children, identify a perpetrator or suspect of a criminal offence, or prevent an imminent threat such as a terrorist attack. Exceptions would be subject to *ex ante* authorisation by a judicial or other independent body and limited in time and geographic reach. The use of facial recognition technologies by law enforcement authorities would also require developers to follow stricter rules.

The EDPS reacted immediately. In his press release of 23 April 2021, the EDPS regretted "*to see that our earlier calls for a moratorium on the use of remote biometric identification systems - including facial recognition - in publicly accessible spaces have not been addressed by the Commission*." The EDPS added that he would "*continue to advocate for a stricter approach to automated recognition in public spaces of human features - such as of faces [...] - for law enforcement purposes.*"[87]

On 7 June 2021, an open letter signed by more than 175 civil society organisations, researchers and activists called for an "*outright ban*" on the use of facial and remote biometric recognition technologies which enable mass surveillance. The letter contends that "*no technical or legal safeguards could ever fully eliminate the threat* [that these technologies] *pose*",[88] considering that they are by design potentially harmful per human liberties and civil rights. The signatories hence urged governments, international organisations and private actors to put an end to the use of biometric recognition technologies in public spaces.

In a joint opinion of 21 June 2021, the EDPB and the EDPS called for a general ban of automated recognition of *all* human features in publicly accessible spaces. They both stressed the need to explicitly clarify that the law enforcement directive[89] (hereinafter the "LED") applies to any processing of personal data falling under the scope of the draft AI Regulation. In a joint statement, the chairperson of the EDPB and the EDPS stated that "[d]*eploying remote biometric identification in publicly accessible spaces means the end of anonymity in those places*". They added that "[a]*pplications such as live facial recognition interfere with fundamental rights and freedoms to such an extent that they may call into question the essence of these rights and freedoms*."

In addition, "*[t]aking into account the extremely high risks posed by remote biometric identification of individuals in publicly accessible spaces, the EDPB and the EDPS called for a general ban on any use of AI for automated recognition of human features in publicly accessible spaces, such as recognition of faces [...] in any context*" (emphasis added). They concluded that a "*general ban on the use of facial recognition in publicly accessible*

85. EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, available at https://www.edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf, para. 32.

86. European Commission, 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, Brussels, 21.4.2021 COM(2021) 206 final 2021/0106 (COD), available at EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu)

87. Available at Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary | European Data Protection Supervisor (europa.eu)

88. Available at Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology - Amnesty International

89. 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.

areas is the necessary starting point if we want to preserve our freedoms and create a human-centric legal framework for AI".[90]

Last, the European Parliament adopted a Resolution on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters on 6 October 2021. Parliament advocated for a moratorium on using facial recognition systems for law enforcement purposes. Parliament noted the limits of some AI softwares which have not proved efficient, are not fully operational and often resulted in discriminatory results (racial and sexual biases). It called on the Commission to implement, through legislative and non-legislative means "*a ban on any processing of biometric data, including facial images, for law enforcement purposes that leads to mass surveillance in publicly accessible spaces*"[91] (para. 31) and on predicting techniques for policing based on behavioural data. Parliament called for strict controls on the use of AI by law enforcement and the judiciary. It advocated a risk based approach with emphasis on transparency, accountability and non-discrimination. This resolution is non-legislative and non-legally binding. Parliament however adopted for the first time an official position which sent a strong signal to the Council for the negotiations of the regulation on AI. The general approach of Council[92] and the subsequent amendments adopted by Parliament[93] however led to the compromise reached in the AI Regulation on the matter.

4. Regulations on the use of facial recognition technologies by law enforcement authorities

The US adopted its first regulations on the use of facial recognition technologies by law enforcement authorities in 2020. It has accordingly been applying such regulations for four years. In the EU, the Charter of Fundamental Rights[94] and the LED both include provisions which are relevant to the use of facial recognition technologies by law enforcement authorities. In addition, the AI Regulation includes provisions which directly deal with both post remote or retrospective and live or real-time facial recognition. In this context, legislators in the US and in the EU should share a common interest in knowing about the regulations adopted and applied across the Atlantic and attempting to learn lessons about this experience whilst taking into account the different context in which these regulations are adopted and implemented. These regulations however remain silent about any analysis based on comparative law as if this experience were completely irrelevant. The US and the EU simply seem to ignore one another and regulate on their own without any consideration for the situation across the Atlantic.

4.1 Regulation on the use of facial recognition technologies by law enforcement authorities in the US

Whereas the US has not yet adopted any regulation about the use of facial recognition technologies by law enforcement authorities at the federal level, US law relies extensively on self-regulation by the technology sector about privacy-related concerns.[95] For instance, the chief executive of Google, Sundar Pichai, explained in a speech in Brussels on 20 January 2020 that Google would not provide any facial recognition service

90. Available at EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination | European Data Protection Supervisor (europa.eu)

91. Available both at European Parliament 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)) - Publications Office of the EU (europa.eu) and at Texts adopted - Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters - Wednesday, 6 October 2021 (europa.eu)

92. European Council (n 86).

93. European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021–2021/0106(COD), 14 June 2023, available at https://artificialintelligenceact.eu/wp-content/uploads/2023/06/AIA-%E2%80%93-IMCO-LIBE-Draft-Compromise-Amendments-14-June-2023.pdf

94. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

95. Mailyn Fidler and Justin (Gus) Hurwitz, "An Overview of Facial Recognition Technology Regulation in the United States", *The Cambridge Handbook of Facial Recognition in the Modern State*, Rita Matulionyte and Monika Zalnieriute (eds.), Cambridge University Press, 2024, p. 216.

as long as authorities would not establish rules and safeguards.[96] In the context of the Black Lives Matter protests, IBM, Amazon and Microsoft announced in June 2020 that they would, in one way or another, stop selling their facial recognition software to police forces across the US.[97] On 9 June 2020, IBM spoke out first. IBM told members of US Congress that it would no longer offer facial recognition technologies since no federal law is available to provide a legal framework on its use. IBM expressed concern about the manner that the technology may be used for mass surveillance and racial profiling. The CEO of IBM wrote in a letter to some members of Congress stating that "*We believe now is the time to begin a national dialogue on whether and how facial recognition technology should be employed by domestic law enforcement agencies*".[98] Amazon followed suit the day after. It put a temporary, one year-long suspension on facial recognition contracts with US police departments and on the sale of its controversial Rekognition software to law enforcement. On 10 June 2020, Amazon stated on its blog that "*We've advocated that governments should put in place stronger regulations to govern the ethical use of facial recognition technology*".[99] Last, the president of Microsoft, Brad Smith, said 11 June 2020 that "*We will not sell facial-recognition technology to police departments in the United States until we have a national law in place, grounded in human rights, that will govern this technology*".[100] Regarding their scope, the decisions of IBM, Amazon and Microsoft apply to the US context only. These decisions include considerations of public relations. In addition, the private sector should not set the tone of the social debate about regulation on the use of facial recognition technologies by law enforcement authorities. City and States have however adopted many different regulations on the matter since 2020. The scope and content of these regulations vary a lot.

4.1.1 No relevant bill in force at federal level

US federal law does not currently regulate the use of facial recognition technologies. No federal guidelines are therefore available to limit or standardise it and to require transparency for government use of facial recognition technologies in places under federal jurisdiction such as ports and airports. There is accordingly no way of knowing how law enforcement authorities can use facial recognition systems at the federal level in the US.[101]

A few bills have however been introduced in Congress since 2016. They all stand no chance of being enacted due to the lack of bi-partisan action in Congress.[102] In June 2021, a bill which would regulate the use of facial recognition by federal government was proposed.[103] On 21 June 2022, the American Data Privacy and Protection Act was introduced. This potential federal privacy regulation bill would include facial recognition.[104]

On 27 October 2022, the Facial Recognition Act has been introduced in Congress. This bill aims "*to place strong limits on law enforcement use of Facial Recognition Technology* [...]*, provides transparency, and requires annual assessments and reporting on the deployment of the technology to protect individuals' rights. Specifically, the bill requires that a warrant be obtained that shows probable cause an individual committed a serious violent felony before FRT is deployed.*"[105] On 21 December 2022, two other bills on facial recognition have been

96. See "Sundar Pichai supports calls for moratorium on facial recognition", *Financial Times*, 20 January 2020, available at https://www.ft.com/content/0e19e81c-3b98-11ea-a01a-bae547046735
97. Elena Sánchez Nicolás, "'Black Lives Matter' protests spread in corona-hit EU", *The Observer*, 9 June 2020, available at https://euobserver.com/social/148590
98. Chris Mills Rodrigo, "IBM terminates facial recognition technology business", *The Hill*, 9 June 2020, available at https://thehill.com/policy/technology/501810-ibm-terminates-facial-recognition-technology-business/
99. Available at https://blog.aboutamazon.com/policy/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition
100. See Matt O'Brien, "Microsoft joins Amazon, IBM in pausing face scans for police", 11 June 2020, *Associated Press*, available at https://apnews.com/article/e5dfcb8c0b003c1134137d33add4c301
101. See Congressional Research Service, "Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations", 24 September 2020, available at Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations (congress.gov)
102. See U.S. Senator Christopher Coons of Delaware
103. 117th Congress Facial Recognition and Biometric Technology Moratorium Act of 2021, S. 2052.
104. 117th Congress American Data Privacy and Protection Act 2022, available at H.R.8152 - 117th Congress (2021-2022): American Data Privacy and Protection Act | Congress.gov | Library of Congress
105. See REPS LIEU, JACKSON LEE, CLARKE, GOMEZ, IVEY, AND VEASEY INTRODUCE BILL TO REGULATE LAW ENFORCEMENT'S USE OF FACIAL RECOGNITION TECHNOLOGY | Congressman Ted Lieu (house.gov)

introduced in Congress.[106] On 7 March 2023, a group of Congress members re-introduced the Facial Recognition and Biometric Technology Moratorium Act in both houses of Congress for consideration in the 118th Congress. The bill would prohibit the use of facial recognition technologies by federal government's agencies. It imposes limits on the use of biometric surveillance systems (such as facial recognition systems) by federal, State and local government entities.

A federal agency or official may not in an official capacity acquire, possess or use in the US any biometric surveillance system or information obtained by such a system unless Congress passes an act which specifically authorises such a use. Such an act of Congress must contain certain provisions such as provisions naming the specific authorised entity and auditing requirements relating to the system. Last, information obtained in violation of this bill shall not be admissible by the federal government in any proceeding or investigation except in a proceeding alleging a violation of this bill.[107]

On 30 October 2023, the Facial Recognition Act was reintroduced.[108] The fact that no federal law governs the use of facial recognition technologies by law enforcement authorities have prompted some city councils and States to regulate it themselves.

On 17 January 2024, a report of the National Academies of Sciences, Engineering and Medicine recommended that the Executive Office of the President consider issuing an executive order on the development of guidelines for the appropriate use of facial recognition technology including on privacy by federal departments and agencies. The report also recommended requiring training and certification of system operators and decision-makers, particularly for applications where errors can significantly harm subjects such as in law enforcement. In addition, the report recommended that the US Departments of Justice and Homeland Security should establish a working group to develop and periodically review standards for reasonable and equitable use by federal, State and local law enforcement agencies. The group should work on issues relating to guidance about the use of facial recognition technology for real-time surveillance of public areas. Last, the report recommended that grants for State and local law enforcement should require that recipients adhere to technical, procedural and disclosure requirements related to the use of facial recognition technology.[109]

4.1.2 Nuanced regulations in force at both city and State level

The city and State regulations of facial recognition technologies include nuanced regulatory bills the approaches of which have been both varied and fluid. On 24 June 2020, **Boston** made an exemption from the ban of using facial recognition for investigative purposes, allowing the Boston police officials to use evidence obtained through facial recognition technology by another agency for investigations into a "*specific crime*" as long as it was not "*generated by or at the request of Boston or any Boston official*."[110] This provision is meant to address a situation in which police officials from other States send to the Boston police department an image of a person that they searching for. In addition, Boston police and other officials are still allowed to follow up on tips from other law enforcement agencies which have used facial recognition software.

The policy of the **Easthampton** Police Department since 1 July 2020 has been to request facial recognition searches using facial recognition technology only through a written request submitted to the Registrar of

106. See Portman introduces two bills on facial recognition, AI in government. See also The Facial Recognition Act of 2022, New Proposed Law and The Facial Recognition Act: A Promising Path to Put Guardrails on a Dangerously Unregulated Surveillance Technology

107. 118th Congress Facial Recognition and Biometric Technology Moratorium Act of 2023, S. 681. See S.681 - 118th Congress (2023-2024): Facial Recognition and Biometric Technology Moratorium Act of 2023 | Congress.gov | Library of Congress. See also Markey, Merkley, Jayapal Lead Colleagues on Legislation to Ban Government Use of Facial Recognition and Other Biometric Technology (senate.gov)

108. See Facial Recognition Act of 2023 (H.R. 6092) and C:\Users\KGHauff.US\AppData\Roaming\SoftQuad\XMetaL\11.0\gen\c\LIEU_013.xml (house.gov)

109. Facial Recognition: Current Capabilities, Future Prospects and Governance, available at Facial Recognition Current Capabilities Future Prospects and Governance | National Academies

110. See Boston-City-Council-face-surveillance-ban

Motor Vehicles, the Department of State Police or the Federal Bureau of Investigation.[111] On 22 September 2020, the **Pittsburgh** City Council adopted an ordinance to regulate the use of facial recognition technologies by cities entities including the Pittsburgh Bureau of Police. The ordinance requires city council approval of such technologies before they are acquired or used, except in "*an emergency situation*."[112] The ordinance references the race, gender and age biases and potential inaccuracy for which facial recognition technology has been widely criticized: "*some of these technologies have the potential to endanger the civil rights and civil liberties of innocent individuals, which means it is incumbent on governments to regulate, scrutinize, and vet these technologies before they can be implemented*". According to the ordinance, the public safety director may authorise the use of facial recognition or predictive policing technologies without city council approval in instances when they believe that "*imminent death, physical harm, or significant property damage or loss can only be prevented by or responded to*" with their "*immediate and temporary use*" for up to 90 days.

On 31 December 2020, **Massachusetts** passed police reform and facial recognition regulations.[113] The latter allow police to perform facial recognition searches to assist with criminal cases or to mitigate "*substantial risk of harm*" after submitting a written request to the registrar of motor vehicles, Massachusetts State Police or the Federal Bureau of Investigation.

Some States regulate specific use by government such as police body cameras. For instance, **Oregon**'s law prevents facial recognition technologies from being used in conjunction with police body cameras.[114]

Colorado Senate Bill 113 of 8 June 2022 limits the use of the technology by law enforcement and government agencies in Colorado. It provides that government agencies which use facial recognition technology have to notify a reporting authority, specify why the technology is being used, produce an accountability report, test the equipment and subject any decisions which result from the technology to human review. Law enforcement is prohibited from using facial recognition to establish probable cause or create a record of actions protected by the First Amendment. In addition, law enforcement needs a warrant and probable cause to use facial recognition to conduct surveillance, tracking or real-time identification. The bill took effect in August 2022.

The bill also establishes a task force to assess the use of facial recognition technology by law enforcement and government agencies in Colorado as well as potential abuses and needed regulations. The task force consists of 15 members, including representatives from the legislature, law enforcement and the District Attorney's Council.[115]

On 1 July 2022, **Alabama**'s Senate Bill 56 about the use of facial recognition technology by law enforcement went into effect. The law has two components. First, it prohibits law enforcement from using a facial recognition match as the sole basis of probable cause or arrest. Second, it prohibits State or local law enforcement agencies from using artificial intelligence or a facial recognition service to engage in ongoing surveillance except for in certain circumstances.[116]

On 21 July 2022, the **New Orleans** City Council adopted an ordinance to allow New Orleans police to use facial recognition. It allows the New Orleans Police Department to request access to facial-recognition technology when it is investigating violent crimes. The ordinance lists 39 specific crimes including murder, rape, kidnap but also simple robbery, stalking and battery of a police officer.

111. See EPD-431-Facial-Recognition
112. Available at City of Pittsburgh - File #: 2020-0647
113. Available at Session Law - Acts of 2020 Chapter 253 (malegislature.gov)
114. 2019 Oregon Revised Statutes S 133.741, available at ORS 133.741 – Law enforcement agency policies and procedures regarding video and audio recordings (public.law)
115. Available at Artificial Intelligence Facial Recognition | Colorado General Assembly. See also Report of the Task Force for the Consideration of Facial Recognition Services 2023 Annual Report Submitted to the Joint Technology Committee, 19 December 2023, available at 2023_annual_report.pdf (colorado.gov)
116. Available at SB56 | Alabama 2022 | Artificial intelligence, limit the use of facial recognition, to ensure artificial intelligence is not the only basis for arrest- | TrackBill

Regarding the applicable procedure, investigators who want to use the technology must first exhaust all other methods of identification and then request permission from a supervisor. The latter verifies the investigator's "*reasonable suspicion*" that the data subject is connected to criminal activity. He then sends the image to the Louisiana State Analytical and Fusion Exchange which analyses law enforcement data for local, State and federal agencies.[117]

A judge or a magistrate commissioner does however not need to approve the request to use facial recognition technology. Police officers do not need to sign an affidavit certifying that they followed New Orleans Police Department policy[118] and exhausted all other means of identifying a person prior to making a request either. This decision of the New Orleans City Council reverses the ordinance of 17 December 2020 which banned the use of facial recognition software.[119] The single reason for this reversal was the rise in homicides.

Some States regulate the use of facial recognition technologies by government or law enforcement. For instance, **Washington** law SB 6280 of 31 March 2020 applies to all public agencies in the State. It requires government agencies including law enforcement to obtain a warrant or court order before using facial recognition technology in investigations except in case of emergency. Public agencies must have a way to have the software independently tested for "*accuracy and unfair performance differences*" across skin tone, gender, age and other characteristics. The law also requires training and public agencies to regularly report on their use of facial recognition technology.[120]

On 4 March 2021, the **Utah** legislature passed a bill which requires law enforcement officers to submit a written request to conduct a facial recognition comparison before performing a facial recognition search and must provide a valid reason for doing so. The request includes a statement about the specific crime being investigated. Law enforcement officers may only request to use facial recognition to investigate felony, violent crime or immediate threats to human life, or to identify a person who is dead, incapacitated or at risk. The request will only be granted if it is necessary to further an investigation in these limited cases and only if the police can demonstrate that the subject of the search is likely connected with the specific crime that they investigate. Two trained employees need to confirm each match once a facial recognition search has been authorised.

In addition to governing its use, the bill sets rules for facial recognition disclosure. The law thus requires the police which uses someone's photo in conjunction with facial recognition technology to notify this person about how it could be used.[121]

Under the legislation adopted in **Maine** on 24 April 2023, law enforcement may request a facial recognition search from the FBI and the Maine Bureau of Motor Vehicles with "*probable cause to believe an unidentified person in an image committed a serious crime*" or when assisting in the identification of a deceased, missing or endangered individual. The Maine State Police and Bureau of Motor Vehicles is required to maintain public records of all search requests "*received and performed*." The law provides that any unlawfully obtained data must be deleted and is inadmissible as evidence, and that the results of a facial recognition search are not sufficient, without other evidence, to justify "*arrest, search or seizure*."[122] Law enforcement can accordingly not use a facial recognition match as the sole basis to arrest or search someone. Nor can local police departments buy, possess or use their own facial recognition software.

On 29 June 2023, **Illinois** signed the Drones as First Responders Act[123] which provides that law enforcement agencies can use drones for security at public events. It however bans fitting them with facial recognition, photography capabilities or weaponry. Facial recognition is allowed only in the instance it can be used to

117. See MetaViewer and library.municode.com
118. See nola.gov
119. See https://podcasts.apple.com/fr/podcast/politico-tech/id1500970749?i=1000633828549
120. See Washington's New Facial Recognition Law | Strategic Technologies Blog | CSIS
121. See le.utah.gov
122. See Title 25, §6001: Facial surveillance
123. Available at Illinois General Assembly - Full Text of HB3902 (ilga.gov)

prevent a terrorist attack or in instances where immediate action is needed to prevent loss of life. Equipping drones with weaponry is however not allowed in any circumstance. The fact that law enforcement agencies could potentially use drones equipped with both facial recognition technologies and weapons clearly shows the dangers of AI in this area.

Here again, evaluating the application of the nuanced regulations which have been in force in these four cities and eight States since 2020 may provide useful data. Other cities, States and international organisations which consider regulating the use of facial recognition technologies by law enforcement authorities could learn valuable lessons that they could take into account in their draft legislation on the matter.

4.2 Regulations on the use of facial recognition technologies by law enforcement authorities in the EU

The LED and the Charter both include provisions which apply to the use of facial recognition technologies by law enforcement authorities. In addition, the AI Regulation includes complex provisions on the matter (4.2.1). It entered into force 20 days after its date of publication in the OJ on 12 July 2024, *i.e.* on 1 August 2024. The AI Regulation becomes applicable in stages. Bans on prohibited AI systems presenting unacceptable risks started applying to all operators six months after the date of the entry into force (Article 113(a) of the AI Regulation), *i.e.* on 2 February 2025 (4.2.2). No transitional regime is set out for prohibited practices. All AI systems which perform prohibited practices must accordingly be taken out of the market by this date. The chapter on penalties will become applicable on 2 August 2025 (4.3.3). In the interim period, the prohibitions are fully applicable and mandatory for all operators of AI systems. Law enforcement authorities should therefore take necessary measures to ensure that they do not use AI systems which could constitute prohibited practices under Article 5 of the AI Regulation. The prohibitions themselves have direct effect.[124] In addition, the requirements and safeguards on the retrospective use of RBI systems for law enforcement purposes will apply from 2 August 2026 (4.3.2). Last, the provisions on obligations for high-risk AI systems under Article 6(2) listed in Annex III of the AI Regulation will start applying two years after the date of entry into force (Article 113 of the AI Regulation), *i.e.* on 2 August 2026 (4.2.3). A transitional regime by 31 December 2030 is however set out for high-risk AI systems which are already available on the market by this date (Article 111(1) and (2) of the AI Regulation).

4.2.1 Common provisions applicable to the use of both live and post-remote facial recognition technologies by law enforcement authorities

Unlike the LED, the AI Regulation broadly[125] defines both law enforcement (Article 3(46) of the AI Regulation) and law enforcement authority (Article 3(45) of the AI Regulation). The AI Regulation includes principles which apply to both real-time and post-remote facial recognition technologies. For instance, no decision which "*produces an adverse legal effect on a person may be taken based solely on the output of the* [...] *remote biometric identification system*" (Articles 5(3) *in fine* and 26(10) of the AI Regulation). This principle means in practice that other evidence need to corroborate the identification before conclusions may be drawn.[126] In accordance with Union law, Member States may introduce more restrictive laws on the use of both live and post-remote facial recognition technologies, pursuant to Articles 5(5) *in fine* and 26(10) *in fine* of the AI Regulation. In addition, measures must be taken to ensure a sufficient level of AI literacy as defined in Article 3(56) of the AI Regulation of staff dealing with the operation and use of AI systems by 2 February 2025 when Article 4 of the AI Regulation starts applying.[127]

124. Commission Guidelines on prohibited artificial intelligence practices (n 9) 135, paras 431 and 432.
125. See Arnoud Engelfriet, *The Annotated AI Act*, Ius Mentis, Amsterdam, 2024, p. 57 and 58.
126. Ibid 86.
127. See Elora Fernandes and Abdullah Elbi, "This Time, Humans Learn About Machines: AI Literacy in the AI Act (Part 1)", 1 October 2024, available at https://www.law.kuleuven.be/citip/blog/this-time-humans-learn-about-machines-ai-literacy-in-the-ai-act-part-1; (Part 2), 4 October 2024, available at https://www.law.kuleuven.be/citip/blog/this-time-humans-learn-about-machines-ai-literacy-in-the-ai-act-part-2/ See also Erica Werneman Root, Nils Müller and Monica Mahay, "Understanding AI literacy", 15 January 2025, available at https://iapp.org/news/a/understanding-ai-literacy; guidance published by the Dutch supervisory authority on 30 January 2025 and available at Aan de slag met AI-geletterdheid | Autoriteit Persoonsgegevens See also Tiago Sérgio Cabral, "AI Literacy Under the AI Act: An Assessment of its Scope", EU Law Analysis, 23 February 2025, available at https://eulawanalysis.blogspot.com/2025/02/ai-literacy-under-ai-act-assessment-of.html?m=1

Facial recognition implies the processing of biometric data within the meaning of the LED. The use of facial recognition technologies by law enforcement authorities must be authorised by law, pursuant to Article 10 of the LED. This provision sets out that the processing of biometric data for the purpose of uniquely identifying a natural person must "*be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:*

(1) where authorised by Union or Member State law;

(2) to protect the vital interests of the data subject or of another natural person; or

(3) where such processing relates to data which are manifestly made public by the data subject."

Article 10 of the LED thus sets out three strict alternative requirements. In its Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement of 17 May 2023, the EDPB considered that processing of "*biometric data can only be regarded as 'strictly necessary' (Art. 10 LED) if the interference to the protection of personal data and its restrictions is limited to what is absolutely necessary, i.e. indispensable, and excluding any processing of a general or systematic nature*."[128]

Regarding the application of the principle of strict necessity in the specific context of Article 10 of the LED, the Court of Justice found that the controller should first satisfy itself that the objective pursued cannot be met by having recourse to non-sensitive data.[129] Second, "*the 'strictly necessary' requirement means that account is to be taken of the specific importance of the objective that such processing is intended to achieve. Such importance may be assessed, inter alia, on the basis of the very nature of the objective pursued – in particular of the fact that the processing serves a specific objective connected with the prevention of criminal offences or threats to public security displaying a certain degree of seriousness, the punishment of such offences or protection against such threats – and in the light of the specific circumstances in which that processing is carried out*."[130]

Regarding the relation between Article 10 of the LED and Article 5 of the AI Regulation, Article 5 of the AI Regulation which prohibits, subject to certain exceptions, the use of AI systems for real-time remote biometric identification in publicly accessible spaces for the purpose of law enforcement, should apply as *lex specialis* to Article 10 of the LED (Recital 38 of the AI Regulation). This prohibition means that law enforcement authorities may not make any other use of real-time RBI even if domestic law permits it.[131] Any processing of biometric data and other personal data involved in the use of AI systems for biometric identification, other than the use of real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, should continue to comply with all requirements resulting from Article 10 of the LED (Recital 39 of the AI Regulation).

Regarding the definition of biometric data, Article 3(34) of the AI Regulation sets out that "*personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data*". The requirement for allowing or confirming

128. EDPB, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, 17 May 2023, available at https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en, p. 6.

129. Ministerstvo na vatreshnite raboti, C-205/21, [2023] (ECLI:EU:C:2023:49), at para. 126.

130. Ministerstvo na vatreshnite raboti, C-205/21, [2023] (ECLI:EU:C:2023:49), at para. 127. See Taner Kuru, "C205/21 VS v Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost: Indiscriminate and Generalised Collection of Biometric and Genetic Data by Law Enforcement Authorities in the EU Is Not Allowed", *European Data Protection Law*, 2/2024 (Vol. 10), p. 223 to 231. See also EDPS comments to the AI Office's consultation on the application of the definition of an AI system and the prohibited AI practices established in the AI Act launched by the European AI Office, 19 December 2024, available at https://www.edps.europa.eu/data-protection/our-work/publications/formal-comments/2024-12-19-edps-ai-offices-consultation-application-definition-ai-system-and-prohibited-ai-practices-established-ai-act-launched-european-ai_en?trk=feed-detail_comments-list-reply_comment-text, p. 7, section 5.

131. See Arnoud Engelfriet (n 125) 86.

unique identification is thus not considered a prerequisite for the qualification of biometric data.[132] Article 3(13) of the LED however provides that "*personal data resulting 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*" (emphasis added). Article 4(14) of the GDPR[133] includes the same bolded phrase. The definition of the AI Regulation does not refer to the functional purpose of both the LED and the GDPR. By considering that unique identification may not always be the primary purpose of all use of biometric data, the AI Regulation includes all personal data relating to the physical, physiological or behavioural characteristics from the human body if resulting from technical processing, thus broadening the scope of the definition provided for in both the LED and the GDPR.[134] Recital 14 of the AI Regulation however specifies that the notion of "biometric data" used in the AI Regulation should be interpreted in light of the notion of biometric data as defined in Article 3(13) of the LED. Such data can allow for the authentication or identification of natural persons. No case law is yet available on the interpretation of this phrase. EDPB guidelines 05/2022 of 12 May 2022 on the use of facial recognition technology in the area of law enforcement however set out that "[b]*iometrics include all automated processes used to recognise an individual by quantifying physical, physiological or behavioural characteristics (fingerprints, iris structure, voice, gait, blood vessel patterns, etc.). These characteristics are defined as 'biometric data', because they allow or confirm the unique identification of that person.*"[135] Biometric applications such as facial recognition systems are indeed typically categorised and operate for either identification or verification (or authentication) purposes,[136] *i.e.* to verify and confirm whether a specific individual is the same person as he or she claims to be[137] by comparing data presented at a sensor with another set of previously recorded data stored on a device such as a smartphone, a passport or an ID card.[138]

Regarding additional requirements, any interference with fundamental rights must be strictly necessary under Article 52(1) of the **Charter** on the principle of proportionality. Data controllers must therefore be able to show compliance with this principle. The EDPS expressed "*concerns about how large-scale remote identification systems in public spaces would meet the necessity and proportionality requirements, and could therefore be considered acceptable interferences of fundamental rights.*"[139] National law would accordingly need to comply with the minimum requirements of the AI Regulation and all requirements of Article 52 of Charter as applied by the Court of Justice.

In addition, facial recognition involves processing a large amount of personal data and affects a large number of data subjects. It may cause a high level of risk to the rights and freedoms of natural persons, of varying likelihood and severity. The controller must carry out an **impact assessment** of the envisaged processing operations on the protection of personal data in accordance with Article 27 of the LED.

In its guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement of 26 April 2023, the EDPB emphasised that facial recognition tools should only be used in strict compliance with the LED. The Board added that these tools should only be used if necessary and proportionate in compliance with the Charter.[140]

---

132. Bilgesu Sumer, Natalia Menéndez González, Abdullah Elbi, Catherine Jasserand, Jan Czarnocki and Els J. Kindt, "AI Acts' Ripple Effect on Biometric Data: Harmonising or Fragmenting the Regulation of Biometric Data", Kostina Prifti, Esra Demir, Julia Krämer, Klaus Heine and Evert Stamhuis (eds), *Digital Governance*, T.M.C. Asser Press, The Hague, 2024, p. 176.
133. EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.
134. Bilgesu Sumer et al. (n 132) 176.
135. Available at edpb_guidelines_202304_frtlawenforcement_v2_en.pdf (europa.eu), emphasis added, p. 7, para. 7
136. See ISO/IEC Standard 2382-37:2022 Information Technology - Vocabulary, Biometric recognition, Term 37.01.03.
137. Bilgesu Sumer, "The AI Act's Exclusion of Biometric Verification", *European Data Protection Law*, 2/2024 (Vol. 10), p. 150; Monika Simmler and Giulia Canova, "Facial recognition technology in law enforcement: Regulating data analysis of another kind", *Computer Law & Security Review*, April 2025, p. 2, section 2.1 and p. 5, section 3.2.2.
138. Commission Guidelines on prohibited artificial intelligence practices (n 9) 98, para. 303.
139. See EDPS comments (n 130) 10, section 9 *in fine*.
140. Available at edpb_guidelines_202304_frtlawenforcement_v2_en.pdf (europa.eu), p. 29, para. 105.

The interplay between the LED and the AI Regulation leads to overlaps between the obligations of data protection and fundamental rights impact assessments. The two assessments must therefore be conducted in conjunction, pursuant to Article 27(4) of the AI Regulation. The purposes of data protection and fundamental rights impact assessments are similar, *i.e.* identify and mitigate risks to the fundamental rights of natural persons. The fundamental rights impact assessment generally examines the possible impact of AI systems on individuals. The scope of the data protection impact assessment is however limited to the risks to the rights and freedoms of individuals resulting from the processing of their personal data.[141] The fundamental rights impact assessment may then focus on aspects of the AI system which are not already covered by the data protection impact assessment.[142] Deployers must *inter alia* "*provide a general indication of the intended period of use and the expected frequency*."[143] In practice, the technical documentation of conformity assessments and the technical information may both assist deployers in drafting data protection impact assessments.

4.2.2 Provisions applicable to the use of either live or post-remote facial recognition technologies by law enforcement authorities

The **use** of **"real-time" facial recognition a/k/a "remote biometric identification systems" or RBI** as defined in Article 3(41) of the AI Regulation[144] - *i.e.* the practice of identifying persons at a distance based on biometric features against features in a reference database - by law enforcement authorities is in principle prohibited in public places, pursuant to Article 5(1)(h) of the AI Regulation. The four cumulative requirements to be met for this prohibition to apply are that **(1)** the RBI system is operated remotely (such as "*cameras installed at walls or ceiling of metro stations for surveillance purposes*"),[145] **(2)** in "*real-time*" (including short delays as clarified in Recital 17 of the AI Regulation), **(3)** in "*publicly accessible places*" within the meaning of Article 3(44) and Recital 19 of the AI Regulation (such as common areas of an airport)[146] and **(4)** "*for the purposes of law enforcement*".[147] A specific example of a system falling within this definition would be the use of a large-scale CCTV network coupled with facial recognition software. The prohibited use of real-time RBI systems by law enforcement under the AI Regulation is necessarily also unlawful under the LED as clarified in Recital 38 of the AI Regulation.

Law enforcement authorities can however still use real-time RBI systems for three exhaustively listed and defined objectives where strictly necessary for:

(1) protection: the **targeted search for specific victims** of abduction, trafficking in human beings, sexual exploitation of human beings and **search for missing persons**. Such search would involve both the localisation and identification of actual[148] victims;[149]

(2) prevention: 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**. Regarding the first alternative, Recital 33 of the AI Regulation adds that such a threat "*could also result from a serious disruption of critical infrastructure*" as defined in Article 2(4) of the Critical Infrastructure Directive[150] such as a power plant, a water supply or a hospital.[151] Regarding the second alternative, the concept "*is an autonomous notion of*

141. Commission Guidelines on prohibited artificial intelligence practices (n 9) 115, para. 373.
142. See Arnoud Engelfriet (n 125) 155 and 158.
143. Commission Guidelines on prohibited artificial intelligence practices (n 9) 116, para. 376.
144. An "*AI system for the purpose of identifying natural persons, **without their active involvement**, typically at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database*" (emphasis added); see also Recital 17 of the AI Regulation. This definition only covers the identification functionality and not the verification functionality.
145. Commission Guidelines on prohibited artificial intelligence practices (n 9) 99, para. 306 *in fine*.
146. Ibid 103, para. 317.
147. Ibid 97, para. 295.
148. *The EU Artificial Intelligence (AI) Act*, Ceyhun Necati Pehlivan, Nikolas Forgó and Peggy Valcke (eds), Wolters Kluwer, Alphen aan den Rijn, 2025, p. 175, section 3.9.2.1.
149. Commission Guidelines on prohibited artificial intelligence practices (n 9) 106, para. 331.
150. Critical Infrastructure Directive: 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, OJ 2022 L 333/164.
151. Commission Guidelines on prohibited artificial intelligence practices (n 9) 107, para. 340 *in fine*.

Union law"[152] and the use of the real-time RBI system may aim to "*detect and follow 'terrorists on the move', i.e. several persons linked to the same threat*"; [153]

(3) investigation: the **localisation or identification of a suspect** of crime, for the purposes of conducting a criminal investigation, prosecution or executing a criminal penalty for offences, referred to in Annex II and punishable in the relevant Member State by a custodial sentence or a detention order for a maximum period of at least four years. Annex II sets out a list of sixteen serious crimes (Recital 33 of the AI Regulation).

Article 5(1)(h) of the AI Regulation thus provides for many broad and far-reaching exceptions and significant loopholes to the principle of prohibition. Only a domestic law which complies with all the requirements and safeguards set out in Article 5(2) to (7) of the AI Regulation may provide the legal basis for the use of real-time RBI systems.[154] Member States may accordingly decide whether and in which of the three situations the use of real-time RBI systems in publicly accessible spaces for law enforcement purposes is permitted on their territory, pursuant to Article 5(5) of the AI Regulation. In the absence of domestic law authorising and regulating the use, law enforcement authorities may not deploy such systems for law enforcement purposes and the use is prohibited since 2 February 2025.[155] The existence of domestic law which complies with the relevant requirements of the AI Regulation is therefore a pre-requisite of such use.[156]

The use of real-time RBI by law enforcement authorities in publicly accessible spaces is however subject to five requirements. **First**, real-time RBI systems must be deployed "*only to confirm the identity of the specifically targeted individual*", pursuant to Article 5(2) and Recital 34 of the AI Regulation. Doing so implies "*a comparison of the data collected real-time with the data collected in the reference database*."[157] **Second**, the latter provision requires the completion of an *ex ante* fundamental rights impact assessment by law enforcement authorities to evaluate the risks of using real-time RBI systems. **Third**, their use must "*comply with necessary and proportionate safeguards and conditions in relation to the use in accordance with the national law authorising such use, in particular as regards the temporal, geographic and personal limitations*" (Article 5(2) and Recital 34 of the AI Regulation). National law must be sufficiently clear to provide adequate indications of conditions and circumstances so that its application is foreseeable for data subjects who are subject to it.[158] **Fourth**, each use must be notified to both the relevant market surveillance and data protection authority, pursuant to Article 5(4) of the AI Regulation. **Fifth**, the use of real-time RBI systems in publicly accessible spaces by law enforcement authorities also requires **for each use** an *ex ante* authorisation by a judicial authority or an independent administrative authority of a Member State whose decision is binding, pursuant to Article 5(3) and Recital 35 of the AI Regulation. The independence of the administrative authority is required for the use by law enforcement authorities of real-time but not post-remote RBI systems without the provision of any reason for this difference of treatment. In any case, the authority must make a double necessity and proportionality assessment of using a real-time RBI system within the limits of domestic law which provides the legal basis for such use, taking the Charter and EU law into consideration.[159]

Law enforcement authorities may however start using real-time RBI systems in a duly justified situation of urgency - "*namely in situations where the need to use the systems concerned is such as to make it effectively and objectively impossible to obtain an authorisation before commencing the use of the AI system*" (Recital 35 of the AI Regulation) such as "*an imminent threat to life*"[160] (scenario of a live shooter) - without an authorisation provided that such authorisation is requested without undue delay, at the latest within 24 hours. If the authorisation is rejected, the use must immediately be stopped. All the data, the results and

152. Ibid 108, para. 346.
153. Ibid 109, para. 348.
154. Ibid 127, para. 413 *in fine* and p. 105, para. 326.
155. Ibid105, para. 326 *in fine*.
156. Ibid 96, para. 290.
157. Ibid 113, para. 359.
158. See EDPS comments (n 130) 10, section 9.
159. Commission Guidelines on prohibited artificial intelligence practices (n 9) 120, para. 381.
160. Ibid 119, para. 378.

outputs of this use including the unlawful reference database, the metadata and the technical processing data[161] must be immediately discarded and deleted, in accordance with Article 5(3) of the AI Regulation.

In addition, Member States may adopt laws which generally provide for the use of real-time RBI by law enforcement authorities, pursuant to Article 5(5) of the AI Regulation. Such laws must set out detailed procedures on how authorisations are requested, issued and exercised. They must also refer to which specific crimes they apply. Member States must notify the laws to the Commission within 30 days after the date of their adoption. The scope of such laws may be more limited than that of Article 5(5) of the AI Regulation. It may accordingly "*only provide for such a possibility in respect of some of the objectives capable of justifying authorised use*", in accordance with Recital 37 of the AI Regulation.

Last, national market surveillance and data protection authorities of Member States will monitor the use of real-time RBI by law enforcement authorities in publicly accessible spaces and submit annual reports to the Commission. The latter will provide them with a template for consistent reporting, pursuant to Article 5(6) of the AI Regulation. In accordance with Article 5(7) of the AI Regulation, the Commission will compile the reports and publish its own reports which will exclude sensitive operational data as defined in Article 3(38) of the AI Regulation. Specific details which reveal ongoing or past investigations such as locations and cameras used should accordingly not be published.[162]

Regarding the use of **post-remote RBI systems** by law enforcement authorities, each use must be linked to the investigation of a specific crime, "*a criminal proceeding, a genuine and present or genuine and foreseeable threat of a criminal offence, or the search for a specific missing person*" and "*be limited to what is strictly necessary for the investigation*" of a specific crime, pursuant to both Article 26(10) and Recital 95 of the AI Regulation. Law enforcement authorities are prohibited to use post-remote RBI systems "*in an untargeted way*".

In the context of an investigation for the targeted search of a person suspected or convicted of having committed a crime, law enforcement authorities must request an *ex ante* or *ex post* – within 48 hours – authorisation by a judicial or administrative authority whose decision is binding and subject to judicial review to use a post-remote RBI system. The possibility of judicial review applies to the use by law enforcement authorities of post-remote but not real-time RBI systems without the provision of any reason for this difference of treatment. In any case, if the authorisation is rejected, the use of the post-remote RBI system must immediately be stopped. The personal data linked to this use must be deleted. If the authority fails to make any *ex post* decision within 48 hours, no possibility to start using the RBI system is provided for.[163] No authorisation is however required when law enforcement authorities use post-remote RBI systems for the initial identification of a potential suspect based on objective and verifiable facts directly linked to the offence, pursuant to Article 26(10) of the AI Regulation. This could for instance be the analysis of CCTV footage capturing the suspect committing an offence[164] or a system used by law enforcement authorities for registering a suspect upon arrest.[165] This provision however raises concerns to the extent that all data subjects are potential suspects within its meaning.

Last, each use must be documented in the relevant police file and must be made available to both the relevant market surveillance authority and data protection authority upon request, excluding the disclosure of sensitive operational data as defined in Article 3(38) of the AI Regulation without prejudice to the powers of supervisory authorities under the LED.

161. Ibid 125, para. 405.
162. Ibid 131, para. 425.
163. See EDPS comments (n 130) 11.
164. See Monika Simmler and Giulia Canova, "Facial recognition technology in law enforcement: Regulating data analysis of another kind", *Computer Law & Security Review*, April 2025, p. 9, section 4.3.
165. See Arnoud Engelfriet (n125) 151.

4.2.3 The use of RBI systems by law enforcement as high-risk systems

When not explicitly prohibited pursuant to Article 5 of the AI Regulation, systems considered high-risk according to Article 6(2) of the AI Regulation include RBI systems (point 1 (a) of Annex III)[166] as having "*a significant harmful impact on the* [...] *fundamental rights of persons in the Union*" (Recital 46 of the AI Regulation).[167] Where a Member State authorises the use of real-time RBI systems in publicly accessible spaces for law enforcement purposes for any of the three objectives listed in Article 5(1)(h) of the AI Regulation, the provisions on high-risk AI systems also apply to this use.[168] According to high-risk AI systems listed in point 1 of Annex III, all RBI systems including after the fact ("post-remote RBI") qualify as high-risk. In addition, high-risk AI systems listed in point 6 of Annex III provide that uses "*by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies in support of law enforcement authorities or on their behalf*" also qualify as high-risk (Recital 59 of the AI Regulation).

The AI Regulation distinguishes between the obligation of providers and deployers. A provider is defined as "*a natural or legal person, public authority, agency or other body that develops an AI system* [...] *or that has an AI system* [...] *developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge*" (Article 3(3) of the AI Regulation). A deployer is defined as "*a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity*" (Article 3(4) of the AI Regulation). In the context of our topic, a provider accordingly refers to the developer of RBI systems whilst a deployer refers to law enforcement authorities. As correctly pointed out by both the EDPB and the EDPS, the deployers as users of facial recognition systems are the data controllers.[169] As such, they are responsible for complying with the requirements for the lawful use of the system.[170]

The AI Regulation focuses on the **obligations of providers**. High-risk AI systems such as RBI can only be placed on the market and used in the EU if specific requirements are met, such as a quality management plan (Articles 16(c), 17 and 18(b) of the AI Regulation). RBI systems will also be permitted subject to an *ex ante* conformity assessment (Article 43 of the AI Regulation) by the provider to show compliance with the requirements or a conformity assessment body (Annexes VI and VII; Articles 3(21), 3(22) and 33(1) of the AI Regulation) before they can be put on the market. In addition, providers must both establish and maintain a risk management system and in particular carry out an adequate AI risk assessment including mitigation measures and post-market lifecycle monitoring (Article 9 and Recital 65 of the AI Regulation). Providers must also comply with data quality requirements which include the obligation to ensure the use of high quality datasets feeding the system to train algorithms, prevent bias as well as minimise risks and discriminatory outcomes. Providers also bear record-keeping obligations which means that high-risk AI systems must keep a record of their use and maintain logs of their activity for a period of at least six months (Article 19(1) of the AI Regulation) to ensure traceability of results and to help monitor incidents (Article 12 of the AI Regulation). Each use must be recorded including both its start and end dates and times, the input data, the reference database with biometric data used and the outcome. Providers are also required to give technical documentation including the provision of all detailed and comprehensive information necessary on the facial recognition functionality and its purpose for authorities to assess its compliance with the requirements set out in Section 2 of Chapter III (Article 11, Recital 71 and Annex IV of the AI Regulation). Providers also bear transparency obligations ("no secret AI") on the understanding that the provision of clear and adequate information to deployers (Article 13 of the AI Regulation) does not affect the obligations of data controllers to make available or give information to data subjects pursuant to Article 13 of the LED. Providers must also ensure effective human oversight to correctly interpret the output of the high-risk AI system and monitoring measures to minimise risk (Article 14 and Recital 73 of the AI Regulation). The output of a facial recognition system is merely an indication that two data subjects

166. See European Commission, Guide for the assessment of prohibited use cases and high risk AI systems (AI Act risk level assessment template); Commission Guidelines on prohibited artificial intelligence practices (n 9) 131, para. 426.
167. Emilija Leinarte, "The Classification of High-Risk AI Systems Under the EU Artificial Intelligence Act", *Journal of AI Law and Regulation*, Volume 1 (2024), Issue 3, p. 262 to 280.
168. Commission Guidelines on prohibited artificial intelligence practices (n 9) 96, para. 291.
169. EDPB-EDPS Joint Opinion 5/2021 (n 85) 9, para. 20.
170. Commission Guidelines on prohibited artificial intelligence practices (n 9) 5, para. 14.

present similarities to a certain degree.[171] Providers must thus take a human oversight by design approach (Article 14(1) of the AI Regulation). Providers must also ensure an appropriate level of accuracy, robustness and cybersecurity (Article 15 of the AI Regulation). The AI Regulation does however not contain any guideline on how to practically perform a test of RBI software by being exposed to vulnerabilities such as changing a few pixels to see if such software still recognises a face. Providers of RBI technologies will also be required to follow data governance practices (Article 10 of the AI Regulation) including the original purpose of the data collection to facilitate compliance with the LED; ethical collection of datasets for training which are representative, as free of errors and bias and complete as possible in view of the intended purpose; and validation data (Recital 67 of the AI Regulation).[172] Providers need to be able to demonstrate that all the requirements are met.[173] Last, providers must have an EU Declaration of Conformity that the AI system complies with all the requirements listed in Section 2 of the AI Regulation (Article 47 and Annex V of the AI Regulation). Providers must also affix to the AI system a CE marking to indicate conformity with all relevant EU legislation (Article 48 of the AI Regulation).

Article 40(1) of the AI Regulation provides for a **presumption of conformity**. This provision sets out that "[h]*igh-risk AI systems* [...] *which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012 shall be presumed to be in conformity with the requirements set out in Section 2 of this Chapter [...], to the extent that those standards cover those requirements or obligations*" (see also Article 41(3) of the AI Regulation on common specifications). Regulation (EU) No 1025/2012 deals with European standardisation whilst Section 2 on requirements for high-risk AI systems of Chapter III on high-risk AI systems includes above-mentioned Articles 8 to 15 of the AI Regulation. The harmonised standards must precisely define the requirements which apply to the relevant AI systems. The Commission has therefore commissioned the European Committee for Electrotechnical Standardization (CEN/CENELEC)[174] to draft ten standards.[175] Conformity with a harmonised standard may only be shown after a formal process of conformity assessment has been successfully completed (Article 43 of the AI Regulation). A certificate of conformity is then drawn up and serves as evidence of conformity (Article 44 of the AI Regulation).[176]

The **obligations of deployers** for high-risk systems include operating in accordance with the instructions of the provider (Article 26(1) of the AI Regulation). They also include the implementation of human oversight and monitoring measures. Law enforcement authorities must assign human oversight to people who have the necessary competence, in particular an adequate level of AI literacy, training and authority as well as the necessary support to properly fulfil those tasks (Article 26(2) and Recital 91 of the AI Regulation). Pursuant to Article 14(5) of the AI Regulation, no action or decision may be taken on the basis of the identification resulting from the use of RBI systems unless such identification has been separately verified and confirmed by at least two human beings (four eyes principle), "[c]*onsidering the significant consequences for persons in the case of an incorrect match by certain biometric identification systems*" (Recital 73 of the AI Regulation). The separate verifications by the different persons could be automatically recorded in the logs generated by the system. Article 14(5) *in fine* of the AI Regulation however allows Member States to provide for an exception to the four eyes principle for the purposes of law enforcement where EU or domestic law considers the application of this requirement disproportionate. The AI Regulation also includes a legal loophole. Article 46(2) of the AI Regulation provides that in a duly justified situation of urgency for exceptional reasons of public security or in the case of specific, substantial and imminent threat to the life or physical safety of natural persons, law enforcement authorities "*may put a specific high-risk AI system into service without the authorisation*" of the market surveillance authority pursuant to the conformity assessment procedure

171. Europol Innovation Lab (n 6) 47.
172. See Justin B. Bullock, Yu-Che Chen, Johannes Himmelreich, Valerie M. Hudson, Anton Korinek, Matthew M. Young and Baobao Zhang, *The Oxford Handbook of AI Governance*, Oxford University Press, 2024.
173. Isabelle Hupont, Marina Micheli, Blagoj Delipetrev, Emilia Gomez and Josep Soler Garrido, "Documenting High-Risk AI: A European Regulatory Perspective", *Computer*, Volume 56, Issue 5, 3 May 2023, p. 18 to 27, available at https://ieeexplore.ieee.org/document/10109295
174. See https://www.cencenelec.eu/about-cenelec
175. See Marta Cantero Gamito and Christopher T Marsden, "Artificial intelligence co-regulation? The role of standards in the EU AI Act", *International Journal of Law and Information Technology*, Volume 32, Issue 1, 2024, eaae011, https://doi.org/10.1093/ijlit/eaae011
176. See Arnoud Engelfriet (n 125) 175.

"*provided that such authorisation is requested during or after the use without undue delay. If the authorisation* [...] *is refused, the use of the high-risk AI system shall be stopped with immediate effect and all the results and outputs of such use shall be immediately discarded*".

The obligations of deployers also include event logging for a period of at least six months unless otherwise provided in applicable EU or domestic law, in particular in EU law on the protection of personal data (Article 26(6) of the AI Regulation), monitoring the functioning of the AI system and informing the provider without providing sensitive operational data (Article 26(5) of the AI Regulation), registering the high-risk AI system in case of public authorities (Article 26(8) of the AI Regulation) and using the information of the provider for the data protection impact assessment (Article 26(9) of the AI Regulation) on matters such as the intended purpose of the high-risk AI system, level of accuracy, performance, specifications for input data and human oversight measures.

In addition, deployers will have to conduct a **fundamental rights impact assessment**, *i.e.* an *ex ante* assessment of how the tool might affect fundamental rights under EU law and reduce risks prior to deployment into first use (Article 27 and Recital 34 of the AI Regulation). Deployers must assess *inter alia* "*the specific risks of harm*" and "*the measures to be taken where those risks materialise*" (Article 27(1)(d) and (f) of the AI Regulation). Regarding the practical implementation of this obligation, the AI Office will develop a template (Article 27(5) of the AI Regulation). Law enforcement authorities bear the obligation to keep the information up to date where necessary.

Regarding the obligation of deployers for the use of the real-time RBI system in publicly accessible spaces, Article 5(2) of the AI Regulation provides that such use "*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*" set up and maintained by the Commission (Article 71(1) of the AI Regulation). The registration must include *inter alia* a summary of the findings of the fundamental rights impact assessment and of the data protection impact assessment (Annex VIII, section C 4 and 5).

The AI Regulation also includes transparency exceptions for law enforcement. The **registration** of all information related to the use of AI in law enforcement must be "*in a secure non-public section of the EU database*". Only the Commission and national authorities must "*have access to the restrictions sections of the EU database*" (Article 49(4) of the AI Regulation). This information is accordingly **not publicly available**. Such exceptions provide for a severe limit to public oversight and scrutiny.

Last, Article 26(10) of the AI Regulation requires deployers to "*submit annual reports to the relevant market surveillance and national data protection authorities on their use of post-remote biometric identification systems*".

Data subjects will have a right to submit **complaints** about AI systems to the relevant market surveillance authority and request explanations about decisions based on high-risk AI systems affecting their rights from 2 August 2026 (Articles 27(1)(f) and 85; Recitals 96 and 170 of the AI Regulation). The AI Regulation does however not include any legal basis for class action.

Regarding **penalties**, the infringement of prohibited AI systems including the use of real-time RBI systems in publicly accessible spaces for the purposes of law enforcement (Article 5(1)(h) of the AI Regulation) may lead to the imposition of administrative fines of up to € 35 million or 7 % of the annual turnover (Article 99(3) of the AI Regulation) and the highest administrative fines for organisations of the EU of up to € 1.5 million (Article 100(2) of the AI Regulation). The fine is limited to the lump sum or percentage, whichever is higher. A special rule applies to small and medium enterprises and start-ups since the lower amount is used for the maximum fine. Penalties will start applying from 2 August 2025 (Article 113(b) of the AI Regulation).

5. Conclusion

From a legal perspective, the use of facial recognition technologies by law enforcement authorities in both the US and the EU remains the Wild West for the time being. This situation shows that specific regulation on the matter is necessary.

The US and the EU deal with similar issues. For instance, databases used by law enforcement authorities for facial recognition purposes include a high number of face photos both in the US and in the EU. In addition, this use equally lacks openness and transparency on the two sides of the Atlantic.

The two judgments of the UK Court of Appeal dated 11 August 2020 in the case Edwards Bridges[177] and of the ECHR dated 4 July 2023 in the case of *Glukhin v. Russia*[178] have not led to any change of practice about the use of facial recognition technologies by law enforcement authorities in South Wales and in the Moscow underground. In addition, the actions of enforcement authorities such as the Government Accountability Office and the US Commission on Civil Rights are limited to the examination of issues related to the use of facial recognition technologies by law enforcement authorities, the issuance of recommendations and the supervision of their implementation in the US. Although the role of supervisory authorities is more developed to monitor the correct application of domestic law of EU Member States enacting the LED, the Belgian supervisory authority has not been notified about the use of facial recognition technologies at the airport of Zaventem in Brussels in 2017.[179]

In this specific context, legislatures in both the US and the EU should know and consider the practical experience gained in their respective jurisdictions before adopting relevant provisions on the matter. Doing so would clarify the reasons why the legislature elects to follow or depart from the experience of other jurisdictions. Legislatures should always bear in mind that regulations may determine what is lawful but may not prohibit facial recognition technologies as such, especially in a context where law enforcement authorities have already been using facial recognition technologies for years. Checking the correct application of regulations and enforcement of regulations should also be anticipated in light of the experience of both the GDPR and the LED. Given the importance of the use by law enforcement authorities of facial recognition technologies, it is to be hoped that robust, constructive and fruitful transatlantic dialogues may lead to a convergence of regulations on the matter in the US and in the EU. As we have seen, the situation of the latter two however diverges at the moment to the extent that no regulation applies at the federal level in the US whilst the relevant provisions of the Charter, the LED and the AI Regulation all apply in Member States of the EU.[180] The report of the National Academies of Sciences, Engineering and Medicine dated 17 January 2024 however recommended that the US Departments of Justice and Homeland Security should establish a working group to address issues relating to guidance about the use of facial recognition technology for real-time surveillance of public areas[181] which are now regulated in the AI Regulation. Conversely, provisions in force in the EU do not necessarily include good practices of US States. For instance, the AI Regulation does regrettably not include any express ban of the use by law enforcement authorities of drones equipped with both facial recognition technologies and weapons as the Drones as First Responders Act signed by Illinois on 29 June 2023.[182]

177. Case No: C1/2019/2670); [2020] EWCA Civ 1058.
178. *Glukhin v. Russia*, Application no. 11519/20.
179. See Gabriela Galindo, "'No legal basis' for facial recognition cameras at Brussels Airport", *The Brussels Time*, 10 July 2019, available at 'No legal basis' for facial recognition cameras at Brussels Airport (brusselstimes.com); Bert Peeters, "Facial recognition at Brussels Airport: face down in the mud", 17 March 2020, available at https://www.law.kuleuven.be/citip/blog/facial-recognition-at-brussels-airport-face-down-in-the-mud/
180. See The Intelligence, 14 August 2024, available at https://podcasts.apple.com/fr/podcast/the-intelligence-from-the-economist/id1449631195?i=1000665240891
181. Facial Recognition: Current Capabilities, Future Prospects and Governance, available at Facial Recognition Current Capabilities Future Prospects and Governance | National Academies
182. Available at Illinois General Assembly - Full Text of HB3902 (ilga.gov)

The long Joint Statement adopted at the EU-US Trade and Technology Council of 4 and 5 April 2024 in Leuven[183] includes a whole section dedicated to artificial intelligence which is repeatedly mentioned. The use of facial recognition technologies by law enforcement authorities in both the EU and the US should be specifically referred to as an issue of common interest in transatlantic relations.

In addition, the non-legally binding resolution unanimously adopted under a no-vote procedure by the United Nations General Assembly on 21 March about impulsing safe, secure and trustworthy artificial intelligence systems[184] is also based on a multi-lateral approach. Proposed by the US and supported by more than 120 other Member States of the UN including China, the resolution emphasises the importance of protecting human rights, safeguarding personal data and monitoring AI for potential risks as well as encourages Member States to enhance privacy policies.

Last, some sixty States including China, Canada and Japan signed the Statement on Inclusive and Sustainable Artificial Intelligence in Paris on 11 February 2025.[185] The latter calls for broad general principles of "open" and "ethical" artificial intelligence without specifically mentioning facial recognition. The US has however elected to refrain from signing it which reflects the positions of its newly elected federal government. Although regrettable, such position is not overly problematic in practice since all relevant regulations are in force at the State, municipal and county level and not at the federal level in the US.

183. Available at Joint Statement EU-US Trade and Technology Council (europa.eu) and at U.S-EU Joint Statement of the Trade and Technology Council | The White House
184. A/78/L.49 available at https://documents.un.org/doc/undoc/ltd/n24/065/92/pdf/n2406592.pdf?token=vr7fj1wLfNU8lfKwXS&fe=true
185. Available at Statement on Inclusive and Sustainable Artificial Intelligence for People and the Planet. | Élysée