COMPARATIVE LAW REVIEW

Comparative Law Review

VOL. 17 · N. 1 · 2026

SPECIAL ISSUE

European Law and Digital Technologies

ISSN
2038 – 8993

OPEN ACCESS JOURNAL

COMPARATIVE LAW REVIEW
The Comparative Law Review is a biannual journal published by the
I. A. C. L. under the auspices and the hosting of the University of Perugia Department of Law.

Office address and contact details:
Email: complawreview@gmail.com

Comparative Law Review is registered at the Courthouse of Monza (Italy) - Nr. 1988 - May, 10th 2010.

COMPARATIVE
LAW
REVIEW
VOL. 17/1 – 2026

SPECIAL ISSUE

European Law and Digital Technologies

Edited by Federica Giovanella

TRANSATLANTIC DEBATE ON AI-POWERED FACIAL RECOGNITION TECHNOLOGIES: EU AND US REGULATORY MODELS

Giulia Formici[*]

TABLE OF CONTENTS:

AI is a transformative force in the field of biometric technologies, particularly in facial recognition; it has spread rapidly to various sectors and applications. Its rise has also triggered significant risks and concerns, leading to the implementation of different regulatory solutions. This paper focuses on two influential examples: the European Union and the United States. The recently adopted EU AI Act introduced an unprecedented and comprehensive framework for AI governance with specific emphasis on remote identification systems. In the US, the regulatory scenario is fragmented, marked by ongoing debate and varying state and municipal initiatives. In the broader context of AI governance, the two models show differences and similarities. These disciplines reveal a pressing challenge: aligning facial recognition technologies with democratic values and fundamental rights.

Keywords: Facial recognition technologies; biometric data; mass surveillance; artificial intelligence; fundamental rights; USA biometric legislation; AI Act.

I. 'ALWAYS IN FOCUS, YOU CAN'T FEEL MY STARE' [1] - UBIQUITOUS BIOMETRIC SURVEILLANCE AND FUNDAMENTAL RIGHTS

Facial Recognition Technologies (FRTs) "refer to the application of automatically identifying or verifying a person from face images and videos" [2]. Verification (or authentication) relies on a one-to-one approach, assessing whether different facial images pertain to the same person, whereas identification uses a one-to-many model, comparing a query face against a dataset or watchlist[3].

---

[*] Giulia Formici, Senior Lecturer in Public Comparative Law, University of Parma, giulia.formici@unipr.it.
This paper is an outcome of the research project "AI-Biometric Systems and Fundamental Rights Protection: Legal Challenges and Regulatory Solutions in a Comparative Perspective", coordinated by Giulia Formici, granted by the University of Parma through the Action "Bando di Ateneo 2024 per la ricerca".

[1] The Section titles draw on Judas Priest's song "Electric Eye", which vividly captures the risks and concerns associated with surveillance technologies.

[2] G. Hua, *Facial Recognition Technologies*, in L.A. Schintler, C.L. McNeely (eds), *Encyclopedia of Big Data*, Cham, 475 (2022).

[3] While verification systems answer the question "Are you the one you declared to be?", identification systems respond to the more complex question: "Who are you?". Some Authors also identify a third form of facial processing' technologies, "ones that seek to infer what someone is like, or even how someone is feeling", aimed at inferring emotional states, behavioural intention and specific characteristics connected to gender, age, ethnical origins" (N. Selwyn *et al*, *FRTs. Key Issues and Emerging Concerns*, in R. Matulionyte, M. Zalnieriute (eds), *The Cambridge Handbook of Facial Recognition in the Modern State*, Cambridge, 12 (2024). To delimit the scope of this paper, the analysis will focus primarily on identification systems.

These technologies have advanced considerably in recent years, largely due to Artificial Intelligence (AI), deep learning techniques, data computing and sophisticated algorithms[4]. Today, FRTs are not only deployed in controlled environments, e.g. borders, airports and sensitive institutional locations, but also in "uncontrolled environments". They draw on "unconstrained visual sources"[5], including photos and videos uploaded online or captured by surveillance cameras. Such operations can be performed either in *real-time*, capturing, comparing and identifying faces almost instantaneously using live or near-live material[6], or retrospectively (*post*) using photographs in existing databases[7].

Given these technical capabilities, FRTs have become one of the most widely adopted and intensively used AI-powered biometric systems[8]. They are pervasive in everyday life, from authentication tools that secure our smartphones or grant access to specific places (e.g. banks), to large-scale identification systems implemented in train stations, stadiums, public spaces and at national borders[9]. Public and private actors alike have been quick to embrace FRTs, particularly in areas such as security, law enforcement, migration control, prevention of disorder and terrorist attacks, as well as in employee identification and humanitarian operations[10].

However, as FRTs rapidly expand, concerns have mounted. Looking at technical shortcomings, these systems remain fallible, with accuracy strongly dependent on dataset quality, and vulnerable to "face variations"[11]. Many studies have documented algorithmic bias and disproportionate error rates in relation to skin colour and texture, gender and racial/ethnic background[12]. The unique and irreplaceable nature of facial images as biometric data[13] adds further complexity: unlike passwords, facial patterns cannot be altered or replaced in the event of data breaches. Beyond these technical and security

[4] A. Akbari, *Facial Recognition Technologies 101: Technical Insights*, in R. Matulionyte, M. Zalnieriute (eds), *The Cambridge Handbook of Facial Recognition*, quot., 29 ff.

[5] G. Hua, *Facial Recognition Technologies*, quot., 475.

[6] R. Pereira, *Remarks on the Use of Biometric Data Systems (and FRTs) for Law Enforcement Purposes*, in D. Vicente *et al* (eds), *The Legal Challenges of the Fourth Industrial Revolution. The European Union's Digital Strategy*, Cham, 206 (2023).

[7] A.R. Martinez, *The Debiasing Paradox: Facial Recognition Technology and Biometric Identification Systems in the Artificial Intelligence Act*, in C. van Oirsouw *et al* (eds), *European Yearbook of Constitutional Law 2023. Constitutional Law in the Digital Era*, Cham, 147 (2024).

[8] These can be defined as tools able to "identify or verify the identity or a claim of persons on the basis of the automated measurement and analysis of their biological (such as fingerprints and iris) or behavioural (such as signature and voice) characteristics", E.J. Kindt, *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*, Cham, 1 (2013). Such systems, based on biometric data and biometric datasets, have been integrated, in recent times, with AI. On these tools and the technical impact of AI, see C. Posthoff, *Artificial Intelligence for Everyone*, Cham (2024).

[9] More generally, on AI-powered biometric systems, see M. Smith, S. Miller, *Biometric Identification, Law and Ethics*, Cham, 2021; A.K. Jain *et al* (eds), *Introduction* to *Biometrics*, Cham (2nd ed. 2025).

[10] For an overview of the FRTs uses and market, S.M. Taylor, *FRT in 'Bloom': Beyond Single Origin Narratives*, in R. Matulionyte, M. Zalnieriute (eds), *The Cambridge Handbook of Facial Recognition*, quot., 44 ff.

[11] A.M. Martinez, *Face Recognition, Overview*, in S. Li, A. K. Jain (eds), *Encyclopedia of Biometrics*, quot., 506. On algorithmic bias see FRA, *Bias in Algorithms – AI and Discrimination* (2022).

[12] L. Moy, *Facing Injustice: How Face Recognition Technology May Increase the Incidence of Misidentifications and Wrongful Convictions*, in 30 William & Mary Bill of Rights J, 337 ff. (2021); E. Haber, *Racial Recognition*, 43 *Cardozo L Rev*, 71 ff. (2021).

[13] "Biometrics 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", EDPB, *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement*, 7 (26 April 2023).

issues, additional risks emerge from function creep, when FRTs are applied beyond their original purpose[14], and from "unintentional collection of additional information"[15].
Thus, the misuse of FRTs may not only affect data protection and privacy but also generate a broader "chilling-effect" on other fundamental rights[16]. Core democratic freedoms, such as freedom of expression and assembly, may be undermined by technologies that foster a constant sense of surveillance[17]. Bulk and indiscriminate processing of biometric data also threatens the presumption of innocence, while opaque and pervasive use of FRTs can erode due-process safeguards[18].
These warnings, coming from different sources, including companies active in the field[19], prompted discussions to establish regulatory frameworks for the governance of AI and/or specifically FRTs, heading to diverse approaches. In recent years, we have witnessed bans, moratoria, but also more comprehensive disciplines in the direction of specific constraints, conditions and limitations of FRTs for various purposes.
Against this backdrop, the present paper examines the different legislatives paths and regulatory solutions adopted to govern FRTs in two influential models: the European Union (EU) and the United States of America (US). In both contexts, widespread use of these technologies – especially by law enforcement authorities – has elicited concern and calls for legislative intervention. Although the case law is still limited on both sides of the Atlantic, regulatory activity has intensified, without yet settling the question. Emerging in democratic systems[20], the EU and US approaches are noteworthy because of their advanced stages of development and because they exemplify the broader challenge of (re)affirming the centrality of fundamental rights and the rule of law in an age of AI-driven surveillance technologies.
Section II explores the EU supranational framework and the recently adopted AI Act[21]. This ambitious act seeks to establish comprehensive governance of AI-systems, with special attention to biometric technologies, including real-time or post Remote Biometric Identification (RBI) systems, among which FRTs.
Section III considers the US context, where the absence of a federal law directly addressing FRTs has led to a fragmented regulatory landscape with various solutions at state and, in some notable cases, even at municipal level.

---

[14] P. Cabana, *Technical and Legal Challenges of the Use of Automated Facial Recognition Technologies for Law Enforcement and Forensic Purposes*, in A. Zavrsnik, K. Simoncic (eds), *Artificial Intelligence, Social Harms and Human Rights*, London, 46 (2023).
[15] i.e. additional medical information or ethnic origin that can be deduced from FRTs.
[16] P. De Hert, *Biometrics and the Challenge to Human Rights in Europe. Need for Regulation and Regulatory Debate*, in P. Campisi (ed), *Security and Privacy in Biometrics*, Cham, 369 ff. (2013); N. Rautenberg, D. Murray, *Making Tangible the Long-Term Harm Linked to the Chilling Effects of AI-Enabled Surveillance: Can Human Flourishing Inform Human Rights?*, in Hum Rights Rev, 293 (1, 2024).
[17] EDPB, *Guidelines 05/2022*, quot.; United Nations High Commissioner for Human Rights, *Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests*, UN Doc. A/HRC/44/24, 24 June 2020.
[18] I. Neroni Rezende, *Facial Recognition for Preventive Purposes*, in L. Winter, S. Ruggeri (eds), *Investigating and preventing crime in the digital era*, Cham, 67 ff. (2022); P. Fussey, D. Murray, F*acial Recognition Surveillance. Policing and Human Rights in the Age of Artificial Intelligence*, Oxford, 2025.
[19] IBM, Amazon, Microsoft, as reported by the European Parliamentary Research Service, *Regulation of Facial Recognition in the EU*, Brussels, 2021.
[20] G. Mobilio, *FRTs: Threats or Opportunities for Democracy?*, in N. Menendez Gonzalez, G. Mobilio (eds), *Next Democratic Frontiers for FRT*, Cham, 13 (2025) for reflections on how authoritarian regimes have implemented FRTs as tools of "digital authoritarianism".
[21] 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).

The final Section takes a comparative perspective, highlighting divergences and areas of convergence as well as trends common to the two legal systems. This analysis is framed in the broader debate on AI governance and democratic values, underscoring the urgent need to align FRTs with the protection of fundamental rights.
As Nobel Laureate in Physics (2024) Geoffrey Hinton warned, AI demands the "urgent and forceful attention of governments and international organizations"[22]. Embodying the promise and perils of rapid technological progress, FRTs encapsulate the broader challenges unleashed by the sudden rise of AI.

II. 'I AM PERPETUAL, I KEEP THE COUNTRY CLEAN' - EU REGULATORY EFFORTS IN THE FIELD OF BIOMETRIC IDENTIFICATION SYSTEMS: WHEN PROHIBITIONS MEET EXCEPTIONS

In the EU, the main legislative act currently providing a harmonized framework for FRTs is the AI Act.
This Regulation did not emerge in a legal vacuum: earlier safeguards were established by the General Data Protection Regulation (GDPR)[23], the Law Enforcement Directive (LED)[24], as well as rulings by national and supranational Courts and interventions by Member State Data Protection Authorities (DPAs)[25]. These measures identified issues and challenges, enhancing guarantees and limiting indiscriminate and generalized biometric surveillance. Nonetheless, "these various norms, which have different targets and are from multiple sources, create a kind of legal patchwork that could undermine the lawful use of this technology"[26]. Against this background, EU Institutions recognized the need for a

[22] https://www.nobelprize.org/prizes/physics/2024/hinton/speech/ (last visited Sept. 25, 2025).
[23] 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).
[24] 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.
[25] On the role of Courts, DPAs and the relevant provisions of EU law governing FRTs prior to the AI Act, see, *ex multis*, V.L. Raposo, *(Do Not) Remember My Face: Uses of FRT in Light of the GDPR*, in 32 Inf & Comm Tech L, 45 ff. (1, 2022); M. Qandeel, *FRT: Regulations, Rights and the Rule of Law*, in Front. Big Data, 7:1354659, 2024; C. Pizzolo, *AI, Biometric Data, and the Effective Protection of Fundamental Rights in the Recent ECJ Case-Law*, in Unione europea e Diritti, 1 ff. (1, 2025); N. Menendez Gonzalez, G. Mobilio (eds), *Next Democratic Frontiers for FRT*, quot.; G. Formici, *Put the Genie Back in the Lamp? AI-Based Biometric Systems and Fundamental Rights Protection in the European Union Artificial Intelligence Act* (forthcoming). On the first ruling on FRTs and their legitimacy (*The Bridges* Case in UK), see A. Pin, *A Novel and Controversial Technology. Artificial Face Recognition, Privacy Protection and Algorithmic Bias in Europe*, in 30 William & Mary Bill of Rights J, 291 (2021); L. Woods, *Automated Facial Recognition in the UK: The Bridges Case and Beyond*, 3 EDPL Rev, 455 (2020); on the first case-law of the ECtHR on FRTs (*Glukhin v. Russia*, App. No. 11519/20, 4 July 2023), see M. Zalnieriute, *Glukhin v. Russia App. No. 11519/20 Judgement*, in 4 American Journal of International Law, 699 (2023).
[26] V.L. Raposo, *The Use of Facial Recognition Technology by Law Enforcement in Europe: A Non-Orwellian Draft Proposal*, in 29 Eur J Crim Policy Res, 515 (2023); for a critical analysis of the issues and limits linked to the application of GDPR and LED to FRTs, see, amongst the others, J. Purshouse, L. Campbell, *Automated Facial Recognition and Policing: A Bridge Too Far?*, in 42 Legal Studies, 209 ff. (2022); G. Mobilio, *Your Face Is Not New to Me – Regulating the Surveillance Power of FRTs*, in 1 Internet Pol Rev, 1 ff. (2023); E. Kavoliunaite-Ragauskiene, *Right to Privacy and Data Protection Concerns Raised by the Development and Usage of FRTs in the EU*, in 16 J of Human Rights Practice, 658 ff. (2024); M. Zalnieriute, *Beyond Procedural Fetishism: The Inadequacy of GDPR in Regulating Facial Recognition Technologies and Public Space Surveillance*, in M. Ebers, K. Sein (eds), *Privacy, Data Protection and Data-Driven Technologies*, Abingdon, 328 ff. (2025).

dedicated legal framework targeting the technology itself and comprehensively addressing the threats it posed to fundamental rights[27].

The 2024 AI Act therefore tackled this necessity by introducing an ambitious, first-ever, regulatory regime on AI. It established a unified supranational discipline governing the development, marketing, implementation and use of different AI systems, with the dual aim of fostering innovation and safeguarding the internal market, while ensuring strong protection of fundamental rights, democracy and the rule of law[28].

This innovative regulatory instrument that underlines the need for trustworthy human-centric AI, assigns particular attention to AI-driven biometric systems. By applying a risk-based approach[29], several of these technologies are identified as unacceptable AI practices: systems inferring emotions of natural persons in workplaces and education institutions[30], biometric categorization technologies[31], untargeted scraping of facial images[32] and real-time RBI systems in publicly available spaces for law enforcement purposes[33] are explicitly prohibited under Art. 5. Such systems are deemed to pose risks irreconcilable with EU values and principles[34].

Other biometric systems, such as those inferring emotions for medical or safety purposes, post-RBI systems and certain non-prohibited categorization systems, are classified as high-risk under Art. 6 (and Annex III)[35].

Focusing on FRTs, it is worth noting that although the AI Act does not explicitly refer to them, they fall within the broader category of "RBI systems". According to Art. 3 (n. 41), these are defined as "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". This formulation evidently covers FRTs as well as voice and gait identification systems[36].

---

[27] See the Resolution of the European Parliament 2020/2016/INI of 6 October 2021, invoking a moratorium on the use of RBI systems (Para. 27). Also the Commission, in the *White Paper on AI – A European Approach to Excellence and Trust*, COM(2020)65 of 19 February 2020, emphasized the importance of a renewed debate on fundamental rights protection imperilled by RBI systems. Several actions were also promoted by civil society organisations, as the "Reclaim Your Face" campaign, promoted by EDRi and supported by almost 200 other NGOs and experts calling on governments to stop facial recognition surveillance.

[28] On the AI Act, see, *ex multis*, G. Cassano, E.M. Tripodi (eds), *Il regolamento europeo sull'Intelligenza Artificiale. Commento al Reg. UE n. 1689/2024*, Rome (2024); C.N. Pehlivan, N. Forgo, P. Valcke (eds), *The EU Artificial Intelligence (AI) Act: A Commentary*, Alphen aan den Rijn (2024); A. Bensoussan, J. Bensoussan, V. Bensoussan-Brulé, *The European AI Act. Summary, Key Points and Article-by-Article Analysis*, Louvain-la-Neuve (2025); D.U. Galetta, L. Hueso Cotino (eds), *The European Union Artificial Intelligence Act*, Naples (2025); G. Malgieri, G. Gonzalez Fuster, A. Mantelero, G. Zanfir-Fortuna (eds), *The EU Artificial Intelligence Act. A Thematic Commentary*, London (2025); A. Mantelero, G. Resta, G. M. Riccio (eds), *Intelligenza Artificiale. Commentario*, Milan (2025); R. D'Orazio, V. Ricciuto (eds), *Il diritto europeo dell'Intelligenza artificiale*, Turin (forthcoming).

[29] P. Dunn, *The AI Act: A Tile in the EU's Digital Risk-Based Approach*, in O. Pollicino *et al* (eds), *La disciplina dell'Intelligenza artificiale*, Milan, 141 ff. (2025).

[30] Art. 5(1)(f). For a definition of these systems, see Art. 3(n. 39).

[31] Art. 5(1)(g). The definition of "biometric categorisation technologies" is provided in Art. 3(n. 40).

[32] Art. 5(1)(e). See also Recital 43.

[33] Art. 5(1)(h) and Art. 5 (2) to (8).

[34] The European Commissions dedicated to these prohibited systems specific Guidelines (*Guidelines on Prohibited AI Practices*, C(2025)884 final, 4 February 2025).

[35] See *infra* in this Paragraph.

[36] N. Menendez Gonzalez, G. Mobilio, *Between Prohibited Risks and High Risk: The Regulation of FRT*, in O. Pollicino *et al* (eds), *La disciplina dell'Intelligenza artificiale*, quot., 65.

In this general framework, the AI Act introduces a further distinction: besides differentiating identification and verification[37], it establishes a novel and highly relevant classification between real-time and post-RBI (Arts. 3 (n. 42) and (n. 43)). The former indicates systems where biometric capture, comparison and identification occur without significant delay, including instant identification and limited short delays[38]. By contrast, post-RBI applies where biometric data has already been captured and comparison and identification occur "after a significant delay", for example by analysis of CCTV footage or pictures or videos from private devices produced prior to use of the systems (Recital 17).

These distinctions, grounded in an assessment of the implications of RBI systems for fundamental rights[39], form the basis of graded risk assessment.

Given its potential for deep intrusiveness, technical inaccuracies, biased outcomes and discriminatory effects (Recital 32), the use of real-time RBI systems is prohibited in publicly accessible spaces[40] for law enforcement purposes[41]. While this first-ever evaluation is a courageous and rigid stand, Art. 5(1)(lett. h) also introduces a significant list of exceptions, only allowing implementation when strictly necessary and for expressly indicated purposes[42].

Paragraphs (2) to (7) of Art. 5, nonetheless, set out specific limitations and requirements governing the above-mentioned exceptional uses. First, deployment must be limited to confirming the identity of a specifically targeted individual, thereby excluding indiscriminate and bulk searches[43] (so-called "fishing expeditions"). Moreover, the nature

[37] The AI Act defines "verification" as "automated one-to-one verification, including authentication, of the identity of natural persons by comparing their biometric data to previously provided biometric data" (Art. 3 (n. 36)). Identification, on the contrary is described as "automated recognition of physical, physiological, behavioural, or psychological human features for the purpose of establishing the identity of a natural person" through the comparison between that biometric data and those stored in a database (Art. 3 (n. 35)). This distinction has clear regulatory impacts: as stated in Annex III, Para. 1 (lett. a), high-risk RBI systems shall not include AI systems used for verification, which are therefore excluded from the set of rules established for high-risk technologies (see also Recital 17).

[38] Recital 17 talks about both live or near-live, "such as video footage, generated by a camera or other device with similar functionality".

[39] While verification systems, including authentication, "are likely to have a minor impact" compared to RBI (Recital 17), real-time systems appear to be "particularly intrusive" if compared to post RBI, to the extent that the first ones "may affect the private life or a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights", Recital 32.

[40] Art. 3 (n. 44). See also some examples at Para. 316 of the European Commission *Guidelines on Prohibited AI Practices*, quot.

[41] Useful definitions are provided in Art. 3 (n. 45) and (n. 46).

[42] Namely: i) targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons; ii) prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack; iii) localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years. The latter condition refers to 32 criminal offences listed in the Council Framework Decision 2002/584/JHA; their level of seriousness has been considered sufficient to justify the profound intrusion represented by real-time RBI systems (Recital 33).

[43] As reported by EDRi, "Emeritus Professor of International Law, Douwe Korff, supports this interpretation on the basis of case law of the Court of Justice of the EU, specifically the PNR (Passenger Name Records) case", https://edri.org/our-work/how-to-fight-biometric-mass-surveillance-after-the-ai-act-a-legal-and-practical-guide/ (last visited Sept. 25, 2025).

of the situation – particularly the seriousness, probability and scale of harm that would result from non-deployment – and the impact on rights and freedoms should be considered (Art. 5(2)(lett. a)-b)). Except for cases of urgency, such systems shall undergo a prior fundamental rights impact assessment (Art. 27) and be registered in the EU database established by Art. 49.

National laws, specifying the necessary and proportionate safeguards, including temporal, geographic and personal limitations, as well as the competent authority and the rules governing the authorization procedure (Art. 5(5)), must also be in place. In fact, each exceptional use of real-time RBI systems shall be approved in advance by judicial or independent administrative authority that evaluates necessity and proportionality on the basis of objective evidence or clear indications, ensuring that deployment remains limited in duration and geographic and personal scope to what is strictly necessary (Art. 5(3))[44].

The AI Act thus leaves Member States a significant margin of discretion: they may decide to partially or fully authorize the use of real-time RBI systems for the exceptional cases identified, while remaining free to adopt stricter rules (Art. 5(5)).

By contrast, post-RBI and other potential uses of FRTs are classified as high-risk and are therefore subject to the complex rules of Chapter III, Section 2 and 3 of the AI Act[45]. These provisions cover a wide range of obligations, including risk management systems, record-keeping duties, transparency requirements, human oversight safeguards and specific responsibilities for different actors in the value chain – providers, importers, distributors and deployers. While a comprehensive analysis of these measures is beyond the scope of this contribution[46], Art. 26 – addressing the obligations of deployers of high-risk AI systems – is particularly significant in relation to post-RBI. Specifically, Art. 26(10) requires prior authorisation by a judicial or administrative authority when such systems are used "in the framework of an investigation for the targeted search of a person suspected

[44] To create additional guarantees, national provisions also need to include notification rules (Art. 5(4)); each use of real-time RBI for the abovementioned purposes and conditions should be notified to the market surveillance authority and the national DPA; these authorities are also required to submit to the Commission annual reports of the use of real-time RBI (Art. 5(6)). Based on the data acquired, the Commission shall, in turn, publish annual reports photographing the deployment of these technologies in the EU (Art. 5(7)). Similarly to what affirmed in the GDPR (Art. 22), the AI Act establishes that "no decision that produces an adverse legal effect on a person may be taken based solely on the output of the real-time RBI system" (Art. 5(3)).

[45] Specifically, we refer to post-RBI, non-prohibited biometric categorisation systems and AI biometric systems (and FRTs) aimed to infer emotions for medical or safety purposes (see V.L. Raposo, *Facial Recognition AI Technology in Healthcare and the Law*, in B. Solaiman, I.G. Cohen (eds), *Research Handbook on Health, AI and the Law*, Cheltenham, 41 ff. (2024)), systems covered by Annex III, points 2 to 8 (including a list of high-risk AI systems, according to their uses). Moreover, as noted by L. Escajedo San-Epifanio, *Biometric Recognition in the AI Act: Exemptions, Prohibitions and High-Risks Specialities*, in D.U. Galetta, L. Hueso Cotino (eds), *The European Union Artificial Intelligence Act*, quot., 187, "on the basis of Art. 111 AIA with the addition of Annex X, a specific statute is foreseen for a set of biometric recognition practices which are used in the field of large-scale IT systems established by EU legislation in law enforcement and border control matters. (..) A systematic interpretation of the AIA brings to light a set of biometric recognition systems which, because of the little or no attention they receive in the AIA, seem to be outside its scope or at least in doubt". For these systems, primarily used for border control, the deadline for ensuring compliance with the AI Act is extended until 31 December 2030. This provides a significant amount of time to implement the required safeguards, with potential implications for the fundamental rights of migrants. It is also worth highlighting that in the European Commission *Guidelines on prohibited artificial intelligence practices*, it has been clarified that "most AI systems that fall under an exception from a prohibition listed in Article 5 AI Act will qualify as high-risk" (para. 501).

[46] For an in-depth analysis, see the books indicated *supra* footnote n. 28; see also X. Tracol, *The Use of FRTs by Law Enforcement Authorities in the US and the EU: Towards a Convergence on Regulation?*, in 15 *Tech & Regulation*, 312 (2025).

or convicted of having committed a criminal offence". Emphasis on the *targeted* character of the search is further reinforced by the prohibition against using post-RBI "without any link to a criminal offence, a criminal proceeding, a genuine and present or genuine and foreseeable threat of a criminal offence, or the search for a specific missing person". As Recital 95 underlines, the intrusive nature of such technologies excludes their use for indiscriminate surveillance or as a means to circumvent the strict conditions that govern real-time RBI[47].

The intricate regulatory framework outlined above, distinguishing different categories of FRTs according to their purposes, field of application, technical features and presumed level of intrusiveness, mirrors the contentious political debate surrounding these technologies. FRTs were in fact among the most disputed AI systems during the legislative process of the AI Act[48], where provisions on biometric technologies underwent multiple revisions reflecting divergent positions among EU Institutions[49].

As a result of political compromise and the inherently controversial nature of FRTs, the final text of the AI Act leaves room for criticism.

Specifically, the broad use of exceptions – particularly regarding real-time RBI for law enforcement – risks neutralizing the effectiveness of existing prohibitions[50]. Interpreted expansively, vaguely worded exemptions can even lead to a "dangerous expansion of [RBI] deployment"[51]. As well, the role of national legislators in disciplining sensitive regulatory

[47] The analysed provision also repeats the necessity for: (i) a documented use of such technologies, with information made available to market surveillance authorities and DPAs upon requests; (ii) a specific obligation for deployers to submit annual reports to those authorities; (iii) a prohibition to negatively affect a person solely on the basis of the post-RBI systems' outputs; (iv) a possibility for Member States to introduce more restrictive laws on the use of such technology. The only exceptional case in which the prior authorisation is not required occurs when post-RBI systems are used "for the initial identification of a potential suspect based on objective and verifiable facts directly linked to the offence" (Art. 26(10)).

[48] F. Palmiotto, *The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation*, in 16 Eur J of Risk Reg, 770 ff. (2025); G. Volpicelli, *Forget ChatGPT: Facial Recognition Emerges as AI Rulebook's Make-or-Break Issue*, in Politico, 14 June 2023, https://www.politico.eu/article/facial-recognition-artificial-intelligence-act-ai-issue-european-parliament/ (last visited Sept. 25, 2025).

[49] See the European Parliament Resolution of 6 October 2021, *supra* footnote n. 27 and R.J. Neuwirth, *Prohibited Artificial Intelligence Practices Revisited*, in V.L. Raposo (ed), *The European Artificial Intelligence Act. Promises and Perils?*, Cham, 131 ff. (2025).

[50] It is also worth underlining that, according to Recital 38, the "use (of real-time RBI systems) for purposes other than law enforcement should not be subject to the requirement of an authorisation". On this point see G.M. Diaz Gonzalez, *Prohibited Artificial Intelligence Practices*, in A.J. Huergo Lora (ed), *The EU Regulation on Artificial Intelligence. A Commentary*, Milan, 37 ff. (2025).

[51] A. Giannini, S. Tas, *Much Ado About Nothing? AI Act and the Prohibition of Real-Time Biometric Identification*, in Verfblog, 10 December 2024; similarly underlining critical aspects and issues in the current AI Act discipline, see N. Nikolinakos, *EU Policy and Legal Frameworks for Artificial Intelligence, Robotics and Related Technologies – The AI Act*, Cham, 388 (2023); R.J. Neuwrith, *Prohibited AI Practices in the Proposed EU AIA*, in 48 Comp L & Sec Rev, 1 ff. (2023); N. Lynch, *Facial Recognition Technology in Policing and Security – Case Studies in Regulation*, in 13 Laws 1 (2024); W. Gasparri, F. Tesi, *Artificial Intelligence and AI Act: From the Individual to the Algorithm?*, in 59 Zbornik Radova, 297 (2025); I. Barkane, L. Buka, *Prohibited AI Surveillance Practices in the AI Act: Promises and Pitfalls in Protecting Fundamental Rights*, in V. Galis, H.O.I. Gundhus, A. Vradis (eds), *Critical Perspectives on Predictive Policing*, Cheltenham, 127 ff. (2025); L. Escajedo San-Epifanio, *Biometric Recognition in the AI Act*, quot.; N. Menendez Gonzalez, G. Mobilio, *Between Prohibited Risks and High Risk*, quot.; M. Durovic, T. Corno, *The Privacy of Emotions: From the GDPR to the AI Act, an Overview of Emotional AI Regulation and the Protection of Privacy and Personal Data*, in M. Ebers, K. Sein (eds), *Privacy, Data Protection and Data-Driven Technologies*, quot., 368 ff.; F. Paolucci, *Enhancing Oversight and Addressing Gaps: Assessing the Impact of the AI Act on Biometric Identification Systems*, in N. Menendez Gonzalez, G. Mobilio (eds), *Next Democratic Frontiers for Facial Recognition Technology (FRT)*, quot., 71 ff. Vague definitions and potential implementation issues have been identified also with regards to the discipline and requirements established for high-risks AI systems (e.g. the

aspects such as authorization procedures and competent authorities further increases the risk of fragmentation among Member States[52].

In this context, the scope of application of the AI Act adds another layer of complexity. Art. 2(3) excludes areas outside EU law and preserves Member States competence in matters of national security, irrespective of the entities entrusted with related tasks. This provision revives a longstanding and contentious issue in CJEU case law[53]: the blurred boundary between law enforcement and national security. This distinction is often seen as unclear, raising risks of confusion over security purposes and responsible authorities[54].

Similar concerns arise from the Act's internal definitions and categorizations. The separation between verification and identification systems, as well as the different risk levels attributed to real-time and post-RBI, have been questioned by scholars who doubt the accuracy of such binary distinctions and the reliability of the resulting risk assessment[55].

In conclusion, the AI Act marks a bold and unprecedented attempt to establish a comprehensive, harmonized framework for FRTs, banning uses deemed unacceptable or excessively risky for fundamental rights due to their potential for creating a scenario of pervasive surveillance. Yet the above analysis reveals a mixed picture. The strong prohibition widely advocated by NGOs and civil society has not materialized: FRTs remain permissible in several contexts, subject to specific rules and safeguards. This is particularly evident in the security domain, where post-RBI systems are allowed and exemptions enable certain uses of real-time RBI.

The true impact of the Act will depend on its implementation – both by national legislators and within existing EU[56] and domestic regulatory frameworks[57] – as well as on how private

conditions imposed by Art. 26(10) seem quite vague and unclear—for example the distinction between targeted and untargeted investigations, or the definition of "objective and verifiable facts". As S. Wachter, *Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond*, in 26 *Yale J of Law & Tech* 672 ff. (3, 2024), affirmed, more generally, "strong lobbying efforts of big tech companies and member states were unfortunately able to water down much of the AIA. An overreliance on self-regulation, self-certification, weak oversight and investigatory mechanisms, and far-reaching exceptions for both the public and private sectors are the product of this lobbying", 672.

[52] As underlined by the recalled *Guidelines* provided by the European Commission, "only a domestic Member State law that fulfils, in particular, the requirements in Art. 5(2-7) AI Act, can allow the use of real-time RBI, as provided by Art. 5(2)" (para. 326). In the absence of such national provisions, the use of the systems under analysis must be therefore considered prohibited as of 2 February 2025, according to the timeline established by Article 113, AI Act.

[53] i.e. CJEU (Grand Chamber), C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others,* 6 October 2020; on this point, see M. Zalnieriute, *A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union*, in 1 The Modern L Rev, 198 ff. (2022).

[54] On this open and still highly discussed aspect, recently (re)emerged with regards to the data retention regime, see E. Celeste, G. Formici, *Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism, and Legislative Inertia*, 25 Germ L J, 427 ff. (2024).

[55] B. Sumer, *The AI Act's Exclusion of Biometric Verification: Minimal Risk by Design and Default?*, in 2 EDPL Rev, 150 ff. (2024).

[56] In several cases, the AI Act expressly recall the other data protection legal frameworks, in particular the GDPR and LED. With regards to real-time RBI, it is stated that the AI Act provisions should apply as "lex specialis in respect to the rules on the processing of biometric data contained in Art. 10 of LED" (Recital 38). See G. Mobilio, *Your Face Is Not New to Me*, quot.; R. Soares Pereira, *Remarks on the Use of Biometric Data Systems (and FRTs) for Law Enforcement Purposes: Security Implications of the Proposal for an EU Regulation on AI*, in D. Vicente *et al* (eds), *The Legal Challenges of the Fourth Industrial Revolution*, Cham, 208 ff. (2023).

[57] i.e. the Italian Legislative Decree no. 139 of 8 October 2021, converted in Law no. 205 of 3 December 2021 introducing a moratorium on the installation of video surveillance systems incorporating FRTs in public spaces or areas open to public (the term of the moratorium has been extended until 31 December 2025, by Art. 8-ter, Law no. 87 of 3 July 2023). On the legislative national interventions on the topic, see also N. Menendez Gonzalez, G. Mobilio, *Between Prohibited Risks and High Risk: The Regulation of FRT*, quot.

operators fulfil the significant compliance obligations attached to high-risk systems. These factors will be decisive in shaping the effectiveness and practical consequences of the AI Act for the future development of FRTs.

III. 'My Tearless Retina Takes Pictures that Can Prove' – Facial Recognition Technologies in the USA: A Fragmented Regulatory Landscape

While the EU struggled to establish a comprehensive framework for biometric data and AI-based biometric systems, leaving space for further development by Member States, the US approach to FRTs is complex, fragmented and multilayered. This Section briefly examines the major regulatory experiences across different levels of governance, highlighting the general landscape, ongoing normative discussions and emerging regulatory trends.

At federal level, no comprehensive federal regulatory framework currently governs biometric data[58] or directly addresses the deployment of FRTs, despite widespread use of biometric technologies by private and public entities[59].

Considering the congressional activity, the debate is still unsettled: various proposals have been introduced, yet none have resulted in enacted legislation. Notable examples include the 2020 *Ethical Use of Facial Recognition Act* that proposed "prohibit(ing) any officer, employee, or contractor of a federal agency from engaging in specified activities with respect to FRT without a warrant until a congressional commission established by this bill recommends rules governing the use and limitations on both government and commercial use of such technology"[60]. In 2022, the *Facial Recognition Act*, designed to restrict use of FRTs by law enforcement agencies, proposed the adoption of transparency measures, annual assessments and required to limit the use of this technology to situations when "a warrant is obtained that shows probable cause that an individual committed a serious violent felony"[61]. The *Facial Recognition and Biometric Technology Moratorium Act of 2023* went further, advocating to prohibit or limit the use of biometric surveillance systems, including

[58] General rules concerning the collection, storage and processing of personal information, also including face images, by federal agencies can be identified in the Privacy Act of 1974 (P.L. 93-579, 88 Stat 1896 (1974)) and in the E-Government Act of 2002 (P.L. 107-347, 116 Statt 2899 (2002)). Nonetheless, as underlined by the Congressional Research Service, *FRT and Law Enforcement: Select Constitutional Considerations*, 2020, "neither act directly addresses FRT or the reliability of algorithms employed to compare compiled photographs", 9. The document also lists applicable but very sectorial and limited federal laws disciplining the collection, use and storage of personal information by private entities (i.e. Driver's Privacy Protection Act or Family Educational Rights and Privacy Act), which may apply to the use of FRTs as well. Still, in C. N. Wright, *Facial Recognition Technology: Federal Agencies' Use and related Privacy Protections*, US Government Accountability Office, 2022, it is highlighted the absence of "federal laws that expressly regulate commercial uses of FRT in particular".

[59] On the vast use of FRTs in the US, see the data provided in US Commission on Civil Rights, *Annual Statutory Enforcement Report on the Civil Rights Implications of the Federal Use of FRTs*, 19 September 2024; M.A. Bigos, *Let's "Face" It: FRT, Police Surveillance, and the Constitution*, in 22 J. High Tech. L., 2021, 52 ff.; Congressional Research Service, *Federal Law Enforcement Use of FRT*, 27 October 2020.

[60] S.3284 - 116th Congress (2019-2020).

[61] H.R.9061 - 117th Congress (2021-2022). On the purposes of this proposal, see https://lieu.house.gov/media-center/press-releases/reps-ted-lieu-sheila-jackson-lee-yvette-clarke-and-jimmy-gomez-introduce (last visited Sept. 25, 2025). On FRTs and the concept of "probable cause", see T.J. Benedict, *The Computer Got It Wrong: FRT and Establishing Probable Cause to Arrest*, in 79 Wash. & Lee L. Rev., 849 ff. (2022).

FRTs, at federal, state and local government levels, while establishing the need for specific legislative intervention by Congress disciplining the use of such technologies[62].
Bill H.R. 3782 of June 2025 intends to prevent federal agencies from using FRT "as a means of identity verification"[63]; the prospects of this initiative remain uncertain, particularly given the persistent lack of bipartisan consensus on the matter, as was the case with previous proposals[64].
In the absence of federal legislation, two main areas of intervention have shaped the debate: initiatives of the executive branch and self-regulation or internal policies adopted by federal agencies.
With regard to executive action directly or indirectly affecting the implementation of FRTs, a relevant measure can be identified in the Executive Order (EO) 14074 of 25 May 2022, issued by President Biden and titled *Advancing Effective Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety*. Among other provisions, Section 13(e) mandated the Department of Homeland Security (DHS), the Department of Justice (DOJ) and the White House Office of Science and Technology Policy (OSPT) to evaluate the impact of biometric technologies on privacy, civil liberties and rights, and to "lead an interagency process regarding the use by Law Enforcement Agencies of FRT and other technologies using biometric information". The resulting report, released in December 2024, set out best practices and guidelines for law enforcement agencies[65], while the DOJ tasked the National Academy of Sciences (NAS) with preparing a dedicated study on the implementation of AI-based biometric technologies[66]. While its outcomes in the field of FRTs were confined to reports and soft law guidance centred on accuracy, standards development and anti-discrimination measures, the EO nonetheless played an important role in highlighting the risks and challenges of FRTs and in encouraging debate on appropriate safeguards[67].
Subsequent initiatives, such as the *Blueprint for an AI Bill of rights*[68] and EO 14110 of 30 October 2023, titled *Safe, Secure and Trustworthy development and use of AI*, established

[62] S.681 - 118th Congress (2023-2024).
[63] H.R.3782 - *To prohibit the Federal Government from using facial recognition technology as a means of identity verification, and for other purposes* - 119th Congress (2025-2026). The proposal, only recently submitted, is still at the initial stage of the legislative process. Introduced by Republican Andrew Ogles, it has now been referred to the House Oversight and Government Reform Committee. The text defines FRTs as "contemporary security system that automatically identifies and verifies the identity of an individual from a digital image or video frame".
[64] US Commission on Civil Rights, *Annual Statutory Enforcement Report*, quot. includes references to various other proposed federal legislations, especially 89 ff.
[65] US DHS, DOJ, OSTP, *Biometric Technology Report*, December 2024.
[66] National Academies of Sciences, Engineering and Medicine, *FRT: Current Capabilities, Future Prospects, and Governance*, The National Academies Press (2024). This document interestingly provides several recommendations, also prompting the adoption of an EO "on the development of guidelines for the appropriate use of FRT by federal departments and agencies and addressing equity concerns and the protection of privacy and civil liberties" from both private and public actors. It additionally underlines that "in light of the fact that FRT has the potential for mass surveillance of the population, courts and legislatures will need to consider the implications for constitutional protections related to surveillance, such as due process and search and seizure thresholds and free speech and assembly rights", 129.
[67] On the EO, more generally, see C. Sbailò, *Governing Artificial Intelligence: Technological Leadership and Regulatory Challenges in an Era of Exponential Growth*, in *DPCE Online*, 67(SP 3), 275 ff. (2024).
[68] *Blueprint for an AI Bill of Rights. Making Automated Systems Work for the American People*, October 2022, https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/ (last visited Sept. 25, 2025). On this set of guidelines, elaborated by the White House Office of Science and Technology Policies, see E. Hine, L. Floridi, *The Blueprint for an AI Bill of Rights: In Search of Enaction, at Risk of Inaction*, in *Minds and Machines*, 1 ff. (2023).

additional general principles and best practices applicable to AI systems[69], and therefore also to FRTs. In particular, EO 14110 instructed "over 50 federal entities to engage in more than 100 specific actions to implement the guidance set forth across eight overarching policy areas", including measures to address algorithmic discrimination[70]. Importantly, these principles and requirements extended not only to public entities but also to private actors[71].

This ambitious framework was nonetheless superseded by President Trump's approach to AI governance[72]. Although the Trump Administration has so far paid limited attention to regulating FRTs, it has outlined a broader direction for the development and implementation of AI in the EO 14179 of 23 January 2025, *Removing Barriers to American Leadership in Artificial Intelligence*, issued with the declared aim of unleashing AI potential, particularly from an economic perspective. The EO emphasized AI as a national security imperative to achieve and maintain global tech dominance. Consistent with this vision, it adopted a deregulatory approach intended to stimulate industry growth, while criticizing the Biden-era EOs for imposing what has been described as an excessive burden on the private sector[73]. Aligned with this deregulatory orientation, the House of Representatives initially included a 10-year moratorium on state and local governments regulations of AI in the *One Big Beautiful Bill of* 2025[74]. Although this clause was ultimately removed for lack of majority support, thereby preserving the possibility for states to legislate in the field of AI governance, and by extension FRTs, its rationale was clearly to avoid regulatory fragmentation that could limit and harness private initiative in this key sector[75].

---

[69] On the President Biden approach to AI governance, see also N.A. Smuha, *Biden, Bletchley, and the Emerging International Law of AI*, in VerfBlog, 11 November 2023; M. Bassini, *The Global Race to Regulate AI: Biden's Executive Order Spillover Effects on the EU AI Act*, in IEP@BU, 1 December 2023, https://iep.unibocconi.eu/publications/global-race-regulate-ai-bidens-executive-order-spillover-effects-eu-ai-act (last visited Sept. 25, 2025); M. Worsdorfer, *Biden's Executive Order on AI and the EU's AI Act: A Comparative Computer-Ethical Analysis*, in 37 *Phil & Tech*, 74 (2024) (and https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4874592, last visited Sept. 25, 2025).

[70] On the requirements and timeline established by the EO 14110, see Congressional Research Service, *Highlights of the 2023 Executive Order on Artificial Intelligence for Congress*, updated 3 April 2024, https://www.congress.gov/crs_external_products/R/PDF/R47843/R47843.8.pdf (last visited Sept. 25, 2025).

[71] The Office of Management and Budget issued in March 2024 a *Memorandum for the Heads of Executive Departments and Agencies "Advancing Governance, Innovation, and Risk Management for Agency Use of AI"*: this document represents a guidance establishing specific requirements for AI governance, including practices such as AI impact assessment, test of AI performance in a real-world context, monitoring, adequate human training, public notice etc.

[72] In the *Initial Rescissions of Harmful Executive Orders and Actions*, 20 January 2025, https://www.whitehouse.gov/presidential-actions/2025/01/initial-rescissions-of-harmful-executive-orders-and-actions/ (last visited Sept. 25, 2025), President Trump revoked EO 14110. Consequently, all Agencies are required to "suspend, revise or rescind" all the interventions and actions linked or implementing the Biden EO.

[73] In the EO it is stressed that "certain existing AI policies and directives acts as barriers to American AI innovation" (Sec. 1). More vastly, on the President Trump Administration approach to AI, see V. Lubello, *From Biden to Trump: Divergent and Convergent Policies in the Artificial Intelligence (AI) Summer*, in *DPCE Online*, 1, 2025, 49 ff.; C. Novelli, A. Gaur, L. Floridi, *Two Futures of AI Regulation under the Trump Administration*, 31 March 2025, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5198926 (last visited Sept. 25, 2025).

[74] P. L. 119-21 (2025).

[75] That provision would have therefore led to federal dominance in the field of AI, possibly creating tensions between different levels of AI governance initiatives. On this aspect, see Congressional Research Service, *Regulating Artificial Intelligence: U.S. and International Approaches and Considerations for Congress*, 4 June 2025, https://www.congress.gov/crs_external_products/R/PDF/R48555/R48555.4.pdf (last visited Sept. 25, 2025); C. Novelli, A. Gaur, L. Floridi, *Two Futures of AI Regulation under the Trump Administration*, quot.,

In this broad scenario, where the prospect of federal rules governing FRTs remains uncertain[76], various federal agencies and executive bodies have gradually adopted self-regulatory measures, policies and best practices on AI, and more specifically on FRTs. Focusing on consumer protection, the Federal Trade Commission has issued guidelines addressing privacy risks linked to FRTs since 2012[77]. Since 2017, the National Institute of Technology and Standards (NIST)[78] has developed standards for the accuracy of FRTs and launched the *Face Recognition Vendor Testing Program*, which evaluates algorithmic performance in one-to-one and one-to-many systems[79]. More recently, various agencies have adopted interim policies[80], such as DHS Directive No. 026-11 (2023), *Use of FR and Face Capture Technologies*[81]. This directive requires independent testing of deployed systems, opt-out and alternative processing options and prohibits exclusive reliance on FRT outputs in law or civil enforcement actions, mandating manual review of results. While these non-legislative governance solutions introduce important principles and guarantees, they also contribute to an increasingly fragmented landscape.

Given this evolving federal framework, state and local governments are likewise adopting significant regulatory measures. While several states have enacted biometric data laws, notably the Illinois *Biometric Information Privacy Act* (BIPA) of 2008[82], some state and local

discussing the possible federal intervention in the field of AI governance through "pre-emption" of state law, based on the Supremacy Clause (Federal US Constitution, Art. VI, Clause 2). See also D.J. Mallinson *et al*, *Artificial Intelligence Policy, the Trump Administration, and Federalism*, in 47 Admin Theory & Praxis, 202 ff. (3, 2035). This issue and in particular the need to ensure a national policy framework for AI, avoiding fragmentation resulting from divergent state-level interventions, has been at the centre of the recent Executive Order 14365 of 11 December 2025, adopted by President Trump (see *infra* footnote n. 109 for more details).

[76] Other areas of intervention able to also impact on FRTs are the immigration agenda, currently characterized by an attempt to expand biometric data collection, and the large language models discipline; in this field, and more generally on provisions concerning accuracy of AI outputs, President Trump intervened with EO 14319 *Preventing Woke AI in the Federal Government* of 23 July 2025, affirming the need to "ensure that artificial intelligence (AI) models procured by the Federal government prioritize truthfulness and ideological neutrality" and consequently to protect "Americans from biased AI outputs driven by ideologies like diversity, equity, and inclusion (DEI) at the cost of accuracy" (see Fact Sheet https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-president-donald-j-trump-prevents-woke-ai-in-the-federal-government/, last visited Sept. 25, 2025).

[77] Federal Trade Commission, *Facing Facts: Best Practices for Common Uses of FRTs*, 22 October 2012. On the non-binding nature of such provisions as well as for an in-depth analysis of the Federal Trade Commission's actions, based on general consumer protection law principles and affecting private companies producing or applying FR software, see M. Filder, J. Hurwitz, *An Overview of FRT Regulation in the United States*, in R. Matulionyte, M. Zalnieriute (eds), *The Cambridge Handbook of Facial Recognition in the Modern State*, quot, 219 ff.

[78] The NIST is a non-regulatory federal agency, part of the US Department of Commerce, with the mission of "promoting US innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life".

[79] This test, periodically revised and updated, sets fundamental benchmarks for industries active in the field of FRTs.

[80] Other federal authorities and agencies adopting internal policies on the implementation and use of FRTs are listed in US DHS, DOJ, OSTP, *Biometric Technology Report*, quot. It is possible to mention DOJ's *Interim Policy and Safeguards for FRT Acquisition and Use*, elaborated in 2023 by the FRT Working Group; Federal Bureau of Investigation's (FBI) *FRT Use Policy Directive* of 2023. Both these policies prohibit the use of results coming from the implementation of FRTs "as the sole basis for enforcement action. Instead, FRT results generate investigative leads that require further investigation to substantiate or invalidate those leads", US Commission on Civil Rights, *Annual Statutory Enforcement Report*, quot., 43.

[81] This Directive covers all use cases of FRTs, not only law enforcement purposes. For more information, see US DHS, DOJ, OSTP, *Biometric Technology Report*, quot., especially 23 ff.

[82] BIPA § 20, 740 Ill. Comp. Stat. 14/20 (2008). This important and innovative law (for its time and within the US context) established rules governing the collection, use, safeguarding, storage, handling, retention and destruction of biometric identifiers and information for commercial purposes. The Act has also

governments have gone further, adopting rules specifically addressing the deployment of FRTs. These regulatory responses may be classified in three categories[83]: outright bans, temporary moratoria and more nuanced normative frameworks. A recent trend marks a transition from comprehensive bans to more targeted legislation, authorizing use of FRTs for specific purposes, predominantly in the field of law enforcement, while simultaneously introducing safeguards and limitations[84].

Without attempting to cover the entire US landscape, it can be said that some regulatory initiatives stand out by virtue of their significance and rationale. In 2019, San Francisco became the first US city to ban use of FRTs by municipal authorities[85], including the Police Department. This strict measure—grounded in concerns over accuracy, discrimination and human rights—was soon replicated by other city councils, often drawing on the American Civil Liberties Union's (ACLU) model bill[86].

In recent years, however, several jurisdictions have reconsidered the scope and effectiveness of such bans and moratoria: Portland, for instance, adopted a resolution in 2023 that could limit its initial prohibition of 2020[87]. A similar trend is evident in New Orleans, where the 2020 ban was then replaced with a framework permitting use in specific cases (i.e. investigation of violent crimes), subject to prior permission by a superior[88]. States such as Virginia[89], Vermont and California have followed comparable paths: Vermont, the first state to ban FRT for law enforcement, has since introduced exceptions for certain

influenced the implementation of FRTs and served as foundation for significant legal actions, such as *American Civil Liberties Union et al. v. Clearview AI Inc.* before the Circuit Court of Cook County. Under the settlement concluding that case in 2022, the company was prohibited from selling its facial surveillance databases to private entities and was required to allow Illinois residents to request the blocking and deletion of their facial data from Clearview's system (for details and legal documents, see https://www.aclu.org/cases/aclu-v-clearview-ai, last visited Sept. 25, 2025). The BIPA and its underlying principles have also inspired the development of biometric data regulatory frameworks in several other states, such as California (Civil Code 1798.100-1798.199), Texas (Tex. Bus. & Com. Code 503-001), Washington (Wash. Rev. Code 19.375.010-19.375.900). In California, the California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100] also sets some specific obligations and requirements for processing of biometric data. H. Corbit, *Face Value: A Proposal for Federal Regulation of FRT Companies*, in 52 Stetson L. Rev., 779 ff. (2023); C. Sobczak, *BIPA and Article III Standing: Are Notice and Consent More than Bare Procedural Rights?*, in 35 Berkley Technical L. J., 1391 ff. (2020).

[83] C. Rabinowicz, *Approaches to Regulating Government Use of FRT*, in Harvard J of Law & Tech, 4 May 2023.

[84] *Ibid.*; see also X. Tracol, *The Use of FRTs by Law Enforcement Authorities in the US and the EU*, quot.; US Commission on Civil Rights, *Annual Statutory Enforcement Report*, quot.

[85] *Stop Secret Surveillance Ordinance*, 190110 – Leg Ver3 of 6 May 2019.

[86] According to the US Commission on Civil Rights, *Annual Statutory Enforcement Report*, quot., "as of 2023, at least 22 local governments have adopted surveillance technology regulations using the ACLU model as template", 88. The model is based on the campaign *Community Control Over Police Surveillance* (CCOPS) that imposes City Council consent and active role in case police intends to buy new surveillance technologies.

[87] Ordinance adopted by the City Council of Portland (Oregon), on 9 September 2020, banning FRTs "for City Bureaus and in places of public accommodations when owned by private entities". The subsequent *Portland City Council Surveillance Technologies Resolution* has been considered as an "overall policy resolution, reconsidering the initial ban" (as affirmed by X. Tracol, *The Use of FRTs by Law Enforcement Authorities in the US and the EU*, quot., 297).

[88] Ordinance City of New Orleans, 21 July, 2022; see also US Commission on Civil Rights, *Annual Statutory Enforcement Report*, quot., 32. On recent developments, aimed at expanding the use of real-time FRTs, see ACLU, *ACLU and ACLU of Louisiana Sound Alarm on New Orleans Police Department's Secret Use of Real-Time Facial Recognition*, 19 May 2025, https://www.aclu.org/press-releases/208236 (last visited Sept. 25, 2025).

[89] A. Powers, K. Simon, J. Spivack, *From Ban to Approval: What Virginia's FRT Law Gets Wrong*, in 26 Rich. Pub. Int. L. Rev., 155 ff. (1, 2022). While in 2021 the use of FRTs by local law enforcement and campus police was prevented, in 2022 a law was adopted to allow this technology in specific situations, imposing safeguards such as an accuracy score of at least 98% based on the NIST standards. The 2022 law has been criticised by the Authors as not able to adequately address the unique risks FRTs pose.

crime-prevention purposes under specific safeguards[90]; California enacted a three-year moratorium in 2019 on the use of FRT in body-worn camera footage, but since it expired on 1 January 2023, the implementation of a new regulatory framework is still to be discussed[91].

Several other states have recently introduced targeted regulations with specific safeguards to address the risks of FRTs. In Massachusetts, for example, a written request to the State Police or the FBI is mandatory to use FRTs in certain criminal cases[92], whereas a Colorado Bill imposes notification, accountability reporting, human oversight and a motivated justification for each deployment[93]. Additional safeguards include the requirement of a warrant or court order[94], limiting implementation of FRTs to certain crimes[95], establishing "probable cause to believe an unidentified person in an image committed a serious crime" and prohibiting reliance on FRT results as the sole basis for arrest or search[96].

Similar requirements and conditions have been established through self-regulating polices: in Detroit, wrongful arrests prompted the Police Department to revise FRT policies, explicitly prohibiting them as the sole justification for arrest[97].

Thus, regulatory efforts in the US have been made at multiple levels of governance, reflecting different approaches and ongoing debate[98]. In the resulting complex and fragmented landscape, moratoria and bans coexist with targeted regulations permitting use

[90] 2020 Vermont Acts and Resolves 799 Section 14.

[91] California Assembly Bill 1215, 8 October 2019. In recent times, AB 1814 failed to be approved.

[92] Massachusetts General Law – Part. I, Title II, Chapter 6, Section 220.

[93] Colorado Senate Bill 113 of 8 June 2022. See https://leg.colorado.gov/bills/sb22-113 (last visited Sept. 25, 2025).

[94] As required, for instance, by the Washington Senate Bill 6280 of 31 March 2020.

[95] See Utah Code of Criminal Procedure, Chapter 23e, *Government Use of FRT*, effective from 5 May 2021.

[96] Similarly to what established by the state of Maine, in Title 25 (*Internal Security and Public Safety*), § 6001, Part 14, Chapter 701 (*Facial Surveillance*).

[97] See Detroit Police Department Directive 307.5 on *Facial Recognition*. On the specific case, involving Robert Williams, see ACLU, *Civil Rights Advocates Achieve the Nation's Strongest Police Department Policy on FRT. Press Release*, 28 June 2024. In Miami, Police Department voluntarily adopted FRTs policies, also coordinating with civic organisations and privacy advocates, as reported by the US Commission on Civil Rights, *Annual Statutory Enforcement Report*, quot., 89. Similar examples can be identified in X. Tracol, *The Use of FRTs by Law Enforcement Authorities in the US and the EU*, quot.

[98] For a broader picture of states and local governments measures on FRTs, see J. Laperruque, *Status of State Laws on Facial Recognition Surveillance: Continued Progress and Smart Innovations*, in Tech.Policy Press, 6 January 2025, https://www.techpolicy.press/status-of-state-laws-on-facial-recognition-surveillance-continued-progress-and-smart-innovations/ (last visited Sept. 25, 2025). Although this paper excludes such issues from its scope for reasons of space, it is worth noting that the absence of robust and comprehensive legislative safeguards at the federal level leaves room for debates on the compatibility of FRTs with several federal constitutional provisions. For instance, applying Fourth Amendment protections against unreasonable searches and seizures to FRTs raises complex questions about the continued relevance of the so-called Third Party Doctrine and the reasonable expectation of privacy in public spaces. Similar concerns arise under the Sixth Amendment Confrontation Clause, which guarantees defendants the right to confront and cross-examine witnesses in criminal proceedings, as well as under the Fourteenth Amendment requirement that prosecutors disclose all evidence. On this latter point, an illustrative case is *State v. Arteaga*, 476 N.J. Super. 36, para. 61 (App. Div. 2023), where the Superior Court of New Jersey held that the government has a duty to disclose details about the FRTs employed and their role in the identification of the suspect. On these highly articulated and delicate aspects, see US Commission on Civil Rights, *Annual Statutory Enforcement Report*, quot., 16 ff.; Congressional Research Service, *FRT and Law Enforcement*, quot.; M. Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of FRT*, in 49 Conn. L. Rev., 1591 ff. (2017); S. Nakar, D. Greenbaum, *Now You See Me, Now You Still Do: FRT and the Growing Lack of Privacy*, in 23 B.U. J. Sci. & Tech. L, 93 ff. (88, 2017); M. Simonitis, *FRT and the Constitution*, in 2 Notre Dame J on Emerging Tech, 357 (2, 2021); A.G. Ferguson, *Facial Recognition and the Fourth Amendment*, in 105 Minn. L. Rev., 1105 ff. (3, 2021); E. Ringel, A. Reid, *Regulating FRT: A Taxonomy of Regulatory Schemata and First Amendment Challenges*, in 28 Comm L & Pol, 3 ff. (1, 2023).

of FRTs under specific conditions, particularly in the public security domain. Voluntary schemes, policies, guidelines and self-regulatory initiatives further complicate the picture. While the fate of the federal legislative proposals remains uncertain, states and local government continue to implement rules aimed at setting limits and imposing safeguards on what is increasingly seen as an invasive technology. It remains to be seen if these measures and requirements could be considered as adequate and proportionate and, consequently, in what way FRTs will ultimately be deemed admissible[99], as well as how recent federal moves towards deregulation will influence the multi-level regulatory measures.

IV. 'I Am Protected Electric Eye' - Different Regulatory Approaches, Similar Challenges: Constitutional Principles in the AI Surveillance Society

As emerged from the previous Sections, the regulation of FRTs in the EU and US is a complex challenge. Although Court action is still limited – in the EU, Data Protection Authorities' measures played a prominent role –, the legislative action recorded on both sides of the Atlantic is quite significant. Considering the peculiarities of the two legal systems[100], there are divergencies and convergencies in the regulatory efforts put in place.
In the EU, a comprehensive approach has been adopted, addressing AI systems as a whole with a focus on fundamental rights through strong and rigorous risk assessment evaluations. In the AI Act, specific provisions dedicated to biometric identification systems and specifically to RBI systems are included; also in terms of potential purposes, this Regulation covers different possibilities of FRT use in fields ranging from law enforcement to health and schools.
In the US, notwithstanding some policies and standards have been set by several federal agencies, states and local government have been more active in regulating FRTs, establishing rules on biometric data collection, retention and processing, as well as explicit implementation of FRTs by private and public entities.
Fragmentation of biometric data protection rules and provisions concerning FRTs *per se* is immediately evident in the US context, due to lack of federal and particularly Congressional intervention so far. In the EU, some level of fragmentation couldn't also

[99] On the need for an "adaptive legal framework" and on the delicate balance between investigative advancements and civil liberties, see P.N. Schuetz, *Fly in the Face of Bias: Algorithmic Bias in Law Enforcement's FRT and the Need for an Adaptive Legal Framework*, in 39 Minn. J. L. & Ineq., 221 ff. (1, 2021); S. Chun, *FRT: A Call for the Creation of a Framework Combining Government Regulation and a Commitment to Corporate Responsibility*, in 21 N.C. J.L. & Tech., 99 ff. (4, 2020). On the need for a legislative intervention of the Congress, also transposing federal agencies policies in binding laws, see J. Zens, *Face It: Only Congress Can Preserve Privacy from the Pervasive Use of Facial Recognition Technology by Police*, in 58 San Diego L. Rev., 143 ff. (1, 2021).

[100] The lack of federal comprehensive laws on data protection – only partly compensated by state's data protection provisions – is one of the relevant aspects differentiating the US and EU regulatory approach towards data protection and new technologies; "the US approach marks (..) a significant departure from the 'regulatory anxiety' of EU lawmakers vis-à-vis disruptive technology and follows the general skepticism in the US legal culture about the role of regulation, most notably when it comes to emerging technologies and possible interferences with human rights", M. Bassini, *The Global Race to Regulate AI*, quot. See also A. Otene, *Two Becoming One: Revisiting the Two Western Cultures of Privacy in Light of Data Protection Laws*, 17 April 2024 (http://dx.doi.org/10.2139/ssrn.5017482, last visited Sept. 25, 2025), recalling the well-known paper by J.Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty,* in 113 *Yale Law J*, 1151 (2004) on the different conception of privacy and data protection on the two sides of the Atlantic. See also L. Barrett, *Ban FRT for Children-And for Everyone Else*, in 26 B. U. J. Sci. & Tech. L., 223 ff. (2, 2020). On the different approaches on AI governance, see R.B.L. Dixon, *A Principled Governance for Emerging AI Regimes: Lessons from China, the European Union, and the United States*, in AI Ethics, 793 ff. (3, 2023).

be excluded. National security exemption and room left to Member States to implement often vague and broad exceptions established by the AI Act could create an uneven landscape, especially when it comes to the use of such AI systems for security purposes. Although the AI Act establishes a stricter framework for FRTs, severely limiting real-time RBI systems for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, its effectiveness and harmonizing capacity remain uncertain. Procedural requirements, along with the designation of national authorities responsible for authorizing real-time RBI technologies for law enforcement uses, are left to national legislators. This could lead to diverging balances between the principles of necessity and proportionality protecting fundamental rights on one hand and security needs on the other. The final outcome will largely depend on how EU-level core principles are transposed into Member State laws concerning implementation of FRTs in the field of public security and on whether procedural safeguards can rationalize and "constitutionalize" the exceptional use of these technologies[101].

In the US, some states and local government, often supported by civil liberties organizations, have adopted moratoria or bans, taking a firm stance against potential or already visible impacts on fundamental rights. More recently, however, this trend has shifted toward nuanced regulatory approaches: specific requirements and limitations are gradually replacing outright prohibitions. At federal level, discussion on bans and moratoria continues, but in many cases these proposed measures serve mainly to halt implementation until Congress enacts binding legislation on allowed uses and safeguards. Despite differing approaches, we can therefore see that the two regulatory landscapes mostly allow use of these technologies under defined limits and conditions. This reflects the longstanding struggle to balance competing interests and rights, and more generally, the difficulty of fully renouncing the potential of new surveillance technologies[102].

The attempt to constitutionalize FRTs by applying constitutional values and principles[103] is still underway and debated, making the future in the EU and US difficult to predict. In the EU, much will depend on the concrete enactment of key rules and the interpretation of important principles and provisions by Member States. The coexistence of stratified regulatory frameworks will also need close monitoring, while the role of Data Protection Agencies and other AI supervisory authorities will be decisive[104]. In other words, the AI Act is a fundamental turning point but not the conclusion of the regulatory debate.

In the US, the next steps of legislative initiatives and the evolving interplay between different levels of governance must be carefully observed: the role of government agencies remains ambiguous, oscillating between policies/guidelines and the call for hard law provisions; also the trend at state and local government level seems to lead to unclear scenarios, while the lack of a uniform approach appears likely to persist, particularly considering the current polarized political debate in the US and the growing predilection for "law and order" policies and legal interventions[105].

---

[101] It is important to recall that, especially when it comes to high-risk systems, the effectiveness of AI Act safeguards and requirements will also highly depend on private actors and their compliance and concrete implementation of the AI Act obligations.

[102] C. Jasserand, *Facial Recognition in Public Spaces and the Principle of Necessity*, in N. Menendez Gonzalez, G. Mobilio (eds), *Next Democratic Frontiers for Facial Recognition Technology (FRT)*, quot., 49 ff.

[103] See, more broadly, E. Celeste, G. Formici, *Constitutionalizing Mass Surveillance in the EU*, quot.

[104] On the role of multiple national and supranational authorities empowered to enforce the AI Act, see H-W. Micklitz, G. Sartor, *Compliance and Enforcement in the AIA through AI*, in 43 Yearbook of EU Law, 2024, 297 ff.; C. Novelli *et al*, *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, in 16 Eur J of Risk Reg, 566 ff. (2, 2025).

[105] M. Filder, J. Hurwitz, *An Overview of FRT Regulation in the United States*, quot., 224.

This uncertain future is also increasingly influenced by overarching trends tied to the broader discourse on AI governance. Although the fragmented, cross-sector US approach to AI differs greatly from the holistic model promoted by the EU AI Act[106], a shared trajectory of deregulation has recently begun to emerge.

This shift is evident in President Trump's EO 14179 *Removing Barriers to American Leadership in Artificial Intelligence* of January 2025 and *America's AI Action Plan*[107], released in July 2025: both documents emphasize simplification and de-regulation as guiding principles, aiming to revoke "policies and directives that act as barriers to American AI innovation, clearing a path for the United States to act decisively to retain global leadership in AI"[108,109].

In parallel, the EU under the current Von der Leyen Commission also seems to be leaning in a de-regulatory direction[110]. Even if concrete measures remain undecided, the *Portfolio Communication on Implementation and Simplification* adopted by the European Commission as well as the Conclusions of the Council of the EU of 24 June 2025 on *Balancing Regulation and Innovation in the Technology -Driven Economy* reveal similar orientation[111]. Here,

[106] "Unlike the EU's AI Act, which provides a legally binding framework, the US adopts a decentralized, sector-specific regulatory strategy, primarily driven by voluntary commitments from private companies and guided by federal agencies. Additionally, state-level initiatives, often influenced by specific local concerns, contribute to a diverse regulatory environment", T. Davtyan, *The US Approach to AI Regulation: Federal Laws, Policies and Strategies Explained*, in 16 Case W. Res. J.L. Tech. & Internet, 223 (2, 2025).

[107] Available at https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf (last visited Sept. 25, 2025).

[108] EO 14179. As affirmed in C. Novelli, A. Gaur, L. Floridi, *Two Futures of AI Regulation under the Trump Administration*, quot., "much of the reasoning favoring deregulation is centred on innovation and ease of business, and a rights-based approach is conspicuous in its absence", 10. Biden's approach, on the contrary, was considered as establishing "unnecessary government control" and "excessively burdensome requirements for companies", Fact Sheet, *President Donald J. Trump Takes Action to Enhance America's AI Leadership*, 23 January 2025, https://www.whitehouse.gov/fact-sheets/2025/01/fact-sheet-president-donald-j-trump-takes-action-to-enhance-americas-ai-leadership/ (last visited Sept. 25, 2025).

[109] Pending the peer-review process, it is worth noting that President Trump adopted EO 14365 "Ensuring a National Policy Framework for Artificial Intelligence" on 11 December 2025, which appears to be fully consistent with the simplification and de-regulation approach characterizing the earlier EOs issued during the Trump Presidency. In particular, EO 14365 recognizes that "US AI companies must be free to innovate without cumbersome regulation. But excessive State regulation thwarts this imperative"; consequently, it establishes that "it is the policy of the United States to sustain and enhance the United States' global AI dominance through a minimally burdensome national policy framework for AI" (Sec. 2). Based on this policy, the EO attributes the Attorney General the duty to establish an "AI Litigation Task Force", "whose sole responsibility shall be to challenge State AI laws inconsistent with the [abovementioned] policy (..), including on grounds that such laws unconstitutionally regulate interstate commerce, are preempted by existing Federal regulations". The Order also introduces a mechanism of evaluation of State AI laws (Sec. 4) as well as restrictions on funding for States with onerous AI laws (Sec. 5). Moreover, Sec. 8 is dedicated to legislation and, specifically, establishes that "The Special Advisor for AI and Crypto and the Assistant to the President for Science and Technology shall jointly prepare a legislative recommendation establishing a uniform Federal policy framework for AI that preempts State AI laws that conflict with the policy set forth in this order". Even if the effects of this recent EO have yet to be fully assessed, they may impact not only on the disciplines on FRTs at the State level, but also on the broader regulatory approach to AI governance in the US, potentially giving rise to tensions between the federal Government and States.

[110] H. Ruschemeier, *The De-Regulatory Turn of the EU Commission*, in VerfBlog, 18 February 2025; R. Csernatoni, *The EU's AI Power Play: Between Deregulation and Innovation*, Carnegie Europe, 2025; L. Lazaro Cabrera, *Europe's Deregulatory Turn Puts the AI Act at Risk*, in Tech Policy.Press, 3 June 2025, https://www.techpolicy.press/europes-deregulatory-turn-puts-the-ai-act-at-risk/ (last visited Sept. 25, 2025).

[111] Pending the peer-review process, the European Commission published, on 19 November 2025, the so-called "Omnibus Package", which includes the *Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework,*

simplification increasingly risks overlapping with deregulation in the digital area, i.e. covering data protection and AI rules, making it a central element of the legislative, political – and economic – agenda, while at the same time sparking concern among digital-rights NGOs[112].

Considering these broader shifts, the future of FRTs is even more uncertain on both sides of the Atlantic and thus requires close monitoring. However, it is clear that FRTs have a canary-in-coal-mine role, exposing the risks and unprecedented challenges posed by AI.

The implementation of FRTs and their increasing use by private and governmental actors in public spaces expands surveillance, control and data-mining capacities, altering the relation between individuals and governing powers. The legislative and political debate should focus on how to promote solutions that impose rigid risk assessments and, when the risks are acceptable, establish procedural limits and safeguards, but also encourage a profound and vaster constitutionalisation process, ultimately able to ensure the guarantee of data protection and privacy as well as, more broadly, of fundamental rights, freedom and non-discrimination principle[113]. This process must be accompanied by public awareness, democratic debate and the accountability of private and public actors[114].

Ultimately, the regulation of FRTs is not just a technical and sectorial matter but a challenge intimately linked to the future of democracy and to the balance between power, surveillance and individual freedoms.

---

and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), COM/2025/837 and the *Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence* (Digital Omnibus on AI), COM/2025/836. The declared aim of these proposals – consistent with the European Commission's previously illustrated shift towards regulatory simplification – is to introduce "technical amendments to a large corpus of digital legislation, selected to bring immediate relief to businesses, public administrations, and citizens alike, and to stimulate competitiveness" (https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal, last visited Jan. 10, 2026) and, with specific reference to the AI governance, to adopt "targeted simplification measures to ensure timely, smooth, and proportionate implementation of certain of the AI Act's provisions" (https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal, last visited Jan. 10, 2026). These proposals therefore intend to amend, *inter alia*, the GDPR and the AI Act, with potential implications also for the regulation of FRTs, especially as regards rules on the processing of biometric data and obligations applicable to high-risks AI-systems. Although the proposals are still at an early stage and have already triggered lively debate (R. Mahieu, *The Ominous Omnibus: Dismantling the Right of Access to Personal Data*, in VerfBlog, 3 December 2025; B. Lazarotto, *The Data Omnibus: The Good, the Bad, and The Ugly Behind the DGA and Data Act Rewrite*, in MediaLaws – Symposium, 19 December 2025; H. Hofmann, *This Is Not Simplification: How to Simplify the Digital Acquis Without Undermining Rights*, in VerfBlog, 3 January 2026), the legislative process warrants close scrutiny, as it may determine the future trajectory of data protection and AI governance in the EU.

[112] See the *Open Joint Letter against the Delaying and Reopening of the AI Act* of 9 July 2025, https://openfuture.eu/wp-content/uploads/2025/07/250709Open-Joint-Letter-against-the-Delaying-and-Reopening-of-the-AI-Act.pdf (last visited Sept. 25, 2025), signed by numerous NGOs.

[113] A regulatory approach mainly focused on procedural safeguards has also been criticized: M. Zalnieriute, *Beyond Procedural Fetishism,* quot. Bigos considers a nationwide ban of government use of FRTs as the only available option nowadays to effectively protect citizens from surveillance (M.A. Bigos, *Let's "Face" It*, quot.). Similarly, L. Barrett, *Ban FRT for Children-And for Everyone Else*, quot.

[114] K. Lachmayer, *AI, Plurality and Democracy. Reflections on the Impact of Large Language Models like ChatGPT on the Rule of Law and Democracy*, in P. Riberi, K. Lachmayer (eds), *Political Representation, Democracy and the Constitution* (forthcoming).