Department of European Public Law
University of Zagreb Faculty of Law

Croatian Yearbook of European Law and Policy

ISSN 1848-9958 (Online) | ISSN 1845-5662 (Print)

Journal webpage: https://www.cyelp.com

It Takes (At Least) Two to Tango in the Rhythm of AI-Enabled Discrimination: How the AI Act Complements EU Non-Discrimination Law?

Konstantinos Lamprinoudis

Suggested citation: K Lamprinoudis, 'It Takes (At Least) Two to Tango in the Rhythm of AI-Enabled Discrimination: How the AI Act Complements EU Non-Discrimination Law?' (2025) 21 CYELP [ONLINE FIRST].

DOI: 10.3935/cyelp.21.2025.615

https://www.cyelp.com/index.php/cyelp/article/view/615

https://orcid.org/0009-0006-5550-9594

IT TAKES (AT LEAST) TWO TO TANGO IN THE RHYTHM OF AI-ENABLED DISCRIMINATION:

HOW THE AI ACT COMPLEMENTS EU NON-DISCRIMINATION LAW

Konstantinos Lamprinoudis*

Abstract: Despite the elaborate equality and non-discrimination legislation in the European Union (EU), the current legal framework has been widely deemed ill-suited to properly address discriminatory instances that may emerge from the use of algorithms and Artificial Intelligence (AI) technologies. Nevertheless, the potential synergies between the EU Artificial Intelligence Act (AI Act) and non-discrimination law remain underexplored. This article suggests that the AI Act may complement EU non-discrimination rules for the purpose of combatting AI-enabled discrimination in a threefold manner: a) by prohibiting certain AI systems that are prone to produce discriminatory outcomes; b) by regulating the requirements that AI systems need to comply with in order to minimise the risk of discrimination; and c) by enabling the persons affected by discriminatory effects to seek legal protection. Each of these prohibitive, regulatory, and enabling functions of the AI Act are examined in turn, with emphasis placed on their interplay with the existing non-discrimination legislation at EU level. Finally, the article concludes that, apart from the significant complementarities between the two legal regimes both at the level of substantive protection granted to individuals and at the level of enforcement, there are other pieces of EU legislation implicated by the AI Act that may also be applicable when addressing AI-enabled discrimination.

Keywords: AI Act, non-discrimination law, EU law, bias, complementarity

1 Introduction

The risk of algorithms used in decision-making practices to discriminate against certain individuals or entire societal groups, thus perpetuating or amplifying existing inequalities, is already well known.[1] Amid the surge of Artificial Intelligence (AI)[2] in various sectors of the

* PhD candidate, Europa Institute, Leiden University, the Netherlands; email: k.lamprinoudis@law.leidenuniv.nl.

[1] For a detailed overview of the various ways in which algorithms may lead to discrimination, see most prominently the pioneering work of S Barocas and A Selbst, 'Big Data's Disparate Impact' (2016) 104(3) California Law Review 671. See also eg EU Fundamental Rights Agency (FRA), 'BigData: Discrimination in Data-Supported Decision Making' (European Union Publication Office 2018).

[2] See the definition adopted by the Organisation for Economic Cooperation and Development (OECD), 'Recommendation of the Council on Artificial Intelligence'

economic and social reality in recent years, concerns about the potentially unfair, biased, or discriminatory outcomes of AI systems have been increasingly raised by scholars and policymakers around the world.[3] In particular, the Council of Europe's Framework Convention on AI requires all signatory parties to adopt measures that 'respect equality, including gender equality, and the prohibition of discrimination' during the lifecycle of AI systems, and that are also directed towards 'overcoming inequalities to achieve fair, just and equitable outcomes'.[4] Similarly, within the context of the European Union (EU), the High-Level Expert Group on AI appointed by the European Commission has, among other things, called for 'diversity, non-discrimination and fairness' as one of the key requirements to achieve 'trustworthy AI'.[5]

Despite the elaborate equality and non-discrimination legislation at EU level,[6] the current legal framework has been widely deemed ill-

(OECD/LEGAL/0449, 2019) as amended by the 'Explanatory Memorandum on the Updated OECD Definition of an AI System' (OECD Artificial Intelligence Papers, No 8, March 2024).

[3] See eg E Ferrara, 'Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies' (2024) 6 Sci 2024; X Ferrer and others, 'Bias and Discrimination in AI: A Cross-Disciplinary Perspective' (2021) 40(2) IEEE Technology and Society Magazine 72. On the difference between the terms 'bias' and 'fairness' deployed mostly in computer science, statistics, and ethics, on the one hand, and the legal notions of 'discrimination' and 'equality', on the other hand, see J Gerards and R Xenidis, 'Algorithmic Discrimination in Europe: Challenges and Opportunities for Gender Equality and Non-Discrimination Law' (European Commission, Publications Office of the European Union 2021) Section 1.5.1, 47.

[4] See Art 10 of the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (Council of Europe Treaty Series No 225, 5 September 2024).

[5] See Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region – Building Trust in Human-Centric Artificial Intelligence' COM (2019) 168 final, 5-6, in the sense that AI systems should be developed and used in a way that 'includes diverse actors and promotes equal access, gender equality and cultural diversity, while avoiding discriminatory impacts and unfair biases'. See also several dispersed references to the need for non-discriminatory AI in other official EU documents: Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region – Artificial Intelligence for Europe' COM (2018) 237 final; Commission, 'White Paper on Artificial Intelligence – A European Approach to Excellence and Trust' COM (2020) 65 final; Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region – Fostering a European Approach to Artificial Intelligence' COM (2021) 205 final.

[6] Apart from certain EU primary law provisions, this framework consists of a set of so-called 'Equality Directives'. See Council Directive 79/7/EEC of 19 December 1978 on the progressive implementation of the principle of equal treatment for men and women in matters of social security [1978] OJ L6/24; Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin [2000] OJ L180/22; Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation [2000] OJ L303/16; Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services [2004] OJ L373/37; Directive 2006/54/EC of the European Parliament and of the Council of 5

suited to properly redress algorithmic or AI-enabled discrimination due to several shortcomings.[7] Most importantly, EU non-discrimination law covers instances of disadvantageous treatment of persons or groups based only on specific personal attributes known as 'protected characteristics' or 'prohibited grounds of discrimination' that are exhaustively listed in the so-called 'Equality Directives' (ie sex, racial or ethnic origin, religion or belief, age, disability, and sexual orientation), and solely in certain areas of life (eg employment, access to goods and services, etc), with the ensuing level of protection varying between the different protected characteristics.[8] Yet, algorithmic tools may often unfairly differentiate between people based on their classification into new, non-traditional groups that do not necessarily correlate with prohibited grounds of discrimination or proxies of these grounds.[9] In addition, although the list of personal traits protected by the right to non-discrimination enshrined in Article 21(1) of the EU Charter of Fundamental Rights (Charter) is open-ended and includes more characteristics than the ones safeguarded under the Equality Directives, the scope of application of the said provision is limited only to cases of implementation of EU law, as per Article 51(1) of the Charter.[10] Furthermore, the already blurred dichotomy between the concepts of 'direct' and 'indirect discrimination' traditionally deployed in the EU non-discrimination doctrine is considered an uneasy fit with

July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast) [2006] OJ L204/23.

[7] See, among others, Gerards and Xenidis (n 3); R Xenidis and L Senden, 'EU Non-Discrimination Law in the Era of Artificial Intelligence: Mapping the Challenges of Algorithmic Discrimination' in U Bernitz and others (eds), *General Principles of EU Law and the EU Digital Order* (Kluwer Law International 2020); R Xenidis, 'Tuning EU Equality Law to Algorithmic Discrimination: Three Pathways to Resilience' (2020) 27(6) Maastricht Journal of European and Comparative Law 736; R Xenidis, 'When Computers Say No: Towards a Legal Response to Algorithmic Discrimination in Europe' in B Brożek, P Palka and O Kanevskaia (eds), *Research Handbook on Law and Technology* (Edward Elgar Publishing 2023).

[8] For this 'hierarchy' of prohibited grounds under EU non-discrimination law, see eg L Waddington and M Bell, 'More Equal than Others: Distinguishing European Union Equality Directives' (2001) 38(3) Common Market Law Review 587, 587; E Howard, 'The Case for a Considered Hierarchy of Grounds in EU Law' (2006) 13(4) Maastricht Journal of European and Comparative Law 445, 445. However, as the Equality Directives only provide for minimum harmonisation, it is up to the Member States to opt for a more extensive protection in their national legislation, by prohibiting discrimination also on the basis of other grounds and/or in other areas of life.

[9] See Gerards and Xenidis (n 3) Section 2.2, 62–66. See also J Gerards and F Zuiderveen Borgesius, 'Protected Grounds and the System of Non-Discrimination Law in the Context of Algorithmic Decision-Making and Artificial Intelligence' (2022) 20(1) Colorado Technology Law Journal 1; S Wachter, 'The Theory of Artificial Immutability: Protecting Algorithmic Groups Under Non-Discrimination Law' (2022) 97(2) Tulane Law Review 149; M Leese, 'The New Profiling: Algorithms, Black Boxes, and the Failure of Non-Discriminatory Safeguards in the European Union' (2014) 45(5) Security Dialogue 494, 502, 504.

[10] Charter of Fundamental Rights of the European Union [2016] OJ C202/389. As clarified by the Court of Justice of the EU (CJEU) in this regard, the fundamental rights guaranteed in the Charter are applicable in all situations governed by EU law. See Case C-617/10 *Åkerberg Fransson* ECLI:EU:C:2013:105, paras 19–22.

the particularities of discriminatory algorithmic operations.[11] When it comes to enforcement, on the other hand, the opaque nature of algorithmic tools, especially in the case of advanced AI machine-learning models, commonly referred to as the 'black box',[12] is most likely to hinder the persons affected from proving that they have been discriminated against when trying to bring a *prima facie* case of discrimination before courts.[13] In fact, these persons may sometimes not even be aware that they have suffered discriminatory treatment.[14] In view of these challenges, recourse to data protection rules, notably those included in the General Data Protection Regulation (GDPR),[15] has often been portrayed as a promising means to provide effective tools to individuals affected by discriminatory algorithmic decisions.[16]

However, the potential synergies between the much-acclaimed EU Artificial Intelligence Act (AI Act)[17] and non-discrimination law remain underexplored. The AI Act constitutes a hybrid form of regulation, in the sense that, albeit designed as a product safety instrument laying down uniform rules for the development, marketing, and use of AI systems with the aim of improving the functioning of the EU internal market, it is also intended to ensure a high level of fundamental rights protection as enshrined in the Charter, including individuals' right to non-discrimination.[18] As such, the AI Act aligns with the horizontal equality clause of Article 10 of the Treaty on the Functioning of the

[11] See eg Gerards and Xenidis (n 3) Section 2.3, 67–73, arguing though that the concept of indirect discrimination is probably more apt compared to its direct counterpart to address the challenges of algorithmic discrimination. For arguments against the alleged diminishing relevance of direct discrimination in the field of algorithms, see J Adams-Prassl, R Binns and A Kelly-Lyth, 'Directly Discriminatory Algorithms' (2023) 86(1) Modern Law Review 144.

[12] See eg F Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015). See also J Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3(1) Big Data and Society.

[13] See Gerards and Xenidis (n 3) Section 1.4.4, 45–46. On the burden of proof in discrimination cases in EU law, see Art 8 of Directive 2000/43/EC, Art 10 of Directive 2000/78, and Art 9 of Directive 2004/113/EC. See also K Henrard, 'The Effective Protection against Discrimination and the Burden of Proof: Evaluating the CJEU's Guidance Through the Lens of Race' in U Belavusau and K Henrard (eds), *EU Anti-Discrimination Law Beyond Gender* (Hart 2019).

[14] See Gerards and Xenidis (n 3) Section 2.4, 11, 73–75.

[15] 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) [2016] OJ L119/1.

[16] See eg P Hacker, 'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Decision-Making Under EU Law' (2018) 55(4) Common Market Law Review 1143.

[17] 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) [2024] OJ L2024/1689. See in particular, recitals 27–28, 31, 44–45, 48, 54–58, 67, and 70.

[18] See Art 1(1) and recitals 1 and 8 of the AI Act. See also M Almada and N Petit, 'The EU AI Act: Between the Rock of Product Safety and the Hard Place of Fundamental Rights' (2025) 62(1) Common Market Law Review 85, 119.

European Union (TFEU) pursuant to which the need to combat discrimination is to be taken into account in all policy areas of EU law.[19] This is also particularly evident in the AI Act's preamble, which extensively refers to the discrimination risks posed by various AI tools, thus reflecting the EU legislator's increased concern about the adverse consequences of AI technologies in this regard.[20]

By definition, the AI Act applies exclusively to systems that qualify as 'AI systems', to the exclusion of all other automated or algorithmic systems.[21] Yet, it is only those AI systems giving rise to the most significant risks to fundamental rights that fall under the AI Act's regulatory regime. Following such a 'risk-based approach',[22] the AI Act covers four categories of AI systems: i) those of unacceptable risk, which are prohibited under Article 5; ii) those of high risk defined under Article 6 in conjunction with Annex III, which are subject to a set of requirements and obligations under Articles 8–27; iii) those of limited risk, which are subject to transparency obligations under Article 50; and iv) those of minimal or no risk, which remain largely unregulated and are subjected to a merely voluntary application of the requirements applicable to high-risk systems under Article 95.

Against this background, this article attempts to shed more light on the ways in which the AI Act complements EU non-discrimination law for the purpose of addressing AI-enabled discrimination. I argue, in particular, that the AI Act contributes to this aim in a threefold manner: a) by prohibiting certain uses of AI that are prone to produce

---

[19] Consolidated Version of the Treaty on the Functioning of the European Union [2016] OJ C202/47. On Art 10 TFEU and 'equality mainstreaming' in EU law, see A Timmer, 'Editorial: Mainstreaming Equality in EU Law and Beyond' (2023) 19(3) Utrecht Law Review 1; E Muir, V Davio and L van der Meulen, 'The Horizontal Equality Clauses (Arts 8 & 10 TFEU) and Their Contribution to the Course of EU Equality Law: Still an Empty Vessel?' (2022) 7(3) European Papers 1381.

[20] See eg recitals 28, 31, 32, 44, 48, 56–60 of the AI Act. See also 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' COM (2021) 206 final, point 3.5.

[21] According to Art 3(1) of the AI Act, an 'AI system' is any 'machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments'. As specified by recital 12 of the AI Act, AI systems present distinct features that distinguish them from 'simpler traditional software systems or programming approaches' and, as such, do not cover 'systems that are based on the rules defined solely by natural persons to automatically execute operations'. See also in detail Commission, 'Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act)' [2025] C(2025) 924 final, points 6, 61–62, emphasising that no automatic determination or exhaustive list of AI systems can be provided, but rather whether a given system fulfils the criteria to be considered an AI system depends on its specific architecture and functionality.

[22] See the Commission's Guidelines on the definition of an AI system (n 21) point 63. Pursuant to recital 26 of the AI Act, this risk-based approach means that the applicable rules are tailored to the intensity and scope of the risks that the AI system concerned can generate. On this approach in AI governance more generally, see M Kaminski, 'Regulating the Risks of AI' (2023) 103 Boston University Law Review 1347.

discriminatory outcomes; b) by regulating the requirements that AI systems need to comply with in order to minimise the risk of discrimination; and c) by enabling the persons affected by the discriminatory effects of AI systems to seek legal protection.[23] Accordingly, this article examines in turn each of these prohibitive, regulatory, and enabling functions of the AI Act, emphasising their interplay with the existing non-discrimination rules (Sections 2, 3 and 4 respectively). Finally, the article concludes that, apart from the significant complementarities between the two legal regimes both at the level of substantive protection granted to individuals and at the level of enforcement, there are other pieces of EU legislation implicated by the AI Act that may also be applicable when addressing AI-enabled discrimination (Section 5).

2 The prohibitive function

The AI Act's 'prohibitive function' is set out in Article 5, which consists of a list of prohibited AI practices. This provision prohibits the placing on the EU market, putting into service, or the use of AI systems for certain practices considered particularly harmful because they conflict, among other things, with the value of equality and the right to non-discrimination, as clarified by the Commission's Guidelines in this regard.[24] Furthermore, the AI Act gives teeth to these prohibitions by providing for severe administrative fines in the case of non-compliance.[25] Although subject to various exceptions, notably in the field of law enforcement and migration, the AI Act's prohibitive function not only ensures that practices entailing severe risks of discriminatory outcomes are in principle legally banned, but it also sets the tone for what is perceived as ethically or socially permissible use of AI in the EU.[26] From this perspective, in addition to their strictly legal nature, the AI Act's prohibitions have some sort of symbolic value, signalling the red lines of the EU legal order with regard to the standards of fundamental rights' protection, including non-discrimination, below which AI practices cannot fall.[27]

---

[23] This taxonomy draws upon a similar typology of US legislation relating to the regulation of AI technologies as proposed in 'Resetting Antidiscrimination Law in the Age of AI' (2025) 138(6) Harvard Law Review 1562, which identifies four primary methods by which various federal and state bills target AI-enabled discrimination: a) prohibition on certain uses of AI; b) regulation of some procedural requirements for the use of AI; c) regulation of the inputs used in AI decision-making; and d) regulation of the outputs produced by AI systems.

[24] See Commission, 'Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)' [2025] C(2025) 5052 final, point 8. See also recital 28 of the AI Act.

[25] See Art 99(3) of the AI Act. The concrete rules on penalties and other enforcement measures applicable to the infringements of the AI Act are to be laid down by the Member States, pursuant to Art 99(1) thereof.

[26] See C Rudschies and I Schneider, 'The Long and Winding Road to Bans for Artificial Intelligence: From Public Pressure and Regulatory Initiatives to the EU AI Act' (2025) 4(57) Digital Society 9–10.

[27] See similarly in this regard K Yeung, A Howes and G Pogrebna, 'AI Governance by Human Rights-Centred Design, Deliberation and Oversight: An End to Ethics

Be that as it may, Article 5 of the AI Act does not affect the prohibition of AI practices infringing other pieces of EU legislation.[28] Even where the use of an AI system is not prohibited by the AI Act itself, it could still be deemed unlawful on the basis of other primary or secondary EU law, including non-discrimination law, which remains fully applicable.[29] For instance, this would be the case where an AI tool relies on individuals' sex to calculate different insurance premiums and benefits contrary to Directive 2004/113,[30] or where such an AI system screens the CVs of job applicants and automatically rejects those with foreign-sounding names in violation of Directive 2000/43. Consequently, one could reasonably wonder what added value the AI Act's prohibitions really provide beyond the existing EU non-discrimination legal framework.

To answer this question, I will examine below each of the prohibited AI practices listed in Article 5 of the AI Act, namely those relating to harmful manipulation, deception, or exploitation, social scoring, crime risk assessment, biometric categorisation, untargeted scraping of facial images, emotion recognition, and real-time biometric identification. Far from engaging in a detailed analysis of these practices and all their adverse consequences for the individual's fundamental rights, I will emphasise their discriminatory potential and then highlight how the AI Act's prohibitions may converge with or even extend the protective reach of EU non-discrimination legislation in this regard.

2.1 Harmful manipulation, deception, or exploitation

The first two prohibitions in Article 5(1) of the AI Act target AI systems that deploy subliminal, purposively manipulative or deceptive techniques (Article 5(1)(a)) or exploit any vulnerabilities of natural persons or groups thereof due to their age, disability, or a specific social or economic situation (Article 5(1)(b)), with the objective or the effect of materially distorting the behaviour of such persons in a manner that may cause them significant harm. As both of these prohibitions aim at protecting individuals against AI practices that subvert and impair their autonomy, decision-making, and free choices, they may complement each other.[31] However, whereas the primary focus of the prohibition in

---

Washing' in M Dubber, F Pasquale and S Das (eds), *The Oxford Handbook of AI Ethics* (OUP 2020).

[28] See Art 5(8) of the AI Act.

[29] See recital 45 of the AI Act. See also the Commission's Guidelines on prohibited AI practices (n 24) point 43.

[30] See Art 5(1) of the said Directive. The former second paragraph of Art 5, which allowed Member States to opt for proportionate differences in individuals' premiums and benefits where the use of sex is a determining factor in the assessment of risks based on relevant and accurate actuarial and statistical data, was declared invalid by the CJEU in its landmark judgement in Case C-236/09 *Test-Achats* ECLI:EU:C:2011:100.

[31] See recital 29 of the AI Act. See also the Commission's Guidelines on prohibited AI practices (n 24), points 59, 122.

Article 5(1)(a) is placed on the nature of the techniques deployed by the AI system in question, it is the characteristics of the persons affected and the exploitation of their specific vulnerabilities that lie at the core of the prohibition in Article 5(1)(b).[32] Accordingly, where both provisions seem applicable, Article 5(1)(a) will take precedence if such exploitation occurs regardless of the specific vulnerabilities of the persons concerned, while Article 5(1)(b) will apply instead if the AI-enabled exploitation affects particularly vulnerable people due to their age, disability, or specific socioeconomic situation.[33] Given that the prohibition in Article 5(1)(b) is explicitly based on certain personal attributes of the individuals or groups concerned in a similar way as non-discrimination law, the rest of my analysis here will deal mostly with that provision in particular.

By referring to 'people with vulnerabilities' instead of 'vulnerable people', Article 5(1)(b) of the AI Act seems to endorse a context-specific understanding of the notion of 'vulnerability',[34] in the sense that certain categories of people are not inherently vulnerable but may become so in specific circumstances, with their vulnerability emerging from multiple different sources.[35] Hence, the emphasis placed by Article 5(1)(b) on human vulnerabilities indicates a more substantive vision of equality in this regard that goes beyond the prohibition of discrimination based on defined personal characteristics.[36] Such vulnerabilities may encompass a wide array of categories, including cognitive, emotional, physical, and other forms of susceptibility that can affect the ability of persons to make informed decisions or otherwise influence their behaviour.[37]

On the one hand, as concerns vulnerabilities due to age or disability, one can think, for instance, of AI systems that exploit the cognitive

---

[32] See the Commission's Guidelines on prohibited AI practices (n 24), points 123–124. For a detailed analysis of the subliminal, manipulative, or deceptive nature of the techniques covered by Art 5(1)(a) of the AI Act, see the Commission's Guidelines on prohibited AI practices (n 24), points 63–75.

[33] ibid, point 125.

[34] See G Malgieri, *Vulnerability and Data Protection Law* (OUP 2023) 96–97.

[35] See F Luna, 'Elucidating the Concept of Vulnerability: Layers Not Labels' (2009) 2(1) International Journal of Feminist Approaches to Bioethics 121. For a conceptual framework of human vulnerability as 'algorithmic vulnerability' tailored to address the particularities of AI technologies, see SA Teo, 'Artificial Intelligence, Human Vulnerability and Multi-Level Resilience' (2025) 57 Computer Law and Security Review, article no 106134.

[36] For the relation between vulnerability and substantive equality, see M Fineman, 'The Vulnerable Subject: Anchoring Equality in the Human Condition' (2008) 20(1) Yale Journal of Law and Feminism. See also with regard to the case law of the European Court of Human Rights (ECtHR) L Peroni and A Timmer, 'Vulnerable Groups: The Promise of an Emerging Concept in European Human Rights Convention Law' (2013) 11(4) International Journal of Constitutional Law 1056, 1074–1082. For the distinction between formal and substantive equality, see eg T Loenen, *The Conceptualization of Equality and Non-Discrimination as Legal Standards: From Formal to More Substantive Equality* (Brill/Nijhoff 2025); S Fredman, 'Providing Equality: Substantive Equality and the Positive Duty to Provide' (2005) 21(2) South African Journal on Human Rights 163.

[37] See the Commission's Guidelines on prohibited AI practices (n 24) point 102.

decline and reduced digital literacy of older people by targeting unnecessary insurance policies or deceptive investments schemes to them, or those that exploit the limited intellectual capacity of mentally disabled persons to influence them to purchase expensive medical products.[38] In this regard, the parallels with non-discrimination law are evident, since both age and disability are also protected traits pursuant to Directive 2000/78.[39] However, whereas discrimination on these grounds is prohibited only in the field of employment and occupation, the prohibition of the AI Act is framed in rather broad terms, not being confined to any specific area. Furthermore, because of the limited material scope of Directive 2000/78, the concept of 'disability' in EU non-discrimination law has been consistently interpreted as comprising any limitation which may hinder a person's full and effective participation in professional life on an equal basis with other workers, and thus relates only to the context of exercising a professional activity.[40] In contrast, as specified by recital 29 of the AI Act, 'disability' under Article 5(1)(b) is to be understood within the meaning of Directive 2019/882, namely as referring more broadly to any impairment which may hinder their full and effective participation in society on an equal basis with others.[41] Thus, the AI Act fully aligns with the definition of disability adopted by the United Nations Convention on the Rights of Persons with Disabilities, to which the EU is also a party.[42]

On the other hand, vulnerabilities based on specific social or economic situations may indicatively concern persons living in extreme poverty, ethnic or religious minorities, migrants, or refugees, covering not only stable and long-term characteristics but also transient circumstances, such as temporary unemployment or over-indebtedness.[43] Unlike EU non-discrimination law which does not recognise socioeconomic status as a prohibited ground of discrimination in itself,[44] the prohibition of Article 5(1)(b) of the AI Act

---

[38] ibid, points 108, 117.
[39] See also explicitly ibid, point 138.
[40] See eg Case C-354/13 *FOA* ECLI:EU:C:2014:2463, paras 53–54; Case C-363/12 *Z* ECLI:EU:C:2014:159, paras 76–77; Case C-13/05 *Chacón Navas* EU:C:2006:456, paras 41–43.
[41] See Art 3(1) of Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services [2019] OJ L151/70. See also explicitly the Commission's Guidelines on prohibited AI practices (n 24) point 108.
[42] See Art 1 of the United Nations Convention on the Rights of Persons with Disabilities (CRPD) adopted in New York on 13 December 2006. See also Council Decision of 26 November 2009 concerning the conclusion, by the European Community, of the United Nations Convention on the Rights of Persons with Disabilities [2009] OJ L23/35.
[43] See recital 29 of the AI Act. See also the Commission's Guidelines on prohibited AI practices (n 24) points 109, 112.
[44] See S Ganty and JC Benito-Sanchez, 'Expanding the List of Protected Grounds within Anti-Discrimination Law in the EU' (Equinet 2021) 36–37. Yet, Art 21(1) of the Charter also prohibits discrimination on the grounds of social origin and property. For an interesting analysis as to why discrimination on socioeconomic criteria should not be protected under Art 21 of the Charter, see Case C-715/20 *KL v X* ECLI:EU:C:2023:281, Opinion of AG Pitruzzella, paras 71–81. For the opposite view,

aims to ensure that AI technologies do not perpetuate or exacerbate existing inequalities by exploiting the vulnerabilities of socially or economically disadvantaged individuals.[45] Yet, since socioeconomic status may intersect with various prohibited grounds of discrimination, such as racial origin, ethnicity, or religion, it can often be used as a proxy linked to these grounds and thereby trigger the applicability of the relevant non-discrimination rules.[46]

Accordingly, where an AI system targets persons in specific socioeconomic conditions based on proxies that closely correlate with protected characteristics, or disproportionately affects such persons that at the same time belong to protected social groups,[47] both Article 5(1)(b) of the AI Act and EU non-discrimination law may apply at the same time.[48] This will be the case, for example, of an AI-predictive algorithm that is used to target with advertisements for predatory financial products persons who are in a dire financial situation and live in low-income neighbourhoods predominantly inhabited by people of a particular ethnic origin.[49] However, where the persons concerned are targeted merely on the basis of their socioeconomic situation without any correlation to protected characteristics, such targeting will not be captured by non-discrimination rules but may only fall under the scope of Article 5(1)(b) of the AI Act, as long as it constitutes a deliberate feature of the system's algorithmic design, or the providers or deployers of that system are aware of the reasonably likely harm that their system may cause and have not taken appropriate corrective measures.[50] The added value of Article 5(1)(b) also manifests in cases where, although an AI system deploys socioeconomic data as a proxy for protected characteristics, the exploitative AI-driven practice in question takes

---

see S Ganty, 'Poverty as Misrecognition: What Role for Antidiscrimination Law in Europe?' (2021) 21(4) Human Rights Law Review 962.

[45] See the Commission's Guidelines on prohibited AI practices (n 24) point 110.

[46] ibid, points 111, 138. For the intersection of socioeconomic considerations with other prohibited grounds, see S Atrey, 'The Intersectional Case of Poverty in Discrimination Law' (2018) 18 Human Rights Law Review 411.

[47] See the Commission's Guidelines on prohibited AI practices (n 24) points 110–111.

[48] As per point 138 of the Commission's Guidelines on prohibited AI practices (n 24), the AI Act's prohibitions do not affect prohibitions based on other grounds or discriminatory practices that do not entail significant harms and that are already prohibited by EU non-discrimination law.

[49] This example is a combination of the ones mentioned in the Commission's Guidelines (n 24), points 110–111.

[50] See the Commission's Guidelines on prohibited AI practices (n 24) point 110, distinguishing between such instances of 'direct discrimination' against socially or economically disadvantaged persons which are covered by the AI Act's prohibition, and those of 'indirect discrimination' which are not automatically considered to exploit these persons' vulnerabilities, as is the case, for example, of AI systems that are inadvertently biased (eg due to tainted training data) and disproportionately impact disadvantaged persons. Thus, instances of 'indirect discrimination' on the basis of individuals' socioeconomic condition alone, without any correlation to protected characteristics, are likely to fall through the cracks of both Art 5(1)(b) of the AI Act and EU non-discrimination law, unless such AI-enabled discrimination is based on those individuals' social origin or property, thus being captured by Art 21(1) of the Charter. However, it is noted that those instances may still be prohibited under Art 5(1)(a) of the AI Act.

place in a social context that is not covered by the protective cloak of the EU Equality Directives. For instance, an AI system which exploits socioeconomic data to target persons with disabilities living in precarious conditions with advertisements for predatory medical services will fall outside the scope of Directive 2000/78,[51] but may still be prohibited under Article 5(1)(b) of the AI Act alone or combined with Article 21(1) of the Charter.

In any event, AI systems that exploit the vulnerabilities of individuals belonging to vulnerable groups other than those defined by age, disability, or a specific socioeconomic situation are left outside the scope of Article 5(1)(b) of the AI Act.[52] By way of illustration, targeting homosexual, bisexual or trans persons with social media advertisements for so-called 'conversion therapies',[53] or pregnant women with advertisements for pricy pregnancy- or maternity-related products, is not prohibited under the AI Act, unless it somehow results from the exploitation of vulnerabilities related to the age, disability, or socioeconomic status of the persons concerned. The question raised here is whether the personal scope of Article 5(1)(b) of the AI Act could be extended in the light of Article 21(1) of the Charter so as to cover also vulnerabilities relating to other personal traits protected therein. In my view, a Charter-conforming interpretation of Article 5(1)(b) of the AI Act would dictate a positive answer. Regardless, such instances may still be captured by Article 5(1)(a) if they leverage on the specific vulnerabilities and weaknesses of the affected persons.[54] Thus, to the extent that such AI practices may also fall outside the scope of non-discrimination law,[55] the complementary nature of the AI Act's prohibitions of manipulative, deceptive, and exploitative systems under Article 5(1)(a)-(b) proves to be of great practical importance in this regard.

2.2 Social scoring

---

[51] This is because Directive 2000/78 does not cover access to goods and services.

[52] See the Commission's Guidelines on prohibited AI practices (n 24) point 103.

[53] See eg H Horton and J Cook, 'Facebook Accused of Targeting Young LGBT Users with "Gay Cure" Adverts' (*The Telegraph*, 25 August 2018) <https://tinyurl.com/5be2jkdf> accessed 20 November 2025; J Hesse, '"Love Is Love": Media Firm Uses LGBT Language to Send Anti-Gay Message' (*The Guardian*, 23 January 2018) <https://tinyurl.com/4yz99ahz> accessed 20 November 2025.

[54] See the Commission's Guidelines on prohibited AI practices (n 24) point 125. These practices could also fall within the scope of Art 21(1) of the Charter. As concerns (trans)gender identity, however, this possibility is questionable: although not mentioned in that provision, gender identity could still be considered as falling under the notion of 'sex' or explicitly recognised as a prohibited ground *per se*, but this scenario remains uncertain for the time being.

[55] This is because discrimination on grounds of sexual orientation under Directive 2000/78 is only prohibited in matters of employment and occupation, while (trans)gender identity has been granted protection only when forming part of prohibited sex discrimination in the context of gender reassignment surgeries. See eg the judgment in Case C-13/94 *P v S and Cornwall County Council* ECLI:EU:C:1996:170. As for equal treatment between women and men in access to and in the supply of goods and services, Directive 2004/113 explicitly excludes advertising from its scope of application. See Art 3(3) thereof.

The prohibition in Article 5(1)(c) of the AI Act addresses AI-enabled evaluation or classification of individuals or groups based on their social behaviour or personal characteristics that leads to detrimental or unfavourable treatment, especially where the data used for this purpose originates from unrelated social contexts or where the treatment is disproportionate to the gravity of the social behaviour. As recital 31 of the AI Act explicitly recognises, given that AI systems enabling these so-called 'social scoring' practices may lead to discriminatory or unfair outcomes for certain individuals and groups and result in their exclusion from society, the AI Act's prohibition in this regard is intended to safeguard, among other things, the right to non-discrimination and the EU value of equality, including equal access to public and private services.[56]

Such practices are increasingly prevalent across the EU: one could think, notably, of the notorious 'childcare benefits scandal' (*toeslagenaffaire*) in the Netherlands concerning the deployment of a self-learning algorithm by the Dutch Tax Administration to assess childcare benefit applications that resulted in falsely targeting thousands of parents from families of lower economic status or an ethnic minority background.[57] Similarly, the algorithm used by the Dutch Education Executive Agency (DUO) to calculate the risk of students committing fraud with the grant for students living away from home was declared discriminatory by the Dutch Data Protection Authority.[58] Likewise, the Danish government's fraud control algorithm used for the distribution of social benefits was found likely to discriminate against people with disabilities, low-income individuals,

[56] See the Commission's Guidelines on prohibited AI practices (n 24) point 148.

[57] See eg 'Dutch Scandal Serves as a Warning for Europe Over Risks of Using Algorithms' (*Politico*, 29 March 2022) <https://tinyurl.com/yemdeuby> accessed 20 November 2025. For a detailed overview of how this system led to discrimination as well as racial profiling, see the report of Amnesty International, 'Xenophobic Machines: Discrimination Through Unregulated Use of Algorithms in the Dutch Childcare Benefits Scandal' (October 2021) <https://tinyurl.com/mtrsk2mx> accessed 20 November 2025. Dealing with follow-up discrimination claims brought by the victims of the benefits affair, the Dutch Institute of Human Rights found that the selection criteria used by the Tax Administration for the discontinuation and recovery of childcare benefits indirectly discriminated against them on the basis of their foreign origin. See College voor de Rechten van de Mens, oordeelnummers 2023–101, 2023–102, 2023–103, 2 October 2023. See also the Institute's preliminary investigation, College voor de Rechten van de Mens, 'Vooronderzoek naar de Vermeende Discriminerende Effecten van de Werkwijzen van de Belastingdienst/Toeslagen' <https://tinyurl.com/usybvx98> accessed 20 November 2025.

[58] See Autoriteit Persoonsgegevens, 'DUO's Approach to Fraud Found to Be Discriminatory and Illegal' (11 November 2024) <https://tinyurl.com/4yn4zxc3> accessed 20 November 2025. See also Autoriteit Persoonsgegevens, 'Onderzoeksrapport fraudeaanpak DUO' <https://tinyurl.com/4v4d7hpt> accessed 20 November 2025. The Data Protection Authority concluded that DUO's algorithm gave rise to direct discrimination based on the students' type of education, distance from the parents' home, and younger age, while also indirectly discriminating against students with a non-European migration background.

migrants, and marginalised racial groups,[59] while the machine-learning system deployed by Sweden's Social Insurance Agency for the same purposes was also found prone to disproportionately flag women, individuals with a foreign background, low-income earners, and individuals without a university degree.[60]

In cases where AI-enabled social scoring is based directly or indirectly on a protected ground of discrimination, this practice, apart from being banned under the AI Act, will be further captured by EU non-discrimination law.[61] However, social scoring practices are not always prohibited, but only in cases where all the conditions of Article 5(1)(c) of the AI Act are cumulatively fulfilled.[62] Pursuant to recital 31 of the AI Act, the prohibition of social scoring does not affect lawful evaluation practices of individuals that are carried out for a specific purpose in accordance with EU and national law.[63] This means that AI scoring systems, which generate a social score by evaluating or classifying individuals, will fall outside the scope of Article 5(1)(c) of the AI Act if they comply with EU sectoral legislation that specifies which type of data can be used as relevant and necessary for the specific legitimate purpose of evaluation and ensures that any detrimental or unfavourable treatment is justified and proportionate to the social behaviour concerned.[64]

By way of illustration, when examining whether an AI-based credit scoring system used by creditors or third entities, such as credit information agencies, to assess a customer's financial creditworthiness and determine their access to credit accordingly is covered by the AI Act's prohibition, the relevant point of reference will be the revised Consumer Credit Directive (CCD).[65] Article 18(3) of the said Directive requires that creditworthiness assessments be based solely on information of an economic or financial nature relating to the consumer's income and expenses and other financial and economic circumstances (eg evidence of income or other sources of repayment,

---

[59] See Amnesty International, 'Coded Injustice: Surveillance and Discrimination in Denmark's Automated Welfare State' (November 2024) <https://tinyurl.com/3murv64h> accessed 20 November 2025.

[60] See Amnesty International, 'Sweden: Authorities Must Discontinue Discriminatory AI Systems Used by Welfare Agency' (November 2024) <https://tinyurl.com/kr8m6x6r> accessed 20 November 2025.

[61] See Art 5(8) of the AI Act and the Commission's Guidelines on prohibited AI practices (n 24) point 181.

[62] See the Commission's Guidelines on prohibited AI practices (n 24) point 175.

[63] See recital 31 of the AI Act.

[64] See the Commission's Guidelines on prohibited AI practices (n 24) points 176–177.

[65] ibid, points 177 (fn 126) 182, and Directive (EU) 2023/2225 of the European Parliament and of the Council of 18 October 2023 on credit agreements for consumers and repealing Directive 2008/48/EC [2023] OJ L2023/2225. For a detailed overview of this Directive, see O Cherednychenko, 'On the Bumpy Road to Responsible Lending in the Digital Marketplace: The New EU Consumer Credit Directive' (2024) 47 Journal of Consumer Policy 241. For the impact of the AI Act on credit scoring in general, see G Spindler, 'Algorithms, Credit Scoring, and the New Proposals of the EU for an AI Act and on a Consumer Credit Directive' (2021) 15(3–4) Law and Financial Markets Review 239.

information on financial assets and liabilities, or on other financial commitments).[66] However, the use of sensitive data within the meaning of Article 9(1) GDPR, such as those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, is prohibited, and so is the use of data obtained from social networks.[67] Accordingly, whereas AI credit scoring systems based on the financial and economic circumstances of the persons concerned to determine their eligibility for a loan will most likely not fall under the scope of Article 5(1)(c) of the AI Act,[68] by contrast, systems relying on other categories of data, such as those drawn from the individuals' social media[69] or smartphone,[70] will be prohibited. Hence, by pointing to the CCD's specification of the type of data that can be deployed for evaluating the borrowers' credit default risk, the AI Act incorporates in its prohibition of AI-enabled social scoring the discrimination concerns relating to the use of so-called 'alternative' data in credit scoring practices, which are opposed to 'traditional' financial data.[71]

---

[66] See also recital 55 CCD, further pointing to the European Banking Authority's (EBA) 'Guidelines on loan origination and monitoring' (EBA/GL/2020/06, 29 May 2020), which provide guidance on the categories of data that may be used for the purposes of creditworthiness assessments (Annex 2).

[67] The same prohibitions also apply when creditors consult credit databases under Art 19(5) CCD. In this regard, the final text of Art 18 CCD follows the recommendations made by the European Data Protection Supervisor (EDPS) in its Opinion 11/2021, points 11–18. However, contrary to what was proposed by the EDPS (Opinion 11/2021, points 17, 41), the use of search query data and online browsing activities is not expressly prohibited, nor are the categories of data that may be used to draw up a personalised offer clearly delineated. As a result, it is possible that a consumer receives, for instance, a predatory loan following an analysis of their search queries that reveal their urgent need to obtain credit. See M L Montagnani and C Paulesu, 'Towards an Ecosystem for Consumer Protection in the Context of AI-based Credit Scoring' (2022) 33(4) European Business Law Review 557, 578.

[68] Nevertheless, absent the conditions of Art 5(1)(c), AI-driven credit scoring systems may still qualify as high-risk in accordance with Art 6(2) combined with Annex III(5)(b) of the AI Act. In that case, compliance with the requirements laid down in relation to high-risk AI systems may ensure that such AI systems do not constitute prohibited social scoring practices. See the Commission's Guidelines on prohibited AI practices (n 24) point 172.

[69] See T Groenfeldt, 'Lenddo Creates Credit Scores Using Social Media' (*Forbes*, 29 January 2015) <https://tinyurl.com/3mu989me> accessed 20 November 2025.

[70] See H King, 'This Startup Uses Battery Life to Determine Credit Scores' (*CNN*, 24 August 2016) <https://tinyurl.com/43mw25h3> accessed 20 November 2025.

[71] Regarding the use of such alternative data not necessarily connected to the individual's financial standing, see M Hurley and J Adebayo, 'Credit Scoring in the Era of Big Data' (2016) 18 Yale Journal of Law and Technology 148; K Langenbucher, 'Consumer Credit in the Age of AI: Beyond Non-Discrimination Law' (European Corporate Governance Institute, Law Working Paper No 663/2022, LawFin Working Paper No 42, 2022). See also N Aggarwal, 'The Norms of Algorithmic Credit Scoring' (2021) 80(1) Cambridge Law Journal 42; N Collado-Rogriguez and U Kohl, 'All Data Is Credit Data: Personalised Consumer Credit Score and Non-Discrimination Law' in U Kohl and J Eisler (eds), *Data-Driven Personalisation in Markets, Politics and Law* (CUP 2021). In fact, among the market developments brought about by digitalisation which prompted the modernisation of the existing framework in the field of consumer credit, particularly important was the use of alternative categories of data, raising concerns over the discrimination risks of algorithmic decisions. See Commission, 'Staff Working Document, Impact Assessment Report accompanying the Proposal for a Directive of the European Parliament and of the Council on consumer credits' SWD (2021) 170 final 3, 18, 27.

2.3 Crime risk assessment

As per Article 5(1)(d) of the AI Act, AI systems assessing or predicting the risk of individuals committing a criminal offence, based solely on their profiling or on assessing their personality traits and characteristics, are prohibited. By associating indicators with the likelihood of a crime occurring, these systems identify patterns within historical data about previously committed crimes and then create individual risk scores to inform law enforcement activities and criminal justice decisions at any stage, such as during the prevention and detection of crimes (eg for the planning of police task forces, monitoring high-risk situations or locations, or conducting controls of persons predicted as potential offenders, etc), but also during the investigation, prosecution, and execution of criminal penalties (eg for assessing the risk of re-offending in the context of decisions about pre-trial detention, probation, or early release).[72] The characteristics assessed for these purposes may indicatively include individuals' nationality, place of birth, place of residence, number of children, level of debt, or type of car.[73] Real-world uses of such AI-enabled predictive systems abound across EU Member States and beyond.[74]

However, the use of historical crime data to predict other persons' future behaviour is likely to perpetuate or even reinforce existing biases, in particular against certain racial or ethnic groups that may be over-represented in criminal records, thereby giving rise to discriminatory racial or ethnic profiling.[75] Since such data-based AI models may influence law enforcement authorities to repeatedly target people from the same over-represented demographics in a disproportionate manner, the output they generate will then be fed back into the system, resulting in self-perpetuating 'feedback loops'.[76] This was the case, notably, of the 'COMPAS' tool used in the US criminal justice system to assess individuals' recidivism risk, which was found to incorrectly generate higher risk rates for black persons and for people of Hispanic origin.[77]

---

[72] See the Commission's Guidelines on prohibited AI practices (n 24) points 190–191.
[73] See recital 42 of the AI Act. According to the Commission's Guidelines on prohibited AI practices (n 24) point 198, this list is only illustrative and not exhaustive.
[74] For an overview of such systems deployed in Europe, see Fair Trials, 'Automating Injustice: The Use of Artificial Intelligence and Automated Decision-Making Systems in Criminal Justice in Europe' (9 September 2021) Section 1.1, 8–18 <https://tinyurl.com/3xscz4n9> accessed 20 November 2025.
[75] See the Commission's Guidelines on prohibited AI practices (n 24) point 190. See also K Lum and W Isaac, 'To Predict and Serve?' (2016) 13(5) Significance 14. Regarding discrimination in racial or ethnic profiling practices in general, see FRA, 'Towards More Effective Policing, Understanding and Preventing Discriminatory Ethnic Profiling: A Guide' (Publications Office of the European Union 2010).
[76] See Ensign and others, 'Runaway Feedback Loops in Predictive Policing' (2018) 81 Proceedings of Machine Learning Research 1–12; L Bennett Moses and J Chan, 'Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability' (2018) 28(7) Policing and Society 806.
[77] See J Angwin and others, 'Machine Bias' (*ProPublica*, 23 May 2016) <https://tinyurl.com/46fez35j> accessed 20 November 2025. See also, M Hamilton,

In a similar vein, the algorithm deployed in a Dutch town to predict the risk of 'mobile banditry' among car drivers or passengers was accused of targeting mostly persons with Eastern European nationalities and/or of Roma ethnicity.[78] Such discriminatory outcomes may also arise due the use of protected personal traits or proxies thereof as variables into the systems concerned. For instance, it has been revealed that the 'HART' system used in the United Kingdom to assess the risk of suspects re-offending in the future and to advise accordingly on whether to charge them or release them into a rehabilitation programme relied on ethnicity data or socioeconomic proxy information, including postcodes.[79]

It is noted that the prohibition in Article 5(1)(d) of the AI Act applies irrespective of whether the personal traits, on the basis of which crime predictions are performed, constitute protected characteristics under non-discrimination law, or whether they form part of sensitive categories of data in the sense of the Law Enforcement Directive, which explicitly prohibits profiling based on such data that results in discrimination against natural persons.[80] Yet, insofar as such practices are targeted at individuals belonging to protected social groups, they will also be captured by Article 21(1) of the Charter, the application of which is triggered by virtue of the AI Act's prohibition that brings AI-enabled crime risk assessments under the scope of EU law.[81] In this regard, Article 5(1)(d) of the AI Act is of great added value, considering, on the one hand, that the EU Equality Directives are only applicable to

---

'The Biased Algorithm: Evidence of Disparate Impact on Hispanics' (2019) 56(4) American Criminal Law Review 1553.

[78] See Amnesty International, 'We Sense Trouble: Automated Discrimination and Mass Surveillance in Predictive Policing in the Netherlands' (EUR 35/2971/2020, 28 November 2020) <https://tinyurl.com/srzsr5bz> accessed 20 November 2025.

[79] See Big Brother Watch, 'Briefing on Algorithmic Decision-Making in the Criminal Justice System' (January 2020) 7–11 <https://tinyurl.com/mr3bhasd> accessed 20 November 2025.

[80] See Art 11(3) of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89. Pursuant to Art 10 of the said Directive, special categories of personal data include those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, and those concerning health or a person's sex life or sexual orientation. The categories of data considered as 'sensitive' largely correspond to the prohibited grounds of discrimination under the EU Equality Directives and Art 21(1) of the Charter, even though they do not fully overlap with those.

[81] In the context of the European Convention on Human Rights (ECHR), instances of discriminatory profiling can be captured by Art 14 (prohibition of discrimination) combined with other ECHR provisions, as well as by Art 1 of Protocol No 12 to the Convention of 4 November 2000 (general prohibition of discrimination). Given that Art 21(1) of the Charter corresponds to Art 14 ECHR in the sense of Art 52(3) of the Charter, the CJEU may thus rely on the case law of the ECtHR on discriminatory racial or ethnic profiling. For an overview of such case law, see ECtHR's Press Unit, 'Factsheet - Racial Profiling' (May 2024) <https://tinyurl.com/bdd3cup9> accessed 20 November 2025.

certain economic settings and not to the field of the State's law enforcement activities,[82] and, on the other hand, that the Law Enforcement Directive applies only to the processing of personal data, excluding aggregate or anonymous data, which do not relate to an identified or identifiable person, but may often be processed by AI systems.[83] Furthermore, the outright prohibition contained in Article 5(1)(d) of the AI Act seems more apt for addressing the systemic and structural nature of certain discriminatory practices, such as racial or ethnic profiling, which is often overlooked or not effectively captured in the context of individual discrimination claims.[84]

That said, AI systems employed to support human assessments of the involvement of a person in a criminal activity that is based on objective and verifiable facts linked to a criminal activity are not covered by Article 5(1)(d) of the AI Act. Likewise, location- or geospatial or place-based crime predictions, which do not entail an assessment of a specific individual but merely make predictions about the likelihood of a crime being committed in certain areas, fall outside the scope of the AI Act's prohibitions, unless the risk score of the place or location constitutes an aspect in the profiling of a person.[85] Nevertheless, these two categories of AI risk assessments may still fall within the ambit of EU non-discrimination rules if they are correlated with prohibited grounds, such as racial or ethnic origin. On the one hand, even in cases of hybrid or semi-automated systems where humans are somehow involved in the decision-making process, the latter tend to favour the outcomes produced by the AI systems regardless of how inaccurate or biased they may be, due to the perception that such systems are generally neutral and reliable, a phenomenon known as 'automation bias'.[86] On the other hand, with regard to geographic crime prediction practices, these may often also prove to be discriminatory, as was the case, for instance, of the 'CAS' system deployed in the Netherlands to predict crime rates in specific areas by relying, among other predictors, on the number of 'non-Western' individuals living in those areas.[87] In such instances, if

---

[82] For a different view on the applicability of Directive 2000/43 in racial or ethnic profiling, see J Klaas, R Beets and M Hendrickx, 'Guide on Strategic Litigation to Combat Ethnic Profiling in the European Union' (Public Interest Litigation Project (PILP-NJCM) 2020) 29 <https://tinyurl.com/yj4ek48y> accessed 20 November 2025.
[83] See recital 21 of the said Directive and the definition of 'personal data' under Article 3(1) thereof.
[84] Regarding racial profiling as structural discrimination, see eg N Crowley, 'To Name and Address the Underlying Problem: Structural Discrimination on the Ground of Racial or Ethnic Origin' (European Commission, Publications Office of the European Union 2022). See also N Dube, 'Wa Baile v Switzerland: An Implicit Acknowledgment of Racial Profiling as Structural Discrimination' (*Strasbourg Observer*s, 26 March 2024) <https://tinyurl.com/3wuynhmm> accessed 20 November 2025.
[85] See the Commission's Guidelines on prohibited AI practices (n 24) points 212–213. For an overview of such systems in Europe, see Fair Trials (n 74) Section 1.2, 19–26.
[86] See Fair Trials (n 74) Section 3.1, 34. On the problem of automation bias in general, see eg K Mosier and others, 'Automation Bias: Decision Making and Performance in High-Tech Cockpits' (1998) 8(1) The International Journal of Aviation Psychology 47.
[87] See Fair Trials (n 74) Section 1.2.1, 19–20. See also S Oosterloo and G van Schie, 'The Politics and Biases of the "Crime Anticipation Systems" of the Dutch Police' (Proceedings of the International Workshop on Bias in Information, Algorithms, and Systems co-located with 13th International Conference on Transforming Digital

totally innocent residents of allegedly high-risk areas are incorrectly targeted, the doctrine of discrimination by association becomes of particular relevance in a way similar to the one upheld by the CJEU in *CHEZ*.[88]

2.4 Untargeted scraping of facial images

Article 5(1)(e) of the AI Act prohibits the use of AI systems to create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage. This practice entails the automatic extraction of data or content containing human faces (eg pictures, videos) along with any associated information (eg geo-localisation, names of the persons depicted) from different sources, such as websites, social media platforms, or CCTV material (eg surveillance cameras installed in airports, streets, parks, etc), without a specific focus on a given individual or group of individuals, in order to build-up a database capable of finding any match between the faces collected therein and digital photos of people.[89] The AI Act's prohibition in this regard comes as a response to the emergence of highly controversial tools like the ones developed by the US company 'Clearview AI' and the Polish website 'PimEyes', which have attracted considerable scrutiny for raising serious privacy-related concerns.[90] Such tools may be widely deployed by both public authorities, notably for law enforcement purposes, and various private entities, including banks, retail stores, and entertainment companies, or by anyone wishing to identify another person for any possible reason.[91]

Apart from their incompatibility with EU data protection rules,[92] AI-driven scraping systems and the ensuing facial recognition databases can also eventually enable or facilitate the discriminatory treatment of certain individuals or groups. To give some examples, such systems may lead to the erroneous arrests of persons of certain racial or ethnic

---

Worlds (iConference 2018) 2018) <https://tinyurl.com/4u84pmfv> accessed 20 November 2025.

[88] See Case C-83/14 *CHEZ Razpredelenie Bulgaria* ECLI:EU:C:2015:480. See also eg G Von Toggenburg, 'Discrimination by Association: A Notion Covered by EU Equality Law?' (2008) 3 European Law Reporter 82.

[89] See the Commission's Guidelines on prohibited AI practices (n 24) points 226–228.

[90] See K Hill, 'The Secretive Company That Might End Privacy as We Know It' (*The New York Times*, 18 January 2020) <https://tinyurl.com/3dsz5pfe> accessed 20 November 2025; D Gershgorn, 'This Simple Facial Recognition Search Engine Can Track You Down Across the Internet' (*Medium*, 9 June 2020) <https://tinyurl.com/yvcvppf4> accessed 20 November 2025.

[91] See R Mac, C Haskins and L McDonald, 'Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart, and the NBA' (*BuzzFeed.News*, 28 February 2020) <https://tinyurl.com/26bse9fr> accessed 20 November 2025; R Metz, 'Anyone Can Use This Powerful Facial-Recognition Tool - And That's a Problem' (*CNN*, 4 May 2021) <https://tinyurl.com/yv6tusxr> accessed 20 November 2025.

[92] See explicitly the Commission's Guidelines on prohibited AI practices (n 24) point 238. For an overview of the legal actions against Clearview AI and the fines imposed on it by Data Protection Authorities across various EU Member States, see noyb, 'Criminal Complaint Against Facial Recognition Company Clearview AI' (28 October 2025) <https://tinyurl.com/2c6k9cnu> accessed 20 November 2025.

origin when utilised by the police to identify suspects of crimes;[93] they may be relied on by supermarkets to deny access to their premises to undesired customers belonging to socioeconomically disadvantaged communities;[94] they may be used by an employer to check whether a job candidate has attended any gay events and thus decide whether or not to hire that person based on their presumed sexual orientation; or they may be privately used by individuals for gender-based cyberviolence and harassment, such as to stalk women, expose trans people, or identify sex workers.[95]

Even though the prohibition of Article 5(1)(e) of the AI Act targets only the creation or expansion of facial recognition databases and not the concrete act of biometric identification through facial recognition,[96] it significantly contributes to the prevention of AI-enabled discrimination. Unlike EU non-discrimination law which can potentially capture solely the discriminatory outcomes of facial recognition technologies as such and not the relevant databases, unless these are based on prohibited classifications,[97] the AI Act intervenes here at an earlier stage by prohibiting the creation or expansion of the relevant databases in the first place. Furthermore, contrary to the EU Equality Directives, Article 5(1)(e) of the AI Act is not confined to specific walks of life but rather applies across sectors.

2.5 Emotion recognition

According to Article 5(1)(f) of the AI Act, the marketing and use of AI systems to identify or infer emotions of natural persons in the areas of workplace and educational institutions are prohibited.[98] These systems enable the identification or inference of a wide range of emotions, such as happiness, sadness, anger, surprise, disgust, embarrassment, excitement, shame, contempt, satisfaction, or amusement, on the basis of the biometric data of the persons concerned relating, for instance, to basic facial expressions, such as a frown or a smile, or gestures such

[93] See K Hill, 'Wrongfully Accused by an Algorithm' (*The New York Times*, 24 June 2020) <https://tinyurl.com/bdzjmuu3> accessed 20 November 2025; E Stokes, 'Wrongful Arrest Exposes Racial Bias in Facial Recognition Technology' (*CBS News*, 19 November 2020) <https://tinyurl.com/mus76pp9> accessed 20 November 2025. See also J Cebreros, 'Facial Recognition Technology and Wrongful Arrests in the Digital Policing Era' 100 (2025) Washington Law Review Online 33-51.

[94] See Big Brother Watch, 'Biometric Britain: The Expansion of Facial Recognition Surveillance' (23 May 2025) 100-4 <https://tinyurl.com/3rz4a877> accessed 20 November 2025. See also GDPRhyb, 'AEPD (Spain) - PS/00120/2021' <https://tinyurl.com/32cz6e43> accessed 20 November 2025.

[95] See European Parliament, 'PimEyes: The Fundamental Rights Implications of Private Use of Facial Recognition Technology and Biometric Databases' (Parliamentary question E-002586/2022, 14 July 2022). See also J Wakefield, 'PimEyes Facial Recognition Website "Could Be Used by Stalkers"' (*BBC*, 11 June 2020) <https://tinyurl.com/mr634yxv> accessed 20 November 2025.

[96] See the Commission's Guidelines on prohibited AI practices (n 24) point 237. For the rules governing biometric identification systems see below Section 2.7.

[97] On the discriminatory potential of facial recognition technologies, see below Section 2.7.

[98] See Art 3(39) and recital 44 AI Act. See also the Commission's Guidelines on prohibited AI practices (n 24) points 244–245.

as the movement of hands, arms or head, or characteristics of those persons' speech, such as a raised voice or whispering.[99] However, since the expression of emotions varies considerably across different cultures and situations, and even across different people within a single situation,[100] emotion recognition tools have been criticised for lacking sufficient accuracy and reliability, but also for being prone to generate discriminatory outcomes.[101] In particular, research has demonstrated that such tools may present higher error rates for people with darker skin tone, being more likely to predict those people as having negative emotions (eg anger, sadness, etc) even when they are smiling;[102] they may perceive emotions more accurately for younger adults than for older persons;[103] and they may show gender bias in the form of an accuracy gap between men and women.[104]

The prohibition of AI-based emotion recognition systems under Article 5(1)(f) of the AI Act explicitly applies only in situations related to work or education, given the imbalance of power existing in those settings.[105] For example, the use of such systems by an employer during the recruitment process, or by an educational institution during admissibility tests for new students, is prohibited.[106] To the extent that these AI tools could lead to detrimental or unfavourable treatment of certain persons or whole groups, such instances will also amount to prohibited discrimination, without prejudice to the respective material scope of each Equality Directive. This means that, whereas discriminatory emotion recognition systems used in the context of work will be captured by EU non-discrimination secondary legislation regardless of whether they affect people because of their racial or ethnic origin, sex, religion, age, disability, or sexual orientation, similar systems used in the context of education will be captured only in cases where they discriminate against certain persons based on their racial

---

[99] See Art 3(39) and recital 18 of the AI Act. See also the Commission's Guidelines on prohibited AI practices (n 24) points 247–252.

[100] See L Feldman Barrett and others, 'Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements' (2019) 20(1) Psychological Science in the Public Interest 1.

[101] See recital 44 of the AI Act. See also the Commission's Guidelines on prohibited AI practices (n 24) point 241.

[102] See R Khan and C Stinson, 'Auditing Facial Emotion Recognition Datasets for Posed Expressions and Racial Bias' (2025) arXiv abs/2507.10755 [cs.CV] <https://tinyurl.com/yc5z3nuh> accessed 20 November 2025.

[103] See E Kim and others, 'Age Bias in Emotion Detection: An Analysis of Facial Emotion Recognition Performance on Young, Middle-Aged, and Older Adults' (AIES '21: Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society, 19–21 May 2021) 638 <https://tinyurl.com/3merafm8> accessed 20 November 2025.

[104] See A Domnich and G Anbarjafari, 'Responsible AI: Gender Bias Assessment in Emotion Recognition' (2021) arXiv abs/2103.11436 [cs CV] <https://tinyurl.com/4hy76uvc> accessed 20 November 2025. For biases in facial recognition in relation to gender, ethnicity, and age, see also J Pahl and others, 'Female, White, 27? Bias Evaluation on Data and Algorithms for Affect Recognition in Faces' (FAccT '22: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency, 21–24 June 2022) 973 <https://tinyurl.com/yctkfhv6> accessed 20 November 2025.

[105] See recital 44 of the AI Act.

[106] See the Commission's Guidelines on prohibited AI practices (n 24) points 254–255.

or ethnic origin under Directive 2000/43.[107] Nevertheless, this limit can be overcome by the simultaneous application of Article 5(1)(f) of the AI Act and Article 21(1) of the Charter in this regard.

It is further noted that, by prohibiting outright any AI-powered emotion recognition practices in work- or education-related situations, Article 5(1)(f) of the AI Act applies irrespective of whether such practices affect individuals on the basis of prohibited grounds under EU non-discrimination law. Conversely, AI systems, which are intended to detect the emotional state of individuals in all other domains than the workplace or education and thus fall outside the ambit of Article 5(1)(f) AI Act,[108] may still be prohibited by the EU non-discrimination rules if they fall within the personal and material scope thereof. This will be the case, for instance, where a customer of a given ethnicity is mistakenly perceived as too angry by an emotion recognition camera when entering a retail store, thus being denied access to certain products.

However, the legal protection granted against the risk of discrimination of emotion recognition tools remains incomplete. The use of such AI systems risks falling through the cracks of both Article 5(1)(f) of the AI Act and non-discrimination law where the disadvantageous treatment of individuals stemming from an erroneous identification or inference of their emotions occurs in an area of life other than work or education and at the same time is not covered by the material scope of the Equality Directives. By way of illustration, where a person's emotions are misunderstood due to a certain medical condition or physical impairment that results in temporary or permanent paralysis of that person's facial muscles, thereby leading to a misdiagnosis for healthcare purposes,[109] neither Article 5(1)(f) of the AI Act nor Directive 2000/78 are applicable. Yet, it is in the context of law enforcement and migration, asylum, or border control management that this gap in protection is most remarkable. This is because AI-based emotion recognition technologies, such as lie detectors ('polygraphs'), may be largely deployed in these areas with potentially adverse consequences for the fundamental rights of the persons affected, including their right to non-discrimination.[110]

---

[107] This is because education is excluded not only from the scope of Directive 2000/78, which applies solely in the field of employment, but also from that of Directive 2004/113 (see Art 3(3) thereof).

[108] For a non-exhaustive overview of the areas, in which AI emotion recognition tools may be used, see the Commission's Guidelines on prohibited AI practices (n 24) point 240. These systems are, however, considered to be of high risk, pursuant to Annex III(1)(c) of the AI Act, and are subject to additional transparency requirements under Art 50. Besides, emotion recognition systems may also be prohibited in certain cases by virtue of Art 5(1)(a) and (b). See in this regard the Commission's Guidelines (n 24) point 266.

[109] See K Vemou and A Horvath, 'EDPS TechDispatch on Facial Emotion Recognition' (European Data Protection Supervisor, Issue 1, 2021) <https://tinyurl.com/2jkkccjr> accessed 20 November 2025.

[110] Although such technologies are not currently used at the EU borders, their development has been tested by EU-funded projects. See eg R Picheta, 'Passengers to Face AI Lie Detector Tests at EU Airports (*CNN*, 2 November 2018) <https://tinyurl.com/47jb82jv> accessed 20 November 2025. For more details, see J

2.6 Biometric categorisation

The prohibition of Article 5(1)(g) of the AI Act covers AI systems that categorise individuals based on their biometric data to deduce or infer a number of sensitive characteristics, namely their race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation.[111] Such categorisation may rely on the physical and physiological features (eg face, skin, eye and hair colour, hand patterns, ear shape, fingerprints, voice, etc.) or behavioural characteristics of the persons concerned (eg keystroke, gait, way of moving, etc), based on which those persons are assigned to specific categories.[112] To give a few examples, prohibited biometric categorisation systems may include a system claiming to be capable of deducing an individual's race from their voice, or their religious affiliation from their tattoos,[113] or a filter categorising users of a social media platform according to their assumed political opinions or sexual orientation by analysing the photos they have uploaded on the platform in order to send them targeted advertisements.[114]

The relevance of EU non-discrimination law is evident in this respect, given that some of the categories to which individuals are assigned based on their biometric features may overlap with protected attributes under the EU Equality Directives and Article 21(1) of the

---

Sánchez-Monedero and L Dencik, 'The Politics of Deceptive Borders: "Biomarkers of Deceit" and the Case of iBorderCtrl' (2020) 25(3) Information, Communication and Society 413; D Ozkul, 'Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe' (Algorithmic Fairness and Asylum Seekers and Refugees (AFAR) Project, Refugee Studies Centre, University of Oxford, 2023) 26–27.

[111] See also recital 30 of the AI Act. For the definition of a 'biometric categorisation system', see Art 3(40) of the AI Act. For a detailed analysis of biometric technologies and the data protection and privacy risks they entail, see Article 29 of the Data Protection Working Party (Art 29 Working Party, the predecessor of the current European Data Protection Board), 'Opinion 3/2012 on developments in biometric technologies' (WP193, 27 April 2012).

[112] See the Commission's Guidelines on prohibited AI practices (n 24) point 278. For a definition of 'biometric data' under the AI Act, see Art 3(34) thereof.

[113] See the Commission's Guidelines on prohibited AI practices (n 24) point 283.

[114] ibid, point 280. Regarding the use of Facebook pictures to extract information about a person's personality traits, see C Segalin and others, 'What Your Facebook Profile Picture Reveals about Your Personality' (Proceedings of the 25th ACM International Conference on Multimedia (MM '17), 23–27 October 2017) 460 <https://tinyurl.com/4sky9384> accessed 20 November 2025. For the ability of facial recognition technology to reveal individuals' "liberal" or "conservative" political affiliation, see M Kosinski, 'Facial Recognition Technology Can Expose Political Orientation from Naturalistic Facial Images' (2021) 11 (article no 100) Scientific Reports. For the ability of algorithms to detect the sexual orientation of persons from their face images, see Y Wang and M Kosinski, 'Deep Neural Networks Are More Accurate than Humans at Detecting Sexual Orientation from Facial Images' (2018) 114(2) Journal of Personality and Social Psychology 246; J Leuner, 'A Replication Study: Machine Learning Models Are Capable of Predicting Sexual Orientation from Facial Images' (2019) arXiv:1902.10739 [cs.CV] <https://tinyurl.com/yu9aax9k> accessed 20 November 2025.

Charter.[115] More specifically, the personal scope of the AI Act's prohibition of biometric categorisation is partly broader compared to that of EU non-discrimination law, by also encompassing characteristics of a sensitive nature that are not recognised as prohibited grounds of discrimination (ie trade union membership and sex life), but also partly narrower, by leaving aside other personal traits that are protected against discrimination (ie sex and age).[116] Moreover, unlike the EU Equality Directives, whose material scope is limited to certain walks of life, Article 5(1)(g) of the AI Act seems to apply horizontally across sectors except for law enforcement. Accordingly, whereas, for instance, an AI-powered tool used by an employer to detect the sexual orientation of job candidates from their face images on their CVs and directly reject homosexual candidates without any interview will be captured by both Directive 2000/78 and the AI Act's prohibition, a similar system deployed by a retail store to recognise homosexual parents using a given social media platform and preclude them from receiving targeted advertisements for baby care products will fall outside the scope of Directive 2000/78, but will still be prohibited under Article 5(1)(g) of the AI Act alone or in combination with Article 21(1) of the Charter. Yet, as in the case of Article 5(1)(b) of the AI Act, the question remains here whether this article could be interpreted in the light of Article 21(1) of the Charter so as to capture also discriminatory outcomes resulting from AI-driven biometric categorisation of individuals based on characteristics other than those mentioned in the AI Act's prohibition, notably sex and age.[117]

In any case, the labelling or filtering of biometric datasets through biometric categorisation systems on the basis of all the characteristics referred to in Article 5(1)(g) of the AI Act, including in the area of law enforcement, falls outside the scope of the prohibition. The rationale behind this derogation is precisely the need to guarantee equal representation for all demographic groups in the relevant datasets and, by extension, to prevent discrimination arising from biased data.[118] In fact, such labelling operations may even be needed sometimes to ensure compliance with the AI Act's requirements for high-risk AI systems under Articles 10 and 17 thereof.[119] However, the legislative choice to leave any categorisation of biometric data in the area of law enforcement outside the realm of Article 5(1)(g) of the AI Act altogether is rather regrettable. As law enforcement constitutes one of the main fields where biometric data are widely used, any discriminatory outcomes stemming from the AI-enabled categorisation of individuals into clusters based on such data risk falling through the cracks of both non-discrimination law and the AI Act.

---

[115] See the Commission's Guidelines on prohibited AI practices (n 24) point 278.
[116] The similarity between the characteristics referred to in Art 5(1)(g) of the AI Act and those listed under Art 9(1) GDPR and Art 10 of the Law Enforcement Directive is easily noticeable.
[117] Yet, the Commission's Guidelines on prohibited AI practices (n 24) point 288 seem to preclude this possibility.
[118] See the Commission's Guidelines on prohibited AI practices (n 24) point 285.
[119] ibid.

2.7 Real-time biometric identification

Pursuant to Article 5(1)(h) of the AI Act, the use of real-time biometric identification (RBI) systems in publicly accessible spaces for law enforcement purposes is in principle prohibited yet subject to certain exceptions envisaged in Article 5(1)(h)(i)–(iii), pursuant to which the use of such systems may be permitted when authorised by Member States' national legislation and as long as the conditions and safeguards provided for by Article 5(2)–(7) are met.[120] The limited ban of RBI technologies constitutes the outcome of a political compromise between the European Parliament and the Council of Ministers, having been one of the most contentious issues during the negotiation process for the adoption of the AI Act.[121] Although the significant derogations featured in the final version of Article 5 of the AI Act admittedly mitigate the AI Act's prohibition in relation to RBI practices, they do not detract from the predominantly prohibitive function of the said provision, the wording and structure of which clearly indicate that, as a rule, such AI-based practices are prohibited.[122] This will be the case when the strict requirements of Article 5(2)–(7) of the AI Act are not fulfilled, such as in the absence of detailed domestic Member State law that expressly allows the use of real-time RBI for one or more of the objectives listed in Article 5(1)(h)(i)–(iii) of the AI Act, or where no fundamental rights impact assessment has been carried out by the law enforcement authority concerned pursuant to Article 5(2) of the AI Act, or where no prior authorisation has been granted by a judicial or an independent administrative authority as per Article 5(3).

RBI within the meaning of Article 5(1)(h) of the AI Act refers to AI systems deployed in physical spaces accessible to an undetermined number of people (eg shops, restaurants, banks, stadiums, museums, public transport, roads, squares, etc) in order to perceive multiple natural persons simultaneously and identify them, without their active involvement, typically at a distance, by comparing those persons' biometric data with the data contained in a database, whereby the capturing of such data and the comparison and identification process

---

[120] According to Art 5(5) of the AI Act, it is up to the Member State to decide whether and in which of the three situations of Art 5(1)(h)(i)–(iii) the use of RBI systems in publicly accessible spaces for law enforcement purposes will be permitted in their territory. For a detailed analysis of the prohibition of RBI systems under the AI Act, see the Commission's Guidelines on prohibited AI practices (n 24) points 326–424. See also A Giannini and S Tas, 'AI Act and the Prohibition of Real-Time Biometric Identification: Much Ado about Nothing?' (*Verfassungsblog*, 10 December 2024) <https://tinyurl.com/46krmw8a> accessed 20 November 2025.

[121] See eg L Bertuzzi, 'AI Act: MEPs Mull Narrow Facial Recognition Technology Uses in Exchange for Other Bans' (*Euractiv*, 6 November 2023) <https://tinyurl.com/33fcty5w> accessed 20 November 2025.

[122] I am thankful to one of the anonymous reviewers of this article for inviting me to address this 'paradox'.

all occur without a significant delay.[123] Most notably, these tools may include live surveillance cameras working with AI-driven facial recognition techniques that scan, for example, all incoming visitors to a concert hall or all passengers in metro stations.[124]

It is known, however, that AI-powered biometric identification technologies may produce biased results or entail discriminatory effects, with their accuracy varying across different demographic groups.[125] More specifically, facial recognition systems have been found likely to lead to false positive outputs for people of specific racial or ethnic origins, mostly for dark-skinned women;[126] they have been found to be less reliable for children and younger people,[127] biased against persons with face disabilities or craniofacial differences,[128] and prone to misclassify transgender individuals.[129] The adverse consequences of potential misidentifications by these systems are particularly far-reaching when operating in real-time in the field of law enforcement, which covers all activities carried out by public authorities (eg the police, prosecutors, etc) or on their behalf (eg public transport companies, sports federations, banks, etc) for the prevention, investigation, detection, or prosecution of criminal offences, or the execution of criminal penalties, including safeguarding against and preventing threats to public security.[130] This is due to the immediate impact and limited opportunities for further checks or corrections in relation to the real-time use of RBI tools, which, apart from raising serious concerns about enabling mass surveillance and infringing the

---

[123] See Art 3(35), (41)-(42) as well as recitals 17 and 19 of the AI Act. See also the Commission's Guidelines on prohibited AI practices (n 24) points 297–318.
[124] See the Commission's Guidelines on prohibited AI practices (n 24) points 306–311.
[125] See recital 32 of the AI Act. See also eg SA Magnet, *When Biometrics Fail: Gender, Race, and the Technology of Identity* (Duke University Press 2011); P Grother, M Ngan and K Hanaoka, 'Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects' (National Institute of Standards and Technology, NISTIR 8280, December 2019) <https://tinyurl.com/yrkj8bh7> accessed 20 November 2025.
[126] See F Bacchini and L Lorusso, 'Race, Again: How Face Recognition Technology Reinforces Racial Discrimination' (2019) 17(3) Journal of Information, Communication and Ethics in Society 321; J Buolamwini and T Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research 77.
[127] See D Michalski, SY Yiu and C Malec, 'The Impact of Age and Threshold Variation on Facial Recognition Algorithm Performance Using Images of Children' (Proceedings of International Conference on Biometrics, 2018) 217–224 <https://tinyurl.com/2r98xz4w> accessed 20 November 2025; FRA, 'Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement' (Publications Office of the European Union 2020) 289.
[128] See MK Scheuerman, J Paul and J Brubaker, 'How Computers See Gender: An Evaluation of Gender Classification in Commercial Facial Analysis and Image Labeling Services' (2019) 3(CSCW) Proceedings of the ACM on Human-Computer Interaction 1; O Keyes, 'The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition' (2018) 2(CSCW) Proceedings of the ACM on Human-Computer Interaction 1.
[129] See S Byrne-Haber, 'Disability and AI Bias' (*Medium*, 11 July 2019) <https://tinyurl.com/4a735y9a> accessed 20 November 2025.
[130] See Art 3(46) of the AI Act. See also the Commission's Guidelines on prohibited AI practices (n 24) points 319–325.

fundamental rights and freedoms of individuals,[131] may also reinforce police bias against certain marginalised minorities or be misused for political, religious, racial/ethnic, or other persecution.[132] A striking example in this respect is drawn from Hungary's newly adopted legislation allowing the police to use real-time facial recognition technology to identify and fine participants in Pride events, which have been banned in the context of the Hungarian government's aggressive policy agenda against sexual and gender diversity.[133]

Unlike non-discrimination law, the use of real-time RBI systems is prohibited under the AI Act irrespective of whether the affected individuals belong to any specific social group. Yet, to the extent that such systems may explicitly target or disproportionately affect persons with protected characteristics under the EU Equality Directives or Article 21(1) of the Charter, the protection granted under the two legal regimes may sometimes overlap, provided that the RBI systems in question are actually prohibited by failing to comply with the requirements set out in Article 5(2)–(7) of the AI Act.

Nevertheless, significant loopholes still exist. All other uses of RBI systems that are not covered by Article 5(1)(h) of the AI Act, such as their deployment by private actors or for purposes other than law enforcement, are not prohibited under the AI Act.[134] In those instances, though, the EU non-discrimination rules still apply, capturing any potential discriminatory outputs of such systems against members of protected social groups. The same holds, most importantly, with regard to the retrospective use of RBI systems for law enforcement purposes, which escapes the AI Act's prohibition and is considered high-risk, being subject to the additional safeguards provided for in Article 26(10) of the AI Act. Whereas real-time RBI technologies enable the capturing of individuals' biometric data, the comparison and identification to occur 'instantaneously, near-instantaneously or in any event without a significant delay' by relying on 'live' or 'near-live' material, in the case of 'post' systems, the biometric data have already been captured and the comparison and identification happen only after a significant delay through material generated before the use of the system on the persons concerned (eg recorded CCTV camera footage).[135] Given that the devices used for real-time and *ex post* RBI are usually one and the same with different functionalities, the discrimination risks will be equally high in both instances, thus making the AI Act's differentiated approach on a purely temporal basis rather problematic.[136]

---

[131] See recital 32 of the AI Act.
[132] See L Arnold, 'How the European Union's AI Act Provides Insufficient Protection Against Police Discrimination' (*Journal of Law and Social Change*, 14 May 2024) <https://tinyurl.com/mznk8598> accessed 20 November 2025.
[133] See P Haeck and C Körömi, 'Hungary on EU Watchlist Over Surveillance at Pride' (*Politico*, 25 April 2025) <https://tinyurl.com/3fd9xz3c> accessed 20 November 2025.
[134] See the Commission's Guidelines on prohibited AI practices (n 24) points 425–428. Instead, these systems fall within the category of high-risk AI systems in accordance with Art 6 and Annex III(1)(a) thereof.
[135] See recital 17 of the AI Act.
[136] See the Commission's Guidelines on prohibited AI practices (n 24) point 310.

3 The regulatory function

The largest part of the AI Act concerns AI systems that pose a high risk to EU public interests and fundamental rights. As per Article 6 of the Act, apart from systems that are used as safety components of products or are products themselves, AI systems will qualify as high risk if used in one of the pre-defined areas mentioned under Annex III of the Act, with the Commission being empowered to amend the list of high-risk systems in light of evolving technological developments.[137] When classifying an AI system as high risk, the extent of the adverse impact caused by that system on fundamental rights protected by the Charter, including non-discrimination and gender equality, is of particular relevance.[138] However, the fact that certain AI systems are deemed as high risk under the AI Act does not indicate that their use is lawful under other pieces of EU or national law.[139] As noted before, the prohibition of certain AI practices under other legal instruments, including non-discrimination legislation, remains unaffected by the AI Act.[140]

In fact, most of the high-risk systems listed in Annex III raise serious discrimination concerns, as also explicitly acknowledged by the AI Act's preamble.[141] For example, the use of RBI systems may lead to biased results and entail discriminatory effects based on age, ethnicity, race, sex or disabilities,[142] while historical patterns of discrimination, among others, against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation, may also be perpetuated by AI systems deployed in education (eg to determine access or admission)[143] and employment (eg for the recruitment or selection of natural persons).[144] Another area in which there is a high risk of discrimination against persons or groups as a

---

[137] See Arts 6(6)–(8) and 7 of the AI Act and recital 52 thereof.
[138] See recital 48 of the AI Act.
[139] See recital 63 of the AI Act.
[140] See Art 5(8) of the AI Act.
[141] Pursuant to Art 6(3) of the AI Act, where an AI system referred to in Annex III does not pose a significant risk of harm to fundamental rights, it will not be considered high risk. Nevertheless, if that system performs profiling of natural persons, it will always be deemed high-risk.
[142] See recital 54 and Annex III(1) of the AI Act. See also Section 2.7.
[143] See recital 56 and Annex III(3) of the AI Act. See also eg D Gándara and others, 'Inside the Black Box: Detecting and Mitigating Algorithmic Bias Across Racialized Groups in College Student-Success Prediction' (2024) 10 AERA Open; R Kizilcec and H Lee, 'Algorithmic Fairness in Education' in W Holmes and K Porayska-Pomsta (eds), *Ethics in Artificial Intelligence in Education: Current Challenges, Practices, and Debates* (Routledge 2022).
[144] See recital 57 and Annex III(4) of the AI Act. See also eg C Rigotti and E Fosch-Villaronga, 'Fairness, AI and Recruitment' (2024) 53 Computer Law and Security Review 105966; Z Chen, 'Ethics and Discrimination in Artificial Intelligence-Enabled Recruitment Practices' (2023) 567 Humanities and Social Sciences Communications. A real-life case in this regard is Amazon's AI recruitment system which was found to disadvantage female job applicants. See J Dastin, 'Insight: Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women' (*Reuters*, 11 October 2018) <https://tinyurl.com/ms3fvhhh> accessed 20 November 2025.

result of the use of AI technologies is the access to and enjoyment of essential private or public services where AI systems may be deployed for a wide range of purposes, such as to determine the eligibility of natural persons for public assistance benefits and services,[145] to evaluate the creditworthiness of natural persons or establish their credit score,[146] or to assess risk and determine pricing for life and health insurance.[147] Similar concerns are raised with regard to AI systems used in the context of law enforcement (eg to assess the risk of a natural person becoming the victim of criminal offences or the reliability of evidence),[148] or migration, asylum and border control management (eg to assist the competent authorities in the examination of applications for asylum and visa or residence permits).[149]

Against this background, the AI Act's so-called 'regulatory function' consists of laying down a number of stringent mandatory requirements and obligations in Articles 8–27 that the 'providers' and 'deployers' of high-risk AI systems must comply with in order to prevent or mitigate any discriminatory outcomes.[150] Even though the AI Act could potentially be viewed as a regulatory instrument in its entirety, the term 'regulatory function' is deployed here as specifically relating to the conditions under which high-risk systems can be placed on the market, put into service, and used, with the aim of minimising the risk of those systems giving rise to AI-enabled discrimination. Accordingly, the AI Act establishes a set of harmonised rules that are complementary to the existing EU non-discrimination legislation.[151]

---

[145] See recital 58 and Annex III(5)(a) of the AI Act. A notorious real-world example in this area is offered by the Dutch fraud detection system 'SyRI', which was declared incompatible with fundamental rights by the District Court of the Hague. See Rechtbank Den Haag, zaaknummer C-09-550982-HA ZA 18-388, 5 February 2020 ECLI:NL:RBDHA:2020:1878.

[146] See recital 58 and Annex III(5)(b) of the AI Act, pointing out that such systems may not only perpetuate historical patterns of discrimination but even create new forms of discriminatory impacts. On the discriminatory potential of credit scoring systems, see eg Hurley and Adebayo (n 71); Langenbucher (n 71).

[147] See recital 58 and Annex III(5)(c) of the AI Act. See in this regard eg M van Bekkum, F Zuiderveen Borgesius and T Heskes, 'AI, Insurance, Discrimination and Unfair Differentiation: An Overview and Research Agenda' (2024) arXiv:2401.11892 [cs.CY] <https://tinyurl.com/yc2mmnz9> accessed 20 November 2025.

[148] See recital 59 and Annex III(6) of the AI Act. See in this regard eg G González-Fuster, 'Artificial Intelligence and Law Enforcement: Impact on Fundamental Rights' (European Parliament's LIBE Committee, PE 656.295, July 2020) <https://tinyurl.com/3a8vm2v4> accessed 20 November 2025.

[149] See recital 60 and Annex III(7) of the AI Act. See in this regard eg C Dumbrava, 'Artificial Intelligence at EU Borders: Overview of Applications and Key Issues' (European Parliamentary Research Service, PE 690.706, July 2021) <https://tinyurl.com/5n83kjw2> accessed 20 November 2025.

[150] See recitals 64 and 66 of the AI Act. For the definition of the terms 'provider' and 'deployer' of AI systems, see Art 3(3) and (4) of the AI Act. Depending on the context, the provider and deployer of a certain AI system may overlap, where the same entity produces and uses that system, for example in the case of an AI credit scoring system developed 'in house' by a financial institution for its own business. See also Art 25(1) of the AI Act listing the circumstances under which a deployer of a high-risk system or any other third party is to be considered a provider.

[151] See recital 9 of the AI Act, referring to 'fundamental rights' in general.

More specifically, the providers of high-risk AI systems must, inter alia, apply appropriate data governance practices; establish risk and quality management systems; draw up and keep the necessary technical documentation; guarantee effective human oversight of the systems' use; and ensure record-keeping as well as transparency, accuracy, robustness, and cybersecurity.[152] The deployers, for their part, are primarily required to take any appropriate technical and organisational measures ensuring that high-risk systems operate in accordance with the instructions for their use; to assign human oversight to natural persons; and to conduct an assessment of the systems' impact on fundamental rights.[153] To guarantee continuous compliance with these *ex ante* conformity requirements for AI systems, the AI Act also entrusts both providers and deployers with an *ex post* monitoring obligation for the purpose of identifying any need to take corrective or preventive actions in a timely manner.[154] Non-compliance with the aforementioned requirements and obligations may lead to the imposition of hefty administrative fines on the operators concerned.[155]

This entire set of rules delineating the AI Act's framework that applies to high-risk AI systems is intended to ensure respect of individuals' fundamental rights, such as their right to not be discriminated against. However, a detailed examination of how all technical requirements and obligations imposed on providers and deployers of AI systems may contribute to combatting discrimination or bias largely exceeds the scope and space of this article. For the purposes of my present analysis, I will exclusively focus below on Article 10 of the AI Act on data quality, governance, and de-biasing, being the only provision which is expressly meant to address the risk of AI-enabled discrimination.

Data quality, management, and de-biasing

Pursuant to Article 10(1) and (3), the datasets used for training, validation, and testing of such systems must be 'relevant, sufficiently representative, and to the best extent possible, free of errors and complete' in view of the system's intended purpose, while also having the appropriate statistical properties.[156] Since the data fed as input into an AI system determine the outputs generated, the high quality of data plays a crucial role in ensuring that AI systems perform as intended and do not result in prohibited discrimination, especially where the outputs may influence the inputs used for future operations, leading to 'feedback loops'.[157] Accordingly, biases embedded in the training data

[152] See Arts 9–19 of the AI Act.
[153] See Arts 26–27 of the AI Act. The obligation to carry out a fundamental rights impact assessment applies exclusively to deployers of the high-risk AI systems mentioned in Annex III(5)(b) and (c) of the AI Act.
[154] See Art 72 of the AI Act combined with Art 3(25) for providers, referring to the establishment of a 'post-market monitoring system', and Art 26(5) for deployers.
[155] See Art 99(4) of the AI Act.
[156] A similar requirement for data to be accurate and kept up to date also exists under Art 5(1)(d) GDPR.
[157] See recital 67 of the AI Act.

of AI systems constitute one of the main sources of algorithmic discrimination;[158] when the underlying data are inherently biased, the results provided by the AI systems concerned will be inclined to perpetuate and even amplify existing discrimination, in particular against persons belonging to certain vulnerable groups.[159] Such tainted data usually result from sampling bias, whereby some population segments are misrepresented, or from historical biases.[160] This will be the case, for instance, when an AI system developed by a financial institution for the purpose of automating loan decisions has been trained with data that contain, among other things, the postal codes of applicants and stem from a period when loans were more readily granted to people living in wealthier neighbourhoods, thereby perpetuating discrimination against residents of low-income neighbourhoods having a migration background.[161]

In light of these considerations, Article 10(2)(f) and (g) of the AI Act requires providers of high-risk AI systems to subject the training, validation, and testing datasets of their systems to data governance and management practices that involve an examination of possible biases, and provide for appropriate measures to detect, prevent, and mitigate any biases identified.[162] However, the AI Act does not define what 'bias' is nor does it determine how to measure it.[163] Further guidance at this point is thus crucial, given the variety of technical mechanisms developed in recent years for the purposes of ensuring fairness and mitigating biases, known as 'fairness metrics'.[164] However, these metrics are not always fit to meet the legal requirements of the EU non-discrimination framework.[165] Under these circumstances, it still

---

[158] See Barocas and Selbst (n 1); Hacker (n 16) 1146–1148. See also P Hacker, 'A Legal Framework for AI Training Data: From First Principles to the Artificial Intelligence Act' (2021) 13(2) Law, Innovation and Technology 257.

[159] This is commonly known in computer science as 'garbage in, garbage out'. See eg Xenidis and Senden (n 7) 156.

[160] See Hacker (n 16) 1146–1148; Barocas and Selbst (n 1) 680.

[161] See Data Protection Authority of Belgium, 'Artificial Intelligence Systems and the GDPR: A Data Protection Perspective' (December 2024) 9.

[162] See recital 67 of the AI Act.

[163] See 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' (2024) 26(3) Yale Journal of Law and Technology 671, 688. According to the High-Level Expert Group on Artificial Intelligence set up by the European Commission, 'Assessment List for Trustworthy AI' (2020) 23, 'bias' is defined as 'systematic and repeatable errors in a computer system that create unfair outcomes, such as favouring one arbitrary group of users over others'. See also Gerards and Xenidis (n 3) Section 1.5.1, 47.

[164] See Wachter (n 163) 688. For the main definitions and measures of algorithmic fairness, see among many others D Pessach and E Shmueli, 'Algorithmic Fairness' (2020) arXiv:2001.09784 [cs.CY] <https://tinyurl.com/4tw6x2mp> accessed 20 November 2025; S Verma and J Rubin, 'Fairness Definitions Explained' (IEEE/ACM International Workshop on Software Fairness (FairWare) 29 May 2018).

[165] See in detail S Wachter, B Mittelstadt and C Russel, 'Bias Preservation in Machine Learning: The Legality of Fairness Metrics Under EU Non-Discrimination Law' (2021) 123(3) West Virginia Law Review 735. See also H Weerts and others, 'Algorithmic Unfairness Through the Lens of EU Non-Discrimination Law: Or Why the Law Is Not a Decision Tree' (Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency, Chicago, June 2023).

remains unclear how de-biasing is to be effectively achieved in practice.[166]

That said, in order to ensure the detection and correction of biases, Article 10(5) of the AI Act explicitly allows providers to process special categories of personal data listed in Article 9(1) GDPR. As such, Article 10(5) is explicitly intended to prevent discrimination that might result from bias in AI systems.[167] The question as to the necessity of using such sensitive data as variables in algorithmic models to prevent the emergence of discriminatory outcomes has given rise to heated academic debate, not least because Article 9 GDPR in principle bans the collection of sensitive data.[168] It has been argued, though, that without knowledge of such data, providers of high-risk AI systems could not audit their systems for potential proxies that are likely to indirectly discriminate against certain protected groups of persons.[169]

In any event, the possibility of de-biasing AI systems through recourse to sensitive data applies only exceptionally and 'to the extent that it is strictly necessary', while also being subject to fundamental rights safeguards and several data protection requirements. This means that the removal of bias should only take place as far as this is mandated by Article 10(2)(f) and (g) of the AI Act, and as long as the provider has designed their intervention in the least intrusive way, in the sense that they must have clearly determined which biases will be targeted, which data will be used, and what risk of unlawful access to data exists.[170] At the same time, the provider must comply with a list of conditions under Article 10(5)(a)–(f) along with other requirements set out in the GDPR, including those of Article 9(2) thereof.[171] In this

---

[166] See M van Bekkum, 'Using Sensitive Data to De-Bias AI Systems: Article 10(5) of the EU AI Act' (2025) 56 Computer Law and Security Review (Article 106115) 10, suggesting that the de-biasing obligation should be clarified either by supervisory authorities or through the adoption of harmonised standards.

[167] See recital 70 of the AI Act.

[168] See M van Bekkum and F Zuiderveen Borgesius, 'Using Sensitive Data to Prevent Discrimination by Artificial Intelligence: Does the GDPR Need a New Exception?' (2023) 48 Computer Law and Security Review (Article 105770). See also I Žliobaitė and B Custers, 'Using Sensitive Personal Data May Be Necessary for Avoiding Discrimination in Data-Driven Decision Models' (2016) 24 Artificial Intelligence and Law 183.

[169] See van Bekkum (n 166) 2–3.

[170] ibid, 9–11.

[171] ibid, 11–14. For an overview of the interplay between the AI Act and the GDPR regarding data processing for the development of AI systems, see Data Protection Authority of Belgium (n 161). See, however, Commission, '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, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)' COM (2025) 837 final. According to recital 33 and Art 3(3) of this Proposal, a new exception would be inserted into the GDPR, namely Article 9(2)(k) and (5), allowing the use of sensitive data not only for the debiasing of AI systems but also for the training, testing, or validation of such systems in general. For more details on the Commission's Digital Omnibus Proposal, see eg H Ruschemeier, 'The Omnibus Package of the EU Commission: Or

regard, as specified by recital 70 of the AI Act, the processing of sensitive data for the purpose of bias correction under Article 10(5) constitutes a matter of 'substantial public interest' within the meaning of Article 9(2)(g) GDPR, as it ensures the protection of the individuals' right to non-discrimination.[172] Therefore, Article 10(5) of the AI Act reflects the legislator's attempt to strike a proper balance between data protection and non-discrimination law with regard to AI de-biasing and, as such, it can contribute to making AI systems less discriminatory.[173]

4 The enabling function

The AI Act did not originally provide for any redress mechanisms for the persons affected by AI systems. Despite repeated references in the Proposal's preamble to the protection of fundamental rights, the obligations imposed on providers and deployers did not give rise to any corresponding right of individuals to seek justice where these obligations have not been complied with, especially if the persons concerned have suffered discriminatory or otherwise unfair or harmful effects by AI-based outcomes.[174] This blind spot was eventually addressed by the European Parliament during the legislative procedure through the introduction of concrete rights and remedies to the benefit of individuals subjected to AI systems.[175]

The final version of the AI Act, as it currently stands, enables or empowers victims of AI-enabled discrimination or bias to seek effective legal redress, by granting them the right to file a complaint with the respective market surveillance authority entrusted with the implementation of the AI Act at the national level of each Member State, and the right to receive explanations about AI decision-making, while also empowering national equality bodies to access the relevant technical documentation.[176] These three mechanisms together constitute what I call the 'enabling function' of the AI Act, which exists without prejudice to and in parallel with any other administrative or

---

How to Kill Data Protection Fast' (*Verfassungsblog*, 17 November 2025) <https://tinyurl.com/yc3hzhet> accessed 20 November 2025.

[172] See S De Luca and M Federico, 'Algorithmic Discrimination Under the AI Act and the GDPR' (European Parliamentary Research Service, PE 769.509, 26 February 2025). It has also been argued, though, that the most plausible ground for such data processing seems to be a concrete 'legal obligation' in the sense of Art 6(1)(c) GDPR to which providers of AI systems are subject under Art 10(2) of the AI Act. See van Bekkum (n 166) 14.

[173] See M van Bekkum (n 166) 7, 11, providing a detailed analysis of the conditions and limits of this provision.

[174] See European Data Protection Board (EDPB) and 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) points 8–9, 18.

[175] See 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)' (P9_TA(2023)0236) amendments 627–630.

[176] See Arts 85, 86 and 77(1) of the AI Act respectively.

judicial remedies already available under EU or national non-discrimination law,[177] including the right of the persons concerned to file a discrimination claim before a national equality body, their right to challenge a discriminatory decision affecting them, as well as their right to request compensation or reparation for the loss and damage sustained because of discriminatory conduct.[178] Accordingly, in the following paragraphs, I will examine how recourse to the aforementioned means of legal redress provided for by the AI Act may complement, facilitate, or even reinforce the existing mechanisms under the non-discrimination framework.

4.1 Right to lodge a complaint with a market surveillance authority

The only actual remedy available to individuals under the AI Act is the right to submit complaints to the relevant market surveillance authority, pursuant to Article 85, which is granted to any person who believes that a provision of the AI Act has been infringed.[179] Each Member State must establish or designate at least one such authority, as per Article 70(1) of the AI Act, with the task of ensuring that the AI systems, which are marketed in their respective territory, comply with the requirements set out in the AI Act.[180] In this regard, the system of

[177] See Art 85 and recital 170 of the AI Act.

[178] See Arts 13 and 15 of Directive 2000/43, Art 17 of Directive 2000/78, as well as Arts 18, 20, and 25 of Directive 2006/54. See also Art 6(2) of Council Directive (EU) 2024/1499 of 7 May 2024 on standards for equality bodies in the field of equal treatment between persons irrespective of their racial or ethnic origin, equal treatment in matters of employment and occupation between persons irrespective of their religion or belief, disability, age or sexual orientation, equal treatment between women and men in matters of social security and in the access to and supply of goods and services, and amending Directives 2000/43/EC and 2004/113/EC [2024] OJ L2024/1499. For more details, see C Tobler, 'Remedies and Sanctions in EC Non-Discrimination Law: Effective, Proportionate and Dissuasive National Sanctions and Remedies, with Particular Reference to Upper Limits on Compensation to Victims of Discrimination' (European Commission, Publications Office of the European Union 2005). For an overview of national enforcement practices, see R Iordache and I Ionescu, 'Effectively Enforcing the Right to Non-Discrimination: Promising Practices Implementing and Going Beyond the Requirements of the Racial Equality and Employment Equality Directives' (European Commission, Publications Office of the European Union 2021); I Chopin and C Germaine, 'A Comparative Analysis of Non-Discrimination Law in Europe 2024: The 27 EU Member States Compared' (European Commission, Publications Office of the European Union 2024) Sections 4 and 5.

[179] Section 4 of Chapter IX of the AI Act titled 'Remedies' comprises both the right to file a complaint and the right to explanations under Arts 85 and 86, respectively, as well as Art 87 on the reporting of infringements and protection of reporting persons. However, as I argue later, the right to explanations does not actually constitute a remedy as such but rather enables the exercise of other remedies available under EU or national law. Likewise, the Whistleblower Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law [2019] OJ L305/17, does not provide any actual remedies to the persons concerned.

[180] According to Art 74(6) of the AI Act, as concerns high-risk AI systems marketed or used by financial institutions regulated under the EU financial services law, the national authority in charge of the financial supervision of those institutions under that legislation should also be designated, within its respective competences, as the

market surveillance and compliance of products established by the Product Safety Regulation applies in its entirety to AI systems covered by the AI Act.[181]

Given the broad formulation of Article 85 of the AI Act, the complaints lodged with a market surveillance authority may concern any infringement of the AI Act's provisions, most prominently those relating to prohibitions or to the obligations of providers and deployers of AI systems. One can think, for instance, of a person who has been denied access to credit in an allegedly discriminatory way due to an AI-generated credit score. In that case, the person affected may file a complaint claiming that they have been subjected to a prohibited AI social scoring system within the meaning of Article 5(1)(c) of the AI Act which used data from their social networks; or that their credit score has been calculated on the basis of a high-risk system without them having been informed about the use of such a system, as required by Article 26(11) of the Act; or that the explanations they obtained from the credit institution concerned are not sufficiently clear and meaningful, in violation of Article 86(1). However, even though no minimum threshold of proving an infringement is required for filing such complaints, and despite the significant benefits of the explanations obtained under Article 86(1), it will probably be quite challenging for individuals to convincingly argue that certain requirements under the AI Act have not been complied with, not least because of their inherently technical nature.

Be that as it may, any complaints submitted by the persons affected are to be taken into account by the relevant market surveillance authorities for the purpose of conducting their activities in accordance with the Product Safety Regulation.[182] It will thus rest ultimately upon these authorities, which benefit from extensive investigative and enforcement powers, to establish whether an infringement of the AI Act has actually occurred and then take appropriate measures, including,

---

market surveillance authority for the purposes of the AI Act. For instance, when it comes to an AI system deployed by a credit institution in a certain Member State to evaluate consumers' creditworthiness or credit score for access to loans, the market surveillance authority under the AI Act will be the national supervisory authority designated pursuant to the CCD. If that AI system is used to determine access to a credit agreement secured by a mortgage, then the relevant market surveillance authority may be the one defined by the Mortgage Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010 [2014] OJ L60/34. Other competent authorities in the field of financial services that can be designated as market surveillance authorities for the purposes of the AI Act include those defined by the legal instruments referred to in recital 158 of the AI Act.

[181] See Art 74(1) and recital 156 of the AI Act, referring to Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 [2019] OJ L169/1.

[182] See Art 85 of the AI Act and Art 11(3)(e) of the Product Safety Regulation. The market surveillance activities of the relevant authorities are listed in Art 11 of the said Regulation.

most importantly, the imposition of fines under Article 99.[183] Regrettably, though, the AI Act lacks a corresponding right of individuals to an effective judicial remedy against the market surveillance authorities, where those authorities do not handle a complaint or do not inform the person concerned about the progress or outcome of the complaint lodged.[184] Pursuant to Article 99(10), such a right seems to be available only to those subject to penalties or other enforcement measures, such as the providers and deployers of AI systems, thus excluding natural persons affected by those systems.

It follows from the foregoing that the right to file a complaint combined with the risk of fines in the event of non-compliance with the AI Act does not really offer proper redress to the affected individuals themselves, such as victims of AI-driven discrimination. Rather, this mechanism may benefit those persons only indirectly through the deterrent effect it exercises on operators, encouraging them to comply with their obligations under the AI Act and thereby to meet the required standards of fundamental rights' protection, including equality and non-discrimination. As such, it merely complements the existing remedies enjoyed by individuals under other EU or national law, such as non-discrimination law.

4.2 Right to explanations

Far more promising than Article 85 of the AI Act, is Article 86, which grants to any person subjected to a decision taken on the basis of a high-risk AI system the right to obtain from the deployer explanations of the individual AI-driven decision concerning them. This right clearly corresponds to the obligation of providers under Article 13(1) and (3)(iv) of the AI Act to develop their AI systems in such a way as to ensure that their operation is sufficiently transparent, while also providing to deployers the necessary information that is relevant to explain the systems' output. Concepts such as 'transparency', 'interpretability', or 'explainability' have become buzzwords in almost every discussion about algorithmic and AI-based operations, although their exact definition still remains blurry and goes far beyond the scope of this article.[185] In fact, the quest for so-called 'eXplainable AI' (XAI) has

---

[183] For the powers granted to market surveillance authorities, see Art 14 of the Product Safety Regulation. The market surveillance measures that the relevant authorities can take if they find that a certain AI system does not conform with the requirements of the AI Act are laid down in Art 16 of the said Regulation.

[184] Interestingly, although the European Parliament proposed the inclusion of such a right, this did not eventually make it into the AI Act's final text. See the Amendments adopted by the European Parliament (n 175) amendment 629.

[185] On the meaning of these concepts, see eg C Castelluccia and D Le Métayer, 'Understanding Algorithmic Decision-Making: Opportunities and Challenges' (Panel for the Future of Science and Technology, European Parliamentary Research Service, European Parliament, 2019) 26. For the lack of common understanding of these terms in the context of AI systems, see AB Arrieta and others, 'Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges Toward Responsible AI' (2020) 58 Information Fusion 82. See also, with a focus on EU law instruments, D Schneeberger and others, 'The Tower of Babel in Explainable Artificial Intelligence (XAI)' in A Holzinger and others (eds), *Machine Learning and Knowledge*

become a fast-growing research field of its own at the crossroads of law, ethics, and computer science, exploring the development of methods that enable humans to understand and interpret the underlying rationale of AI results.[186]

As clarified by recital 171 of the AI Act, the explanations offered by deployers under the Act are meant to provide a basis on which the affected persons are able to exercise their rights.[187] Accordingly, far from being a remedy in itself, the AI Act's right to explanations constitutes an 'enabler' of remedies, by ensuring the effective exercise of individuals' rights provided for by other EU or national law. These may include, most notably, the rights conferred on individuals by Article 22(3) GDPR, or the similar rights enshrined in Article 18(8) CCD in the context of creditworthiness assessments, but also the remedies granted under the EU non-discrimination legislation.[188] Besides, the explanations obtained may also be instrumental for the exercise of the right to file a complaint with a market surveillance authority under Article 85 of the AI Act, by exposing possible irregularities regarding compliance with the Act, such as the existence of inaccurate or biased datasets.

Taking a closer look at the conditions for the application of Article 86(1) of the AI Act, one cannot help but draw a comparison with the similarly worded provision of Article 22(1) GDPR, which triggers the applicability of the right to obtain information under Article 15(1)(h) GDPR. The right to explanations established under the AI Act concerns any decision taken by the deployer 'on the basis of the output from a high-risk AI system' and which 'produces legal effects or similarly

---

Extraction (Springer 2023); P Hacker and JH Passoth, 'Varieties of AI Explanations Under the Law: From the GDPR to the AIA, and Beyond' in A Holzinger and others (eds), *xxAI - Beyond Explainable AI* (Springer 2022).

[186] See eg A Adadi and M Berrada, 'Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)' (2018) 6 IEEE Access 52138. For an overview of such XAI methods, see A Holzinger and others, 'Explainable AI Methods: A Brief Overview' in A Holzinger and others (eds), *Machine Learning and Knowledge Extraction* (Springer 2023).

[187] In this regard, the AI Act's right to an explanation constitutes an expression of 'rights-enabling transparency' in the terms used by Hacker and Passoth (n 185) 344. See Case C-203/22 *Dun & Bradstreet Austria* ECLI:EU:C:2025:117, paras 55–56, where the Court explicitly ruled that the right of access to information under Art 15(1)(h) GDPR is intended to enable the individuals concerned to effectively exercise the rights conferred on them by Art 22(3) GDPR, namely the right to express their point of view on that decision and to contest it, while emphasising that the rights enshrined in Art 22(3) GDPR would not satisfy in full their purpose if the persons affected by an automated decision were not able to understand the reasons behind that decision. See in a similar vein Case C-817/19 *Ligue des droits humains* ECLI:EU:C:2022:491, para 195, where the Court pointed out that the opacity of machine learning technologies might deprive the persons concerned of their right to an effective judicial remedy under Article 47 of the Charter.

[188] In *Dun & Bradstreet Austria* (n 187) para 54, the Court also noted that the right to information is necessary to enable the persons affected to exercise their right to rectification, to erasure, or to restriction of processing in accordance with Arts 16, 17 and 18 GDPR respectively, their right to object to the processing of their data under Art 21 GDPR, their right of action and their right to compensation conferred by Arts 79 and 82 GDPR respectively.

significantly affects that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights'.[189] Although the notion of a 'decision producing legal effects or similarly significant effects' corresponds to that of Article 22(1) GDPR, Article 86(1) of the AI Act further draws an explicit link between the impact of such a decision and individuals' fundamental rights.[190] Such a reference to fundamental rights aligns with the AI Act's declared objective to ensure a high level of protection for the rights enshrined in the Charter and should be interpreted as encompassing also equality and non-discrimination, given the Act's explicit acknowledgement of the adverse impact that AI systems may have on these rights.[191] Moreover, unlike Article 22(1) GDPR that refers to decisions 'based solely on automated processing', the scope of Article 86(1) of the AI Act is significantly broader, as it concerns any decision taken 'on the basis of output', thus covering also decisions that entail some degree of human involvement.[192] This extended reach of the AI Act's right to explanations is particularly important due to the risk of automation bias traced even in hybrid or semi-automated decision-making processes.[193] On the other hand, though, the application of Article 86(1) of the AI Act is limited to those decisions reached through the use of (high-risk) AI systems, whereas Article 22(1) GDPR applies to automated decision-making in general, a concept capturing both algorithmic and AI-driven decisions.[194]

Turning to the type of explanations that must be provided by the deployer, Article 86(1) of the AI Act specifies that these must be 'clear and meaningful' and concern 'the role of the AI system' in the decision-making procedure as well as 'the main elements of the decision'.

---

[189] As argued by L Metikoš and J Ausloos, 'The Right to an Explanation in Practice: Insights from Case Law for the GDPR and the AI Act' (2025) Law, Innovation and Technology 1, the reference to the person's own considerations reflects an underlying balancing exercise that is left for the decision-subject to undertake.

[190] See A Engelfriet, *The Annotated AI Act: Article-by-Article Analysis of European AI Legislation* (ICTRecht 2024) 291. For a definition of the notion of a 'decision producing legal effects or similarly significant effects' under Art 22(1) GDPR, see Art 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (WP251rev.01, 3 October 2017, as last revised and adopted on 6 February 2018) 22. As the CJEU ruled in Case C-634/21 *SCHUFA Holding (Scoring)* ECLI:EU:C:2023:957, paras 44–50, this concept also covers the establishment by a credit information agency of a probability value in the form of a credit score, on which a third party, such as a credit institution, to which the score is transmitted, draws strongly to establish, implement, or terminate a contractual relationship with the person concerned.

[191] See eg recitals 48, 54, 56–60 of the AI Act and implicitly Article 10 thereof.

[192] See A Engelfriet (n 190) 291. For the definition of decision-making 'based solely on automated processing' under Art 22(1) GDPR, see Art 29 Working Party, 'Guidelines on Automated Individual Decision-Making' (n 190) 20–21.

[193] See Fair Trials (n 74) Section 3.1, 34.

[194] See in this regard T Rodríguez de las Heras Ballell, 'Guiding Principles for Automated Decision-Making in the EU' (European Law Institute 2022) 9. Nevertheless, it follows from the broad definition of AI systems in Art 3(1) of the AI Act that these cover any system using AI technologies, including those that do not involve the processing of personal data within the meaning of Art 4(1) GDPR but can still adversely affect individuals' interests or fundamental rights. See EDPB and EDPS, 'Joint Opinion 5/2021' (n 174), point 16, 8.

Following the CJEU's ruling in *Dun & Bradstreet Austria* that the right of individuals to receive 'meaningful information about the logic involved' in automated decision-making pursuant to Article 15(1)(h) GDPR combined with Article 22(1) is tantamount to 'a genuine right to an explanation',[195] there is no reason to interpret the AI Act's concept of 'explanations' in a different way. Accordingly, persons affected by an AI-based decision will be entitled to receive explanations of the procedure, principles, and input data that were actually used to obtain the specific result concerning them.[196] These explanations must be further provided in a concise, transparent, intelligible and easily accessible form, while general information about complex algorithms (eg the scoring formula behind an AI-generated credit score) does not satisfy this requirement.[197] Whether such an explanation further requires the implementation of XAI techniques will depend on the concrete application context and the functioning of the specific AI system deployed.[198] Be that as it may, the disclosure of the most important features of individual AI outputs can contribute to the detection of possible discrimination, as affected persons will be able to determine to what extent an AI-based decision might have been driven by variables correlated with protected attributes under EU non-discrimination law.[199]

Nevertheless, as per Article 86(3) of the AI Act, the right to explanations established therein applies only to the extent that such a right is not otherwise provided for under EU law. In fact, apart from the now expressly recognised right to obtain an explanation under Article 15(1)(h) GDPR, a similar sector-specific right is provided for by Article 18(8)(a) CCD[200] and Article 76(5) of the Anti-Money Laundering Regulation.[201] Accordingly, where the conditions set out by these

---

[195] See *Dun & Bradstreet Austria* (n 187) para 57.

[196] ibid, para 58. This so-called 'local' explanation of a specific individual decision under the AI Act has also been advocated by D Schneeberger and others (n 185) 71. See also Hacker and Passoth (n 185) 349–350, 363–364, warning though that a local explanation may create a 'misleading illusion of simplicity' of the decision-making process.

[197] See *Dun & Bradstreet Austria* (n 187) paras 59–61, where the Court also noted that the complexity of the operations carried out cannot relieve the controller of the duty to provide an explanation.

[198] See Hacker and Passoth (n 185) 345–346, 363–364, emphasising that explanations need to be adapted to different contexts, goals, and addressees.

[199] See also in the same vein ibid 365, referring to 'fairness-enabling transparency'.

[200] Individuals' right to an explanation under Art 18 CCD forms part of a broader right 'to request and obtain from the creditor human intervention', comprising also the right to express their own point of view to the creditor, and to request a review of the assessment of their creditworthiness and of the credit granting decision by the creditor. However, Art 18(8)(a) and recital 56 CCD specify that such a right exists only without prejudice to the application of the GDPR. For more details, see Ž Škorjanc 'The Right to Explanation of a Credit Score: A Holistic Approach under the GDPR, AI Act, and Directive (EU) 2023/2225 on Credit Agreements for Consumers' (2025) 6(3) Global Privacy Law Review 91.

[201] Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing [2024] OJ L2024/1624, which explicitly

provisions are fulfilled, persons affected by AI-based decision-making may rely on the right to explanations enshrined therein, to the exclusion of Article 86(1) of the AI Act. In any case, it follows from this matrix of partly overlapping rights established under different EU law instruments that victims of discriminatory or unfair AI decisions will always be entitled, one way or another, to obtain explanations about AI-generated decisions affecting them.

Regrettably, however, unlike Article 22(3) GDPR, the right to an explanation under Article 86(1) of the AI Act is not accompanied by a corresponding right of persons affected by an AI-driven decision to request human intervention, to express their point of view, and to contest that decision.[202] Under these circumstances, the existing remedies provided for by EU or national law become highly relevant. As concerns victims of AI-enabled discrimination or bias, in particular, they may challenge the decision in question on the basis of non-discrimination legislation but only insofar as one or more prohibited grounds or proxies thereof are triggered. If this is not the case or it is not proved to be so, those persons may have recourse to their respective rights under Article 22(3) GDPR, provided that the AI-enabled decision-making process concerned is fully automated in the sense of Article 22(1). For the rest, and regardless of the degree of automation of the decision-making, the right to compensation under both non-discrimination law and the GDPR, as well as the remaining set of rights conferred on individuals by the GDPR, remains fully available.

4.3 Access to documentation by national equality bodies

Rather overlooked so far is Article 77(1) of the AI Act. This provision empowers national authorities or bodies which supervise or enforce the respect of fundamental rights obligations under EU law to request and access any documentation related to the use of high-risk AI systems that is deemed necessary for effectively fulfilling their mandates. As specified by recital 157 of the Act, such a possibility also explicitly concerns national equality bodies established in each Member State under the EU Equality Directives with the duty to implement EU non-discrimination law and monitor its application at national level.[203]

To understand why access to technical documentation about AI systems is crucial for equality bodies to effectively exercise their competences in the field of AI-driven discrimination, one should first look at what such documentation entails. Pursuant to Article 11 of the

---

grants this right to explanation for decisions resulting from both automated and AI-based processes.

[202] See also Art 18(8) CCD, pursuant to which, apart from the right to an explanation, persons affected by automated credit decisions can further express their view and request a human assessment on behalf of the creditor. For its part, Art 76(5) of the Anti-Money Laundering Regulation provides the right of the persons concerned to challenge the automated decision in question.

[203] For the role and competences of these national equality bodies, see T Kádár, 'Equality Bodies: A European Phenomenon' (2018) 18(2–3) International Journal of Discrimination and the Law 144.

AI Act, the documentation drawn up and kept by the provider of a high-risk system demonstrates whether that system complies with the requirements of the AI Act and must contain, at a minimum, the elements set out in Annex IV thereof. Among these elements features a detailed description of the system's key design choices, including the rationale and assumptions made with regard to persons or groups for whom the system is intended, its main classification choices, and the relevance of the different parameters deployed; information about the metrics used to measure potentially discriminatory impacts; and detailed information about the system's limitations in performance, including the degree of accuracy for specific persons or groups of persons, as well as the foreseeable unintended outcomes and sources of discrimination risks in view of the system's intended purpose.[204]

Accordingly, when faced with discrimination claims of individuals affected by AI-generated decisions, access to such technical documentation may prove to be a tool of major practical assistance in the hands of national equality bodies for the purpose of proving and assessing the potentially discriminatory nature of the high-risk systems concerned. If the documentation provided is insufficient to ascertain whether an infringement of non-discrimination rules has occurred, equality bodies may also request the market surveillance authority to organise the testing of the AI system through technical means.[205]As such, the AI Act not only leaves the competences of national equality bodies intact but it further strengthens them by adding new tools to their legal toolbox under the EU and national non-discrimination framework.[206] This is particularly important, taking into account that the so-called 'individual-rights-based' approach that is currently prevalent in the enforcement of EU non-discrimination law is rather ill-suited to address the challenges posed by algorithmic and AI-based decision-making, which argues in favour of increased reliance on public enforcement mechanisms in this field.[207]

5 Concluding remarks

It follows from the preceding analysis that the AI Act complements to a considerable extent EU non-discrimination law when it comes to combatting AI-enabled discrimination both at the level of substantive protection granted to individuals and at the level of enforcement. Each of the three different functions performed by the AI Act contributes in this direction by assuming a distinct role.

More specifically, through its prohibitive function, the AI Act targets certain harmful AI practices, which may not always be captured by the EU non-discrimination framework, and thus results in expanding the personal and material scope of the latter. This is all the more so,

[204] See Annex IV(2)(b), (2)(g), and (3) of the AI Act.
[205] See Art 77(3) of the AI Act.
[206] See Art 77 and recital 157 of the AI Act.
[207] See Xenidis and Senden (n 7) section IV.1. See also Gerards and Xenidis (n 3) 11, 76–77.

considering that Article 5 of the AI Act suffices to bring the practices concerned within the ambit of the Charter, thereby triggering the applicability of Article 21(1) thereof. It is noted in this regard that the AI Act's prohibitions explicitly cover practices that are likely to produce not only discriminatory but also unfair or biased outcomes that would otherwise fall outside the reach of EU non-discrimination law.[208] Indeed, Article 5 of the AI Act applies without even necessarily requiring any finding of discrimination whatsoever. Rather, it prohibits certain AI practices merely due to the unacceptable risks they inherently entail for individuals' fundamental rights, including their right to non-discrimination. As such, the prohibitions in Article 5 of the AI Act may also be of great value from a procedural point of view, by discharging the persons affected from the burden of proving the *prima facie* discriminatory design or effects of the specific AI system in question.[209] In addition, the AI Act's prohibitive function permits action at various points in the AI value chain, including at the earlier stages of an AI system's lifecycle, such as when placing it on the market and putting it into service, even before its actual deployment.[210] This is particularly useful, given that the desired protection under non-discrimination legislation often comes too late.[211]

As concerns its regulatory function, the AI Act reinforces the EU non-discrimination framework through its preventative and safety logic.[212] This is because it provides for specific requirements that aim to minimise the risk of AI-driven discrimination throughout the AI systems' lifecycle, particularly in relation to the design and quality of the datasets used for the development of AI systems, along with a number of other obligations.[213] Although under EU non-discrimination law a certain practice may sometimes be found discriminatory even before its implementation and without the existence of any identifiable victims,[214] it is doubtful whether and at which precise stage of an AI system's lifecycle non-discrimination rules could step in to capture that system's potentially discriminatory effects prior to their use. In this regard, Article 10 of the AI Act makes it possible to detect early on where biases lie in the functioning of an AI system and take appropriate action

---

[208] See eg the Commission's Guidelines on prohibited AI practices (n 24) points 148, 165, 190. For the difference between the notions of 'bias' and 'discrimination', see eg Gerards and Xenidis (n 3) 47; Gerards and Zuiderveen Borgesius (n) 7, suggesting a distinction between instances of differentiation based on protected grounds that fall under the scope of non-discrimination law and other types of unfair differentiation in the context of AI technologies. This distinction also seems to be recognised by the AI Act. See eg recital 27 referring to 'discriminatory impacts and unfair biases that are prohibited by Union or national law', recitals 32 and 52 using the terms 'biased results' and 'discriminatory effects', and recital 70 referring to 'discrimination that might result from the bias in AI systems'.

[209] See similarly in this regard 'Resetting Antidiscrimination Law in the Age of AI' (n 23) 1571.

[210] See the Commission's Guidelines on prohibited AI practices (n 24) point 42.

[211] See Hacker (n 158) 279.

[212] See the Commission's Guidelines on prohibited AI practices (n 24) point 42.

[213] See the Commission's AI Act Proposal (n 20) point 1.2.

[214] See Case C-54/07 *Feryn* ECLI:EU:C:2008:397, para 23; Case C-81/12 *Asociația Accept* ECLI:EU:C:2013:275, para 36.

to remedy them. Besides, since the AI Act applies horizontally across all sectors,[215] its regulatory function contributes to the prevention or mitigation of AI-enabled discrimination beyond the limited areas of life covered by the EU Equality Directives.

Lastly, the AI Act's enabling function strengthens not only the private enforcement of EU non-discrimination law by individual victims of discrimination but also the public one entrusted to national equality bodies. As already shown above in Section 4.1, the right to lodge a complaint with a market surveillance authority can only benefit the persons concerned in an indirect way, while this is also the case for the power granted to equality bodies to request access to technical documentation about high-risk systems, which may be of paramount importance to individuals having recourse to the administrative means of redress that are available before these authorities under non-discrimination law. The right to explanations under Article 86 of the AI Act may instead prove to be a more powerful tool for those persons to overcome the challenges posed by the lack of transparency of AI models and, by extension, to successfully bring their discrimination claims before courts. All in all, it can be concluded that instead of providing individuals with proper means of redress against instances of AI-driven discrimination on its own,[216] the AI Act rather enables them to avail themselves more effectively of the mechanisms already existing under EU or national non-discrimination legislation. This becomes particularly evident, taking also into account that no civil liability regime is established for providers or deployers of AI systems in the event of violation of the AI Act's rules, as this would be covered by a different legal instrument, namely the AI Liability Directive,[217] which is, however, about to be withdrawn by the European Commission due to an alleged lack of foreseeable agreement between the Member States.[218] Thus, it is only on the basis of non-discrimination provisions that claims for damages or reparation of loss suffered due to the discriminatory effects of an AI-based decision may be sought by the individuals affected.

Apart from the aforementioned significant complementarities between the AI Act and EU non-discrimination law, it should also not be overlooked that the AI Act's provisions are expressly meant to complement other pieces of EU law, thus creating a patchwork of different legal instruments that may be potentially applicable when addressing AI-enabled discrimination. For instance, the prohibition of using AI systems for social scoring practices under Article 5(1)(c) of the

---

[215] See recital 9 of the AI Act. The AI Act does not apply, however, to areas falling outside the scope of EU law, nor to AI systems for military, defence or national security purposes, nor to those specifically developed and put into service for the sole purpose of scientific research and development. See Art 2(3)ff.

[216] See similarly in this regard Arnold (n 132).

[217] Commission, 'Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)' [2022] COM/2022/496 final.

[218] See the Commission's work programme 2025, 'Moving Forward Together: A Bolder, Simpler, Faster Union' COM (2025) 45 final, 11 February 2025, Annex IV, point 32.

AI Act largely relies on the types of data that may be deployed for creditworthiness assessments by reference to the specific provisions of the CCD. Similarly, the prohibition of AI-based crime predictions based on certain personal traits pursuant to Article 5(1)(d) of the AI Act corresponds to the prohibition of discriminatory profiling on the basis of sensitive categories of data under the Law Enforcement Directive, while when a person wishes to file a complaint with a market surveillance authority, the relevant procedure will be governed by the Product Safety Regulation. Most prominently, the AI Act's right to explanations applies only where this right is not already granted by other provisions of EU legislation, such as Article 15(1)(h) GDPR or Article 18(8) CCD. It therefore seems that combatting discrimination in the field of AI operations may sometimes 'take more than two to tango'.

It is too early to say whether and to what extent the AI Act will be interpreted and applied as a standalone legal instrument or in parallel with EU non-discrimination law, in particular Article 21(1) of the Charter. A test case in this respect could perhaps arise in the near future with regard to Hungary's envisaged use of AI facial recognition technologies in Pride events, which has been deemed by civil society organisations contrary to Article 5(1)(h) of the AI Act, urging the European Commission to take action accordingly.[219] In the same vein, it is yet to be seen how the AI Act's rules may interact with other pieces of EU secondary sectoral legislation in cases of discriminatory AI systems. In any event, it will certainly contribute to the diversification of the existing tools against discrimination available under EU law.

[219] See Civil Liberties Union for Europe, EDRi, European Center for Not-for-Profit Law (ECNL) and Hungarian Civil Liberties Union, 'Legal Analysis: New Biometric Surveillance Laws in Hungary Violate the Prohibition of Real-Time Remote Biometric Identification Under the AI Act' (28 April 2025) <https://tinyurl.com/ynchuwrx> accessed 20 November 2025; ECNL, Liberties and the Hungarian Civil Liberties Union, 'Civil Society Calls on Commission to Act: Hungary Escalates Rule of Law Breaches by Banning Pride Scheduled for 4 October 2025' (29 September 2025) <https://tinyurl.com/bdfxrt4j> accessed 20 November 2025.