Algorithmic Decision Making: Compliance with the Fundamental Rights to Privacy and Non-Discrimination in light of the EU Framework

Publication developed within the framework of the Jean Monnet Module Key Fundamental Rights Issues in the EU, directed by Veronica Corcodel (Project 101175180 — RIseEU)

Amanda Araujo, Ana Laura Carmo, Camila Souza and Luana Ferreira

September 2025

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Contents

1 Introduction

In the contemporary digital age, while the widespread benefits of technological advancement across various economic and social sectors are widely acknowledged, innovation must be pursued with responsibility and foresight.

Algorithmic Decision Systems (ADS) are typically employed to process large volumes of data, offering advantages such as rapid data handling, scalability, and a reduction in human error. These systems are designed to infer correlations or extract information that informs and supports decision-making processes.[1]

As artificial intelligence (AI) becomes increasingly embedded in social life, understanding and regulating the design and governance of Automated Decision-Making Systems (ADMSs) – including AI-driven systems – has become a critical concern.

ADS can be examined from multiple perspectives: public sector applications (e.g., fraud detection in social security systems), private sector uses (e.g., recruitment tools or credit scoring), or from the standpoint of their impact on individuals, particularly regarding the protection of fundamental rights. These technologies raise a host of ethical, legal, political, and technical challenges.

Although ADS present considerable opportunities and practical benefits, it is essential to mitigate associated risks, such as bias, inaccuracy, and lack of transparency, while implementing adequate safeguards to protect the rights and freedoms of data subjects. A principled approach to risk mitigation is necessary to preserve core fundamental rights, including equality, privacy, dignity, autonomy, and free will.

[1]Claude Castelluccia and Daniel Le Métayer, *Understanding Algorithmic Decision-Making: Opportunities and Challenges* (Scientific Foresight Unit (STOA), European Parliamentary Research Service, PE 624.261, March 2019) https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf Accessed 12 May 2025.

Regarding regulatory responses, a range of mechanisms may be considered as possible: national legislation, self-regulation, or co-regulation; binding legal instruments (hard law) or non-binding frameworks (soft law). Regulation may be general or sector-specific and may involve various enforcement modalities, including regulatory authorities, oversight bodies, or certification schemes.

A central question remains: Are existing legal instruments sufficient to address the emerging challenges posed by ADS? This paper seeks to address this issue by presenting the relevant legal framework, including the Charter of Fundamental Rights of the European Union (CFREU), the European Convention on Human Rights (ECHR), the Artificial Intelligence Act, the General Data Protection Regulation (GDPR), and the Law Enforcement Directive (LED), and analyzing how courts have interpreted and applied these norms. The objective is also to assess whether judicial decisions are effectively upholding and safeguarding fundamental rights in the context of algorithmic decision-making.

2 Legal Framework

In recent years, several "Internet Bills of Rights" have emerged, outlining principles and rights for the digital age in response to the challenges of the digital revolution. The European Declaration on Digital Rights and Principles for the Digital Decade, proclaimed on December 15, 2022, while primarily declaratory, not only reinforces the rights enshrined in the Charter of Fundamental Rights of the European Union (CFREU) but also introduces specific references to fundamental rights and ethical standards concerning AI. Recital 3 emphasizes that "*digital transformation should not entail the regression of rights*," and Article 18 introduces a right absent from the Charter: protection against unlawful online surveillance, pervasive tracking, and interception, thereby reinforcing EU values in the digital context.[2]

[2]Edoardo Celeste, 'Digital Constitutionalism, EU Digital Sovereignty Ambitions and the Role of the European Declaration on Digital Rights' in A Engel, X Groussot and GT Petursson (eds), *New Directions in Digitalisation: Perspectives from EU Competition Law and the Charter of Fundamental Rights* (Springer 2024), https://link.springer.com/chapter/10.1007/978-3-031-65381-0_13 Accessed 12 May 2025.

The CFREU affirms the inviolability of human dignity (Article 1), the right to privacy in personal and family life, residence, and communications (Article 7), equality before the law (Article 20), a broad prohibition of discrimination (Article 21), encompassing grounds such as sex, race, ethnicity, religion, political opinion, and sexual orientation. It also defines principles such as gender equality in all areas including employment and remuneration (Article 23), that although not directly enforceable, guide policy and legislative processes.

Although the Charter primarily applies to EU institutions and Member States when implementing Union law (Article 51 - principle of subsidiarity),[3] any limitation of rights must be legally justified, respect their essential content, and be in accordance to the principle of proportionality (Article 52). Furthermore, Article 52(1) states that, in line with proportionality, restrictions are allowed only when necessary to serve legitimate Union interests or to safeguard the rights of others.

Rooted in the notion of the EU as a "Union of values," the CFREU underscores that technology must serve society and place individuals at its center. The CFREU thus delineates a set of fundamental rights and principles[4] that should not be disregarded by any Member State of the EU. Its primacy in EU law and its essential role in safeguarding human dignity and freedom are well established.

The rights protected by the CFREU align closely with those guaranteed by the European Convention on Human Rights and Fundamental Freedoms (ECHR), that was originally adopted in 1950 and subsequently amended, being the first legally binding international instrument to give effect to certain rights proclaimed in the Universal Declaration of Human Rights, transforming them into enforceable obligations. It's a supranational legal instrument that aims to protect human rights

[3]Koen Lenaerts and José Antonio Gutiérrez-Fons, 'The Place of the Charter in the European Legal Space' in *The EU Charter of Fundamental Rights – A Commentary* (2nd edn, 2021) 1711–1734, ISBN: 978-1-50993-347-1; Charter of Fundamental Rights of the European Union [2012] OJ C 326/391 (CFREU).

[4]Article 52(5) CFREU, distinguishes between 'rights,' which are judicially enforceable, and 'principles,' which guide legislative and administrative action but are not directly invoked in court proceedings. This distinction shapes how different Charter provisions apply to ADM oversight.

and political freedoms in Europe. Notably, Article 14 in conjunction[5] with Article 8, reaffirms the rights to privacy and non-discrimination, which are also emphasized in the CFREU, as seen above.

Although some EU Member States have withdrawn from aspects of the ECHR framework, it doesn't diminish the Convention's significance in shaping the human rights standards to which ADMSs must adhere.

In this context, the European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment[6], adopted by the European Commission for the Efficiency of Justice (CEPEJ) in 2018, is of particular relevance and outlines five principles critical for the ethical deployment of AI in ADMSs: (1) Respect for Fundamental Rights and (2) Non-discrimination: AI must uphold human rights and avoid reinforcing biases; (3) Quality and Security: Systems should be built on verified data and developed in secure environments, in cooperation with legal professionals; (4) Transparency, Impartiality, and Fairness: Processing must be intelligible to individuals, with external audit mechanisms ensuring accountability;

(5) Under User Control:[7] Users must understand and retain control over AI systems, with robust oversight and meaningful human participation.

The Artificial Intelligence Act (AI Act),[8] in Recitals 6 and 7, reinforces a human-centric approach, requiring that AI systems respect fundamental rights and promote human well-being. The Act underscores the need to respect fundamental

[5]Article 14 of the ECHR is not a standalone provision and only applies in conjunction with another substantive ECHR right, such as Article 8 on privacy. The ECtHR has consistently held this position, as confirmed in cases like *Sidabras and Džiautas v. Lithuania*, App nos. 55480/00 and 59330/00 (ECtHR 2004). https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-23517%22]}

[6]Council of Europe, *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment,* https://rm.coe.int/carta-etica-traduzida-para-portugues-revista/168093b7e0#_Toc530141229 accessed 5 May 2025.

[7]Anna Levitina, 'Humans in Automated Decision-Making under the GDPR and the AI Act' (2024) 138 *Revista CIDOB d'Afers Internacionals* 121, https://www.cidob.org/en/publications/humans-automated-decision-making-under-gdpr-and-ai-act accessed 13 May 2025, DOI: https://doi.org/10.24241/rcai.2024.138.3.121/en.

[8]Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689 accessed 5 May 2025.

rights and to prevent discriminatory outcomes. Moreover, Article 14 mandates continuous human oversight throughout the ADMS lifecycle – from design to deployment and outcome evaluation.

In turn, data protection is a core concern in ADMSs, especially given the reliance on large datasets for algorithm training. The AIA complements the General Data Protection Regulation (GDPR), together forming an integrated legal framework for data-driven technologies.

Under the GDPR, automated decision-making (ADM) is generally prohibited (Art. 22), with exceptions subject to strict conditions. The European Data Protection Board (EDPB), and previously the Article 29 Working Party, have issued guidelines clarifying the interpretation and application of these provisions.

In the law enforcement context, the Law Enforcement Directive (Directive (EU) 2016/680), (LED)[9] similarly restricts ADM (Article 11), permitting it only under narrow exceptions and requiring safeguards to prevent discriminatory outcomes (Article 11(3)). Human oversight must be substantive and autonomous – mere formal validation of algorithmic outputs is insufficient[10]. Otherwise, such superficial involvement could amount to regulatory evasion, undermining the protective intent of the law.

These themes will be further explored and analyzed in the sections that follow.

[9]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, https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng Accessed 5 May 2025.

[10]Vera Lúcia Raposo, 'The Use of Facial Recognition Technology by Law Enforcement in Europe: A Non-Orwellian Draft Proposal' (2022), *European Journal on Criminal Policy and Research,* https://doi.org/10.1007/s10610-02209512-y Accessed 5 May 202

3 ADM in Practice: Risks and Examples

ADM is regulated by the GDPR, since it is a process that relies on large amounts of data.[11] Some authors consider that Article 22 of the GDPR stipulates a right of the data subject, while others consider it a prohibition, as is the case with the Data Protection Working Party.[12] The prohibition would make it an obligation for organizations to avoid certain automated decisions, while a right would force data subjects to exercise the right actively. Nevertheless, the article states that a data subject must not be subject to a decision "based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." Profiling, a specific type of ADP, covered in Article 22, is also defined in Article 4(4) of the same provision as "automated processing of personal data consisting of the use of personal data to evaluate (...) that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".[13]

However, ADM might not even rely on a human overseeing its decisions, if the system is entirely automatic.[14] Although ADM has advantages, such as the

[11]Panel for the Future of Science and Technology, *STUDY: European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 624.261* (March 2019) https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf Accessed 14 May 2025.
[12]Predecessor of the European Data Protection Board. Article 29 Data Protection Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, WP 251 (adopted 3 October 2017) http://ec.europa.eu/justice/data-protection/index_en.htm Accessed 14 May 2025.
[13]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 (General Data Protection Regulation) [2016] OJ L119/1
[14]Panel for the Future of Science and Technology, *STUDY: European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 624.261* (March 2019) https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf Accessed 14 May 2025.

improvement of efficiency and the lowering of costs of public and private services, it can also violate human rights by neglecting privacy and augmenting discrimination.[15]

In the public sector, ADM is used for urban planning, criminal justice, decisions about welfare entitlements, etc.[16] However, transparency is not always guaranteed in its execution.

In 2020, the Dutch Hague District Court presented a landmark ruling that stopped an automated surveillance system used to detect welfare fraud, under a Dutch ministry[17]. The *SyRi* ADM system, intended to combat fraud through the combination of data of several unknown risk indicators such as residence or education, held by the Dutch government.[18] A report created using *SyRi* about any citizen could initiate investigations by the competent authorities. Inclusively, the targeted citizens were never informed of the creation of a report, and it was never disclosed how the algorithm worked.[19] Ultimately, the Court considered that the *SyR*I legislation violated article 8(2) of the ECHR, since "considering the principle of transparency, the principle of purpose limitation and the principle of data minimization, the *SyRI* legislation was insufficiently transparent or verifiable to conclude that the interference with the right to respect for private life, which the use

[15]Miriam Stankovich, Erica Behrens and Julia Burchell, *Toward Meaningful Transparency and Accountability of AI Algorithms in Public Service Delivery* (August 2023) 4-30. https://www.dai.com/uploads/ai-in-public-service.pdf Accessed 14 May 2025.
[16]Ibid.
[17]Adamantia Rachovitsa and Niclas Johann, 'The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case' (2022) 22 *Human Rights Law Review, Oxford* 1 https://academic.oup.com/hrlr/article/22/2/ngac010/6568079 Accessed 14 May 2025.
[18]Ibid. '2. The District Court of The Hague's Judgment'.
[19]Ibid.

of *SyRI* may entail, is necessary, proportional and proportionate.".[20] The court also stated that "the *SyRI* legislation in no way provides information on which objective factual data can justifiably lead to the conclusion that there is an increased risk."[21] Inclusively, the Court considered that the lack of transparency regarding the algorithm carried the risk of being discriminatory.[22]

In the private sector, there have also been cases of increased bias and lack of transparency regarding ADM. In 2024, Derek Mobley started the first class action to challenge ADM in the hiring system.[23] The plaintiff claimed to have been discriminated against by a biased algorithm, used by the company "Workday", and, consequently, rejected from over 100 jobs, for being "black, older than 40, and having anxiety and depression.".[24] The case is still ongoing, but it could set a precedent for holding AI vendors accountable for ADM discrimination. Inclusively, in 2020, Amazon had to ban an ADM recruiting tool for penalizing resumes with the word "woman".[25] Recent research from the University of Melbourne in 2025, says that it "estimates that about 30% of Australian employers use AI recruitment tools, with that figure expected to grow in the next five years."[26] It also warns that candidates subject to AI interviews may be discriminated for having accents and disabilities[27]. Another problem presented is the data used by the algorithms. The datasets that train the algorithm mostly use data from the United States of America, not reflecting

[20]*NJCM and Others v The Dutch State (SyRI case)*, District Court of The Hague,), ECLI:NL:RBDHA:2020:1878, C/09/550982 / HA ZA 18-388 (5 February 2020), para 6.86, https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBDHA:2020:1878 Accessed 14 May 2025.
[21]Ibid, para 8.87
[22]Ibid, para 6.91
[23]Daniel Wiessner, 'Workday Must Face Novel Bias Lawsuit over AI Screening Software' (*Reuters*, 15 July 2024) https://www.reuters.com/legal/litigation/workday-must-face-novel-bias-lawsuit-over-ai-screening-software-2024-07-15/ Accessed 14 May 2025.
[24]Ibid.
[25]Jeffrey Dastin, 'Insight – Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women' (*Reuters*,11October2018) https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG/ Accessed 14 May 2025.
[26]Josh Taylor, 'People Interviewed by AI for Jobs Face Discrimination Risks, Australian Study Warns' *(The Guardian*, 14 May 2025) https://www.theguardian.com/australia-news/2025/may/14/people-interviewed-by-ai-for-jobs-face-discrimination-risks-australian-study-warns Accessed 14 May 2025.
[27]Ibid.

groups in other countries. Researchers inclusively stated, “In a human process, you can go back to the recruiter and ask for feedback, but what I found is recruiters don’t even know why the decisions have been made, so they can’t give feedback.”[28] Not knowing how the algorithm works inevitably violates the right to an explanation (Art. 22 and Recital 71 of the GDPR) and puts individuals' capacity to challenge decisions and enforce their rights at risk.

Should we allow algorithms to make decisions for us if we can’t even comprehend how they work? Is ADM compatible with protecting Human Rights? The following point proposes to answer these questions.

4 Is ADM Compatible with the CFREU?

ADM presents a considerable challenge to European human rights law, particularly in relation to privacy and non-discrimination, under Articles 8 in conjunction with Article 14 of the ECHR, and Articles 7, 8 and 21 of the CFREU. While technological innovation is not intrinsically incompatible with fundamental rights, how algorithmic systems process personal data, generate predictive outputs, and influence decision-making raises questions as to whether existing legal standards adequately constrain such systems. Critical to this assessment is the proportionality test in Article 52(1) CFREU, which governs the circumstances under which rights may be lawfully limited.

Under Article 52(1), any limitation on the exercise of rights and freedoms must be provided for by law, respect the essence of the right, and be necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. In theory, this structure provides a mechanism for evaluating whether ADM infringes fundamental rights. In practice, however, the opacity and autonomy of algorithmic processes complicate assessments of legality, necessity, and proportionality. As Mantelero argued, the conventional

[28]Ibid.

proportionality test may prove insufficient in the ADM context due to the unpredictable and dynamic nature of machine learning, and the structural imbalance between data subjects and data controllers.[29]

This is particularly acute concerning Article 8 ECHR, which guarantees the right to respect for private and family life, home and correspondence. The European Court of Human Rights (ECtHR) has interpreted this right expansively to include informational privacy. In cases such as *S. and Marper v. United Kingdom*, the Court held that indefinite retention of biometric data from individuals not convicted of any crime constituted a disproportionate interference with privacy, in part due to the absence of adequate safeguards.[30] The Court's reasoning is significant for ADM systems, where similar concerns arise regarding long-term retention, profiling, and the repurposing of data without meaningful individual control or understanding.

The jurisprudence of the Court of Justice of the European Union (CJEU) has likewise emphasised the limits of automated data processing. In *Digital Rights Ireland*, the CJEU struck down the Data Retention Directive for violating Articles 7 and 8 of the Charter, due to its disproportionate retention of telecommunications data without sufficient safeguards for access, oversight, or data minimisation.[31] Subsequent cases, such as *Schrems I* and *II*, affirmed the requirement for equivalent levels of protection when personal data is transferred to third countries, particularly in relation to bulk surveillance powers.[32]

---

[29]Alessandro Mantelero, 'AI and Big Data: A blueprint for a human rights, social and ethical impact assessment' (2018) 34 *Computer Law & Security Review* 754. https://www.sciencedirect.com/science/article/pii/S0267364918302012 Accessed 16 May 2025.

[30]*S. and Marper v United Kingdom* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008). https://hudoc.echr.coe.int/eng?i=001-90051 Accessed 16 May 2025.

[31]Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications and Others* [2014] ECLI:EU:C:2014:238. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed 16 May 2025.

[32] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650; Case C-311/18 *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* [2020] ECLI:EU:C:2020:559. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362 https://curia.europa.eu/juris/liste.jsf?num=C-311%2F18 Accessed 16 May 2025.

These cases collectively signal that privacy infringements through ADM must be strictly necessary and accompanied by legal clarity, access controls, and independent oversight. Yet in many algorithmic systems deployed across Europe, these conditions remain unmet. A core issue is the lack of transparency, commonly referred to as the 'black box' problem, whereby the logic, purpose, and effects of an algorithm are inaccessible to the individual and often to regulators. As Pasquale illustrated, the opacity of automated systems undermines accountability and denies data subjects meaningful opportunities to contest decisions.[33]

The GDPR has attempted to address these risks by requiring transparency and human oversight in significant automated decisions, yet the provision is limited in scope, and its exceptions, such as the performance of a contract or explicit consent, are often invoked in ways that circumvent meaningful protection.[34] Moreover, the GDPR's requirement to provide "meaningful information about the logic involved" in automated decision-making remains under-defined, allowing for a minimum threshold of explanation that may be insufficient for effective redress.[35]

Beyond individual rights, ADM also raises concerns related to discrimination on a wide range of grounds. Unlike privacy, which focuses on individual autonomy and dignity, non-discrimination addresses the equitable distribution of burdens and benefits. The ECtHR has long recognised that differential treatment which lacks an objective and reasonable justification may constitute violation of the ECHR, especially where the disadvantage results in significant social exclusion or marginalisation. In *D.H. and Others v Czech Republic*, the Court accepted that statistical evidence of disproportionate placement of Roma children in special

[33]Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015). https://www.hup.harvard.edu/books/9780674970847 Accessed 16 May 2025.
[34]Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation' (2017) 7(2) International Data Privacy Law 76. https://academic.oup.com/idpl/article-abstract/7/2/76/3860948?login=false Accessed 16 May 2025.
[35]Andrew D Selbst and Julia Powles, 'Meaningful information and the right to explanation' (2017) 7(4) International Data Privacy Law 233. https://academic.oup.com/idpl/article-abstract/7/4/233/4762325?redirectedFrom=fulltext&login=false Accessed 16 May 2025.

schools amounted to prima facie indirect discrimination, shifting the burden to the state to justify the practice.[36]

This reasoning is directly relevant to algorithmic systems trained on biased datasets or developed using criteria that inadvertently replicate historical patterns of discrimination. According to Eubanks, automated systems deployed in social welfare and policing disproportionately target already marginalised populations, embedding existing inequalities into digital infrastructure.[37] Unlike overt discriminatory intent, these systems may generate discriminatory outcomes through seemingly neutral mechanisms. The concept of indirect discrimination is essential in evaluating whether ADM outputs, even if not designed with discriminatory intent, result in unjustified disadvantages.

However, identifying and proving algorithmic discrimination poses challenges, as the need for comparators, statistical evidence, and access to algorithmic logic creates a high threshold for claimants. Scholars have proposed a more structural approach, grounded in collective harms and the recognition of 'group privacy' or 'group discrimination' as legal constructs. Mittelstadt argues that existing legal frameworks insufficiently capture harms arising from predictive analytics that target or profile communities, rather than individuals.[38] Similarly, Taylor has called for legal recognition of group-based harms in the context of data analytics, noting that individuals may be affected by inferences drawn about them as members of a group, even when no personal data is directly involved.[39]

---

[36] *D.H. and Others v Czech Republic* App no 57325/00 (ECtHR, 13 November 2007). https://hudoc.echr.coe.int/eng?i=001-83256 Accessed 17 May 2025.

[37] Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St. Martin's Press 2018). https://us.macmillan.com/books/9781250074317 Accessed 17 May 2025.

[38] Brent Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30(4) *Philosophy & Technology* 475. https://link.springer.com/article/10.1007/s13347-017-0253-7 Accessed 17 May 2025.

[39] Linnet Taylor, 'What is data justice? The case for connecting digital rights and freedoms globally' (2017) 4(4) *Big Data & Society* 1. https://journals.sagepub.com/doi/abs/10.1177/2053951717736335 Accessed 17 May 2025.

Given these challenges, scholars and human rights advocates have called for stronger safeguards such as algorithmic impact assessments, fairness audits, and the ex ante regulatory oversight. Edwards and Veale argue that impact assessments should not merely evaluate technical risks but should incorporate legal and ethical considerations, including distributive justice and power asymmetries.[40] While the forthcoming EU Artificial Intelligence Act proposes risk-based regulation, questions remain as to whether the proposed safeguards will adequately address systemic discrimination and whether the enforcement mechanisms will be sufficiently robust and effective to ensure compliance.

Responsibility for ensuring rights-compliant ADM lies with both states and private actors. While the Charter primarily binds the EU and the Member States when implementing EU law, its principles increasingly influence the interpretation of national legislation, especially in domains like social protection, border management, and criminal justice. Private companies that deploy ADM in employment, credit, or content moderation contexts are directly bound by secondary EU law, including the GDPR and anti-discrimination directives. Moreover, as the ECtHR has made clear, States have positive obligations to protect individuals from rights infringements by third parties, including through adequate regulatory frameworks and enforcement.

While ADM can in theory be reconciled with the privacy and equality guarantees of the CFREU and ECHR, the current legal and institutional landscape falls short of ensuring such compatibility in practice. Existing safeguards, including proportionality review, transparency, and human oversight, are often inadequate or poorly enforced. Structural inequalities embedded in data and design persistently elude individual-centric remedies, calling for a more collective systemic approach to rights protection. Without a commitment to regulatory innovation, meaningful accountability, and the doctrinal expansion of legal concepts to address group harms,

[40]Lilian Edwards and Michael Veale, 'Slave to the algorithm? Why a right to an explanation is probably not the remedy you are looking for' (2017) 16(1) *Duke Law & Technology Review* 18. https://scholarship.law.duke.edu/dltr/vol16/iss1/2/ Accessed 17 May 2025.

the promise of algorithmic efficiency risks coming at the expense of fundamental rights.

5 Towards Human Rights-Compliant ADM: A Condensed Critical and Propositional Analysis

The transition toward Algorithmic Decision-Making (ADM) that fully respects Human Rights within the European Union requires more than a mere enumeration of compliance mechanisms; it demands a critical examination of their practical limitations and a commitment to their effective operationalization. Although instruments such as the 1 Charter of Fundamental Rights of the European Union (CFREU)[41] provide a robust normative foundation, their application in algorithmic contexts reveals complex challenges that call for incisive approaches and deep reflection on the very nature of technological governance.

The proposal of Fundamental Rights Impact Assessments (FRIA) as a preventive mechanism to identify and mitigate risks associated with ADM systems is commendable. Their inclusion as a requirement for public authorities under the EU Artificial Intelligence Regulation (AI Act)[42], underscored by institutions such as the, represents a significant normative advancement[43]. Methodological frameworks developed by the European Law Institute (ELI) and the Dutch government[44] provide initial models for implementation. However, the actual effectiveness of FRIA critically depends on overcoming considerable practical challenges that reduce them to mere bureaucratic exercises.

---

[41]Charter of Fundamental Rights of the European Union [2000] OJ C364/1 https://www.europarl.europa.eu/charter/pdf/text_en.pdf accessed 14 May 2025.

[42]European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts* COM(2021) 206 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 accessed 17 May 2025.

[43]Ada Lovelace Institute, *The Ada Lovelace Institute in 2024* (2024) 2.https://www.adalovelaceinstitute.org/blog/the-ada-lovelace-institute-in-2024/ accessed 14 May 2025.

[44]Government of the Netherlands, *Dutch government presents vision on generative AI* (18 January 2024) https://www.government.nl/latest/news/2024/01/18/dutch-government-dutch-government-presents-vision-on-generative-ai accessed 14 May 2025.

A big obstacle lies in establishing transparent and objective thresholds for what constitutes a "high-risk" ADM system that would mandatorily trigger an FRIA. The absence of precise criteria may result in underutilizing assessments, leaving potentially harmful systems unscrutinized and their excessive, superficial application to low-impact systems, thereby diluting their purpose. Additionally, ensuring the independence and technical competence of evaluators is essential. How can we guarantee that evaluators possess technical expertise in AI and a profound understanding of Human Rights and the specific social contexts in which these systems are deployed? The risk of regulatory capture or superficial evaluations remains high without robust answers.

Critically, questions persist regarding the genuine capacity of FRIA to substantially influence the design and implementation of ADM systems beyond formal compliance. For them to be truly preventive, FRIA must be integrated from the earliest stages of the algorithmic lifecycle (rights by design), and their outcomes must have the authority to enforce substantial modifications or even halt the development of systems posing unacceptable risks. This requires political will and strong enforcement mechanisms to ensure that FRIA recommendations are effectively implemented, an issue the AI Act begins to address. However, its practical effectiveness remains to be demonstrated.

Transparency constitutes a cornerstone of democratic ADM governance, and the AI Act imposes relevant obligations. However, the distinction between technical transparency and the provision of intelligible explanations to affected individuals is crucial. Implementation faces the tension between the right to information and the protection of intellectual property or security interests. While the AI Act attempts to strike a balance, its practical application in critical sectors remains uncertain. The very notion of "comprehensible explanation" in the context of "black-box" systems is fraught with difficulty; explainable AI (XAI) is advancing, yet it still faces significant limitations. Determining a level of transparency sufficient for public scrutiny and accountability without imposing unfeasible burdens is a political and ethical issue[45].

[45]See NSS Advogados, "O Regulamento de Inteligência Artificial" (2024). https://www.nss.pt/images/_Data/Publicacoes-outrosmateriais/ROA_NSS_O_Regulamento_de_Intelige%CC%82ncia_Artificial.pdf accessed 14 May 2025.

The AI Act proposes a liability framework, but its practical enforcement is difficult[46]. Innovative approaches are relevant, yet it is essential to delineate how these could overcome practical barriers, such as proving causality in algorithmic discrimination[47]. The proposed AI Liability Directive aims to facilitate redress, but its interaction with the AI Act and national legal regimes requires careful calibration. Equally crucial is clarifying the liability of those who delegate decision-making to AI systems, even without comprehending their operations.

The GDPR and AI Act coexistence creates a complex regulatory ecosystem, raising questions about synergies, conflicts, and coordinated oversight. Coordinated supervision between Data Protection Authorities and the new AI Act supervisory bodies poses a significant challenge, necessitating effective mechanisms of inter-agency cooperation[48].

Ensuring ADM compliance with Human Rights transcends technical considerations and calls for ethical and political reflection on the kind of society we wish to construct. "Rights by design" is a foundational principle but relies on cultural change and appropriate incentives. Collective rights and the systemic impacts of ADM, such as disinformation, surveillance, and the exacerbation of inequality, demand deeper scrutiny. Institutionalizing ethical reflection through meaningful public participation is essential. Ultimately, AI governance represents a fundamentally democratic challenge.

While the EU regulatory framework has evolved significantly, other expected challenges remain underexplored. Technologies such as emotion detection could be utilized for decision making processes. However, some of these technologies do not use biometric data, as defined in the GDPR. Thus, they cannot fall under the AI Act

---

[46]Jota,'AI Act e PL 2338: "Uma análise crítica das estruturas regulatórias de IA" (*Jota Info)* (10 June 2024) https://www.jota.info/artigos/ai-act-e-pl-2338-uma-analise-critica-das-estruturas-regulatorias-de-ia accessed 17 May 2025.

[47]Ada Lovelace Institute, 'The Ada Lovelace Institute in 2024' (2024) https://www.adalovelaceinstitute.org/blog/the-ada-lovelace-institute-in-2024/ accessed 14 May 2025.

[48]Ahmed Sarra, 'Artificial Intelligence in Decision-making: A Test of Consistency between the EU AI Act and the GDPR' (2025) 11(1) *Athens Journal of Law* 55–76. https://www.athensjournals.gr/law/2025-11- 1-3-Sarra.pdf accessed 17 May 2025.

obligation to inform natural persons of their contact with such technology.[49] Scholars such as Czarnocki argue that new definitions for emotion recognition technology are needed.[50]

The need for new Human Rights is also starting to emerge in policy and academic discourse. With the rise of algorithms and AI, the discussion of rights such as the "Human Right to Psychological Continuity"[51], the right to "mental integrity"[52] and the "Human Right to Explanation" have grown.

Some scholars argue that AI technologies could become not only disruptive to autonomy over the body, but also the mind.[53] Although the right to freedom of thought (Articles 9 and 10 of ECHR and The EU Charter, respectively) already offers protection in this area, some proposals have been made regarding threats to mental privacy, personal identity, and psychological integrity.[54] ADM increasingly relies on profiling and emotion recognition that can shape individuals identities by assigning opaque labels and influencing decision-making. This type of disruption can interfere with a person's sense of identity, autonomy, privacy and cognitive freedom.

---

[49]Jacek Czarnocki, 'Will new definitions of emotion recognition and biometric data hamper the objectives of the proposed AI Act?' (2021) *Proceedings of the 2021 International Conference of the Biometrics Special Interest Group (BIOSIG)*, Darmstadt, Germany, 1–4. https://ieeexplore.ieee.org/abstract/document/9548285 accessed 17 May 2025.

[50]Ibid.

[51]Sjors Ligthart, 'Towards a Human Right to Psychological Continuity? Reflections on the Rights to Personal Identity, Self-Determination, and Personal Integrity' (2024) 5(2) *European Convention on Human Rights Law Review* 199 https://doi.org/10.1163/26663236-bja10092; Siobhán O'Sullivan, Hervé Chneiweiss, Alessandra Pierucci and Karen S Rommelfanger, "Neurotechnologies and Human Rights framework: do we need new rights?", report of the round table co-organized by the Steering Committee for Human Rights in the fields of Biomedicine and Health (CDBIO), Council of Europe (16 December 2022) https://www.coe.int/en/web/human-rights-and-biomedicine/assessing-the-relevance-and-sufficiency-of-the-existing-human-rights-framework-to-address-the-issues-raised-by-the-applications-of-neurotechnologies accessed 17 May 2025.

[52]Vera Tesink and others, 'Right to Mental Integrity and Neurotechnologies: Implications of the Extended Mind Thesis' (2024) 50 *Journal of Medical Ethics* https://jme.bmj.com/content/50/10 accessed 17 May 2025.

[53]Sjors Ligthart, 'The Right to Mental Integrity in the Age of Neurotechnology: Constructing Scope and Exploring Permissible Limitations' (2025) 12(1) *Journal of Law and the Biosciences* lsaf010 https://doi.org/10.1093/jlb/lsaf010 accessed 17 May 2025.

[54]Sjors Ligthart, 'Towards a Human Right to Psychological Continuity? Reflections on the Rights to Personal Identity, Self-Determination, and Personal Integrity' (2024) *European Convention on Human Rights Law Review* https://doi.org/10.1163/26663236-bja10092 accessed 17 May 2025.

A Human Right to Explanation is also discussed in literature.[55] Some scholars state that the GDPR does not offer a true right to an Explanation, since Article 22 is ambiguous and has a limited scope.[56] Inclusively, ADM is a complex process that cannot always be understood and easily explained. In the case *State v. Loomis*[57] the Wisconsin Supreme Court judge said not to have understood an algorithm that influenced his decision on the conviction of an African American man, despite having been given many explanations on its functioning.[58] These challenges pose difficulties to transparency and explainability that are essential to upholding the rights of privacy and non-discrimination. The creation of a Human right to Explainability could strengthen enforcement and clarify the problem.

6 Conclusion

The development and deployment of ADM systems within the European Union entail a landscape of interwoven promises and risks. Pursuing genuinely Human Rights-compliant ADM, aligned with the CFREU and other international instruments, requires more than technological optimism or the mere adoption of regulatory frameworks. It demands an enduring commitment to critical rigor, ethical vigilance, and the continuous adaptation of governance approaches.

Critically examine the limitations of proposed solutions, identify persistent gaps, and thoughtfully consider the practical and political implications of regulatory choices. Embedding a "rights by design" perspective is essential. Still, it must be

[55]Michael Veale and Lilian Edwards, 'Explainability and Responsibility in AI: A Human Rights-Based Approach' (2021) 25(2) *IEEE Internet Computing*, 116 https://doi.org/10.1109/MIC.2020.3045821 accessed 17 May 2025.
[56]Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7(2) *International Data Privacy Law* 76, https://doi.org/10.1093/idpl/ipx005 accessed 17 May 2025.
[5]A risk assessment tool called *COMPAS's* ("Correctional Offender Management Profiling for Alternative Sanction") was used in an "algorithmic based sentencing" of an African American man charged for crimes related to a drive by shooting. "The algorithm deemed the defendant to be at high risk of recidivism. Consequently, the sentencing court denied him the possibility of parole and handed down a six year sentence." Ellora Israni, 'Algorithmic Due Process: Mistaken Accountability and Attribution in *State v Loomis*' (Harvard Journal of Law & Technology JOLT Digest, 31 August 2017) https://jolt.law.harvard.edu/digest/algorithmic-due-process-mistaken-accountability-and-attribution-in-state-v-loomis-1 accessed 17 May 2025.
[58] Ibid.

accompanied by broader ethical and political reflection on the values we seek to embed in algorithmic systems and the digital future we aspire to build.

The most pressing research gaps lie precisely in empirical assessments of the effectiveness of the governance mechanisms proposed by the AI Act and related frameworks. How is FRIA being implemented in practice? What are the tangible outcomes of transparency obligations? How are accountability mechanisms functioning in cases of algorithmic harm? The political questions remain unresolved: To what extent should technological innovation yield to the protection of fundamental rights? How can we prevent AI regulation from reinforcing existing power imbalances or generating new forms of exclusion? How will evolving AI technologies force the continuous update of the law, and the creation of new fundamental rights? These questions have no easy answers, but their ongoing debate is vital for the democratic legitimacy of AI governance.

In summary, the path toward Human Rights-respecting ADM is arduous, and demands informed skepticism, a proactive stance toward risk anticipation, and an unwavering commitment to the fundamental values that underpin the European project. The CFREU offers the compass, but navigation through this novel algorithmic terrain will depend on our collective ability to translate its rights and principles into robust and meaningful practices, ensuring that technology serves humanity and not the other way around.