

The European Court of Human Rights and the Age of Artificial Intelligence*

Jurisprudential Foundations for Future Adjudications

Thomas Nektarios Papanastasiou

Associate Professor of International Economic Law and Law of Energy
School of Law, Neapolis University Pafos

Georgios Pavlidis

Associate Professor of International and EU Economic Law
School of Law, Neapolis University Pafos

As artificial intelligence (AI) systems increasingly influence domains central to human rights—expression, fairness in judicial proceedings, and equality—the jurisprudence of the European Court of Human Rights (ECtHR) has the potential to offer foundational guidance. While the Court has yet to rule extensively on AI per se, its existing case-law on digital surveillance, algorithmic decision-making, facial recognition, and online expression can provide useful interpretive tools. This article critically examines key ECtHR judgments that could shape the legal framework for confronting AI-related challenges under the European Convention on Human Rights (ECHR).

1. Setting the Stage

Artificial Intelligence (AI) has recently evolved from a specialized and largely unfamiliar branch of computer science into a transformative force that promises to reshape numerous aspects of society, including healthcare, transportation, and public administration. The integration of AI into decision-making processes has introduced both opportunities and challenges, particularly concerning the protection of fundamental human rights,¹ which are the focus of this paper.

Recognizing these significant implications of AI, the Council of Europe has taken proactive steps to address their impact. In 2024, it adopted the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law,² which is the first international legally binding treaty in

this domain. The 2024 Convention requires that all activities across the AI system lifecycle comply with human rights standards and respect key principles such as transparency, accountability, and non-discrimination³

For its part, the European Union enacted the Artificial Intelligence Act in 2024,⁴ which harmonizes the legal framework for AI deployment and use in the EU. The Act categorizes AI systems based on risk levels, and it imposes more stringent requirements on high-risk applications, especially those affecting fundamental rights. The philosophy of the Act aligns with both the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights (ECHR).

* This study was prepared in the context of the Jean Monnet Center of Excellence AI-2-TRACE-CRIME and was funded by the European Union. Views and opinions expressed are however those of the author 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.

1. E. Aizenberg, J. Van Den Hoven, "Designing for human rights in AI" (2020) Big Data & Society 7.2.
2. 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) was opened for signature on 5 September 2024 and, as of May 2025, has fifteen signatories, including the European Union.

3. R. Rodrigues, "Legal and human rights issues of AI: Gaps, challenges and vulnerabilities" (2020) Journal of Responsible Technology 4: 100005.
4. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024.

Despite these developments, the European Court of Human Rights (ECtHR) has yet to extensively adjudicate cases directly involving AI. Nevertheless, its existing jurisprudence on digital surveillance, data protection, and algorithmic decision-making could provide a useful framework for addressing AI-related human rights concerns. As AI application continue to be deployed in various sectors, the ECtHR's interpretative approaches can help delineate the boundaries between technological innovation and human rights protection. This article aims to explore precisely how the Court's existing case-law can guide the adjudication of emerging AI-related challenges, in line with the principles of the ECHR.

2. Freedom of Expression and AI-Driven Content Moderation (Article 10 ECHR)

The ECtHR has progressively addressed the complexities of freedom of expression in the digital age, particularly concerning the responsibilities of online platforms and the implications of AI-driven content moderation. AI systems in this context can automatically detect, evaluate, and manage online content based on predefined rules and standards. While the Court has not yet ruled directly on AI systems, its jurisprudence can provide us a framework for understanding the intersection of technology and freedom of expression.

In *Delfi AS v. Estonia* ([GC], 2015),⁵ the Court held that an online news portal could be held liable for defamatory comments posted by anonymous users. Although Delfi had mechanisms like word filters and a notice-and-take-down system, the defamatory comments remained online for some time before being removed following a complaint. The Court's decision emphasized the platform's role in facilitating public discourse and its responsibility to prevent harm, especially when it profits from user engagement. This is increasingly pertinent with the rise of AI moderation tools, because it recognizes the principle that platforms exercising a degree of editorial control may bear responsibility for third-party content.

Conversely, in *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary* (2016),⁶ the Court distinguished between different types of content and the context in which comments are presented. The Court found that imposing liability on a news portal for offensive but non-defamatory comments was a disproportionate interference with freedom of expression. The Court distinguished this case from its earlier decision in *Delfi*, clarified the standards for intermediary liability, and indicated that platforms should not be held strictly liable for user-generated content if they have effective mechanisms to address unlawful material. As

AI systems increasingly curate and moderate online content, the Court's nuanced approach highlights the importance of context in determining liability, as well as the significance of platforms taking reasonable steps to address unlawful material.

The *Sanchez v. France* ([GC], 2023) case⁷ further explored the boundaries of liability in the digital realm. Here, a politician was held criminally liable for failing to remove hate speech posted by third parties on his publicly accessible Facebook page. The Court found no violation of Article 10, emphasizing the applicant's role in facilitating the comments and his failure to act promptly. However, this reasoning arguably imposes a disproportionate burden on individuals to monitor third-party content—an issue of growing relevance in the context of AI-driven platforms. The deployment of AI-driven tools for content moderation inevitably raises concerns about transparency, accountability, and the risk of over-censorship. In this context, the recommendations of the Council of Europe's on AI and freedom of expression⁸ highlight the dual obligations of states: to refrain from unjustified interference and to ensure a favorable environment for the exercise of freedom of expression, including in the digital sphere. AI systems, if not properly regulated, may inadvertently suppress lawful expression or create echo chambers, undermining the pluralism essential to democratic societies.

At the level of the EU, the Digital Services Act (DSA)⁹ draws from ECtHR jurisprudence, including the *Delfi* and *Magyar* cases, to establish a framework for intermediary liability. The EU DSA emphasizes the need for proportionate measures, transparency, and the protection of fundamental rights in content moderation practices.

As a broader guiding principle, the ECtHR has consistently affirmed the importance of media pluralism and diversity in safeguarding freedom of expression. In *Manole and Others v. Moldova* (2009),¹⁰ the Court underscored the state's obligation to ensure a diverse media landscape. As AI systems play an expanding role in the dissemination of information, it is important to ensure that they do not marginalize minority voices, reinforce existing biases, suppress opposition

5. *Delfi AS v. Estonia* [GC], App no 64569/09 (ECtHR, 16 June 2015).

6. *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, App no 22947/13 (ECtHR, 2 February 2016).

7. *Sanchez v. France* [GC], App no 45581/15 (ECtHR, 15 May 2023)

8. *Council of Europe*, Recommendation of the Committee of Ministers to Member States on the impacts of digital technologies on freedom of expression, CM/Rec(2022)13, 6 April 2022; *Council of Europe*, Recommendation of the Committee of Ministers to member States on promoting a favourable environment for quality journalism in the digital age, CM/Rec(2022)4, 17 March 2022, etc. at the 1429th meeting of the Ministers' Deputies).

9. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, p. 1–102.

10. *Manole and Others v. Moldova*, App no 13936/02 (ECtHR, 17 September 2009).

perspectives, or restrict discussion on politically sensitive issues.

3. AI-Driven Surveillance, Facial Recognition, and the Right to Privacy (Article 8 ECHR)

The ECtHR has developed jurisprudence addressing how surveillance technologies interact with the right to privacy under Article 8 of the European Convention on Human Rights. While the Court has not yet ruled extensively on AI per se, its existing case law on digital surveillance, facial recognition, and data retention provides critical insights into how AI-driven surveillance might be evaluated under the Convention.

In *Glukhin v. Russia* (2023),¹¹ the ECtHR examined the use of facial recognition technology by Russian authorities to identify and arrest a peaceful protester. The Court found that the deployment of facial recognition technology in this context violated both Article 8 (right to privacy) and Article 10 (freedom of expression) of the Convention. The judgment emphasized the “highly intrusive” nature of facial recognition technology and the absence of adequate legal safeguards governing its use in Russia. The Court underscored that the use of such technology, particularly in the context of political demonstrations, requires “the highest level of justification” and must be accompanied by clear legal frameworks, oversight mechanisms, and remedies for individuals affected. This provides a clear standard for Member States deploying AI-based surveillance tools.

The ECtHR has also addressed the broader issue of mass surveillance and data retention. In *Zakharov v. Russia* (2015),¹² the Court held that Russia’s legislation allowing for the interception of communications lacked sufficient safeguards against abuse, thereby violating Article 8. The Court criticized the “almost unlimited degree of discretion” granted to authorities and the absence of effective oversight mechanisms. Thus, the Court established foundational principles for assessing the legality and proportionality of automated, large-scale data processing systems, including those powered by AI in the future.

Similarly, in *Big Brother Watch and Others v. the United Kingdom* (2021),¹³ the Court examined the UK’s bulk interception regime and found violations of Article 8 due to inadequate safeguards and oversight. The judgment highlighted the necessity for surveillance measures to be “in accordance with the law,” meaning they must be accessible, foreseeable, and provide adequate protection against arbitrary interference.

This will be very pertinent as AI-driven surveillance measures become prevalent in the future.

In *Podchasov v. Russia* (2024),¹⁴ the ECtHR addressed the issue of encryption backdoors mandated by the state. The Court concluded that requiring service providers to weaken encryption or create backdoors for law enforcement access constitutes a violation of Article 8. The judgment emphasized that such measures could lead to general and indiscriminate surveillance, undermining the privacy of all users. The judgement is very pertinent, because AI has the potential to weaken the security of communications and expose users to potential profiling, data mining, or misuse by both state and non-state actors using powerful AI tools.

While the ECtHR has not yet ruled directly on AI-driven surveillance systems, the principles established in its case law provide a framework for assessing such technologies. The first consideration here is legality, since surveillance measures must have a clear legal and accessible basis. Second, interference with privacy must be necessary in a democratic society and proportionate to the legitimate aim pursued. Third, adequate safeguards must be in place to prevent abuse, including oversight mechanisms and remedies for individuals. Finally, the use of technologies that process sensitive data, such as biometric information, requires heightened scrutiny and justification. As AI technologies become increasingly integrated into surveillance tools, adherence to these principles will be essential to ensure compliance with the ECHR.

4. Digital Justice, Algorithmic Evidence, and the Right to a Fair Trial (Article 6 ECHR)

The integration of AI into judicial processes presents both opportunities and challenges concerning the right to a fair trial under Article 6 of the ECHR. While AI can enhance efficiency and consistency, it also raises concerns about transparency, accountability, and the preservation of fundamental procedural safeguards.

The ECtHR has already addressed issues related to the use of digital evidence and algorithmic tools in legal proceedings. In *Yüksel Yalçınkaya v. Türkiye* ([GC], 2023),¹⁵ the Court found violations of Article 6 due to the reliance on data from the By-Lock messaging app as decisive evidence without proper disclosure and scrutiny. The Court emphasized the necessity of procedural safeguards when digital evidence plays a central role in convictions. This will be important in the future, as AI-generated or AI-processed evidence becomes more prevalent in judicial proceedings.

11. *Glukhin v. Russia*, App no 11519/20 (ECtHR, 4 July 2023).

12. *Roman Zakharov v. Russia* [GC], App no 47143/06 (ECtHR, 4 December 2015).

13. *Big Brother Watch and Others v. the United Kingdom* [GC], App nos. 58170/13 and 2 others (ECtHR, 25 May 2021).

14. *Podchasov v. Russia*, App no 33696/19 (ECtHR, 13 February 2024).

15. *Yüksel Yalçınkaya v. Türkiye* [GC], App no 15669/20 (ECtHR, 26 September 2023).

Similarly, in *Sigurður Einarsson and Others v. Iceland* (2019),¹⁶ the Court examined the use of e-discovery tools that filtered vast datasets. While no violation was found in that case, the Court highlighted the importance of defense access and transparency in data filtering processes, principles that are critical when algorithmic tools pre-select evidence.

This brings us to the issue of transparency, which is a cornerstone of a fair trial. The opacity of AI algorithms, often protected as trade secrets, can impede the ability of parties to understand and challenge the evidence against them. The European Ethical Charter on the Use of AI in Judicial Systems¹⁷ underscores the need for AI tools to be transparent and explainable, ensuring that their use does not undermine the rights of the defense, including the right of appeal.

The principle of judicial independence requires that judges critically evaluate AI-generated recommendations and prioritize values and considerations that algorithms cannot fully capture. Judges must not abdicate their responsibility to exercise independent judgment and must avoid blindly deferring to an AI system's output. Evidently, AI should be used to assist, not replace, human judges, ensuring that the administration of justice remains public, transparent, and accessible.

As AI technologies continue to evolve, it is important to establish effective legal frameworks that ensure their use in judicial processes aligns with the principles of the ECHR.¹⁸ This entails more than requiring transparency and explainability in AI algorithms used in legal contexts.¹⁹ It also demands the establishment of clear lines of accountability for decisions influenced or made by AI systems. Moreover, it is important to maintain human oversight in all stages of AI-assisted decision-making to preserve judicial independence and the right to a fair trial. Finally, it is necessary to provide effective remedies for individuals affected by decisions involving AI, including the right to appeal and challenge the evidence.

5. Algorithmic Discrimination and Biased Systems (Articles 14 and Protocol No. 12)

The integration of AI into decision-making processes has raised serious concerns regarding potential violations of the right to equality under Article 14 of the ECHR and Protocol No. 12. While the ECtHR has not yet adjudicated cases directly in-

volving AI-induced discrimination, its existing jurisprudence provides a foundational framework for addressing such issues in the future.

The ECtHR has recognized that systemic biases can lead to indirect discrimination. In *D.H. and Others v. the Czech Republic* [GC], 2007,²⁰ the Court found that the disproportionate placement of Roma children in special schools amounted to indirect discrimination, even without explicit intent. This precedent is pertinent to AI systems trained on historical data that may reflect societal biases, leading to discriminatory outcomes without overt discriminatory intent.

Similarly, in *Buturugă v. Romania* (2020),²¹ the Court acknowledged the state's failure to protect a woman from cyber-violence perpetrated by her former partner, highlighting the need to address technology-facilitated discrimination and violence. This case illustrates the importance of proactive measures to prevent and address discrimination enabled by digital technologies.

AI systems can inadvertently perpetuate discrimination due to biased training data, flawed algorithmic design, or lack of contextual understanding. The opacity of AI decision-making processes complicates the identification and redress of discriminatory outcomes.²² The European Union Agency for Fundamental Rights (FRA) has already highlighted instances where AI applications in predictive policing and content moderation have led to discriminatory practices against certain groups, such as ethnic minorities and women.²³

In the same context, the European Court of Justice (ECJ) in *Ligue des Droits Humains*²⁴ addressed the use of AI in processing Passenger Name Record (PNR) data, recognizing the risks of discrimination inherent in algorithmic profiling. The ECJ emphasized the need for strict safeguards to prevent discriminatory outcomes in such automated systems. Since then, both the EU and the Council of Europe have taken steps to address algorithmic discrimination through policy and legal instruments.²⁵ Despite these efforts, challenges remain in ensuring effective legal remedies for individuals affected by

16. *Sigurður Einarsson and Others v. Iceland*, App no 39757/15 (ECtHR, 4 June 2019).

17. European Commission for the Efficiency of Justice (CEPEJ), European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment (CEPEJ(2018)14).

18. A. Reiling, "Courts and artificial intelligence" (2020) *International Journal for Court Administration*, Vol. 11:2.

19. A. Mantelero, "AI and Big Data: A blueprint for a human rights, social and ethical impact assessment" (2018) *Computer Law & Security Review* 34.4, pp. 754-772.

20. *D.H. and Others v. the Czech Republic* [GC], App no 57325/00 (ECtHR, 13 November 2007).

21. *Buturugă v. Romania*, App no 56867/15 (ECtHR, 11 February 2020).

22. G. Pavlidis, "Unlocking the black box: analysing the EU artificial intelligence act's framework for explainability in AI" (2024) *Law, Innovation and Technology* 16.1, pp. 293-308.

23. *European Union Agency for Fundamental Rights*, Bias in Algorithms: Artificial Intelligence and Discrimination, 2022.

24. Court of Justice of the European Union, Judgment of 21 June 2022 in the Case C-817/19 (*Ligue des droits humains ASBL v Conseil des ministres*).

25. Both the EU AI Act and the Council of Europe's Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law mandate that AI systems respect human rights principles, including non-discrimination.

algorithmic discrimination. The complexity and opacity of AI systems can hinder individuals' ability to contest discriminatory decisions, necessitating the development of more accessible and transparent mechanisms for redress.

In addition to ensuring transparency, regulators must develop and enforce legal frameworks that proactively prevent discriminatory outcomes in AI applications. It is also important to establish accessible avenues for individuals to challenge and seek remedies for discriminatory decisions made by AI systems. Finally, regulators must encourage the use of diverse and representative data sets by developers in training AI systems to mitigate inherent biases. Thus, European legal systems can better safeguard against algorithmic discrimination, ensuring the alignment of AI technologies with the fundamental rights enshrined in the ECHR.²⁶

6. Conclusion

The ECtHR has not yet been asked to adjudicate AI-specific cases, but its jurisprudence offers critical tools for addressing the human rights challenges posed by algorithmic systems.²⁷ Whether in content moderation, facial recognition, legal proceedings, or profiling, the Court's insistence on proportionality, procedural fairness, and safeguards against arbitrariness sets the benchmarks. As AI technologies evolve, the ECtHR's interpretive principles are expected to play a vital role in ensuring that innovation remains anchored in the values of the ECHR.²⁸ Nevertheless, one must consistently account for the inherent complexity of the Court's jurisprudence, as well as the politically sensitive role of the Committee of Ministers in overseeing the execution of judgments by member states.²⁹

References

- Aizenberg, E, Van Den Hoven, J., "Designing for human rights in AI" (2020) *Big Data & Society* 7.2.
- Council of Europe, Recommendation of the Committee of Ministers to Member States on the impacts of digital technologies on freedom of expression, CM/Rec(2022)13, 6 April 2022
- Council of Europe, Recommendation of the Committee of Ministers to member States on promoting a favourable environment for quality journalism in the digital age, CM/Rec(2022)4, 17 March 2022
- European Commission for the Efficiency of Justice (CEPEJ), European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment (CEPEJ(2018)14)
- European Union Agency for Fundamental Rights, Bias in Algorithms: Artificial Intelligence and Discrimination, 2022.
- Keller, H. & V. Gurash, "Rethinking the Execution of Judgments of the European Court of Human Rights" (2023) *European Human Rights Law Review* (2), pp. 152–168.
- Mantelero, A., "AI and Big Data: A blueprint for a human rights, social and ethical impact assessment" (2018) *Computer Law & Security Review* 34.4, pp. 754–772.
- Papanastasiou, T.N., "The Effectiveness of the Administration of Justice in the Occupied Territories: The Unreasonable Delays of the Immovable Property Commission" (2022) *Cyprus Law Review (in Greek)* Vol. 3, pp. 373–381.
- Pavlidis, G., "Unlocking the black box: analysing the EU artificial intelligence act's framework for explainability in AI" (2024) *Law, Innovation and Technology* 16.1, pp. 293–308.
- Reiling, A., "Courts and artificial intelligence" (2020) *International Journal for Court Administration*, Vol. 11:2.
- Risse, M., "Human rights and artificial intelligence: An urgently needed agenda" (2019) *Human Rights Quarterly* 41.1, pp. 1–16.
- Rodrigues, R., "Legal and human rights issues of AI: Gaps, challenges and vulnerabilities" (2020) *Journal of Responsible Technology* 4: 100005.
- Smuha, N., "Beyond a human rights-based approach to AI governance: Promise, pitfalls, plea" (2021) *Philosophy & Technology* 34.1, pp. 91–104
- Szappanyos, M., "Artificial Intelligence: Is the European Court of Human Rights Prepared?" (2023) *Acta Humana–Emberi Jogi Közlemények* 11.1. pp. 93–110.
- 26. M. Risse, "Human rights and artificial intelligence: An urgently needed agenda" (2019) *Human Rights Quarterly* 41.1, pp. 1–16.
- 27. M. Szappanyos, "Artificial Intelligence: Is the European Court of Human Rights Prepared?" (2023) *Acta Humana–Emberi Jogi Közlemények* 11.1. pp. 93–110.
- 28. For a more critical view: N. Smuha, "Beyond a human rights-based approach to AI governance: Promise, pitfalls, plea" (2021) *Philosophy & Technology* 34.1, pp. 91–104.
- 29. The politically charged role of the Committee of Ministers becomes especially pronounced in cases involving complex and unresolved geopolitical conflicts, such as the Cyprus cases. These cases exemplify how the Committee's supervisory role becomes entangled in broader political dynamics, revealing a persistent tension between legal obligation and political feasibility in the Council of Europe's human rights enforcement system. See, T.N. Papanastasiou, "The Effectiveness of the Administration of Justice in the Occupied Territories: The Unreasonable Delays of the Immovable Property Commission" (2022) *Cyprus Law Review (in Greek)* Vol. 3, pp. 373–381; H. Keller & V. Gurash, "Rethinking the Execution of Judgments of the European Court of Human Rights" (2023) *European Human Rights Law Review* (2), pp. 152–168.