INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

ISSN: 2582-6433

November 2026

RESEARCH ARTICLE

Justice in the Black Box: A Socio-Legal Study of AI-Generated Digital Evidence under the Bharatiya Sakshya Adhiniyam, 2023 and Its Impact on Access to Justice in India

Adv. Asma Khan

Advocate, High Court of Madhya Pradesh, Bench at Indore
Ph.D. Research Scholar (Law), Renaissance University, Indore

www.ijlra.com

ABOUT THE JOURNAL

International Journal for Legal Research and Analysis (IJLRA)

ISSN: 2582-6433

IJLRA provides a platform for scholarly writing and discussion on law, legal research and interdisciplinary questions. Research articles explore legal principles, institutions, policy and contemporary developments.

Journal website: www.ijlra.com

PUBLICATION INFORMATION

International Journal for Legal Research and Analysis
ISSN: 2582-6433

Editorial note

The views and arguments expressed in this article are those of its author. Readers should consult the original legal authorities and sources cited in the manuscript.

Copyright and permissions are subject to the applicable publication agreement.

ARTICLE DETAILS

Justice in the Black Box: A Socio-Legal Study of AI-Generated Digital Evidence under the Bharatiya Sakshya Adhiniyam, 2023 and Its Impact on Access to Justice in India

Author: Adv. Asma Khan

Advocate, High Court of Madhya Pradesh, Bench at Indore
Ph.D. Research Scholar (Law), Renaissance University, Indore

Journal: International Journal for Legal Research and Analysis
ISSN: 2582-6433

Justice in the Black Box: A Socio-Legal Study of AI-Generated Digital Evidence under the Bharatiya Sakshya Adhiniyam, 2023 and Its Impact on Access to Justice in India

Adv. Asma Khan

Advocate, High Court of Madhya Pradesh, Bench at Indore
Ph.D. Research Scholar (Law), Renaissance University, Indore

ABSTRACT

The Bharatiya Sakshya Adhiniyam, 2023 has modernised Indian evidence law by placing electronic and digital records on par with conventional documents. Yet the statute was drafted for a world in which machines store and transmit information; it is largely silent on a world in which machines interpret it. Artificial intelligence systems now produce inferences whose internal reasoning cannot be fully explained even by their developers. This article argues that the certificate-based model of authentication under Section 63 of the Adhiniyam tests the integrity of the container but not the reliability of the conclusion, and that this doctrinal gap is not socially neutral. In a criminal justice system where nearly three of every four prisoners are undertrials, most of them poor and with limited formal education, the burden of an unexplainable algorithm falls hardest on those least equipped to challenge it. Drawing on Articles 14, 20(3), 21 and 39A of the Constitution, official data on prisons and forensic capacity, and comparative developments in the United States, the United Kingdom and the European Union, the article proposes a reliability-centred framework for AI-generated evidence in India, anchored in disclosure, contestability, corroboration and equal access to independent expertise. Keywords: Bharatiya Sakshya Adhiniyam; Artificial Intelligence; Digital Evidence; Black-Box Algorithms; Access to Justice; Fair Trial; Deepfakes; Socio-Legal Study

I. INTRODUCTION

Evidence law has always been a theory of trust. It tells a court whom to believe, how far, and for what reason. For over a century and a half, Indian courts answered these questions within a framework designed around human witnesses and paper documents. The Bharatiya Sakshya Adhiniyam, 2023 (hereinafter "BSA"), which came into force on 1 July 2024, consciously

moved that framework into the digital age by recognising electronic and digital records as documents and, in defined circumstances, as primary evidence.[1]

The reform, however, arrives at a moment when the nature of digital evidence itself is changing. A CCTV clip, an e-mail or a call detail record is a record of something that happened. A facial recognition "match", an AI-sharpened video frame or a software verdict that an audio clip is "synthetic" is something different: it is an opinion generated by a machine, through a process its user cannot see and its developer often cannot fully explain. Scholars have described such systems as "black boxes", whose inputs and outputs are visible but whose inner reasoning is not.[2] This article asks three questions. First, does the BSA framework, built around authentication of electronic records, adequately test the reliability of AI-generated inferences? Second, who in Indian society bears the cost when it does not? Third, what constitutional and institutional safeguards are needed so that technology widens rather than narrows access to justice? The study combines doctrinal analysis of statutes and precedents with a socio-legal reading of official data on prisons, forensic capacity and policing. Its central claim is that the problem of black-box evidence is not merely technical; it is a problem of power, poverty and equality before the law.

II. FROM DIGITAL RECORD TO ALGORITHMIC INFERENCE

It is useful to distinguish three kinds of machine-related evidence. The first is the stored record: a WhatsApp message, a photograph or a CCTV file. The legal question here is authenticity, that is, whether the record is what it claims to be and has not been altered. The second is the deterministic computer output: a hash value, a call detail record or a GPS log, produced by fixed rules that give the same result each time the same input is processed. The third, and the subject of this article, is the AI-generated inference: a probabilistic conclusion produced by a model that has "learnt" patterns from training data, such as a face-match score, a voice-identification result, an "enhanced" image or a deepfake-detection verdict.

The third category behaves less like a document and more like a witness. Andrea Roth has accordingly described such outputs as "machine testimony", which carries the hearsay dangers of human testimony, namely flawed perception, ambiguity and bias, without the safeguards of oath, demeanour and cross-examination.[3] Its opacity has three layers. Technical opacity arises because deep-learning models reason through millions of weighted parameters that do not translate into human explanation. Proprietary opacity arises because vendors shield source code and training data as trade secrets.[4]

Institutional opacity arises because investigating agencies rarely disclose which tool was used, at what threshold, and with what known error rate.

Indian experience illustrates all three. The Delhi Police acquired its facial recognition system under directions of the Delhi High Court in Sadhan Haldar v. NCT of Delhi to trace missing children, and the Court was later told that the system's accuracy was about two per cent.[5]

Responses under the Right to Information Act later revealed that the police treated a match of 80 per cent similarity as "positive" before proceeding with further inquiry.[6]

Neither the threshold nor its scientific basis is prescribed by any statute. Such a system can thus move a citizen from anonymity to suspicion on the strength of a number that no court has validated.

III. THE LEGAL FRAMEWORK: BUILT FOR AUTHENTICITY, SILENT ON RELIABILITY

A. The certificate model under the BSA. Section 61 of the BSA declares that nothing in the Adhiniyam shall deny the admissibility of an electronic or digital record merely because it is electronic, subject to Section 63.[7] Section 63, which replaces Section 65B of the Indian Evidence Act, 1872, requires a certificate in the form prescribed in the Schedule, now in two parts: Part A by the person in charge of the device, and Part B by an expert, who must record details such as the hash value of the record.[8] This is a welcome improvement. Yet every element of the certificate concerns integrity: that the device was operating properly, that the record was produced in the ordinary course and that it has not been altered. None of it asks whether the algorithm that produced an inference was validated, what its error rate is, what data it was trained on, or whether a human reviewed its output. A perfectly authenticated output can still be perfectly wrong.

B. Judicial evolution. The Supreme Court in Anvar P.V. v. P.K. Basheer made the certificate mandatory for secondary electronic evidence,[9] relaxed the position in Shafhi Mohammad v. State of Himachal Pradesh,[10] and restored it in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal.[11] This jurisprudence is rich on procedure but thin on reliability, because the cases concerned stored records, not machine inferences. At the same time, courts have spoken of electronic evidence with considerable confidence; in Tomaso Bruno v. State of Uttar Pradesh, the Court emphasised the value of scientific and electronic evidence such as CCTV footage in criminal investigation.[12] That confidence was justified for recordings; it cannot be transferred automatically to algorithmic conclusions. C. Expert opinion. Section 39(2) of the BSA makes the opinion of the Examiner of Electronic Evidence notified under Section 79A of the Information Technology Act, 2000 a relevant fact.[13] In theory, the expert stands between the machine and the court. In practice, when the analysis is performed by proprietary software, the expert may simply report what the tool concluded. The expert then becomes a conduit for the machine rather than a check upon it, and cross-examination reaches the human messenger but not the algorithmic author.

D. Procedural expansion without a reliability standard. The Bharatiya Nagarik Suraksha Sanhita, 2023 ("BNSS") requires forensic experts to visit crime scenes in offences punishable with seven years or more, mandates audio-video recording of searches and permits proceedings in electronic mode.[14] These provisions will multiply the volume of technology-generated

evidence, much of it processed by AI-assisted tools, without any corresponding standard for testing machine-made conclusions.

E. Regulatory and judicial responses so far. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, notified on 10 February 2026, define "synthetically generated information" and require intermediaries to label it.[15] The Rules, however, regulate platforms, not courtrooms. The judiciary, for its part, has been cautious about its own use of AI. The Punjab and Haryana High Court, after consulting ChatGPT in a bail matter, clarified that the reference was not a basis for its decision;[16] the Delhi High Court held that AI chatbot responses cannot form the basis of adjudication;[17] and the Kerala High Court, in July 2025, issued a policy prohibiting the district judiciary from using AI tools to arrive at findings or judgments.[18] A striking asymmetry follows. Courts distrust AI as an aid to their reasoning, yet no rule requires similar scrutiny when the same kind of technology is tendered as evidence against a citizen.

IV. THE SOCIO-LEGAL DIMENSION: WHO BEARS THE COST OF THE BLACK BOX?

Law does not operate in a vacuum. A doctrinal gap becomes a social injury when it falls on people already disadvantaged by poverty, caste, gender, religion, language or geography. This Part examines how black-box evidence interacts with the realities of Indian criminal justice.

A. Inequality of arms. The State has access to Central and State Forensic Science Laboratories, the National Cyber Forensic Laboratory and vendor support for proprietary tools.[19] The typical accused, by contrast, is represented by a private counsel of modest means or by a legal aid lawyer working for a small honorarium, with no budget for an independent digital forensic expert. The Part B certificate under Section 63 itself requires an expert, so a poor accused cannot even produce a counter-certificate. The black box is therefore not equally dark for everyone: the prosecution can at least call the vendor, while the defence faces the output alone. Equality before the law becomes a formal promise without a functional means of testing the evidence.

B. The undertrial and the forensic queue. According to the National Crime Records Bureau, undertrials constituted 72.[6] per cent of India's prison population at the end of 2024, numbering about 3.[71] lakh persons.[20] Nearly two-thirds of undertrials had not studied beyond Class X, and Madhya Pradesh recorded a prison occupancy rate of 147.[1] per cent, among the highest in the country.[21] Forensic capacity has not kept pace. A national study of forensic laboratories by Project 39A found large vacancies and noted that examination rates in cyber forensics have consistently lagged behind pendency;[22] while the Union Government has stated that data on pending forensic cases is not even maintained centrally.[23] In this setting, an algorithmic "match" recorded in a case diary can weigh heavily at the stage of arrest and bail, while any challenge to it waits in a long forensic queue. As Malcolm Feeley observed in a different context, the process itself becomes the punishment.[24] C. Encoded bias and marginalised

communities. AI systems learn from historical data, and historical data in criminal justice reflects historical policing. Global research has shown that commercial facial analysis systems perform markedly worse on darker-skinned women,[25] and the United States National Institute of Standards and Technology documented demographic differences in false-match rates across many algorithms.[26] In India, a study by the Vidhi Centre for Legal Policy warned that facial recognition in Delhi policing is likely to affect Muslims living in over-policed areas disproportionately.[27] Prison data also shows that in States such as Uttar Pradesh and Bihar, the share of Scheduled Caste undertrials exceeds their share of the population.[28] Communities such as the Denotified Tribes still carry the stigma of colonial "criminal tribe" laws. When data drawn from such patterns trains a predictive or identification tool, prejudice is converted into probability. The danger is not only error but legitimacy: bias acquires the aura of scientific neutrality, and the feedback loop of over-policing, more data and further suspicion becomes self-justifying. D. Gender, deepfakes and the liar's dividend. Women experience the black box in two opposite ways. As victims of morphed images and non-consensual synthetic intimate content, they must prove that a realistic image is fake, often before police stations that lack tools for verification, and while managing stigma, family pressure and fear of further circulation. Conversely, as survivors who rely on genuine recordings of abuse, harassment or threats, they increasingly face the defence that the evidence is itself a deepfake. Chesney and Citron call this the "liar's dividend": the mere possibility of synthetic media allows wrongdoers to deny authentic evidence.[29] In domestic violence and sexual harassment cases, where a recording may be the only corroboration of an act committed in private, this tactic can silence survivors. The 2026 labelling rules are a step forward, but labels on platforms do not resolve contests over authenticity in a magistrate's court.

E. Language, literacy and meaningful participation. Technical evidence is usually explained in English and in specialised vocabulary such as "confidence score", "false positive rate" or "model hallucination". For an accused with limited schooling who follows proceedings in Hindi or another regional language, such evidence is almost impossible to understand, let alone to rebut through instructions to counsel. A trial the accused cannot comprehend is fair only on paper. The comprehension gap is sharpest in rural and district courts, where specialised digital forensic training for advocates and legal aid counsel is rarely available. F. Automation bias and public trust. Human decision-makers tend to over-rely on automated outputs, treating them as more objective than human judgment.[30] Investigators may close lines of inquiry once software returns a match; prosecutors may present the output as conclusive; courts may hesitate to question what appears to be science. Every wrongful conviction founded on an unexplainable machine conclusion will damage public trust in the justice system, especially among communities whose relationship with the police is already strained. Justice must not only be done but must be seen to be done, and a decision that cannot be explained cannot be seen.

V. CONSTITUTIONAL IMPLICATIONS

Article 21. Since Maneka Gandhi v. Union of India, any procedure depriving a person of liberty must be fair, just and reasonable.[31] The Supreme Court has described a fair trial as the heart of criminal jurisprudence, requiring that the accused have a genuine opportunity to test the case against him.[32] Cross-examination is the principal instrument of that testing. When a decisive piece of evidence is the product of an algorithm that cannot be interrogated, the right to cross-examine is hollowed out.

Article 14. In E.P. Royappa v. State of Tamil Nadu, the Court held that arbitrariness is antithetical to equality.[33] An evidentiary conclusion that cannot be explained or reproduced is, from the citizen's perspective, arbitrary. Where error rates are higher for particular groups, the tool also produces unequal outcomes for persons who are similarly situated, raising concerns of indirect discrimination.

Article 20(3) and privacy. In Selvi v. State of Karnataka, the Court held that involuntary narco-analysis, polygraph and brain-mapping tests violate the right against self-incrimination and personal liberty.[34] Emerging AI tools that claim to infer deception or emotion from voice, face or behaviour raise similar concerns. Further, mass facial recognition without a specific enabling statute must satisfy the tests of legality, necessity and proportionality laid down in K.S. Puttaswamy v. Union of India.[35]

Article 39A. Free legal aid is a constitutional guarantee, and the Court has insisted that it be real and available from the earliest stage.[36] In an age of algorithmic evidence, legal aid without access to forensic expertise is like a shield without a handle. Meaningful legal aid must now include the means to examine the machine.

VI. COMPARATIVE PERSPECTIVES

In the United States, scientific evidence is tested under the Frye standard of general acceptance or the Daubert factors of testability, peer review, known error rate, standards and acceptance.[37] Applying Frye, a Washington court in State v. Puloka excluded AI-enhanced video, finding that the tool used opaque methods to show what the model predicted rather than what the camera recorded.[38] Notably, it was the defence that sought to rely on the AI evidence, which shows that reliability rules protect both sides. In State v. Loomis, by contrast, the Wisconsin Supreme Court permitted the use of a proprietary risk-assessment tool at sentencing, subject to cautionary warnings, despite the defendant's inability to examine its methodology, a ruling widely criticised for accepting opacity.[39] Recognising the gap, the federal Advisory Committee on Evidence Rules published a proposed Rule 707 in 2025 to subject machine-generated evidence offered without an expert to the reliability standards applied to expert testimony; after public comment, the proposal was sent back for revision and has not yet been adopted.[40]

In the United Kingdom, the Court of Appeal in R (Bridges) v. Chief Constable of South Wales Police held police use of live facial recognition unlawful, partly because it left too much discretion to individual officers.[41] The European Union's Artificial Intelligence Act classifies

AI systems used in law enforcement and the administration of justice as high-risk, mandates human oversight and gives affected persons a right to an explanation of individual decisions.[42] These models are not for blind transplant; India must account for its own scale, resource constraints and social diversity. They do, however, show a convergence: AI evidence requires a reliability inquiry distinct from mere authentication. VII. TOWARDS A RIGHTS-BASED REFORM FRAMEWORK

The following reforms are proposed, combining legal change with institutional and social measures.

1. A statutory reliability test. The BSA should be amended to define "AI-generated evidence" and to require, before admission, a judicial assessment of reliability based on factors adapted to Indian conditions: validation studies, known error rates including demographic variation, the version and threshold used, provenance of training data and the extent of human review. A new Part C to the Schedule certificate could require these disclosures.

2. Disclosure and contestability. The duty to supply documents to the accused under Section 230 of the BNSS should be interpreted, or amended, to include algorithmic documentation. Trade-secret claims can be accommodated through confidentiality orders and court-appointed experts, but they must never defeat the accused's right to test the evidence.

3. A rule of corroboration. By statute or binding judicial guidelines, an AI-generated inference should not by itself be the basis for arrest, framing of charge or conviction. It should be treated like other weak forms of evidence that require independent corroboration.

4. A defence forensic fund. The National and State Legal Services Authorities should establish panels of independent digital forensic experts and a dedicated fund so that legal aid beneficiaries can challenge AI evidence. Without this, every other safeguard will remain the privilege of those who can afford it. 5. Bias audits and accreditation. AI tools used by police and forensic laboratories should be accredited, independently audited for demographic bias and publicly reported upon. Facial recognition for policing should be governed by a specific law, as Puttaswamy requires, rather than by executive orders.

6. A victim-centred deepfake protocol. Cyber cells should offer time-bound forensic verification for complainants, particularly women, in cases of synthetic sexual content. Courts should also refuse to accept a bare plea that evidence is a deepfake without some expert foundation, so that the liar's dividend does not defeat genuine survivors.

7. Judicial and professional education. State Judicial Academies, Bar Councils and law schools should offer training on AI evidence, building on the Kerala High Court's policy. Expert reports should also carry a plain-language summary, in the language of the court, explaining what the tool did and how confident it is.

VIII. CONCLUSION

The Bharatiya Sakshya Adhiniyam has answered the question of whether digital evidence may enter the courtroom. The question that now confronts Indian law is how far an unexplainable machine may be believed once it enters. The present framework checks whether a record is genuine; it does not check whether an algorithmic conclusion is true. This gap is not socially neutral. It burdens the undertrial who cannot afford an expert, the community that is over-policed and therefore over-represented in data, the woman who must prove that an image of her is fake or that a recording of her abuse is real, and the litigant who cannot follow technical evidence in a language that is not his own. Technology can strengthen justice in India by producing faster investigations, better evidence and fewer wrongful convictions, but only if the law insists that machines, like witnesses, must be tested. A constitutional democracy cannot allow liberty to depend on a conclusion that neither the court nor the accused can understand. Opening the black box is therefore not a technical preference but a constitutional necessity, and it is the condition on which the promise of equal justice under Article 14, the guarantee of a fair trial under Article 21 and the commitment to legal aid under Article 39A can remain meaningful in the age of artificial intelligence.

References and Notes

1 'The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), ss. 2(1)(d) and 57, Explanations

4 to 7.

2 Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (Harvard University Press 2015) 3-4.

3 Andrea Roth, 'Machine Testimony' (2017) 126 Yale Law Journal 1972.

4 Rebecca Wexler, 'Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System' (2018) 70 Stanford Law Review 1343

5 'Internet Freedom Foundation, 'Delhi Police's Facial Recognition Sweep at Jantar Mantar is Unreliable and Unlawful' (2026), discussing Sadhan Haldar v. NCT of Delhi (Delhi High Court, 2018).

6 80% Accuracy in Facial Recognition Database is a Positive Match for Delhi Police: Report' Deccan Herald (New Delhi, 2022).

7 BSA, s. 61.

8 BSA, s. 63(4) read with the Schedule (Parts A and B of the Certificate).

9 Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

10 Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.

11 Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

12 Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 SCC 178. 13BSA, S. 39(2); Information Technology Act, 2000, s. 79A.

13 BSA, s. 39(2); Information technology act, 2000, s. 79A

14 Bharatiya Nagarik Suraksha Sanhita, 2023, ss. 105, 176(3) and 530.

15 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, notified by MeitY on 10 February 2026, inserting r. 2(1)(wa).

16 Jaswinder Singh @ Jassi v. State of Punjab, CRM-M-22496-2022 (P&H HC, 27 March 2023).

17 Christian Louboutin SAS v. M/s The Shoe Boutique - Shutiq, CS(COMM) 583/2023 (Delhi HC, 22 August 2023).

18 High Court of Kerala, Policy Regarding Use of Artificial Intelligence Tools in District Judiciary (19 July 2025).

19 Ministry of Home Affairs, Rajya Sabha Unstarred Question No. 2630 (18 December 2024).

20 National Crime Records Bureau, Prison Statistics India 2024 (Ministry of Home Affairs 2026); see also '#DataViz: Who Are India's 371,000 Prisoners Awaiting Trial?' The News Minute (2026).

21 ibid; 'Prison Statistics India Report 2024' Drishti IAS (2 June 2026).

22 Project 39A, National Law University Delhi, Forensic Science India Report (in collaboration with the Ministry of Home Affairs), analysing laboratory data from 2013 to 2017.

23 Rajya Sabha Unstarred Question No. 2630 (n 19).

24 Malcolm M. Feeley, The Process is the Punishment: Handling Cases in a Lower Criminal Court (Russell Sage Foundation 1979).

25 Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research 77.

26 Patrick Grother, Mei Ngan and Kayee Hanaoka, Face Recognition Vendor Test Part 3: Demographic Effects (NISTIR 8280, December 2019).

27 Jai Vipra, The Use of Facial Recognition Technology for Policing in Delhi (Vidhi Centre for Legal Policy 2021); see 'Policing via Facial Recognition Technology May Affect Vulnerable Groups, Says Report' BloombergQuint (2021).

28 Indians in Jails: Many are Young, Poorly Educated and Awaiting Trial' Scroll.in (2025), analysing NCRB data.

29 Robert Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753.

30 Danielle Keats Citron, 'Technological Due Process' (2008) 85 Washington University Law Review 1249.

31 Maneka Gandhi v. Union of India, (1978) 1 SCC 248.

32 Zahira Habibullah Sheikh v. State of Gujarat, (2004) 4 SCC 158.

33 E.P. Royappa v. State of Tamil Nadu, (1974) 4 SCC 3.

34 Selvi v. State of Karnataka, (2010) 7 SCC 263.

35 K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

36 Hussainara Khatoon v. Home Secretary, State of Bihar, (1980) 1 SCC 81; Khatri (I) v. State of Bihar, (1981) 1 SCC 627.

37 Frye v. United States, 293 F. 1013 (D.C. Cir. 1923); Daubert v. Merrell Dow Pharmaceuticals Inc., 509 U.S. 579 (1993).

38 State of Washington v. Puloka, No. 21-1-04851-2 (Wash. Super. Ct., King County, 29 March 2024).

39 State v. Loomis, 881 N.W.2d 749 (Wis. 2016).

40 Advisory Committee on Evidence Rules, Proposed Federal Rule of Evidence 707 (Machine-Generated Evidence), published for comment in August 2025; see Proskauer Rose LLP, 'Machine-Generated Evidence Challenges the Federal Rules' (29 July 2026).

41 41 R (Bridges) v. Chief Constable of South Wales Police [2020] EWCA Civ 1058.

42 Regulation (EU) 2024/1689 (Artificial Intelligence Act), arts 14 and 86 and Annex III, points 6 and 8.