

Risks and Legal Regulation of Automated Sentencing Models in Environmental Justice

Bona Song

*School of Marxism, Jining Normal University, Ulanqab 012000, Inner Mongolia, China,
302405@jnnu.edu.cn*

Abstract

The use of artificial intelligence in legal decision-making has created new possibilities for consistency, speed and structured reasoning, but it also raises serious concerns when algorithmic systems influence sentencing. This article examines the risks and legal regulation of automated sentencing models in the specific context of environmental justice. Environmental offences such as illegal pollution, hazardous waste disposal, deforestation, industrial contamination and wildlife crime often create cumulative ecological harm and unequal social burdens. These burdens frequently fall on communities that already face weak participation in environmental governance and limited access to remedies. The article adopts a doctrinal, comparative and normative legal research method. It analyses selected case law, international instruments, AI governance frameworks, environmental justice literature and data-protection standards. The article finds that automated sentencing models may reproduce biased enforcement data, obscure legal reasoning, encourage automation bias, weaken due process and fail to account for cumulative community harm. It argues that the problem is not simply whether AI is accurate, but whether its use is transparent, contestable, accountable and sensitive to environmental justice. The article concludes that automated sentencing systems should not replace judicial discretion. They may be used only as carefully controlled decision-support tools subject to mandatory algorithmic impact assessment, independent audit, explainability, meaningful human oversight, community participation and a right to challenge algorithmic outputs.

Keywords: Artificial intelligence; automated sentencing; environmental justice; algorithmic bias; environmental crime; due process; AI regulation; human rights.

1. Introduction

Artificial intelligence has moved legal systems beyond simple digitisation. Courts, regulators and public agencies increasingly use data-driven tools to organise records, identify risk patterns and support decisions that affect individual rights and public interests. The attraction of these systems is clear: they promise speed, consistency and the ability to process large volumes of information. Their danger is also clear. Algorithmic systems may operate as forms of black-box governance when affected persons cannot understand how a recommendation was produced or how it influenced a legal decision [1]. In public decision-making, this concern becomes a question of technological due process because legal authority must remain reasoned, transparent and contestable [2].

Environmental justice makes this issue especially important. Environmental justice is commonly understood as the fair treatment and meaningful involvement of all people in the development,

implementation and enforcement of environmental laws and policies [3]. Environmental rule-of-law literature shows that many jurisdictions have environmental laws on paper but continue to face weak enforcement and unequal implementation in practice [4]. Therefore, a sentencing model trained on past enforcement data may inherit the same patterns of inequality that environmental justice seeks to correct.

Automated sentencing models are not hypothetical in the broader criminal justice debate. In *State v. Loomis*, the Wisconsin Supreme Court considered the use of the COMPAS risk assessment tool at sentencing and held that limited use of the tool did not violate due process, while also warning that such tools must not become determinative of incarceration or sentence severity [5]. The public debate around COMPAS intensified after ProPublica reported racial disparities in risk classifications, showing how a formally neutral score may produce contested social effects [6]. These lessons are directly relevant to environmental sentencing because environmental enforcement data may also reflect unequal inspection, reporting and prosecution patterns.

Environmental crimes differ from ordinary offences in important respects. They may involve corporate actors, technical scientific evidence, transboundary impacts, delayed ecological harm, public health consequences and cumulative burdens on vulnerable communities. A sentencing decision in such cases cannot be reduced to the seriousness of a single incident. It may require assessment of remediation, deterrence, restoration, community vulnerability and intergenerational harm. For that reason, any algorithmic recommendation used in environmental sentencing must be examined not only for statistical accuracy but also for legal legitimacy and environmental justice impact.

The research problem addressed in this article is whether automated sentencing models can be legally regulated in a way that preserves due process, judicial discretion and environmental justice. The article has four objectives: to explain how automated sentencing models may operate in environmental justice cases; to identify major legal and ethical risks; to evaluate selected legal and regulatory responses; and to propose safeguards for responsible governance.

The article addresses the following research questions: What risks arise when automated sentencing models are applied to environmental justice? How do transparency, explainability, human oversight and accountability affect the legality of such systems? Which regulatory principles can be drawn from AI law, data protection, human rights and environmental law? What safeguards are necessary before such tools can be used responsibly?

2. Methodology

This article uses a doctrinal, comparative and normative legal research method. It is doctrinal because it analyses legal rules, cases, statutes, regulatory instruments and principles relevant to automated decision-making and environmental sentencing. It is comparative because it examines selected approaches from the European Union, the United States, Canada and international organisations. It is normative because it evaluates whether current legal safeguards are adequate and proposes a governance model suitable for environmental justice.

The technical concept of AI is used in a broad legal sense, referring to computational systems capable of classification, prediction, pattern recognition and decision support [7]. The risk analysis is based on established scholarship showing that algorithmic systems can produce disparate impact through historical data, proxy variables, measurement choices and institutional context [8]. The analysis also uses the classic

concept of bias in computer systems, which recognises that bias may arise from technical design, pre-existing social patterns or emergent interaction between a system and its environment [9].

The environmental justice framework is based on distributive, procedural, recognition and restorative dimensions. Schlosberg's account of environmental justice is useful because it treats justice as more than distribution and includes recognition, participation and capabilities [10]. Bullard's environmental justice scholarship is also central because it demonstrates how environmental burdens are historically linked to race, class and unequal political power [11].

The sources were selected according to three criteria. First, legal instruments and cases were included where they directly address AI governance, automated decision-making, due process, data protection, environmental justice or environmental liability. Second, academic sources were included where they are widely cited or directly relevant to algorithmic bias, explainability, fairness or environmental justice. Third, policy frameworks were included where they provide official standards for high-risk AI, human oversight, transparency or public-sector automated decision systems.

The article does not present empirical testing of an existing environmental sentencing algorithm. The figures and graphs are therefore analytical tools that organise the doctrinal findings. They should be read as legal-risk visualisations, not as statistical measurements from a deployed system.

Table 1. Research method and analytical focus

Method component	Application in this article	Purpose
Doctrinal legal analysis	Cases, statutes, legal instruments and regulatory standards are examined.	To identify binding and persuasive legal safeguards.
Comparative analysis	EU, U.S., Canadian and international approaches are compared.	To evaluate alternative regulatory models.
Normative analysis	Risks are assessed against due process, judicial discretion and environmental justice.	To propose a responsible governance framework.
Qualitative risk mapping	Risks are grouped by bias, transparency, accountability, human rights and environmental justice impact.	To show where legal controls are needed before and during deployment.

3. Results and Analysis

3.1 Conceptual Framework for Automated Environmental Sentencing

The first analytical finding is that automated sentencing in environmental justice must be treated as a decision-support process and not as a substitute for adjudication. An environmental sentencing tool may receive structured information about the offence, the offender, prior compliance history, environmental damage, economic benefit, public health impact, remediation status and risk of recurrence. The model may then generate a risk score, penalty recommendation or suggested aggravating and mitigating factors. However, the legally relevant decision remains the sentence imposed by the court or competent authority.

Environmental justice research shows that environmental burdens are often distributed unequally across race, income, geography and political power [12]. Community-based environmental justice scholarship also demonstrates that affected communities must participate in identifying harm and shaping remedies, rather

than being treated only as data points within an administrative system [13]. A sentencing model that ignores these dimensions may appear objective while missing the social meaning of environmental harm.

Figure 1 presents the legally acceptable pathway. The model may assist with organising data and identifying patterns, but the final decision must be reasoned by a human judicial authority. The safeguard layer is not optional; it is the condition that makes algorithmic assistance compatible with legality.

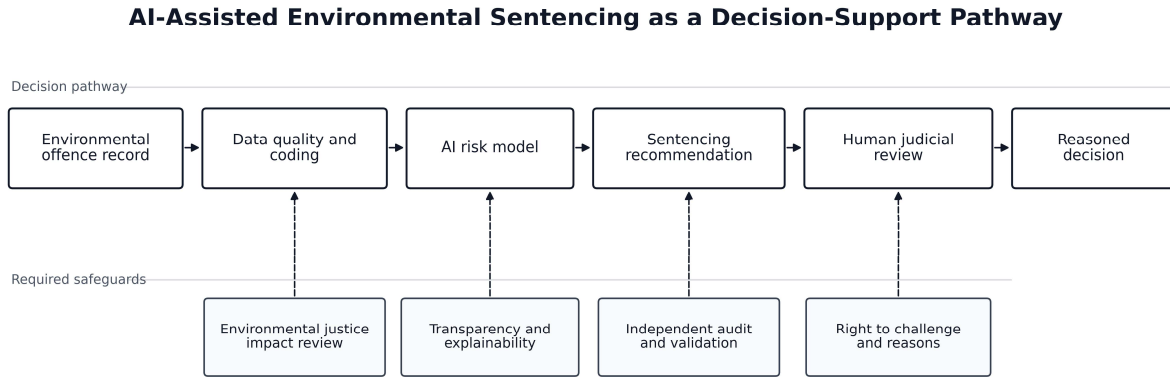


Figure 1. Conceptual framework for AI-assisted environmental sentencing as a decision-support pathway.

3.2 Risk Typology

The second analytical finding is that automated sentencing creates a cluster of connected risks. The most important risk is algorithmic bias. In environmental justice, bias may arise because enforcement data does not necessarily represent actual harm. It may represent where regulators inspected, where communities complained, where evidence was easiest to collect or where enforcement agencies had political capacity. If such data becomes training data, the model may reproduce administrative history rather than environmental reality.

Opacity is another central risk. High-stakes legal decisions require reasons that can be understood and challenged. Interpretable models are especially important where a decision affects liberty, penalties, corporate liability or community restoration [14]. Algorithmic accountability scholarship therefore emphasises documentation, auditability and procedures that allow legal actors to test whether a system complies with legal norms [15].

Automation bias is also significant. Even where a system is advisory, judges or regulators may give excessive weight to its output because it appears scientific or neutral. This can narrow judicial discretion and shift responsibility away from the human decision-maker. In environmental cases, the risk is particularly serious because ecological damage, community vulnerability and cumulative exposure cannot always be expressed accurately through simplified numerical scores.

Table 2. Risk typology for automated sentencing models in environmental justice

Risk category	How it may arise	Legal or environmental justice concern	Minimum safeguard
---------------	------------------	--	-------------------

Risk category	How it may arise	Legal or environmental justice concern	Minimum safeguard
Historical enforcement bias	Training data reflects unequal inspections, complaints or prosecutions.	Past inequality is converted into future sentencing guidance.	Pre-deployment data audit and environmental justice impact assessment.
Proxy discrimination	Variables such as location, land use, income or industry type indirectly represent protected or vulnerable status.	Neutral variables may reproduce social disadvantage.	Proxy review and fairness testing before use.
Opacity	The model gives a score without legally meaningful explanation.	Affected parties cannot challenge the basis of the recommendation.	Interpretable design and reason-giving requirements.
Automation bias	Judges or regulators over-rely on the algorithmic recommendation.	Judicial discretion and individualised sentencing are weakened.	Mandatory human review with reasons for reliance or departure.
Privacy and surveillance	Personal, geospatial, health or community data is used without adequate limits.	Vulnerable communities may be exposed to intrusive monitoring.	Data minimisation, security and lawful processing standards.
Accountability gap	Developers, vendors, agencies and courts divide responsibility.	No actor is clearly answerable for an unjust recommendation.	Clear institutional responsibility, audit logs and appeal mechanisms.
Loss of environmental context	The model fails to account for cumulative harm, ecological sensitivity or restoration needs.	The sentence may be technically consistent but environmentally unjust.	Community impact evidence and ecological expert review.

Figure 2 shows how risk can travel through the sentencing process if biased data is not controlled at the beginning. It also shows where legal safeguards should interrupt the pathway.

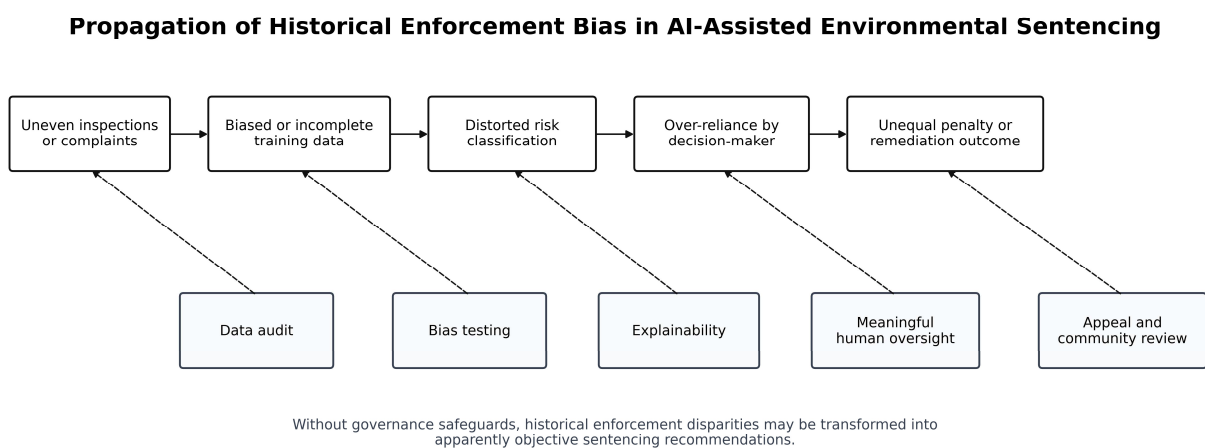


Figure 2. Risk transmission pathway from unequal enforcement data to unequal sentencing outcomes.

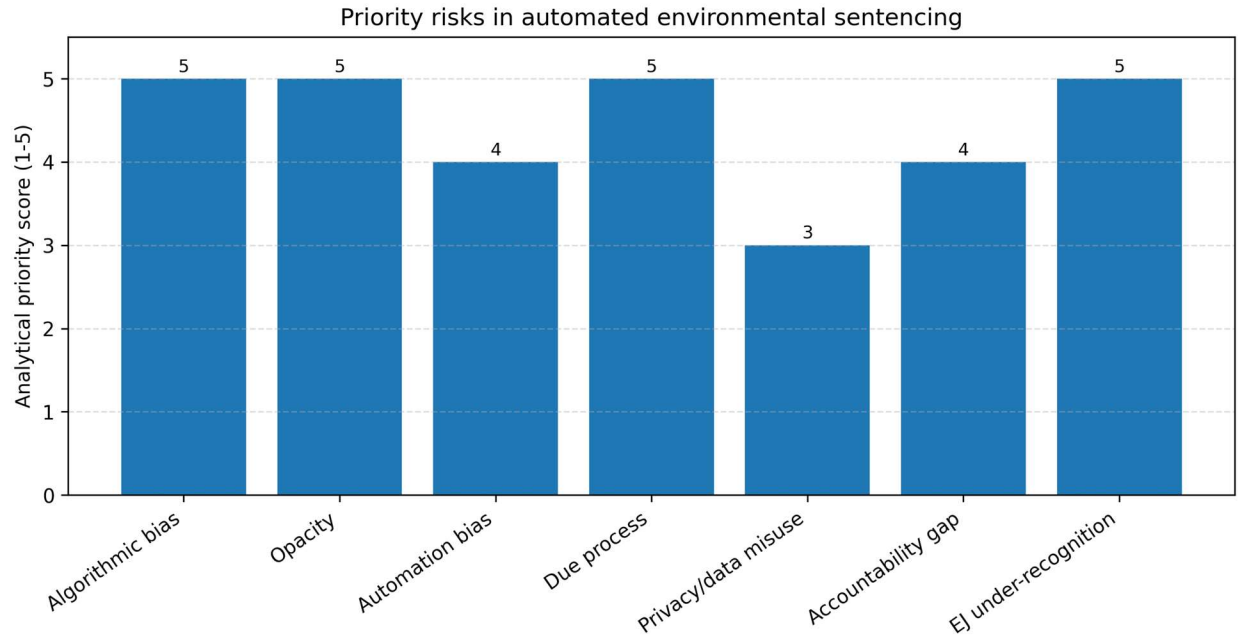


Figure 3. Priority risks in automated environmental sentencing. The scores are qualitative legal-risk scores, not empirical measurements.

3.3 Transparency, Due Process and Data Protection

The third analytical finding is that transparency and due process are not merely ethical preferences; they are legal requirements. The General Data Protection Regulation is relevant because Article 22 restricts decisions based solely on automated processing where those decisions produce legal or similarly significant effects, subject to limited exceptions and safeguards [16]. Sentencing is a legal effect in the strongest sense. Even where a model is advisory, the parties must understand whether and how the algorithm influenced the decision.

The European Union Artificial Intelligence Act provides the most detailed binding AI governance model among the frameworks reviewed. It classifies certain AI systems used by judicial authorities, or on their behalf, to assist in researching, interpreting or applying law to facts as high-risk systems [17]. This is important for environmental sentencing because any tool used to assist a court in applying sentencing law to environmental facts should be subject to high-risk controls.

International soft-law instruments support the same direction. The OECD AI Principles call for trustworthy AI that respects human rights, democratic values, transparency and accountability [18]. UNESCO's Recommendation on the Ethics of Artificial Intelligence emphasises human dignity, human rights, fairness, sustainability, transparency and human oversight [19]. These standards are not sentencing statutes, but they help define what responsible governance should require.

Technical risk-management frameworks also matter. The NIST Artificial Intelligence Risk Management Framework treats AI risk management as a life-cycle process involving governance, mapping, measurement and management [20]. Canada's Directive on Automated Decision-Making similarly requires public institutions to assess impact and apply measures such as transparency, testing, human intervention and

monitoring according to the level of risk [21]. These approaches are useful because they shift attention from one-time approval to continuing oversight.

Table 3. Comparative regulatory safeguards relevant to AI-assisted legal decision-making

Framework	Legal status	Safeguards most relevant to sentencing	Relevance to environmental justice
GDPR, Article 22 [16]	Binding EU data-protection law	Restriction on solely automated decisions with legal or similarly significant effects; safeguards for human intervention and contestation.	Supports the principle that sentencing cannot be fully automated.
EU Artificial Intelligence Act [17]	Binding EU AI regulation	High-risk classification, risk management, data governance, transparency, human oversight and monitoring.	Provides the strongest model for judicial AI safeguards.
OECD AI Principles [18]	International soft-law standard	Human rights, transparency, robustness, accountability and inclusive benefit.	Supports rights-based and democratic control of AI tools.
UNESCO AI Ethics Recommendation [19]	International ethical standard adopted by UNESCO member states	Human dignity, fairness, sustainability, transparency, oversight and redress.	Connects AI governance with environmental sustainability and vulnerable communities.
NIST AI RMF 1.0 [20]	Voluntary technical risk-management framework	Govern, map, measure and manage AI risks across the system life cycle.	Useful for audits, validation and post-deployment monitoring.
Canada Directive on Automated Decision-Making [21]	Binding federal policy instrument for Canadian government institutions	Algorithmic impact assessment, notice, testing, human intervention and monitoring based on impact level.	Useful model for public-sector deployment controls.

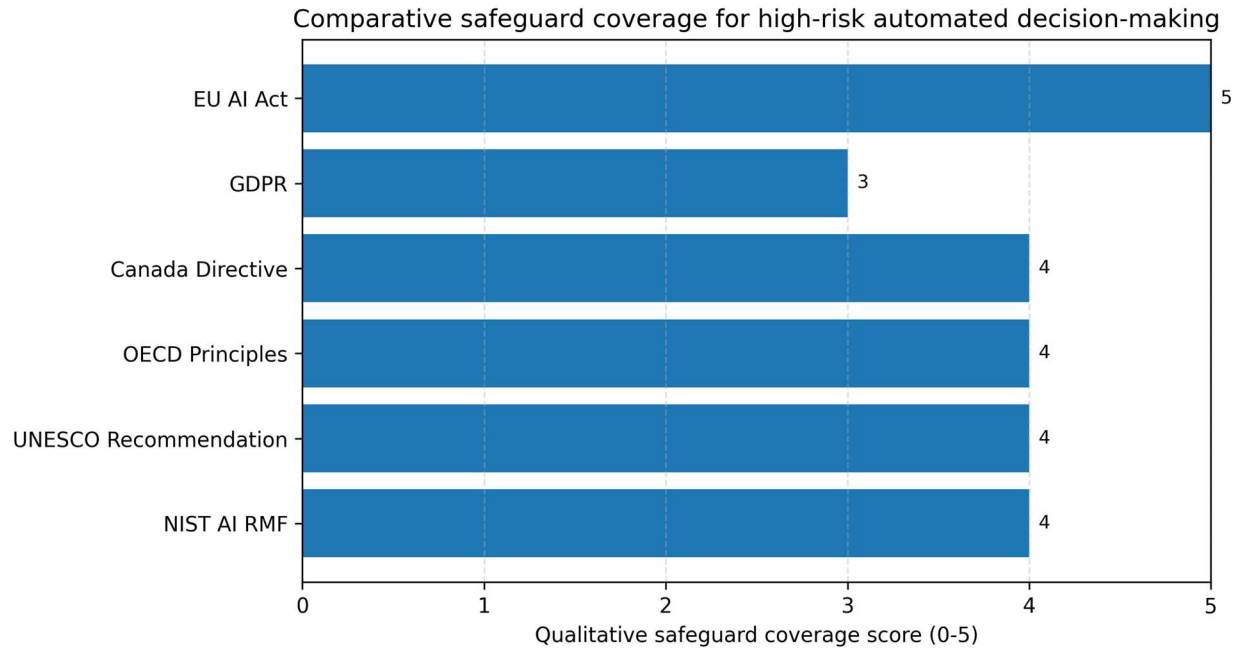


Figure 4. Comparative safeguard coverage for high-risk automated decision-making frameworks. The score is a qualitative mapping of coverage, not a ranking of legal quality.

3.4 Human Rights and Environmental Law Principles

The fourth analytical finding is that automated sentencing must satisfy both human-rights principles and environmental law principles. Article 14 of the International Covenant on Civil and Political Rights protects fair trial guarantees, including equality before courts and the right to a fair and public hearing by a competent, independent and impartial tribunal [22]. If algorithmic evidence or recommendations cannot be meaningfully challenged, those guarantees are weakened.

Environmental justice also requires participation. The Aarhus Convention is significant because it links access to environmental information, public participation in decision-making and access to justice in environmental matters [23]. Although the Convention is regional in legal operation, its structure reflects a broader principle: environmental decisions affecting communities should not be made through inaccessible technical processes.

Indian environmental jurisprudence provides useful substantive principles for environmental sentencing. In *Vellore Citizens Welfare Forum v. Union of India*, the Supreme Court of India recognised the precautionary principle and the polluter-pays principle as essential features of sustainable development [24]. In *M.C. Mehta v. Union of India*, the Court developed the principle of absolute liability for hazardous industries causing harm [25]. These principles show why environmental sentencing must consider prevention, restoration and accountability, not only offender risk.

Privacy principles are also relevant because automated sentencing may use personal, geospatial, financial or community data. In *Justice K.S. Puttaswamy v. Union of India*, the Supreme Court of India recognised privacy as a constitutionally protected right and emphasised legality, legitimate aim and proportionality in restrictions affecting privacy [26]. These principles support strict controls on the collection and use of data in AI-assisted environmental sentencing.

Table 4. Case-law and legal principles relevant to automated environmental sentencing

Authority	Core principle	Application to automated environmental sentencing
State v. Loomis, 881 N.W.2d 749 (Wis. 2016) [5]	Algorithmic risk tools may be used only with caution and must not determine the sentence.	AI output should be advisory, explainable and subject to judicial reasons.
Vellore Citizens Welfare Forum v. Union of India, (1996) 5 SCC 647 [24]	Precautionary principle and polluter-pays principle.	Models must account for prevention, restoration and ecological harm.
M.C. Mehta v. Union of India, AIR 1987 SC 1086 [25]	Absolute liability for hazardous industrial activity.	Corporate environmental harm cannot be treated as ordinary low-risk offending.
Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 [26]	Right to privacy and proportionality.	Data used in AI sentencing must be lawful, necessary and proportionate.
ICCPR, Article 14 [22]	Fair trial and equality before courts.	Affected parties must be able to contest algorithmic inputs and outputs.
Aarhus Convention [23]	Environmental information, participation and access to justice.	Community impact and participation must be part of environmental AI governance.

4. Discussion and Recommendations

The analysis shows that the strongest danger of automated environmental sentencing is not only technical inaccuracy. It is false objectivity. When a recommendation appears numerical and scientific, decision-makers may treat it as more neutral than it really is. Critical work on algorithmic power has shown how mathematical models can magnify inequality when they are opaque, scalable and difficult to challenge [27]. Similar concerns arise in public administration when automated systems profile vulnerable populations and reshape access to public authority [28].

Environmental sentencing is particularly vulnerable to dirty data. If inspection patterns are uneven, if community complaints are under-recorded or if corporate violations are resolved informally, the dataset will not represent the real distribution of environmental harm. Research on predictive policing warns that systems trained on unlawful or biased institutional data can reproduce those defects as prediction [29]. The same logic applies to environmental enforcement data.

Transparency must also be understood carefully. Some scholarship initially argued that data-protection law could support a right to explanation for algorithmic decisions [30]. Other scholars have shown that the GDPR does not create a simple or complete right to explanation and that meaningful accountability requires more than disclosure of a general system description [31]. For sentencing, the practical conclusion is that parties need legally usable explanations: what data was used, what factors influenced the recommendation, what limitations exist and how the judge evaluated the output.

Fairness is not a single technical metric. Machine-learning scholarship shows that fairness definitions can conflict, and the correct choice depends on the social and legal context [32]. In environmental justice, context includes cumulative pollution, ecological sensitivity, community vulnerability, indigenous and local

knowledge, remediation needs and the ability of affected communities to participate. A model that performs well on general accuracy may still be unjust if it ignores these dimensions.

Environmental rule-of-law development also requires institutions that can monitor compliance, enforce remedies and provide access to justice. UNEP's later work on environmental rule of law emphasises that implementation, enforcement and institutional capacity remain central to environmental protection [33]. AI governance must therefore be located within broader institutional reform rather than treated as a purely technical upgrade.

The discussion supports a cautious regulatory position. Automated sentencing models may be useful for organising large case records, identifying similar precedents, checking consistency, flagging repeat violations, estimating remediation needs and supporting judicial reasoning. They should not calculate or impose a sentence. They should not be used where the system is proprietary and unchallengeable, where validation data is unavailable, or where environmental justice impact has not been assessed.

Table 5. Recommended safeguard model for AI-assisted environmental sentencing

Stage	Required safeguard	Purpose
Before deployment	Algorithmic impact assessment and environmental justice impact assessment.	Identify bias, rights risks, ecological blind spots and community impacts before use.
Before deployment	Independent validation using representative environmental enforcement data.	Test accuracy, error rates and differential impact across communities and offender types.
Design stage	Preference for interpretable models in high-stakes sentencing contexts.	Ensure that judges and parties can understand the basis of recommendations.
Judicial use	Mandatory disclosure of model purpose, data categories, limitations and confidence level.	Allow parties to contest the recommendation and protect due process.
Judicial use	Meaningful human oversight with written reasons.	Prevent automation bias and preserve judicial responsibility.
After deployment	Periodic independent audits and publication of transparency reports.	Detect drift, bias, data errors and unintended environmental justice effects.
Governance	Environmental justice review board with legal, scientific, technical and community representation.	Ensure that cumulative harm and community experience are included in oversight.
Remedies	Right to challenge, correction of records and review of affected decisions.	Provide accountability when algorithmic error or bias affects sentencing.

5. Conclusion

Automated sentencing models may appear attractive because environmental offences can involve complex records, technical evidence and repeated regulatory violations. Properly designed tools may assist courts and regulators by organising information, identifying patterns and supporting consistency. However, the use of AI

in environmental sentencing creates serious risks when the system is opaque, biased, untested or treated as authoritative.

This article finds that environmental justice requires more than standard algorithmic accuracy. Sentencing in environmental cases must consider cumulative ecological harm, public health consequences, corporate accountability, remediation, deterrence, community vulnerability and meaningful participation. These factors cannot be safely reduced to an unexplained score.

The legal position should therefore be clear. Automated sentencing models must not replace judicial discretion. They may be used only as subordinate decision-support tools. Their use should be conditional on algorithmic impact assessment, environmental justice review, independent audit, explainability, data-protection safeguards, meaningful human oversight and a right to challenge. Without these safeguards, automated sentencing would risk reinforcing the very inequalities that environmental justice seeks to remedy.

Responsible governance of AI in environmental justice must balance innovation with legality, ecological protection and human dignity. The goal is not to reject technology, but to ensure that technology strengthens the rule of law, protects vulnerable communities and preserves public trust in environmental adjudication.

References

- [1] Pasquale F. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press; 2015.
- [2] Citron DK. Technological Due Process. *Washington University Law Review*. 2008;85(6):1249-1313.
- [3] United States Environmental Protection Agency. *Learn About Environmental Justice*. Washington, DC: U.S. EPA; 2020. Available at: https://19january2021snapshot.epa.gov/environmentaljustice/learn-about-environmental-justice_.html
- [4] United Nations Environment Programme. *Environmental Rule of Law: First Global Report*. Nairobi: UNEP; 2019. Available at: <https://www.unep.org/resources/assessment/environmental-rule-law-first-global-report>
- [5] *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).
- [6] Angwin J, Larson J, Mattu S, Kirchner L. Machine Bias. *ProPublica*. 23 May 2016. Available at: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>
- [7] Russell S, Norvig P. *Artificial Intelligence: A Modern Approach*. 4th ed. Harlow: Pearson; 2021.
- [8] Barocas S, Selbst AD. Big Data's Disparate Impact. *California Law Review*. 2016;104(3):671-732.
- [9] Friedman B, Nissenbaum H. Bias in Computer Systems. *ACM Transactions on Information Systems*. 1996;14(3):330-347.
- [10] Schlosberg D. *Defining Environmental Justice: Theories, Movements, and Nature*. Oxford: Oxford University Press; 2007.
- [11] Bullard RD. *Dumping in Dixie: Race, Class, and Environmental Quality*. 3rd ed. Boulder, CO: Westview Press; 2000.
- [12] Mohai P, Pellow D, Roberts JT. Environmental Justice. *Annual Review of Environment and Resources*. 2009;34:405-430.
- [13] Cole LW, Foster SR. *From the Ground Up: Environmental Racism and the Rise of the Environmental Justice Movement*. New York: New York University Press; 2001.
- [14] Rudin C. Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead. *Nature Machine Intelligence*. 2019;1:206-215.

- [15] Kroll JA, Huey J, Barocas S, Felten EW, Reidenberg JR, Robinson DG, Yu H. Accountable Algorithms. *University of Pennsylvania Law Review*. 2017;165(3):633-705.
- [16] 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). *Official Journal of the European Union*. 2016;L119:1-88.
- [17] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). *Official Journal of the European Union*. 2024.
- [18] Organisation for Economic Co-operation and Development. Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449. Paris: OECD; 2019.
- [19] UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO; 2021.
- [20] National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. Gaithersburg, MD: NIST; 2023.
- [21] Treasury Board of Canada Secretariat. Directive on Automated Decision-Making. Ottawa: Government of Canada; updated 24 June 2025. Available at: <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592>
- [22] United Nations. International Covenant on Civil and Political Rights. Adopted 16 December 1966, entered into force 23 March 1976.
- [23] United Nations Economic Commission for Europe. Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters. Aarhus, Denmark; 25 June 1998.
- [24] *Vellore Citizens Welfare Forum v. Union of India*, (1996) 5 SCC 647.
- [25] *M.C. Mehta v. Union of India*, AIR 1987 SC 1086; (1987) 1 SCC 395.
- [26] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
- [27] O'Neil C. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown; 2016.
- [28] Eubanks V. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press; 2018.
- [29] Richardson R, Schultz JM, Crawford K. Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. *New York University Law Review Online*. 2019;94:192-233.
- [30] Goodman B, Flaxman S. European Union Regulations on Algorithmic Decision-Making and a Right to Explanation. *AI Magazine*. 2017;38(3):50-57.
- [31] Wachter S, Mittelstadt B, Floridi L. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*. 2017;7(2):76-99.
- [32] Barocas S, Hardt M, Narayanan A. *Fairness and Machine Learning: Limitations and Opportunities*. Cambridge, MA: MIT Press; 2023.
- [33] United Nations Environment Programme. *Environmental Rule of Law: Tracking Progress and Charting Future Directions*. Nairobi: UNEP; 2023.