AGORA International Journal of Juridical Sciences, http://univagora.ro/jour/index.php/aijjs
ISSN 1843-570X, E-ISSN 2067-7677
Vol. 19, No. 1 (2025), pp. 87-95

THE JURISPRUDENCE OF ALGORITHMS: RETHINKING LEGAL THEORY IN THE AGE OF AI

D. M. MINGHIRAȘI

Dragos Marius Minghirași
Università degli studi della Campania ”Luigi Vanvitelli”, Italy
https://orcid.org/0009-0003-2639-3180, E-mail: minghirasidragosmarius@yahoo.com

Abstract*: This paper explores the evolving interface between artificial intelligence and legal theory, arguing that the rise of algorithmic governance necessitates a fundamental reassessment of jurisprudence. Through theoretical analysis, case studies, and interdisciplinary literature, the article investigates how AI challenges established doctrines of legal interpretation, procedural fairness, and legal personhood. The paper proposes a framework for understanding the epistemological and normative implications of algorithmic decision-making in legal contexts and offers policy recommendations for a just and transparent integration of AI into the rule of law.*

Keywords: *artificial, intelligence, theories, jurisprudence.*

Introduction

The proliferation of artificial intelligence in public and private decision-making is transforming legal systems worldwide. From risk assessment in criminal justice to predictive policing and automated contract enforcement, AI technologies increasingly influence core legal functions. This development raises profound questions about the future of legal reasoning, the legitimacy of machine-made decisions, and the theoretical foundations of law itself. The purpose of this paper is to analyze how algorithmic logic intersects with traditional legal thought and to propose new ways to conceptualize legal authority in the age of AI.

1. Theoretical Frameworks

To understand how artificial intelligence challenges and reshapes legal theory, it is essential to ground the analysis within established theoretical frameworks that define law’s nature, function, and legitimacy. As Lessig (1999) famously argued, “code is law”—meaning that digital architecture can function as a form of regulation as powerful as legal norms. This challenges traditional distinctions between legal and technical governance (Lessig, 1999). This section explores key jurisprudential perspectives through which the legal implications of AI may be critically examined and reinterpreted.

Legal Positivism vs. Natural Law

Legal positivism posits that law is the product of recognized human authority, while natural law holds that law must align with moral principles. AI disrupts this dichotomy by introducing rule-based systems not grounded in either human will or moral reasoning. The deterministic nature of algorithms echoes the positivist emphasis on rules but lacks the normative dimension central to natural law. Moreover, the opacity of AI decisions challenges the requirement of legal certainty and transparency.

Critical Legal Studies and Posthumanism

Critical legal theorists argue that law often reflects dominant social and economic structures. AI, as a tool created and deployed within these structures, risks reinforcing systemic biases. Posthumanist approaches further complicate this picture by questioning the centrality of the human subject in law, suggesting that AI may function as a legal actor in hybrid systems of governance.

Legal Realism and Predictive Analytics

Legal realists emphasize the role of judges' discretion and social context in decision-making. AI's reliance on data-driven prediction runs counter to this view, favoring past patterns over contextual nuance. The tension between statistical inference and human judgment raises new questions about fairness, especially in areas like bail decisions and parole.

Procedural Justice and Due Process

AI systems challenge traditional notions of due process. The lack of explainability in algorithmic decisions undermines procedural fairness (Pasquale, 2015), particularly the right to understand and contest decisions. Rawlsian and Habermasian theories emphasize transparency and reason-giving, both of which are at risk in black-box models.

2. Legal Case Studies and Domains

2.1.COMPAS and Risk Assessment Tools

Used in U.S. criminal justice to assess recidivism risk, COMPAS has been criticized for racial bias and lack of transparency. The *Loomis v. Wisconsin* case exemplifies the legal challenges of relying on opaque algorithms in sentencing. The Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) is one of the most widely used risk assessment tools in the United States criminal justice system. Developed by the private company Northpointe (now Equivant), COMPAS is designed to assist judges, parole officers, and other legal actors in evaluating the likelihood that a defendant will reoffend, or fail to appear in court. It does this through a proprietary algorithm that processes up to 137 factors, including criminal history, socio-demographic data, and responses to questionnaires.

One of the most significant controversies surrounding COMPAS is its opacity. Because the algorithm is proprietary, its internal logic is not publicly available—even to the courts that rely on it. This has led to criticism that defendants and their attorneys are unable to contest or understand the basis on which risk scores are assigned. From a rule of law perspective, this raises profound concerns about due process, the right to a fair trial, and the ability to challenge evidence used in sentencing. The "black box" nature of such tools violates core principles of legal reasoning: transparency, justification, and accountability. Legal decisions, especially those involving deprivation of liberty, must be based on reasons that are comprehensible and open to scrutiny. Algorithmic opacity fundamentally disrupts this norm.

In 2016, ProPublica conducted an influential investigation into COMPAS that found the tool exhibited racial bias: African-American defendants were more likely to be falsely labeled high risk, while white defendants were more often rated low risk despite reoffending. While Northpointe disputed the findings, arguing that the tool was “equally accurate” across races, the study sparked a widespread debate about fairness, bias, and algorithmic accountability.

These findings illuminate a key issue in AI and law: algorithms trained on historical data can inherit and perpetuate systemic discrimination. When the input data reflects societal inequalities, the algorithm may encode and reproduce those patterns, reinforcing the very disparities the legal system is supposed to combat.

In *State v. Loomis* (2016), the Wisconsin Supreme Court considered whether the use of COMPAS in sentencing violated due process. Eric Loomis was sentenced in part based on a COMPAS risk score, which he argued denied him the ability to challenge the accuracy of the assessment due to the tool's proprietary nature. The court upheld the use of COMPAS, but acknowledged serious concerns. It ruled that COMPAS could be used only as one factor among many, and courts must include warnings about its limitations, especially its lack of transparency and potential bias.

While the court stopped short of declaring COMPAS unconstitutional, the decision underscores the tension between technological efficiency and constitutional safeguards. It also shows how legal systems are struggling to adapt to AI-based tools within the constraints of existing legal doctrines. The COMPAS case challenges foundational assumptions in legal theory about individual responsibility, equality before the law, and the nature of adjudication. It raises difficult questions such as:

- Can justice be individualized when it is partially determined by statistical generalizations?
- Should a defendant's sentence be influenced by factors beyond their control (e.g., demographics)?
- How can legal actors verify the fairness of decisions they cannot fully understand?

The integration of AI tools like COMPAS into legal systems signals a shift from normative, human-centered judgment to probabilistic, data-driven decision-making. This evolution calls for new theoretical frameworks that can reconcile algorithmic reasoning with legal values such as due process, dignity, and equality.

2.2.GDPR and the Right to Explanation

Article 22 of the GDPR gives individuals the right not to be subject to automated decisions without meaningful human intervention. This provision reflects European legal culture's emphasis on individual rights and accountability. The General Data Protection Regulation (GDPR), which came into effect in 2018, is widely regarded as one of the most ambitious and comprehensive data protection frameworks in the world. Among its various innovations, Article 22 addresses the growing role of automated decision-making, including profiling, in areas that significantly affect individuals. It asserts a key principle: individuals have the right not to be subject to decisions based solely on automated processing, including profiling, if those decisions produce legal effects or similarly significant impacts.

Article 22(1) of the GDPR reflects a deep-rooted European legal tradition that values dignity, autonomy, and individual agency. It presupposes that decisions affecting people in serious ways—such as loan approvals, hiring, policing, or access to public services—should not be made in a way that precludes human judgment. It aims to safeguard fundamental rights, including the right to fair treatment, non-discrimination, and effective remedies.

One of the most discussed and controversial aspects of Article 22 is whether it creates a "right to explanation" for individuals subjected to algorithmic decisions. While the text itself

does not explicitly use that phrase, Recital 71 of the GDPR suggests that data subjects should have the right to obtain an explanation of the decision reached after such assessment. Legal scholars have debated whether this amounts to a legally binding right or a more aspirational principle. For instance, Wachter, Mittelstadt, and Floridi (2017) argue that the GDPR does not establish a robust right to explanation in its current form, particularly given the ambiguous language and lack of enforcement mechanisms. Others, such as Selbst and Powles, contend that a de facto right exists when Article 22 is read in conjunction with Articles 13–15, which require transparency about automated decision-making logic.

Regardless of its precise legal weight, the notion of a right to explanation has powerful normative implications. It embodies the demand for algorithmic transparency and accountability, challenging the dominance of opaque AI systems (often referred to as "black boxes") in decision-making processes. In legal contexts, the ability to contest decisions and understand their rationale is fundamental to procedural fairness and effective remedy, enshrined in Article 47 of the EU Charter of Fundamental Rights.

Despite its normative appeal, enforcing the right to explanation faces practical and technical obstacles. AI systems, especially those based on machine learning, often operate through complex statistical correlations rather than clear logical rules. Providing a meaningful explanation of such systems' outputs—especially in non-technical terms comprehensible to laypeople—is a nontrivial task. Furthermore, commercial secrecy and intellectual property protections are frequently cited by companies as reasons for withholding detailed algorithmic disclosures. This creates a tension between data subjects' rights and business interests, a challenge yet to be fully resolved in regulatory practice (Cohen, 2019).

In contrast to the EU's precautionary and rights-based approach, jurisdictions like the United States have so far adopted a more laissez-faire model, placing greater emphasis on innovation and market regulation than on individual rights. However, even in the U.S., recent legal developments—such as the AI Bill of Rights (2022) and the Algorithmic Accountability Act—reflect growing concern about the unchecked deployment of AI systems. The evolving jurisprudence in Europe suggests that AI regulation will increasingly pivot around the principles articulated in GDPR, especially transparency, fairness, and accountability. Future EU legislation, such as the AI Act, is expected to reinforce these safeguards, potentially operationalizing the right to explanation more clearly and mandating ex-ante risk assessments**,** post-hoc audits, and human-in-the-loop protocols for high-risk systems.

2.3.SyRI Case in the Netherlands

The Dutch court struck down SyRI, a welfare fraud detection system, due to its invasive data collection and lack of transparency. The case underscores the importance of proportionality and necessity in algorithmic governance. The SyRI (Systeem Risico Indicatie) case represents a pivotal moment in European jurisprudence regarding automated decision-making**,** algorithmic surveillance, and fundamental rights. The 2020 ruling by the District Court of The Hague marked one of the first instances in which a national court invalidated a state-run AI surveillance system for violating constitutional and international human rights norms.

SyRI was developed by the Dutch Ministry of Social Affairs and Employment as a tool to combat welfare fraud and benefit misuse. The system aggregated data from multiple

government agencies—such as tax authorities, housing registries, education institutions, and employment databases—to construct risk profiles of individuals and neighborhoods deemed susceptible to fraud. These profiles were generated through a proprietary, opaque algorithm and transmitted to local authorities for further investigation, often triggering social service audits or benefit reviews.

Importantly, the exact criteria and logic used in risk scoring were not disclosed to the public or even fully to oversight bodies, leading to concerns about the black-box nature of the system. Furthermore, the targeted neighborhoods were often low-income and immigrant-dense, raising additional concerns regarding discrimination and stigmatization. A coalition of civil society organizations, including the Dutch section of the Public Interest Litigation Project (PILP), brought a case against the Dutch government, arguing that SyRI violated several fundamental rights, including: the right to private life under Article 8 of the European Convention on Human Rights (ECHR); the principles of transparency, proportionality, and necessity; the prohibition of discrimination, implicitly raised through the disproportionate impact on vulnerable communities.

The plaintiffs asserted that the indiscriminate data aggregation**,** lack of algorithmic transparency, and absence of effective redress mechanisms constituted a violation of data protection norms as enshrined in both the GDPR and the Dutch Constitution. In a landmark decision delivered on February 5, 2020, the District Court of The Hague ruled that the SyRI legislation was incompatible with Article 8 ECHR, which guarantees the right to respect for private and family life. The court concluded that SyRI failed the test of proportionality and necessity, core principles under Article 8 ECHR, and struck down the law that formed its legal basis. The SyRI case has wide-ranging implications for the jurisprudence of algorithmic governance. It signals a growing judicial willingness to scrutinize state use of AI, particularly where opacity**,** data aggregation, and automated decision-making intersect with fundamental rights. Moreover, it offers a concrete illustration of how European courts are integrating human rights frameworks into digital and algorithmic contexts, moving beyond traditional privacy law to encompass procedural and distributive justice (Manolescu, 2016).

The SyRI decision contrasts sharply with approaches in other jurisdictions, particularly the United States, where algorithmic systems are often insulated from judicial scrutiny by doctrines of proprietary secrecy, standing, and executive deference. The Dutch ruling demonstrates that human rights law, especially as interpreted by European courts, provides a more expansive and protective framework for algorithmic accountability. It also contributes to the emerging body of European jurisprudence that includes Digital Rights Ireland, Schrems I and II, and La Quadrature du Net, all of which reflect increasing skepticism toward large-scale data processing that lacks adequate individual safeguards.

2.4.AI Judges in Estonia and China

Estonia and China have piloted AI systems for resolving small claims. While efficient, these systems raise concerns about dehumanization and the erosion of deliberative justice. The advent of automated judicial systems in countries like Estonia and China reflects a significant shift in how legal institutions conceptualize the role of technology in dispute resolution. These initiatives illustrate a broader global trend toward the digitization and automation of legal processes, particularly in the domain of low-value, high-volume cases. However, these

developments raise critical concerns about the limits of algorithmic reasoning, due process, and the risk of dehumanizing justice.

Estonia, long known for its advanced digital infrastructure and e-governance, announced in 2019 its intention to develop an AI-based judge for resolving small claims disputes, typically involving amounts below €7,000. The initiative, spearheaded by the Estonian Ministry of Justice and the government's Chief Data Officer Ott Velsberg, aimed to increase efficiency and reduce judicial backlog. The Estonian AI judge was not meant to fully replace human magistrates but to handle preliminary stages of litigation, such as evaluating documentation, verifying procedural compliance, and issuing decisions in uncontested or minor cases. The process allowed parties to appeal to a human judge, thereby preserving a layer of oversight.

In essence, while Estonia's experiment is rooted in democratic oversight and voluntary usage, it exemplifies the delicate balance between technological pragmatism and preserving the human touch in legal decision-making. China represents a more expansive and integrated use of AI in judicial systems, underpinned by its strategy of Smart Courts. The Supreme People's Court of China has promoted the integration of AI, big data, and blockchain into court procedures to modernize the legal system and improve adjudication efficiency.

In several provinces, AI-based systems have been deployed to assist judges in drafting decisions, predict case outcomes, and in some instances, deliver rulings in automated online courts. For example, Hangzhou's Internet Court has experimented with AI judges that interact via digital avatars to guide proceedings, assess evidence, and in streamlined processes, even render final decisions in routine civil or administrative matters, especially in e-commerce disputes. While Chinese AI courts report impressive efficiencies—some boasting resolution times of under 30 minutes—critics argue that these gains come at the cost of due process**,** deliberation, and access to meaningful appeal mechanisms.

The implementation of AI judges in both Estonia and China raises pressing theoretical and normative issues. Central among them is the tension between efficiency and justice. While automation may enhance procedural throughput, it risks compromising:

- Deliberative reasoning: The human judge is not merely a calculator of norms but an interpreter of lived realities, equipped to weigh evidence and circumstances that may not be easily quantified.
- Judicial empathy and moral reasoning: Emotions, ethical intuitions, and discretionary judgment remain essential to fair outcomes, especially in civil law contexts.
- Public legitimacy: Automated judgments, particularly if opaque or perceived as arbitrary, may undermine trust in judicial institutions, which derive their authority not only from outcomes but also from process.

From a jurisprudential standpoint, these developments invite reflection on Lon Fuller's "inner morality of law," Dworkin's theory of law as integrity, and Habermasian proceduralism, all of which emphasize that justice cannot be fully reduced to rule-application but requires discursive justification and human engagement.

Comparative Reflections

Yeung (2018) introduces the concept of "algorithmic regulation" as a new modality of power operating through predictive analytics. Such mechanisms reconfigure the role of law by embedding behavioral incentives into digital systems (Yeung, 2018).

- Estonia's model emphasizes augmentation, transparency, and appealability, aligning with liberal-democratic values and procedural fairness.
- China's model, by contrast, prioritizes instrumental efficiency and centralized control, embedded in a surveillance-capable legal infrastructure, raising alarms about algorithmic authoritarianism.

Together, these examples demonstrate that the technological design and legal-cultural context are inseparable in shaping how AI tools affect justice. They also highlight the need for international normative frameworks to guide, constrain, and harmonize the development of automated judicial systems.

3. Major challenges in the intersection between artificial intelligence and law

3.1.Opacity and Accountability

One of the most pressing challenges in the application of artificial intelligence to legal systems is the inherent opacity of many machine learning models, particularly those utilizing deep neural networks. These systems are often described as "black boxes" due to the difficulty—even for their developers—of explaining precisely how they reach particular outputs. This lack of transparency undermines legal accountability, a cornerstone of any just system.

Traditional legal reasoning demands that decisions be traceable, reviewable, and justified. In contrast, algorithmic decisions may lack clear explanations, making it difficult for affected parties to contest outcomes, for courts to review legality, or for institutions to assign liability in case of error or harm. This creates a structural tension between technological opacity and the rule of law's demand for reason-giving and procedural fairness.

Moreover, questions arise about shared or diffused responsibility. If a harmful decision results from a combination of data bias, model training, and institutional misuse, who is legally and morally responsible? The software developer? The deploying institution? The programmer? These are open questions at the heart of emerging AI governance frameworks.

3.2.Bias and Discrimination

Bias in AI systems is not merely a technical flaw—it is a systemic legal and ethical concern. Calo (2017) outlines key policy dilemmas in AI regulation, including fairness, autonomy, and institutional oversight. Algorithms trained on historical legal data may unintentionally replicate and reinforce structural inequalities that exist in society. For example, if past policing or sentencing data reflect racial disparities, an algorithm built on such data is likely to amplify those biases, resulting in discriminatory outcomes cloaked in the guise of objectivity.

The growing use of predictive tools, without robust ethical oversight, risks entrenching systemic harms (Calo, 2017). High-profile examples, such as the COMPAS algorithm used in the U.S. criminal justice system, have demonstrated how algorithmic decision-making can produce disparate impacts even when race or gender is not an explicit variable. Such cases raise constitutional and human rights questions, particularly regarding equal protection, due process, and non-discrimination principles.

To mitigate these risks, legal scholars and data scientists are advocating for bias audits**,** fairness metrics, and inclusive design processes. However, the deeper challenge remains: can algorithms trained on inherently biased social data ever truly be neutral? And how should legal systems weigh algorithmic efficiency against normative values of justice?

3.3.Autonomy and Legal Personhood

The rapid development of advanced AI systems also raises fundamental questions about agency, responsibility, and legal personality. As AI systems perform increasingly complex tasks—such as negotiating contracts, making legal recommendations, or resolving disputes—some scholars and policy makers have asked whether such entities might eventually require a form of legal personhood.

However, granting legal personhood to AI would disrupt traditional concepts of moral agency, intention, and liability, which are deeply embedded in legal theory. Current legal frameworks are built around the idea that only humans or human-created institutions (like corporations) can hold rights and obligations. AI, by contrast, is an artefact with no consciousness, no will, and no capacity for moral judgment.

Yet, the issue is not purely speculative. In the European Parliament's 2017 proposal on "Civil Law Rules on Robotics," lawmakers considered the notion of electronic personality for the most advanced autonomous systems. While not adopted, the idea sparked intense debate. Critics argue that creating such a legal category risks absolving human actors of responsibility, while proponents claim it could fill accountability gaps when damages are caused by systems that act unpredictably.

The broader theoretical implication is that the presence of autonomous systems in legal processes forces a reconsideration of foundational legal concepts, including autonomy, intention, and culpability.

3.4.Legitimacy and Public Trust

Perhaps the most vital long-term determinant of AI's role in law is its perceived legitimacy. In any democratic society, laws are not obeyed merely because they are enforced—they are followed because they are seen as legitimate: created through fair processes, applied equally, and open to contestation. The introduction of AI into legal processes disrupts these expectations, especially when the decision-maker is non-human, opaque, or unaccountable.

Trust is fragile. It can be eroded by a single unjust outcome, particularly if the process that produced it appears arbitrary or inaccessible. AI's technical nature, combined with its often bureaucratic implementation, risks creating a perception of dehumanized justice, where individuals feel alienated rather than heard. To preserve legitimacy, human oversight must be preserved, especially in high-stakes decisions. Legal systems must incorporate meaningful explanation rights, accessible appeal mechanisms, and clear lines of responsibility. Public education also plays a role: citizens must understand not only what AI is doing in legal contexts, but why it is being used and how their rights are protected.

In this sense, legitimacy is not just a policy outcome—it is a cultural and institutional project. Lawmakers, judges, technologists, and civil society must work together to shape a model of algorithmic justice that aligns with core democratic values.

Conclusions

The integration of AI into legal systems compels a reexamination of foundational legal principles. Jurisprudence must evolve to address the normative and epistemological challenges posed by algorithmic governance. This paper has proposed a multidisciplinary framework for understanding these changes and has highlighted the need for transparent, accountable, and human-centered legal technologies. Only by reconciling legal tradition with technological innovation can we ensure that AI serves the rule of law rather than subverts it.

REFERENCES

1. Calo, R. (2017). *Artificial Intelligence Policy: A Primer and Roadmap*. UC Davis Law Review, 51(2), 399–435.
2. Cohen, J. E. (2019). *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford University Press.
3. Lessig, L. (1999). *Code and Other Laws of Cyberspace*. Basic Books.
4. Manolescu A.A.(2016), *Protecting human rights in a globalized world. A European perspective,* Agora International Journal of Juridical Sciences, vol. 10, nr.1, Agora University Press, ISSN 1843-570x
5. Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press.
6. Yeung, K. (2018). Algorithmic Regulation: A Critical Interrogation. *Regulation & Governance*, 12(4), 505–523.