

**THE ITALIAN LAW 132/2025:
AN 'ORDINARY' INSTRUMENT TO GOVERN THE 'EXTRAORDINARY'**

Serena Quattrocchio

(Full Professor of Criminal Procedure – University of Turin)¹

Law 132/2025, published in the Official Journal on 25 September 2025, aims to adapt the domestic legal system to the progressive—though not yet complete—entry into force of Regulation (EU) 2024/1689 on artificial intelligence. The statute has a general scope and is examined, in this and in the following contribution, from the specific perspective of criminal justice, both procedural and substantive. The complexity of the AI Act and the high number of delegations conferred upon the Government do not yet allow a comprehensive view of the overall framework; however, some fundamental guidelines may already be identified.

Artificial Intelligence; criminal Justice; 132/2025

Summary: 1. The Regulatory Framework. – 2. The Structure of the Law. – 3. Interrelations with Criminal Justice. – 4. Artificial Intelligence and Judicial Activity. – 4.1. Exclusion—but Not Complete—of Certain Doubts. – 5. Artificial Intelligence and the Organisation of Justice. – 6. Delegation Concerning the Training of Artificial Intelligence Systems. – 7. Delegation to Regulate the Use of AI in Police Functions. – 7.1. Delegations Concerning Preliminary Investigations and Related Adjustments. – Conclusive Remarks.

1. Adopted without particular political emphasis and through a legislative process that did not appear to generate significant public debate, Law No. 132/2025² represents the first comprehensive parliamentary intervention aimed at establishing principles, regulatory standards, and delegated legislative powers concerning the future governance of artificial intelligence in Italy.

This initiative must be understood within the broader and well-established trajectory of the European Union, which for over a decade has sought to position itself as a central regulatory actor in the field of artificial intelligence. Unlike other global

¹ This study complements the research of *2023-IT-NET₄FEU New European Tools for the Financial interests of the EU*, GA 101140609 2023-IT-NET₄FEU.

² Submitted to the Senate (S-1146), in Spring 2024, reached the other Chamber (C-2316) last summer, to be finally approved by the Senate (S-1146 B) in Fall 2025.

contexts—where the development of AI technologies has largely remained in the hands of powerful multinational digital corporations possessing unparalleled economic and computational resources—the European approach has been characterized by an explicit institutional ambition to shape the normative environment within which AI evolves.

Beginning with early soft law instruments on robotics and algorithmic systems in 2016, the European Commission progressively articulated a dual strategy. On the one hand, it sought to anticipate and mitigate the risks associated with automated decision-making, data-intensive technologies, and large-scale algorithmic systems. On the other hand, it aimed to promote innovation and competitiveness within the internal market, positioning AI as a driver of socio-economic development for European citizens and enterprises alike.

Central to this trajectory was the recognition that artificial intelligence presents not merely technological challenges, but structural transformations affecting the protection of fundamental rights. The regulatory process culminated in the adoption of Regulation (EU) 2024/1689—the so-called AI Act—which now constitutes the primary normative framework governing AI within the Union.

The legal basis chosen for the Regulation—Articles 114 and 16 TFEU, concerning the establishment and functioning of the internal market and data protection—has not been free from criticism³. Scholars have observed that grounding such a far-reaching instrument in internal market provisions risks underestimating its profound constitutional implications. Artificial intelligence systems increasingly affect individual autonomy, equality, procedural fairness, and democratic accountability. The risk profile extends far beyond consumer protection or market harmonization and includes forms of mass surveillance, automated profiling, and decision-making processes capable of directly shaping individuals' legal positions.

It is therefore no coincidence that commentators have emphasized the ethical and normative discontinuity introduced by AI technologies. As Luciano Floridi noted, artificial intelligence «*exacerbates old ethical problems, reshapes some of them, and creates new ones*»⁴. The Regulation's architecture—structured around a risk-based approach and differentiated obligations—reflects an attempt to reconcile innovation with rights

³ U. Pagallo, *The Politics of Data in EU Law: Will It Succeed?*, in *Digital Society*, 2022, spec. 4 ff.

⁴ L. Floridi, *The Ethics of Artificial Intelligence: exacerbated problems, renewed problems, unprecedented problems*, in *American Philosophical Quarterly*, 2024, 61(4), 301

protection, yet it inevitably leaves open interpretative tensions that national legislators must confront.

In this context, Law 132/2025 performs a coordinating and complementary function. Although EU regulations are directly applicable and do not require formal transposition, domestic intervention remains necessary to ensure institutional alignment, allocate competences among national authorities, and regulate aspects falling outside the strict scope of the Regulation. In doing so, however, the Italian legislature inevitably intersects with sectors—such as criminal justice—that the AI Act touches only indirectly but whose constitutional sensitivity is particularly acute.

The choice to analyze the law from the perspective of criminal justice is therefore not incidental. Criminal proceedings represent a paradigmatic site where algorithmic systems may affect liberty, equality of arms, evidentiary standards, and judicial independence. Even where the AI Act does not explicitly target criminal adjudication, its conceptual framework and normative categories inevitably influence this domain. In particular, this text (and its implementation, by the Government), will set the boundaries for using AI as an investigative instrument, not only for the detection of crime risk but, theoretically, for any kind of solution used by LEAs in investigations (see para. 7). This may turn to be extremely relevant in the overlapping of national and European Public Prosecutor Office inquiries into PIF crimes.

2. Law 132/2025 combines directly operative provisions with a significant number of delegating clauses empowering the Government to adopt subsequent legislative decrees. This structural feature renders the statute programmatic in part: its full normative impact will depend on future implementing measures⁵.

Article 1 defines the general objectives of the law. It promotes the “proper, transparent, and responsible use” of artificial intelligence, explicitly framing such use within an anthropocentric paradigm. This formulation echoes the vocabulary of the AI Act and earlier European ethical guidelines, emphasizing that AI systems must remain subordinate to human agency and oversight.

⁵ B. Galgani, *La L. n. 132/2025: “testata d’angolo” o “pietra di inciampo” nella definizione dei rapporti tra amministrazione della giustizia (penale) e intelligenza artificiale?*, in *Dir. Pen. Proc.*, 2025, 1445; V. Vasta, *Diritto dell’Unione europea e intelligenza artificiale. Riflessi sul procedimento penale*, in *questa Rivista*, 2024, 271 ss.; M. Torre, *Il Regolamento europeo sull’intelligenza artificiale: i profili processuali*, in *Proc. Pen. Giust.*, 2024, 6 ss.; C. Teresi, *L’AI Act nell’ottica del processual-penalista: uno sguardo preliminare*, in *Pen. Dir. Proc.*, 20 giugno 2024.

The anthropocentric principle performs both symbolic and substantive functions. Symbolically, it reaffirms that technological innovation cannot displace human accountability. Substantively, it requires that AI systems be designed and deployed in ways that preserve human decision-making authority, prevent harm, and ensure traceability and explainability.

Article 3 articulates foundational principles governing AI deployment: transparency, correctness, accountability, and proportionality. These principles resonate with existing European instruments, including Directive 2016/680 on data protection in criminal matters and the CEPEJ Ethical Charter on the use of AI in judicial systems. The emphasis on transparency, however, must be carefully distinguished from explainability. While transparency concerns access to information regarding system functioning, explainability entails the capacity to provide meaningful reasons capable of being scrutinized within legal proceedings⁶. The distinction is particularly relevant in criminal contexts, where the right to challenge evidence and reasoning is constitutionally protected.

Notably, the law does not explicitly reference the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, despite clear conceptual affinities⁷. This omission underscores the fragmented yet overlapping landscape of European AI governance.

From a structural standpoint, the law operates along three principal axes:

1. Regulation of AI use in professional and public administration contexts;
2. Specific provisions concerning judicial activity and the organization of justice;
3. Broad delegations empowering the Government to regulate sensitive sectors, including law enforcement and criminal investigations.

⁶ v. U. Pagallo, *Algoritmi e conoscibilità*, in *Rivista di Filosofia del Diritto*, 2020, 93 ss.; see recently, D.E. Mathew et alii, *Recent Emerging Techniques in Explainable Artificial Intelligence to Enhance the Interpretable and Understanding of AI Models for Human*, in *Neural Processing Letters*, 2025, Vol. 57, art. n. 16.

⁷ Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CM(2024)52-final). In particular, art. 1 co. 2: «Each Party shall adopt or maintain appropriate legislative, administrative or other measures to give effect to the provisions set out in this Convention. These measures shall be graduated and differentiated as may be necessary in view of the severity and probability of the occurrence of adverse impacts on human rights, democracy and the rule of law throughout the lifecycle of artificial intelligence systems. This may include specific or horizontal measures that apply irrespective of the type of technology used». See A. Sirotti Gaudenzi, *Convenzione del Consiglio d'Europa. Spazio allo strumento dei trattati*, in *Guida al Diritto. Dossier 4/2024*, ed. on line.

The presence of numerous delegations significantly amplifies the transformative potential of the statute. While the directly applicable provisions appear moderate and carefully framed, the delegated legislative powers—particularly those concerning police functions and preliminary investigations—open the door to substantial modifications of both substantive and procedural criminal law.

This dual character—formally cautious yet structurally expansive—renders Law 132/2025 a normatively complex instrument. On its face, it presents itself as a technical coordination measure aligned with the AI Act. Beneath this surface, however, it establishes the legal infrastructure for potentially far-reaching institutional change.

3. Although Law 132/2025 is not formally conceived as a criminal statute, several of its provisions directly or indirectly intersect with the administration of criminal justice. These intersections reveal the depth of the structural transformation potentially triggered by the introduction of AI systems into legal processes.

Article 13 addresses the use of artificial intelligence within the context of regulated professions, including legal practice. It requires professionals to inform clients clearly and comprehensively whenever AI tools are employed in the provision of services. At first glance, this obligation appears consistent with existing duties of loyalty, transparency, and informed consent. However, its practical implications are far from straightforward⁸.

Legal professionals often lack the technical expertise necessary to fully understand the functioning of advanced algorithmic systems, especially large-scale machine learning models. The requirement to provide “clear and comprehensive” information may therefore prove difficult to operationalize. Moreover, the provision does not specify sanctions or procedural consequences in the event of non-compliance. The absence of an enforcement mechanism risks transforming what could be a meaningful safeguard into a largely declaratory principle.

More significant are the provisions concerning public administration. Article 14 promotes the adoption of AI systems to enhance administrative efficiency, reduce procedural delays, and improve service quality. These objectives resonate strongly within the justice system⁹, where chronic backlog and resource constraints have long been structural concerns.

⁸ B. GALGANI, *La L. 132/2025*, cit., 1452.

⁹ As to the approach by the Italian Consiglio di Stato, Supreme Court of Administrative Justice, G.

At the same time, the law reiterates the centrality of the human decision-maker. Even when AI systems are employed, responsibility remains exclusively attributed to the public official. This formal reaffirmation of human accountability is normatively reassuring but raises complex issues of practical allocation of responsibility. When decisions are shaped—whether explicitly or implicitly—by algorithmic outputs, the distinction between human judgment and technological influence becomes less clear. The attribution of exclusive responsibility to officials may not satisfy the standard of fairness, though, as the decision to select one system instead of another is not in the hands of individuals, rather of the public administration.

The tension between efficiency and accountability is particularly acute in criminal justice. Criminal proceedings are not merely administrative processes; they are constitutional arenas in which individual liberty, equality of arms, and procedural fairness are directly at stake. The introduction of AI into this domain must therefore be assessed not only in terms of functional optimization, but in light of the structural guarantees embedded in due process.

4. Article 15 constitutes the normative core of the statute with respect to criminal justice. It addresses the use of artificial intelligence in judicial activity and attempts to draw a clear boundary between permissible technological support and impermissible delegation of decisional authority.

The provision affirms that the interpretation of the law, the assessment of facts, the evaluation of evidence, and the adoption of judicial decisions remain the exclusive prerogative of the magistrate. Artificial intelligence systems may be used solely as decision-support tools. In other words, AI may assist but never replace the human judge.

This distinction reflects widespread concern regarding automated adjudication. Fully automated decision-making in criminal matters would raise profound constitutional objections, not least because criminal punishment expresses collective

Avanzini, *Intelligenza artificiale, machine learning e istruttoria procedimentale: vantaggi, limiti ed esigenze di una specifica data governance*, in A. Pajno, F. Donati, A. Perrucci, *Intelligenza artificiale e diritto: una rivoluzione?*, vol. 2, Bologna, 2022, 75 ss.; B. Marchetti, *Intelligenza artificiale, poteri pubblici e rule of law*, in F.G. Scoca, M.P. Chiti, D.U. Galetta (a cura di), *Liber Amicorum per Guido Greco*, Torino, 2024, 529 ss.; R. Cavallo Perin, I. Alberti, *Atti e procedimenti amministrativi digitali*, in R. Cavallo Perin, D.U. Galetta (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, II ed., 2025, 138 ss.

moral judgment and entails the coercive exercise of state power. Such decisions cannot be reduced to probabilistic calculations without altering their normative meaning.

Yet, from a technical standpoint, the boundary between decision-support systems (DSS) and decision-making systems is less robust than it appears. Both rely on algorithmic processing of data; both generate outputs derived from statistical inference or rule-based computation. The difference lies not in their computational architecture but in their formal legal status and in the degree of human intervention¹⁰.

The risk, therefore, is not the formal substitution of the judge, but a more subtle transformation of judicial reasoning. Algorithmic outputs may exert a powerful cognitive influence. When presented with predictive analytics, risk scores, or structured recommendations, judges may feel compelled—consciously or unconsciously—to align their reasoning with the technological suggestion. Departing from the algorithmic output may require additional justification, thereby shifting the motivational burden.

This phenomenon, sometimes described as “automation bias,” has direct implications for judicial independence¹¹. Independence is not merely institutional; it is also epistemic. If algorithmic systems progressively shape the cognitive environment within which decisions are made, the autonomy of judicial reasoning may be indirectly constrained.

Furthermore, consistency and predictability—often invoked as advantages of AI, besides being features of criminal law—must be evaluated with caution. While uniformity of application is a fundamental component of legal certainty, criminal justice is not solely concerned with statistical coherence. It also embodies principles of individualization, contextual evaluation, and moral judgment. An excessive emphasis on predictive regularity risks transforming adjudication into a technocratic exercise, privileging efficiency over deliberative reasoning¹².

¹⁰ S. Quattrocchio, *Decidere o decidere di non decidere? Cosa l'intelligenza artificiale può offrire al giudizio penale*, in A. Pajno, L. Violante (a cura di), *Biopolitica, pandemia e democrazia*, vol. III, Bologna, 2021, 271

¹¹ A. Završnik, *Criminal justice, artificial intelligence systems, and human rights*, *Era Forum*, 2020, 567 ff.; S. Quattrocchio, *Artificial Intelligence, Computational Modelling and Criminal Proceedings*, Cham, 2020, 73 ff.

¹² E. Morozov, *To Save Everything, Click Here*, London, 2013.

4.1. Although Article 15 excludes automated decision-making in formal terms, it does not eliminate deeper concerns.

First, the law does not address in detail the evidentiary status of algorithmically generated outputs. If AI systems are used to analyze patterns, reconstruct events, or generate synthetic evidence, complex questions arise concerning admissibility, reliability, and contestability. Criminal procedure is structured around the possibility of contradiction: evidence must be open to scrutiny and challenge. When evidentiary elements are derived from opaque computational processes, effective contestation may become practically unattainable.

Second, the growing diffusion of generative AI tools—particularly large language models—introduces new challenges. The law does not explicitly regulate their use in drafting judicial opinions¹³. Formally, such use might be compatible with the idea of decision support. Substantively, however, delegating portions of legal reasoning to generative systems raises serious concerns regarding authorship, verification, and disciplinary accountability¹⁴. Judicial decisions require not only correctness but also personal responsibility. The reasoning must be attributable to the judge as an individual office-holder, beyond the formal act of signature.

Third, equality of arms may be indirectly affected. If prosecutorial authorities or investigative bodies have privileged access to advanced AI tools while defence counsel lack comparable resources, structural imbalances may emerge. The principle of procedural parity cannot be reduced to formal rights; it must also consider the material conditions under which those rights are exercised.

In light of these considerations, the legislative exclusion of automated adjudication appears necessary but insufficient. The real challenge lies not in preventing the overt replacement of judges, but in ensuring that the integration of AI does not progressively reshape the epistemic and normative foundations of criminal adjudication.

5. Beyond adjudicative activity strictly understood, Law 132/2025 also addresses the use of artificial intelligence in the organisational dimension of the justice system. Article 15(2) assigns to the Ministry of Justice the task of regulating and coordinating AI applications designed to enhance administrative efficiency, case management, and the allocation of judicial resources.

¹³ B. Galgani, *La L. 132/2025*, cit., 1454.

¹⁴ See e.g. the Spanish regulation Real decreto ley n. 6/2023, 19.12. 2023.

At this level, the functional advantages of AI appear particularly evident. Algorithmic tools may assist in managing caseload distribution, forecasting procedural timelines, identifying bottlenecks, and optimizing administrative workflows. In systems historically burdened by structural delays, such applications may contribute meaningfully to improving access to justice.

Yet even organisational uses are not normatively neutral. Case allocation mechanisms, priority-setting algorithms, and performance-monitoring systems inevitably influence the practical exercise of jurisdiction. The criteria embedded in such systems—whether explicit or implicit—may affect which cases are handled first, how judicial resources are distributed, and which forms of litigation receive greater institutional attention.

Moreover, the law does not clearly require centralized technical standardization or interoperability across judicial offices. The absence of a robust governance architecture risks generating fragmentation, with different courts adopting heterogeneous tools developed by private vendors. Such decentralization could undermine equality before the law and create uneven technological dependencies.

The exclusion of the High Council of the Judiciary (CSM) from the Permanent Observatory on AI established at the Ministry of Justice is also noteworthy. Given the constitutional role of the Council in safeguarding judicial independence, its marginalization from strategic decisions concerning technological transformation raises institutional concerns¹⁵.

The question of public versus private development is equally crucial. If core judicial infrastructures are built upon proprietary systems controlled by commercial entities, the justice system may become dependent on external actors whose primary objectives are not aligned with constitutional guarantees. Investment in publicly developed, transparent, and auditable AI systems thus appears essential to preserving institutional autonomy.

6. Article 16 confers to the Government a broad delegation to regulate the data, algorithms, and mathematical methodologies used in the training and validation of AI systems. Although the provision is framed in general terms, its implications are particularly significant in sensitive sectors such as criminal justice and law enforcement.

¹⁵ B. Galgani, *La L. 132/2025*, cit., 1451.

Training data fundamentally shape algorithmic behavior. Biases embedded in historical datasets may be amplified through machine learning processes, generating discriminatory outcomes even in the absence of explicit intent. The regulation of data quality, representativeness, and provenance is therefore not merely a technical matter but a constitutional imperative.

The delegation also concerns experimentation spaces—so-called regulatory sandboxes—and assigns oversight responsibilities to national digital authorities. While experimentation may foster innovation, it must be carefully balanced against fundamental rights protection. Criminal justice cannot become a laboratory for untested technologies whose error margins remain insufficiently understood.

A central challenge lies in reconciling technological neutrality with legal certainty. Rapid technological evolution renders highly detailed statutory definitions vulnerable to obsolescence. At the same time, excessive reliance on technical standards risks shifting normative authority from democratically accountable institutions to technocratic bodies. The balance between flexibility and democratic legitimacy will prove decisive.

7. Perhaps the most delicate aspect of Law 132/2025 lies in Article 24, which delegates to the Government the regulation of artificial intelligence in the context of police functions and preliminary investigations.

The delegation is formulated in broad terms, leaving substantial discretion to the executive branch. This legislative choice amplifies the transformative potential of future implementing decrees, particularly given the intrusive nature of many AI-based investigative tools.

Predictive policing technologies are likely to occupy a central position. These systems analyze historical crime data to identify risk patterns, forecast potential offenses, or allocate patrol resources¹⁶. While often justified on efficiency grounds,

¹⁶ For a definition, A. Selbst, *Disparate Impact in Big Data Policing*, in *Georgia Law Review*, 2017, vol. 52, 114. On the Italian approach to it, E. Pietrocarlo, *La predictive policing nel regolamento europeo sull'intelligenza artificiale*, in *Leg. Pen.*, 26.9.2024, 1 ss.; v. anche, *ex multis*, L. Camaldo, *Intelligenza artificiale e investigazione penale predittiva*, in *RIDPP*, 2024, 233 ss.; L. Belvini, *Intelligenza artificiale e circuito investigativo*, Bari, 2025, 213 ss.; M. Lanzi, *Le attività di predictive policing, tra efficienza applicativa e criticità applicative*, in *Ind. Pen.*, 2023, 262 ss.; S. Lonati, 'Predictive policing': dal disincanto all'urgenza di un ripensamento, in *MediaLaws*, 2022, 302 ss.

predictive models raise profound concerns regarding profiling, discrimination, and the presumption of innocence¹⁷.

The AI Act prohibits certain forms of risk assessment based exclusively on profiling but permits high-risk systems that incorporate additional data sources. This distinction is conceptually fragile. In practice, the boundary between exclusive profiling and multi-factor analysis may prove difficult to operationalize, leaving room for expansive interpretations¹⁸.

Facial recognition technologies constitute an even more contentious domain. Although real-time biometric identification in publicly accessible spaces is generally prohibited under Article 5 of the AI Act, broad exceptions exist for serious crimes, counter-terrorism, and the search for missing persons. These exceptions, if interpreted expansively, risk transforming a nominal prohibition into a flexible authorization regime¹⁹.

From a criminal procedural perspective, the integration of such technologies must be assessed against principles of proportionality, necessity, and judicial oversight. Intrusive surveillance measures cannot be justified solely on predictive utility. They must remain anchored to individualized suspicion and subject to robust adversarial review.

7.1. Article 24(5) further delegates regulatory authority concerning the use of AI during preliminary investigations. The legislature explicitly references defence rights, personal data protection, non-discrimination, and proportionality as guiding criteria²⁰.

These references are essential but require concrete operationalization. Transparency, in particular, must be understood not merely as institutional disclosure but as procedural explainability. Defendants must be placed in a position to understand, challenge, and contest algorithmically derived evidence or investigative leads.

The possibility that AI systems may generate synthetic or probabilistic evidence raises additional complications. Criminal adjudication traditionally requires proof

¹⁷ F. Palmiotto, *Is Predictive Policing prohibited in EU? Yes, it should be*, in *eulawlive.com*, 19.12.2024

¹⁸ S. Quattrocolo, *Criminal Law Enforcement through AI*, in *W. Barfield, U. Pagallo, Research handbook on the law of artificial intelligence. Current and future directions*, 2nd ed., 2025, Cheltenham, 349 ff.

¹⁹ F. Palmiotto, *Facial Recognition Before the European Court of Human Rights*, in *European Review of Digital Administration and Law*, 2025, vol. 6, Issue 1, 101 ss.

²⁰ B. Galgani, *La L. 132/2025*, cit., 1457.

beyond reasonable doubt, supported by evidence subjected to adversarial testing. Algorithmic inferences—however statistically robust—cannot substitute for evidentiary demonstration unless integrated within procedural safeguards ensuring reliability and contestability²¹.

Article 24 also authorizes adjustments to substantive criminal law, including the potential introduction of new offenses related to AI misuse and the extension of corporate liability frameworks. These delegations signal that the legislative impact of Law 132/2025 extends beyond procedural adaptation; it may reshape the substantive contours of criminal responsibility in the digital age.

The broader European normative environment—including the Law Enforcement Directive, the E-Evidence Package, and the Digital Services Act—will inevitably interact with these domestic measures. The resulting regulatory landscape is likely to be complex and multilayered, demanding careful coordination to avoid inconsistencies.

8. Law 132/2025 presents itself, at first glance, as a technically ordinary instrument designed to coordinate national law with the European AI Act. Its language is measured, its principles are familiar, and its structure appears cautious.

Yet beneath this apparent ordinariness lies the potential for extraordinary institutional transformation. Artificial intelligence, when integrated into criminal justice, does not merely enhance efficiency; it alters the epistemic environment within which legal decisions are produced. It affects how evidence is generated, how risk is assessed, how cases are prioritized, and how judicial reasoning is structured.

The decisive challenge is therefore not whether AI will enter the justice system—it already has—but under what normative conditions. Safeguarding human autonomy, judicial independence, equality of arms, and procedural fairness requires more than formal prohibitions of automated decision-making. It demands sustained interdisciplinary dialogue between legal scholars, practitioners, computer scientists, and policymakers.

Ultimately, the success of this legislative framework will depend on whether such dialogue can produce a shared conceptual vocabulary capable of translating

²¹ F. Palmiotto, *The black box on trial: the impact of algorithmic opacity on fair trial rights in criminal proceedings*, in M. Ebers, M. Cantero Gamito (a cura di), *Algorithmic Governance and Governance of Algorithms: Legal and Ethical Challenges*, Cham, 2021, 49 ss.

technological complexity into legally meaningful standards. Only then can an “ordinary” legislative instrument adequately govern the “extraordinary” transformations brought about by artificial intelligence.