

Challenges and Strategies for Safeguarding the Principles of Criminal Law in Electronic Criminal Proceedings at the Trial Stage

1. Sirous Nazari[✉]: Department of Law, Qo.C., Islamic Azad University, Qom, Iran

2. Ali Arman^{✉*}: Department of Law, Bo.C., Islamic Azad University, Borujerd, Iran

3. Soheili Ebrahimzadeh[✉]: Department of Law, Shahab Danesh University, Qom, Iran

*Correspondence: 5579145802@iau.ir

Abstract

The transition from “place-based justice” to “data-driven justice” in the digital age has confronted criminal proceedings with fundamental challenges. Although the introduction of videoconferencing and artificial intelligence technologies promises to expedite judicial proceedings, it also places fundamental principles of criminal justice—including the right to presence and effective confrontation, the principle of public hearings, equality of arms, and judicial independence—at risk. Employing a descriptive-analytical method and a comparative approach, the present article examines the adverse implications of these developments and proposes legal and technical solutions. The findings indicate that technological mediation, by creating “emotional blindness” and eliminating vital body-language cues, impairs judges’ intuitive understanding, while reliance on an “algorithmic judge” reduces adjudication to “black-box justice” and opaque computational processes. Furthermore, infrastructural inequality results in a manifest violation of the principle of equality of arms. To address these challenges, this study proposes the adoption of a “hybrid model” in which electronic proceedings do not serve as an absolute substitute for in-person proceedings but rather as a conditional complement to them, subject to the defendant’s consent. The establishment of a system of “filtered transparency,” including real-time image blurring and delayed broadcasting to protect privacy in publicly accessible online courts; the creation of a dedicated tunnel within the National Information Network, with priority allocation for judicial data traffic to ensure stable connectivity; and the application of the “human-in-the-loop” principle to prevent the uncritical automation of judicial decisions constitute the principal strategies proposed for this emerging framework.

Keywords: electronic criminal proceedings, judicial artificial intelligence, transparency, black-box justice, equality of arms.

Received: 02 March 2026

Revised: 07 July 2026

Accepted: 14 July 2026

Published: 20 July 2026



Copyright: © 2026 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Citation: Nazari, S., Arman, A., & Ebrahimzadeh, S. (2026). Challenges and Strategies for Safeguarding the Principles of Criminal Law in Electronic Criminal Proceedings at the Trial Stage. *Legal Studies in Digital Age*, 5(4), 1-24.

1. Introduction

If the preliminary-investigation stage is regarded as the “foundation” upon which a criminal case is constructed, the trial stage constitutes its “external façade” and the moment at which justice becomes manifest. It is at this stage that the evidence collected is subjected to critical examination, the parties confront one another before an impartial judge, and the public conscience supervises the performance of the judiciary through the “publicity of proceedings.” With the emergence of

“electronic proceedings” and the introduction of “online courts” and “artificial intelligence” into this solemn domain, criminal justice is undergoing a profound transformation, which may be described as a transition from “place-based justice” to “data-driven justice.”

Under the traditional paradigm, a “court” is a physical place with distinctive architecture whose solemnity, silence, and procedural rituals naturally induce the parties to speak truthfully and submit to the authority of law. In electronic proceedings, however, the court is reduced to an “internet link” or a “videoconference session.” This change of setting is not merely formal; it transforms the nature of adjudication and defence. When a judge sees the defendant not standing in the dock but confined within a small frame on a monitor, and when defence counsel, instead of standing and delivering a compelling argument, must remain concerned about internet interruptions, the “psychology of adjudication” changes. The central challenge examined in this article is therefore the following fundamental question: Has technology succeeded in transferring the “spirit of adjudication” into cyberspace, or has it merely digitised its “body”? Principles of criminal justice, including the right to presence, the principle of public hearings, and equality of arms, evolved over centuries within physical environments. Now that “presence” has been translated into “connectivity” and “publicity” into “live streaming,” do the former safeguards remain effective? At the same time, the heavy shadow of “artificial intelligence” now hangs over the judicial bench. Expert systems and judicial algorithms, introduced with promises of “eliminating human error” and enabling “accurate prediction,” carry the risk of producing a “machine judge” and “black-box justice,” in which judicial decisions are issued not on the basis of legal reasoning and the judge’s inner conviction, but through opaque mathematical calculations.

Within the Iranian legal system, following the adoption of the Regulation on the Use of Computer Systems and the Judicial Transformation Document, online hearings have become a routine practice. Field reports and doctrinal legal analyses, however, indicate that this rapid transition has sometimes occurred at the expense of fundamental procedural principles. The weakening of “effective confrontation” with witnesses, difficulties in the immediate presentation of documents, and security challenges relating to participant identification constitute only part of the problem. This article examines the confrontation between “tradition” and “modernity” at the most sensitive stage of criminal proceedings. It employs a descriptive-analytical research method, and its data have been collected through library and documentary sources. In proposing solutions, the study also adopts a comparative approach, drawing on international experience alongside the capacities of the domestic legal system. Its purpose is to move beyond superficial assessments and examine the profound effects of technology on the “quality of adjudication.” The structure of the article is designed so that the first section critically examines, through the lens of scientific scepticism, the full range of challenges and threats associated with electronic and intelligent courts. The second section then adopts a reform-oriented approach and draws upon international experiences, including Australian hybrid models, Council of Europe standards, and domestic capacities, to propose strategies for the “reconstruction of criminal proceedings on the basis of criminal-law principles” in the digital environment. The article seeks to demonstrate how technology may be placed at the service of “human-centred justice,” “judicial fairness,” and compliance with the fundamental principles of criminal law without requiring a return to the age of pen and paper, so that the online court becomes not a caricature of justice but a new manifestation of fairness.

2. Challenges to Fair Trial in Electronic Courts

The trial stage, which rests upon the principles of “adversarial proceedings,” “publicity,” and “judicial immediacy,” faces profound challenges when transferred to the digital environment, challenges that destabilise the foundations of criminal-justice principles. In electronic courts, “technological mediation” replaces “direct communication” and filters reality. The most significant challenge concerns “presence” and “confrontation,” because videoconferencing eliminates behavioural details, including body language, thereby impairing the judge’s “judicial discernment” in reaching an “inner conviction” and increasing the danger that “virtual truth” will replace “objective truth.” A second challenge arises from the introduction of “artificial intelligence” into adjudication. Algorithms may contain hidden biases and, by reducing the human being to a “statistical datum,” may transform judicial independence into a “statistical calculation,” thereby creating the danger of the algorithmic judge. Moreover, the live transmission of court hearings in cyberspace places the principle of “publicity” in conflict with privacy and the prospect of “merciless public judgment.” Finally, differences in access to high-quality internet services and communication equipment between the state and the defendant severely undermine the principle of “equality of arms.”

2.1. *Challenges to the Principles of Presence and Face-to-Face Confrontation*

The “right to presence” and the “right of confrontation” are fundamental criminal-procedure principles in legal systems throughout the world. Their underlying rationale is that the judge must see and hear the evidence “directly,” while the defendant must have the opportunity to challenge the complainant and witnesses in court. In traditional law, presence meant “physical co-location” within an environment in which the “courtroom atmosphere” influenced the conscience and conduct of the parties. Electronic proceedings, however, introduce the concept of “virtual presence” and assume that sound and image are sufficient to achieve justice. From the perspective of legal psychology and legal doctrine, this assumption presents serious difficulties. A judge’s “inner conviction” is not a mechanical process produced merely by hearing spoken words; rather, it is an intuitive process shaped by observing the trembling of a defendant’s hands, changes in a witness’s facial colour, and non-verbal interactions within the courtroom (Ashouri, 2023). Regardless of its technical quality, videoconferencing functions as a “filter” that eliminates a substantial proportion of these vital signals. Face-to-face confrontation is also an instrument for discovering the truth. When the accused and the complainant confront one another directly, their tension and reactions may reveal the truth. In the online environment, this tension is reduced and a form of “safe distance” emerges, which may embolden false testimony. The legislature should not sacrifice the quality of adjudication merely to reduce transportation costs. Transforming a hearing into a “video call” risks reducing adjudication to a lifeless administrative formality. This subsection examines four fundamental challenges arising from the physical absence of the parties in order to demonstrate why technology has not yet become a complete substitute for the “judicial bench.”

2.1.1. *Reduced Mutual Understanding and Loss of Body Language in Videoconference Hearings*

It has been asserted that only 7% of human communication is verbal, whereas 93% is non-verbal, taking the form of tone of voice and body language (Ažubalytė & Titko, 2022). In criminal adjudication, where the purpose is to discover internal intent and establish factual truth, such non-verbal indications may possess evidentiary value comparable to that of the spoken words themselves. Conducting hearings by videoconference disrupts the transmission of these indications and gives rise to a phenomenon that may be described as “emotional blindness” in adjudication (Ažubalytė & Titko, 2022). The “reduction of mutual understanding and absence of body language” in electronic proceedings under Article 659 of the Code of Criminal Procedure creates a rupture in the process of “truth-finding.” Although the legislature, for the purpose of expediting proceedings under Article 3 of the Code of Criminal Procedure, has authorised videoconferencing through the “National Justice Network,” this mediation challenges both the “principle of judicial immediacy” and the “physical presence” necessary for attaining the “ordinary judicial knowledge” contemplated by Article 211 of the Islamic Penal Code (Hayat Poursofli, 2021). Vital indications contributing to the formation of the judge’s “inner conviction,” including “body language,” may be lost or distorted within the screen frame and through network disruptions envisaged by the Note to Article 655 of the Code of Criminal Procedure. This “perceptual distance” increases the risk of incomplete inferences and, by undermining the “right to an effective defence” under Article 190 of the Code of Criminal Procedure, conflicts with the spirit of a fair trial.

A. Camera-Framing Limitations and the Elimination of “Microexpressions”

In online proceedings, the judge usually sees only the defendant’s “head and shoulders,” while video compression may eliminate indications of stress. Millisecond changes in facial muscles are lost in the pixelated image (Ažubalytė & Titko, 2022), and this “flat” and “shallow” representation, by failing to communicate the person’s actual emotional state, directly and adversely affects “judicial intuition.”

B. Audio Delay and Disruption of the Rhythm of Proceedings

Delayed responses make it difficult for the judge to distinguish “slow internet connectivity” from “hesitation by the defendant” (Ažubalytė & Titko, 2022). The human mind may unconsciously interpret such delay as evidence of “dishonesty” or “low intelligence.” This form of “technological bias” may cause judges unintentionally to develop a more negative perception of defendants.

C. Absence of Eye Contact

Genuine eye contact is impossible in videoconferencing. Looking either at the monitor or at the camera lens creates a contradictory and unnatural situation (Ažubalyté & Titko, 2022). This “communicative disjunction” may, on the one hand, give the judge the impression that the defendant is being evasive and, on the other, deprive the defendant of the ability to understand the feedback conveyed through the judge’s gaze.

D. The Effect of “Psychological Distancing”

Unlike the solemnity of physical presence, in which the “courtroom setting” itself forms part of the punitive experience, defendants tend to behave more casually online. Such informality, which arises from the digital medium, may mistakenly be interpreted by the judge as “lack of remorse” or “disrespect for the court,” potentially resulting in a harsher sentence.

2.1.2. The Challenge of “Effective Confrontation” with Witnesses and the Complainant Online

The right of confrontation is embedded in human-rights instruments and Article 35 of the Constitution (Akhundi, 2015). It permits the defendant to stand face to face with those who testify against him or her and to challenge their credibility through cross-examination (Khaleghi, 2024). Although electronic proceedings transmit the image of the witness, they neutralise the “effect of confrontation” (Moazenadegan & Rosta, 2017). An analysis of the problem of “effective confrontation with witnesses and the complainant” in electronic proceedings reveals a profound conflict between “technological convenience” and the “principles of fair trial.”

Authorising the taking of testimony and confrontation by videoconference through the “National Justice Network” under Article 659 of the Code of Criminal Procedure compromises the “principle of the judge’s direct reception of evidence.” The absence of “face-to-face confrontation” and the inability to perceive “body language” deprive the judge of the “ordinary judicial knowledge” envisaged by Article 211 of the Islamic Penal Code. This perceptual deficiency, by weakening the defendant’s right to challenge witnesses under Articles 190 and 362 of the Code of Criminal Procedure, reduces “adversarial proceedings” to “administrative formalities” and conflicts with the spirit of Article 2 of the Code of Criminal Procedure by undermining the credibility of testimony and eliminating effective supervision.

A. Reduction of the “Psychological Pressure to Tell the Truth”

By placing the witness in a safe and familiar environment, electronic proceedings reduce the “psychological cost” of lying. The witness may feel that he or she is merely delivering a “video report,” and the digital “objectification” of the defendant may facilitate false testimony.

B. Inability to Conduct Effective Cross-Examination and Rehabilitation

In the online environment, psychological techniques and rapid sequences of questions employed by defence counsel lose much of their effectiveness. Delays and judicial reminders to “wait for one’s turn” give a dishonest witness time to reconstruct the narrative. The turn-based structure of online platforms is unsuitable for “rapid legal challenges” and effectively disarms the defendant.

C. The Challenge of Identifying the Accused in an Identification Parade

In an online court, zooming in on the defendant’s face and displaying the defendant’s name creates a form of “system-generated suggestion.” The proper conduct of a “virtual identification parade” requires sophisticated software that has not yet been incorporated into Iran’s judicial case-management system.

D. Severance of the Emotional Connection between the Complainant and the Judge

The same difficulty also affects victims. A complainant who has suffered sexual assault or violence seeks to communicate his or her pain to the judge. Expressing emotion and crying before a webcam may be less impactful than doing so in person. The judge may fail to understand the depth of the complainant’s psychological injury through a monitor, and this may affect sentencing or compensation to the complainant’s detriment. Online proceedings may therefore prejudice both the defendant’s ability to defend and the complainant’s ability to communicate harm.

2.1.3. *The Possibility of Coaching or Threatening Witnesses Outside the Camera's Field of View*

A fundamental principle governing the reception of testimony is the “independence of the witness” and the witness’s “freedom of will.” Unlike the judge’s control over a physical courtroom, the “camera frame” in electronic proceedings reveals only part of reality, while events occurring “behind the camera” or “under the table” constitute a blind spot in justice that may compromise the reliability of testimony.

A. Covert Direction of Testimony

In cyberspace, the risk of “non-verbal coaching” by individuals outside the camera frame, using signs or hand gestures, constitutes a form of invisible and untraceable fraud that does not ordinarily arise in physical proceedings. A witness may also read “dictated text” sent through a messaging application while the judge assumes that the witness is independently reflecting before answering.

B. Invisible Threats and Coercion

More dangerous than coaching is the possibility of “threats.” In cases such as domestic violence, the complainant may effectively be “confined at home” and threatened by the accused standing behind the camera. The judge’s inability to guarantee the “physical safety of the testimonial environment” may legally invalidate the statements obtained under such conditions (Ashouri, 2023).

C. Absence of Technical Control Mechanisms

Current Iranian practice does not include protocols such as the use of a 360-degree camera, although rotating a camera would not itself constitute a definitive solution. As long as the witness is not situated in a “judicially supervised location,” there remains a presumption of the “possible contamination of testimony,” and the unconditional acceptance of testimony delivered from a private home reflects judicial naivety.

D. The Challenge of Verifying the Witness’s True Identity

Face coverings and poor image quality increase the risk of “witness substitution” and make identity fraud difficult to detect, particularly in delegated testimony where the trial judge has not previously seen the witness.

2.1.4. *Inability to Present Physical Documents Immediately during a Virtual Hearing*

The inability to present physical evidence immediately during electronic proceedings under Article 659 of the Code of Criminal Procedure creates a structural conflict between “technical limitations” and the “adversarial principle” (Keykha & Ehsanifar, 2023). Requiring documents to be uploaded in advance under the Note to Article 655 of the Code of Criminal Procedure deprives the defendant of the “legitimate element of surprise” and the “right to an immediate defence,” breaches the safeguards established by Article 190 of the Code, and prevents the judge from examining the “authenticity of the document” in real time. This impairs the formation of “ordinary judicial knowledge” and conflicts with the standards of a “fair trial” under Article 2 of the Code of Criminal Procedure.

A. The Death of the “Element of Surprise” in Technical Questioning

The delay required to upload and display documents destroys the “constructive tension of the hearing” and gives a dishonest witness an opportunity to formulate an explanation. Advance access to documents effectively deprives counsel of the legitimate forensic tool of “surprise.”

B. Inability to Conduct a “Sensory Examination” of Evidence

Physical examination of such features as scratches on paper or the weight of a weapon cannot be conducted through a “document scan” or webcam. Judicial reliance on an “image of the evidence” rather than the “evidence itself” diminishes its evidentiary quality and may result in serious judicial error in offences involving physical objects.

C. Technical Challenges and Incompatible Formats

The dependence of justice upon “bandwidth” and “software code” demonstrates the fragility of electronic proceedings. Technical failures in displaying files may discourage the judge from examining crucial evidence.

D. The Divide between the “Original Document” and the “Digital Copy”

Given the requirement to inspect the “original document” under Article 96 of the Code of Civil Procedure and analogous criminal-law principles, showing a document to the camera is insufficient for determining authenticity. The current alternative of postal delivery is itself inconsistent with the speed expected of electronic proceedings.

2.2. Challenges Posed by Artificial Intelligence to Judicial Independence

Artificial intelligence has transformed the foundations of “adjudication.” Whereas electronic proceedings merely alter the “instrument” of justice, artificial intelligence changes the “actor,” facilitating a transition from the paradigm of a “human judge equipped with technology” to one of “computational adjudication.” Phenomena such as “predictive justice” and the “robot judge,” despite their promise of speed and the emphasis placed by the Judicial Transformation Document on “emerging technologies and artificial intelligence” ([Center for Monitoring the Implementation of the Judicial Transformation, 2024](#)), also possess a darker dimension. Adjudication is not a mechanical activity; it combines the “interpretation of law,” the “understanding of social circumstances,” and “moral intuition.” The dominance of algorithms creates a risk that adjudication will be reduced from a “normative” process to a “statistical” exercise. Moreover, challenges such as “algorithmic discrimination,” “opacity,” and the “weakening of judicial independence” threaten the legitimacy of judicial decisions. Reducing the judge to a machine operator would amount to the “death of judicial justice.” It is therefore essential to identify the precise boundary between “artificial intelligence as an assistant” and “artificial intelligence as a master.”

2.2.1. The Challenge of the “Algorithmic Judge”

The concept of the “algorithmic judge” refers to the use of artificial-intelligence and machine-learning systems to analyse cases, evaluate evidence, and issue judgments or recommend outcomes ([Zekos, 2022](#)). Although judicial systems are currently operating primarily at the stage of “intelligent assistance,” the danger that “human judgment will be replaced by machine computation” and that the “algorithmic judge” will emerge is serious. This phenomenon challenges “judicial independence” and the “principle of individualisation of punishment.” The Judicial Smartification Directive and Article 650 of the Code of Criminal Procedure authorise the use of intelligent systems ([Beiki Shouraki & Fallah, 2024](#)); however, excessive reliance on “system-generated drafts” reduces the judge from an “independent interpreter and jurist” to a “mere approver.” This clearly conflicts with Article 211 of the Islamic Penal Code, which bases judgment on “ordinary knowledge” and “inner conviction,” as well as with the defendant’s right to human adjudication under Article 2 of the Code of Criminal Procedure. Algorithms lack a qualitative understanding of the offender’s circumstances and motives under Article 18 of the Islamic Penal Code. The dominance of statistical data therefore leads to the “mechanisation of justice.”

A. The Nature of Adjudication: Interpretation versus Calculation

Criminal adjudication is fundamentally an “interpretive and hermeneutic act” requiring an “understanding of context” in order to apply an abstract legal rule to the fluid reality of a case. Artificial intelligence, by contrast, is a “computational machine” grounded in formal logic and statistics that identifies “correlations between data” rather than “causes” or “meaning.” To an algorithm, stealing bread out of necessity and stealing a ring are merely data records, whereas a human judge understands the offender’s motive and circumstances. Reducing adjudication to an algorithm eliminates the “human element” and produces a rigid and inflexible form of “machine justice” that directly contradicts the principle of the “individualisation of punishment.”

B. Conflict with Constitutional and Jurisprudential Principles

Within the Iranian legal system, and pursuant to Article 167 of the Constitution, the judicial office is a position of religious authority grounded in Imami jurisprudence and requires qualifications such as “justice” and “ijtihad,” or authorisation by a qualified mujtahid ([Mousavi, 2016](#)). In *Shara’i al-Islam*, al-Hilli defines adjudication as the “religious authority to issue judgments and administer public interests on behalf of the infallible Imam,” an authority that can be vested exclusively in a natural person ([al-Hilli, 1994](#)). Three fundamental jurisprudential challenges consequently arise:

1. **Ijtihad and knowledge:** Artificial intelligence relies on induction and the analysis of past data and is, at best, an “imitator,” whereas a judge must possess independent juristic competence and the capacity to derive legal rulings.

2. **Intent and performative declaration:** Adjudication requires “intentionality” and a serious will to issue a binding judgment, capacities that a non-conscious machine does not possess.
3. **Justice as an ingrained moral disposition:** A machine has no human soul and therefore cannot possess justice as an ethical or religious disposition.

The system’s statistical knowledge cannot substitute for the inner certainty contemplated by the doctrine of “judicial knowledge” under Article 211 of the Islamic Penal Code.

C. Reduction of Justice to Efficiency

The principal incentive for adopting artificial intelligence is to escape “case congestion” and “protracted proceedings” (Rahnema & Zafari Kurehtash, 2025). This approach, however, removes adjudication from the realm of “desert-based justice” and reduces it to “instrumental justice” and an instrument of “risk management.” Under this utilitarian logic, human dignity is violated, and defendants are reduced to numbers in risk-management tables. The unsupervised use of “decision-support systems” optimises judgments only statistically, not in terms of their intrinsic justice.

D. Inability to Understand Abstract and Ethical Concepts

Legal concepts such as “self-defence,” “undue hardship,” and “the best interests of the child” are fluid and cannot be defined mathematically. Artificial intelligence is incapable of understanding “common sense” and ethical nuance. For example, a father who throws his child from a window to save the child from a fire, causing a broken leg, may be classified by a trained algorithm as having committed “assault and battery,” whereas a human judge would understand the doctrine of “necessity” and issue an acquittal. As Aristotle observed, equity corrects the law when its generality is defective; the algorithmic judge, however, is a “merciless executor of the law” incapable of “equitable flexibility.”

E. Freezing of Judicial Precedent and the Death of Legal Dynamism

Law is a living phenomenon that develops through transformative judgments delivered by courageous judges. Because an algorithm is trained on historical data, it is inherently “conservative.” It may therefore fail to recognise social change and cause the legal system to “freeze,” bringing the dynamism of “ijtihad” to a halt. This phenomenon may be described as the “dictatorship of the past over the future.”

F. The Accountability Challenge

When a human judge errs, remedial mechanisms are available under Article 171 of the Constitution and through the Judges’ Disciplinary Prosecutor’s Office. Errors produced by artificial-intelligence systems, such as the conviction of an innocent person, create a serious “accountability gap.” It remains unclear whether responsibility lies with the software manufacturer, the judge who approved the output, or the artificial-intelligence system itself, which lacks legal capacity.

2.2.2. *Bias in Artificial-Intelligence Algorithms and Racial and Social Discrimination*

The myth of “algorithmic neutrality” is among the greatest illusions of the digital age (Park, 2025). Contrary to the widespread assumption that computers adjudicate in a “pure,” “objective,” and “fair” manner because they lack emotions, artificial intelligence may systematise and intensify social discrimination. In systems involving “intelligent judges” and “predictive policing,” society confronts what may be described as “mathematical weapons of mass destruction,” because algorithms inherit both the assumptions of their designers and data contaminated by historical discrimination (Park, 2025). The mechanisms of such bias and the danger of the “technologisation of inequality” in criminal justice are examined below.

A. The Data-Laundering Mechanism

Bias in artificial intelligence is not magical; it is the direct product of the quality of input data. Data science recognises the well-known principle of “garbage in, garbage out.” Artificial-intelligence systems are trained on “historical data,” including records generated through decades of disproportionate policing in poor neighbourhoods and minority communities. When supplied with these distorted statistics, the machine wrongly attributes criminality to these groups. The process by which human prejudice is passed through mathematical equations and thereby presented as legitimate may be called the “technological laundering of discrimination.” The concealment of bias behind the appearance of “science” and “objectivity” makes it the most dangerous form of discrimination.

B. Proxy Variables

Removing sensitive variables such as race or religion from the code is ineffective because the algorithm may identify “proxy variables,” such as postal code or educational background, and use them to infer a person’s social class or ethnicity with a high degree of accuracy (Brayne, 2020). In the Iranian judicial system, this creates a risk of “discrimination against marginalised communities,” whereby a law-abiding citizen may be assessed as high-risk solely because of “geographical determinism,” in violation of the fundamental principle that criminality and punishment are personal.

C. The COMPAS Case Study

The American risk-assessment software COMPAS is a prominent example of this crisis. Research revealed that the system, despite claims of neutrality, relied on questions correlated with poverty and was significantly biased against Black defendants. Its “false-positive” rate, under which low-risk defendants were incorrectly classified as high-risk, was twice as high for Black defendants as for White defendants (Vaccaro, 2019). The uncritical importation of such software into Iran without a “fairness audit” would reproduce class-based inequalities.

D. Negative Feedback Loops

Predictive-policing algorithms forecast crime in deprived areas, causing more officers to be deployed there and consequently resulting in the recording of a greater number of minor offences. These new data then appear to confirm the system’s original prediction. Under this process, which may be described as the “mechanisation of labelling” (Shahpouri & Bashiriyeh, 2019), the algorithm does not predict reality; it “produces” it, while simultaneously shielding offences committed by affluent groups from scrutiny.

E. Legal Challenge: Conflict with the Iranian Constitution

Systematic algorithmic bias against particular groups constitutes a clear violation of Articles 19 and 20 and paragraph 9 of Article 3 of the Constitution, which require the elimination of unjust discrimination. The complex legal challenge is that “discriminatory intent” cannot readily be established in such systems, while Iranian law has not yet developed adequate mechanisms for controlling this form of “indirect discrimination.”

F. Effects on Distributive Justice

These biases may also impair access to legal resources. If case-scheduling systems classify cases involving legal representation or high-value monetary claims as “more important,” the cases of disadvantaged groups will be marginalised. This produces “two-speed justice,” with an accelerated route for elites and a defective route for the broader population, thereby violating distributive justice (Donoghue, 2020).

2.2.3. The Black-Box Challenge

In modern legal systems, including Iran and Imami jurisprudence, the requirement that judgments be “reasoned” means that a court decision must not consist merely of a “result”; it must reflect a transparent and logical “process” that permits review by superior courts and the parties. The introduction of artificial intelligence confronts this principle with the “black-box problem,” in which the logic by which neural networks process inputs and produce outputs may be unknown even to the designers of the algorithm. This “inherent opacity” and “lack of interpretability” are existentially incompatible with the necessarily transparent and intelligible nature of adjudication.

A. Conflict with Article 166 of the Constitution: An Unreasoned Judgment

Under Article 166 of the Constitution, judgments must be reasoned and supported by legal authority, and judicial reasoning must be “persuasive” (Ghafouri, 2013). The output of an intelligent system, such as a statement that there is a 92% probability that a person’s statement is false, is an “opaque statistical proposition,” not legal reasoning. Such a situation resembles a return to the era of “trial by ordeal,” when people trusted judgment to supernatural forces (Gholamlou, 2019). A decision based on a black-box output lacks “rational justification.” Moreover, in electronic proceedings, the production of “template-based judgments” and excessive reliance on “default text” within the case-management system, notwithstanding the efficiency objectives of Articles 649 and 3 of the Code of Criminal Procedure, create a risk that “judicial reasoning” will degenerate into “administrative form completion.” Such “unreasoned judgments” violate Article 166 of the Constitution and Article 374 of the Code of Criminal Procedure, undermine transparency and the “principle of inner conviction,” and remove proceedings from the framework of “procedural justice” and the “protection of defence rights.”

B. The Crisis of Interpretability in Neural Networks

The black-box problem is rooted in the mathematical complexity of artificial neural networks. Unlike “rule-based systems” that follow linear logic, deep-learning systems operate through non-linear processes. Criminal adjudication seeks to establish “causal relationships,” whereas the machine searches for “statistical correlations” (Wischmeyer, 2019). If the judge cannot understand the machine’s logic, the judge is pushed toward “blind imitation,” and justice is entrusted to a process that is inherently “uninterpretable” and “unaccountable.”

C. Violation of the Right of Defence and the Adversarial Principle

The right of defence requires an opportunity to challenge the evidence. Yet how can a black-box algorithm be “questioned and cross-examined”? Defence counsel is confronted with an unexplained number and cannot determine which factor produced the negative score assigned to the client (Wischmeyer, 2019). This creates an extreme form of “informational inequality” and reduces the process to a modern inquisitorial proceeding in which the defendant remains in complete darkness.

D. Trade Secrets as a Barrier Surrounding Justice

Developers of judicial software frequently classify their algorithms as “trade secrets” and refuse to disclose them. This results in the “privatisation of judicial logic” and gives the commercial interests of a private company priority over the “public right to justice” and “transparency” (Wischmeyer, 2019). In the Islamic and Iranian legal systems, where adjudication is an exercise of sovereign authority (Asadi, 2024), judicial reasoning must not be “confidential” or “monopolised by a commercial enterprise.” Such secrecy prevents lawyers and superior judicial authorities from auditing algorithms.

E. Impossibility of Hierarchical Judicial Review

Appellate courts and the Supreme Court are responsible for reviewing the correctness of the reasoning adopted by lower courts (Bazgir, 2010). When a judgment is based upon a black-box output, however, the higher court sees only the resulting number and cannot review the underlying processing. “Superior judicial supervision” therefore becomes practically impossible, and systematic algorithmic errors may be repeated at every stage of adjudication without being detected.

2.2.4. Weakening Judicial Independence through System-Generated Recommendations

Judicial independence has traditionally been discussed in relation to political or financial pressure (Seibert-Fohr, 2022). In the age of artificial intelligence, however, an invisible threat known as “algorithmic authority” has emerged (Schwarcz, 2025). When an “intelligent” system presents a recommendation, the judge experiences psychological pressure to accept it. This phenomenon, known as “automation bias,” reduces the judge from an “independent decision-maker” to a “passive confirmer.”

A. The Psychological Phenomenon of Automation Bias

The human brain is naturally inclined to reduce “cognitive effort” and may prefer to accept a machine-generated solution rather than undertake an independent analysis of the data (Schwarcz, 2025). Judges may accept system recommendations because the machine appears “objective,” “neutral,” and “accurate” (Schwarcz, 2025). In Iran, given the volume of pending cases, resisting the “confirm” button requires considerable determination. When “thinking” is outsourced to a machine, judicial independence is sacrificed to “technological convenience.”

B. Risk Aversion and the Avoidance of Responsibility

“Occupational risk management” is another factor that weakens judicial independence. Disagreeing with the system’s recommendation entails substantial risk, whereas agreeing with it provides a safe institutional position, a condition that may be described as “sheltering behind the algorithm” (Schwarcz, 2025). This incentive structure encourages judges to prefer “following the machine” over exercising judicial courage.

C. Institutional Pressure and Productivity Criteria

Judges are often evaluated on the basis of “statistics” and the speed with which they dispose of cases (Amiri, 2023). When professional advancement is linked to “quantity,” artificial intelligence becomes an instrument for the “mass production of judgments.” Under these conditions, judicial independence and critical examination of system outputs may be interpreted as “slowness” and “inefficiency” (Schwarcz, 2025), transforming artificial intelligence from an assistant into an “unwritten compulsory authority,” or master.

D. Anchoring Effects in Sentencing

In psychology, the first number presented often becomes the reference point for subsequent judgment (Vaccaro, 2019). A sentencing recommendation generated by a system may channel the judge's "mental range," so that instead of adjudicating independently, the judge merely "adjusts the system's recommendation" (Vaccaro, 2019). By substituting the "number on the screen" for a comprehensive assessment of the defendant's circumstances, this phenomenon compromises the judge's independence in the "individualisation of punishment."

E. Conflict with Jurisprudence and the Requirement of Ijtihad

In Imami jurisprudence, adjudication requires "ijtihad" (Mousavi, 2016). Approving a black-box output amounts to blind imitation and empties the jurisprudential concept of adjudication of its meaning. This creates a "conflict between electronic adjudication and the requirements of ijtihad and judicial knowledge," as well as with Article 211 of the Islamic Penal Code, which requires the acquisition of ordinary judicial knowledge through direct engagement. Excessive reliance on decision-support systems under Articles 649 to 659 of the Code of Criminal Procedure and on case-management algorithms transforms the judge from an "independent juristic interpreter" into a "system operator" and produces "judicial rigidity." By depriving the judge of initiative in the "individualisation of punishment" under Article 18 of the Islamic Penal Code, this process reduces "Islamic adjudication" to a form of "administrative mass production."

2.3. Challenges to Publicity and Oversight

The "publicity of proceedings" is a legacy of the Enlightenment and an antidote to inquisitorial and secret courts. Its underlying philosophy is that "justice must not only be done; it must also be seen to be done" (Akhundi, 2015). In physical proceedings, the free presence of observers prevented judicial authoritarianism and collusion. In virtual proceedings, however, replacing the "open door" with an "access link" creates the paradox of "exclusive publicity." Depending on the level of access provided, an online court may be either the "most public" or the "most secretive" form of adjudication (Reiling & Contini, 2022). Despite the Judicial Transformation Document's emphasis on the development of electronic proceedings, the protocol governing the presence of observers remains unclear. Eliminating public scrutiny on the grounds of "bandwidth limitations" or "privacy" reduces adjudication to a "private meeting" and revives the age of "secret trials." Conversely, genuine online publicity also creates risks such as "unlawful recording" and "viral dissemination," because unlike the physical world, the internet does not recognise a meaningful concept of "forgetting," and the permanent preservation of mistakes may completely destroy a person's reputation.

2.3.1. Restrictions on Public and Media Access to Online-Court Links

In a traditional court, attendance is limited by the "physical capacity of the courtroom." In an online court, physical restrictions disappear but are replaced by "systemic-access restrictions" (Reiling & Contini, 2022). The principal problem is that existing electronic-proceedings infrastructure, including platforms such as Skyroom or Adobe Connect used by the judiciary, has been designed primarily for communication among the parties and does not provide a defined role for "the general public" or "the media."

A. The Emergence of "Semi-Secret Courts"

When a hearing is conducted by videoconference, the session administrator, whether the judge or court clerk, sends the access link by text message only to the complainant, the defendant, and their lawyers. No other person receives the link. This practice violates Article 352 of the Code of Criminal Procedure. Under the law, proceedings are presumed public unless an exception applies, such as cases involving sexual morality or national security. In current electronic proceedings, however, "non-publicity has become the default," because members of the public have no means of entering the hearing. This produces a form of "structural censorship." The judge does not need to issue an order closing the proceedings; the system itself keeps the doors closed by default (Reiling & Contini, 2022). Consequently, public oversight of significant cases, including major economic-corruption cases previously attended by journalists, disappears in the online environment.

B. The Challenge Faced by Journalists and Judicial Observers

The media constitute the fourth estate and serve as the eyes and ears of society in the courts. In a physical court, journalists present their identification cards and enter the courtroom. In a virtual court, however, verification of a journalist's identity is more complex. How is a journalist to learn the time of the hearing or obtain the access link? If the journalist enters, may the judge "remove" that person from the session? On many current platforms, an increase in participants reduces audio and video quality. The judge may therefore remove journalists under the pretext of "preventing internet disruption." This technological power to exclude observers is more dangerous than formal legal authority because it is justified on technical grounds and is difficult to challenge.

C. Discrimination in Access

Even when a court link is published on a public website, as in pilot live-streaming schemes, the principle of publicity remains affected by the "digital divide." Publicity must be "inclusive." In a traditional court, even an elderly rural resident could enter and observe. In an online court, however, the observer requires high-speed internet, a smartphone, and digital literacy. Judicial oversight may therefore become limited to the "urban middle and affluent classes," while the voices of poor and marginalised people, who are disproportionately represented among criminal defendants, remain unheard (Reiling & Contini, 2022). "Digital publicity" may thus result in a form of "judicial elitism."

D. Absence of a Unified Hearing-Information Portal

In leading jurisdictions, a daily list of court hearings, accompanied by public links, is published on judicial websites. In Iran, neither the Sana system nor the case-management system provides such a public output. This deficiency constitutes a principal barrier to transparency. Citizens do not know which hearings are being held on a given day and therefore cannot seek to attend them. Transparency requires "active disclosure," not merely "the absence of obstruction." As long as hearing calendars remain confidential or inaccessible, electronic proceedings will remain effectively non-public.

2.3.2. The Risk of Unlawful Recording and Selective Dissemination of Hearings Online

In physical courts, mobile phones and cameras are generally prohibited unless specific authorisation is granted. This restriction allows the judge to retain control over the court's "media output." In an online hearing, however, defendants, complainants, witnesses, and observers participate from their own homes, where no one can physically search them.

A. The Phenomenon of "Fragmented Justice"

The most harmful consequence is the selective publication of video clips. Social-media users tend to prefer sensational clips rather than lengthy legal arguments (Donoghue, 2020). The viral dissemination of such excerpts may condemn the defendant before judgment and, by inflaming public opinion, place severe pressure on the judge's independence.

B. Violation of the Privacy of Witnesses and Victims

In sensitive cases, no effective guarantee prevents the covert recording of an online hearing and its subsequent dissemination for retaliatory purposes. This risk may deter victims from filing complaints, because current platforms lack effective technical mechanisms for preventing screen recording and therefore contain a substantial security vulnerability (Ghane & Zarei, 2022).

C. Transformation of the Court into a "Media Circus"

The possibility that the hearing will be recorded may encourage lawyers to replace legal advocacy with "populist speeches," reducing proceedings from a process of "truth-finding" to one of "content production" (Khaloui Tafti & Aghaabbasi, 2021). This dramatic environment destroys the solemnity necessary for fair adjudication.

D. Difficulties in Enforcing Criminal Sanctions

Although the Note to Article 353 of the Code of Criminal Procedure criminalises the publication of trial proceedings before the judgment becomes final, identifying the person responsible for dissemination, particularly online, is extremely difficult (Mansourabadi & Foroughi, 2016). Such conditions demonstrate the inability of existing laws to respond to the speed of digital publication, because the destructive effects of a "trial by public opinion" are considerably more severe and irreversible than the penalties imposed by law.

2.3.3. *Conflict between “Live-Streaming the Trial” and “Protecting the Defendant’s Reputation”*

Modern criminal law is founded upon the principles of the “personal character of punishment” and the “protection of human dignity.” Even when a person is guilty, his or her reputation and that of the family remain protected, except in narrowly defined legal circumstances. The internet, however, is a merciless, global, and permanently remembering environment. Live-streaming a hearing may subject the defendant to trial and destruction in the “court of public opinion” before a final judgment has been issued.

2.3.4. *Verification of Participants’ Identities in Virtual Hearings*

In a traditional courtroom, identity verification is a simple physical process. In a virtual court, however, the judiciary deals with “data.”

A. Ineffectiveness of Passwords

Text-message login or password-based access to judicial platforms such as Skyroom proves only that “the user knows the password,” not that “the user is the authorised person.” A defendant may transfer the password to a third party, such as an unauthorised legal representative or debt collector, and exploit poor webcam quality and the judge’s unfamiliarity with the defendant’s appearance to deceive the court. This may constitute a clear instance of “unauthorised legal representation.”

B. The Emerging Threat of Deepfakes in Judicial Proceedings

More dangerous than physical substitution is the live artificial-intelligence manipulation of the defendant’s face and voice through deepfake technology. The inability of judges and current case-management systems to distinguish an “intelligent avatar” from a “real human being,” particularly in cybercrime cases, may undermine the integrity of the entire proceeding.

C. The Challenge of Continuous Authentication

Initial identity verification does not prevent the covert substitution of another person, such as an expert, during the hearing. The absence of biometric technologies, including continuous facial or iris processing, capable of providing “continuous authentication” and immediately alerting the judge when the person in the camera frame changes, makes lengthy electronic hearings highly vulnerable.

D. Legal Gaps concerning the Consequences of Virtual Identity Fraud

Unlike physical proceedings, the law remains silent regarding the status of a judgment, including whether it is void or should be treated as a judgment in absentia, when virtual identity fraud is discovered after the decision has been issued. Moreover, in the absence of accurate biometric logs, claims such as “it was not me; the system had been hacked” make technical proof of fraud extremely difficult and create opportunities to evade punishment.

2.4. *Challenges to Defence Rights and Equality of Arms*

The principle of “equality of arms” requires that each party be afforded a reasonable opportunity to present evidence without being placed at a “substantial disadvantage” (Skundric, 2023). In electronic proceedings, defensive capacity no longer consists solely of legal knowledge; it also includes “internet bandwidth,” “webcam quality,” “communication software,” and “access to data” (Peloso, 2024). The infrastructural superiority of a state prosecutor over an ordinary defendant transforms the “digital divide” directly into a “justice divide,” because superior communication quality may unconsciously influence the judge’s perception of the parties’ arguments in favour of the prosecutor. In addition to technical inequality, the integrated recording functions of platforms and the absence of a “secure channel” for confidential consultation between lawyer and client paralyse the right to an “effective defence” and leave the defendant unprotected against unexpected questions (Reiling & Contini, 2022). These obstacles may transform the process into “one-sided adjudication” serving state authority.

2.4.1. *Restrictions on Private Lawyer–Client Consultation during an Online Hearing*

The lawyer–client relationship is founded upon trust and confidentiality. During a hearing, moments arise in which counsel must immediately intervene and tell the client, “Do not answer that question,” or “Explain this point.” In a physical courtroom, this may be achieved by whispering into the client’s ear or touching the client’s hand. In an online court, however, this “real-

time communication” is severed and no secure alternative is provided. On the videoconferencing platforms commonly used by the Iranian judiciary, all participants occupy a single “audio room.” Every word spoken is heard by the judge, the prosecutor, and the opposing party. This condition may be described as “defensive exposure” (Reiling & Contini, 2022). If counsel attempts to advise the client during the hearing, everyone can hear the communication, resulting in the disclosure of defence strategy.

2.4.2. *Internet Disconnection as an Obstacle to an Effective Defence*

In virtual proceedings, internet instability affects the vital artery of the court. Interruptions in audio and video transmission disrupt the coherent rhythm of the defence, prevent timely objections, and unfairly impose the consequences of deficient national infrastructure upon the defendant. At the same time, processing communication through a screen requires additional cognitive energy and produces “Zoom fatigue.” The resulting mental and physical exhaustion encourages judges to rely on cognitive shortcuts, terminate hearings prematurely, and resort to stereotypical judgments. Beyond technical and physical harm, the intervening screen reduces the defendant from a suffering human being to a pixelated frame, creating conditions for distraction and “moral numbness.” By generating emotional blindness and eliminating human empathy, this dangerous condition may make it psychologically easier for judges to impose severe sentences and may sacrifice the human spirit of adjudication to speed and automation.

2.4.3. *Inequality of Technical Resources between the State Prosecutor and the Ordinary Defendant*

Equality of arms requires the parties to contest the case under equal conditions. In electronic proceedings, however, one party, the prosecutor, possesses an arsenal of technology, whereas the other, the disadvantaged defendant, enters the process empty-handed and equipped with defective tools. This “infrastructural inequality” shifts the neutrality of proceedings in favour of the state (Peloso, 2024).

Psychological research indicates that people unconsciously evaluate individuals with poor audio and video quality as “less intelligent,” “less trustworthy,” and “less important” (Williams, 2021). In an online court, the prosecutor connects from an office in the prosecution service using high-speed access to the National Justice Network, an HD webcam, a professional microphone, and appropriate lighting. The prosecutor’s voice is clear and the image authoritative. The defendant may connect from a prison booth or a rural home. The image may be dark and pixelated, the voice distorted, and the audio affected by echo. This difference in quality creates a “perceptual bias” in the judge’s mind. The prosecutor’s submissions sound “clear” and “logical,” whereas the defendant’s arguments appear “ambiguous” and “irritating” because of background noise. The judge must expend effort to understand the defendant but can understand the prosecutor easily. Under the principle of “processing fluency,” the mind tends to regard information that is easier to process as more credible (Williams, 2021).

During a hearing, the parties may need to examine a large file, such as closed-circuit television footage. Because the prosecutor is connected to an internal server, the file can be opened and displayed immediately. If defence counsel wishes to present a similar file, it must first be uploaded. Where the lawyer’s internet connection is weak, the upload may take ten minutes or fail altogether. This technical inability places counsel at a disadvantage. The lawyer may be compelled to state, “I will submit a written brief later,” thereby losing the opportunity to influence the hearing immediately. Such inequality in access to data disturbs the balance of proceedings.

Many defendants participate in online hearings from prison. Their connection environment is not “neutral.” They are commonly seated in a small room, wearing handcuffs and prison clothing, while a prison officer stands over them outside or partially within the camera frame. Prison noise, shouting, and loudspeakers interfere with their concentration. This is an “environment of intimidation.” The defendant cannot speak freely for fear of subsequent retaliation by prison officers. By contrast, the prosecutor sits in a safe and comfortable office. This asymmetry in the “security of the connection environment” restricts the defendant’s freedom of expression.

3. Strategies for Safeguarding Fundamental Principles at the Trial Stage

In its present form, electronic criminal adjudication is less a “substantive transformation” toward modern justice than a “hastily implemented formal change” in which procedural principles such as presence, publicity, and defence have been sacrificed to technical and infrastructural limitations. What, then, is the appropriate solution? The strategies proposed in this section are founded upon the doctrine of the “hybrid model.” Under this model, electronic adjudication is accepted not as an “absolute substitute” for physical proceedings but as a “complementary mechanism” subject to strict conditions.

3.1. Strategies for Safeguarding Defence Rights

The first priority in any reform must be the “empowerment of the defence.” These strategies begin with the “right to choose the form of proceedings” and extend to the provision of “technical tools for lawyer–client consultation.”

3.1.1. Making Online Hearings Conditional upon the Defendant’s “Express Consent”

Several important strategies may be proposed in this regard.

Changing the Default from Compulsion to Choice: The first step toward legitimising electronic adjudication is to make it conditional upon the “free will” of the parties, particularly the defendant. In legal philosophy, the defendant is a “party” to the proceedings, not their “object.” Imposing an online hearing on a person who cannot adequately articulate a defence in the virtual environment therefore constitutes a clear “deprivation of the right of defence” (Reiling & Contini, 2022).

Proposed Amendment to Article 659 of the Code of Criminal Procedure: The law should make virtual hearings conditional upon the defendant’s “express and written consent” and should prohibit the undesirable practice of interpreting “silence as consent.” The court must be required to hold an in-person hearing whenever the defendant or counsel declares that the virtual format interferes with an “effective defence,” except in circumstances of force majeure.

Eliminating “Systemic Compulsion” in Scheduling: The hidden threat that an in-person hearing will be scheduled substantially later than an immediate online hearing undermines the consent of a detained defendant. By prohibiting significant differences in scheduling, the judiciary must ensure that those requesting physical proceedings are not subjected to a temporal penalty.

A Graduated Approach Based on the Seriousness of the Offence: To balance “system efficiency” and “defence rights,” electronic adjudication may be treated as the default only for minor offences classified in degrees 7 and 8. In serious offences, including those punishable by more than two years’ imprisonment, the defendant’s right to choose physical attendance must be treated as an absolute condition.

Guaranteeing a “Right of Withdrawal” during the Hearing: The defendant’s initial consent must not be treated as irrevocable. If infrastructural problems, including poor audio or video quality, prevent the presentation of documents or mutual understanding between the judge and the defendant, the defendant must have the right to request an adjournment and conversion of the hearing to an in-person format. Deficiencies in public infrastructure must not be compensated for by imposing an “incomplete defence” upon the accused.

3.1.2. Creating “Virtual Waiting Rooms” and “Consultation Rooms” for Lawyers and Clients

Software-architecture reform requires movement beyond basic video communication toward a “virtual judicial complex.” Several important strategies may be proposed.

Creation of a “Virtual Booth” for Confidential Consultation: The principal weakness of electronic adjudication, namely the absence of private space for lawyer–client consultation, requires intervention in “software architecture” and a transition from simple video-call platforms to a “virtual judicial complex.” The case-management system should permit the immediate transfer of counsel and the client to an isolated, doubly encrypted, and strictly non-recordable space. The relevant button would serve as the digital equivalent of a “request for an adjournment to consult” in a physical courtroom, and judicial approval should be mandatory.

Designing a “Virtual Waiting Environment”: Replacing the physical court corridor with a digital waiting room would prevent the simultaneous and disorderly entry of users into the principal hearing link. Before the formal commencement of the

hearing, this environment would permit technical testing of internet connections and microphones, final coordination of defence submissions, preliminary review of documents, and initial identity verification by the court clerk. It would also significantly reduce the defendant's anxiety.

Private Chat and a Guarantee of “Automatic Deletion”: Court software should include a “note-sending tool,” consisting of a private chat function available exclusively to lawyer and client. To prevent violations of professional confidentiality, these written communications must never be retained in the judiciary's server logs. A technical guarantee that the messages will be “automatically deleted” at the end of the hearing is a fundamental condition for trust in the system.

Changes in Judicial Practice and Technical Training: Software capabilities alone are insufficient. These tools must be recognised as a “settled defence right,” rather than an impediment that wastes time. A directive issued by the Judiciary's Legal Department should require judges to respect this right, while technical-training programmes should enable lawyers to use these functions effectively and without unnecessary delay.

3.1.3. *Guaranteeing the Right to Physical Presence in Cases Involving Severe Punishment*

Virtual adjudication should not constitute a uniform procedure applicable to all offences. In modern law, procedural safeguards must be proportionate to the seriousness of the offence and the degree of risk faced by the defendant ([Hungerford-Welch, 2024](#)). Conducting online trials in cases involving a person's life or long-term liberty amounts to gambling with justice and impairs the judge's attainment of the “psychological certainty” required in offences such as murder.

Proposed Regulatory Amendment and Statutory Prohibition: Electronic-proceedings regulations should be amended to prohibit virtual trials absolutely in offences punishable by deprivation of life, life imprisonment, amputation, first- to third-degree discretionary imprisonment exceeding ten years, and political or press offences, except in narrowly defined circumstances such as the defendant's presence abroad or the outbreak of an infectious disease.

Technology's Inability to Evaluate Complex Evidence: Adjudication of serious crimes requires the meticulous assessment of evidence, including crime-scene reconstruction, examination of the alleged weapon, and face-to-face confrontation with witnesses. Because videoconferencing is inherently incapable of conveying the “sensory atmosphere” of the hearing, including the trembling of the defendant's voice, even hybrid systems should require that certain stages, such as the “final defence” and the “testimony of key witnesses,” be conducted in person. A human being's fate must not depend upon internet bandwidth.

Preventing the Reduction of Judicial Sensitivity: The small monitor frame and physical distance may psychologically reduce the judge's sensitivity and prevent an understanding of the seriousness of the harm or the development of “human empathy.” Requiring physical attendance confronts the judge with the full gravity of the case, including the presence of the victim's family and the defendant, and with the real dimensions of judicial responsibility, thereby promoting meticulous decision-making.

Preserving the Legitimacy of the Judiciary and Public Order: In serious offences, physical presence should be treated as a “mandatory requirement,” not a “waivable right.” Contrary to the position adopted by some scholars ([Beiki Shouraki & Fallah, 2024](#)), even when the defendant consents to an online trial, criminal proceedings involving grave offences should remain physical. This preserves “public order,” demonstrates the solemnity and seriousness of the judiciary, prevents the perception that proceedings are being conducted superficially, and strengthens public confidence in severe judgments.

3.1.4. *Requiring Courts to Make Complete Audio and Video Recordings for Review*

One of the greatest contradictions in electronic proceedings is continued reliance upon a “written record of the hearing,” which reflects the clerk's selection, interpretation, and potential human error, rather than upon the “recorded reality.” In the digital age, the video file should itself constitute the official record of the hearing so that the defendant's tone, pauses, and precise statements remain protected against distortion.

Changing the Paradigm through Legislative Reform: Addressing this challenge requires the adoption of a provision in the Code of Criminal Procedure stating: “In electronic proceedings, the audio and video file shall constitute an integral part of

the criminal case file, and in the event of inconsistency with the typed record, the recording shall prevail and possess superior evidentiary authority.”

Fundamental Transformation of Judicial Supervision: Recording hearings would enable appellate courts and the Supreme Court to observe directly the psychological conditions of the hearing, including pressure exerted upon the defendant, the conduct of the trial judge, or the precise moment of a confession, rather than relying exclusively on written documents (Khaloui Tafti & Aghaabbasi, 2021). Awareness among trial judges that their conduct is subject to this form of “superior visual supervision” would improve judicial behaviour and safeguard defence rights.

An Artificial-Intelligence Solution to Technical Problems: To address the large volume of video recordings and the difficulty of searching them, the judicial case-management system should incorporate Persian “speech-to-text” technology. By automatically transcribing the proceedings and linking each word to the corresponding point in the video, the system could permit keyword searches, such as for the word “knife,” and direct access to the precise second at which the word was spoken. This approach would combine the accuracy of video with the speed of textual search.

Guaranteeing Equality of Arms in Access to the Record: Current practices that deny defendants copies of the hearing video on privacy or security grounds impair defence rights. The defendant and counsel should have access to the video as one of the “most important documents in the case,” enabling them to draft defence submissions and appeals with precise references to timestamps. A proposed solution is to provide lawyers with “read-only” or “watermarked” access through their online case dashboards, allowing them to review the hearing without permitting uncontrolled public dissemination.

3.2. *Strategies for the Supervision of Artificial Intelligence and Adjudication*

The strategies in this section are founded upon a new doctrine of “algorithmic accountability.” Under this doctrine, no algorithm should be used in a court unless it is “transparent,” “interpretable,” and “subject to human control.” The paradigm of “automated adjudication” must be replaced with one of “augmented intelligence,” in which artificial intelligence does not replace the judge but strengthens the judge’s analytical capacities (Schwarcz, 2025).

1 1-2-2. The “Human-in-the-Loop” Principle: Final Human Supervision of the Judgment

The “human-in-the-loop” principle is the cornerstone of artificial-intelligence ethics. It provides that, in sensitive decision-making processes, the machine must never have the “final word.” The decision-making cycle must always begin and end with a human being. In adjudication, this means that artificial intelligence may only make a “recommendation,” while the responsibility for “selection” and “signature” remains entirely with the judge (Schwarcz, 2025). To counter judges’ tendency to accept system recommendations passively because of convenience, the software should not provide a “rapid approval” button. Introducing such “deliberate friction” would require the judge to type the reasons for accepting an artificial-intelligence recommendation into a text field. This compulsory pause would move the judge out of “autopilot mode” and restore critical reflection.

Safeguarding Judicial Independence and Encouraging “Judicial Courage”: Judges must have the right to reject an artificial-intelligence recommendation without fear of disciplinary action or loss of points in performance-evaluation systems. Amending judicial-evaluation rules to award positive credit to judges who reject machine recommendations on reasoned grounds (Keykha & Ehsanifar, 2023) would encourage judges to resist potential algorithmic errors.

Statutory Prohibition of Fully Automated Adjudication in Criminal Matters: Unlike approaches adopted in certain jurisdictions for minor civil disputes, the issuance of a criminal judgment by a machine is inherently invalid because criminal adjudication requires the formation of an “inner conviction.” The Code of Criminal Procedure should expressly invalidate any judgment or order based entirely upon automated data processing without substantive human approval and classify such conduct as a disciplinary offence. Such a provision would create a barrier against the temptation of the “complete automation of justice.”

Requirement of a “Declaration of Responsibility”: To prevent judges from sheltering behind algorithms and being reduced to operators, each judgment should include a certification that the judge treated the intelligent system’s output solely as a form of “circumstantial evidence” and personally assumed final legal and ethical responsibility for examining the case.

3.2.1. *Making Judicial Algorithms Transparent and Permitting Challenges to Their Results*

Justice must not occur in darkness. If artificial intelligence affects the defendant's fate, the defendant has the right to know how it operates. The "black-box" problem must be addressed through "explainable artificial intelligence." Transparency is the antidote to algorithmic authoritarianism. Under fair-trial principles, every person affected by an algorithmic decision has the right to understand the "logic of that decision."

The technical solution is that judicial software must not merely produce an output. It must incorporate explainable-artificial-intelligence modules capable of translating the output into human language.

The legal solution is to require all judiciary software contractors to ensure that "decision-making or decision-support algorithms are open source or, at a minimum, available to an auditing panel selected from the Bar Association, the Lawyers' Centre, and academic institutions." Such "algorithmic auditing" would assure the legal community that the program code does not contain racial bias or logical error. Justice must not become a "secret formula."

3.2.2. *Prohibiting the Use of Artificial Intelligence in Sensitive Criminal Cases*

A principle of risk management provides that "where the cost of error is irreparable, automation must stop." Criminal proceedings include cases involving life, bodily integrity, and fundamental liberty, including retributive punishment, the death penalty, and life imprisonment. In such cases, even a 1% algorithmic error may produce an irreversible catastrophe. A fundamental strategy for safeguarding justice is therefore the "zoning of artificial-intelligence competence." The legislature should designate areas in which "algorithmic adjudication" is absolutely prohibited.

Under the European Union Artificial Intelligence Act, judicial systems are classified as "high-risk" (Kim, 2025). Iran should go further and establish a domestic classification of criminal cases.

Legal Strategy: An "Executive Regulation on the Classification of Judicial Artificial Intelligence" should establish the following three levels.

Green Level—Permitted: Traffic offences, municipal violations, and eighth-degree discretionary offences. Artificial intelligence may recommend a judgment.

Yellow Level—Conditional: Financial crimes and computer fraud. Artificial intelligence may act only as a search and research assistant and may not recommend a punishment.

Red Level—Prohibited: Offences against bodily integrity, including homicide and bodily injury, sexual offences, and political and security offences.

At the "red level," human, motivational, and ethical complexities are so extensive that no machine can understand them. From the perspective of legal philosophy, punishment constitutes a form of society's "moral condemnation" (Tadin, 2021). A machine cannot condemn because it possesses no moral agency. If artificial intelligence enters capital cases, there is a danger that death will become "bureaucratized." The system calculates, recommends execution, and the judge signs. Such a cold and mechanical process diminishes the moral gravity of taking a human life. In order to mitigate the use of capital punishment, the process of imposing a death sentence should remain "difficult," "time-consuming," and "filled with doubt" so that the principle of caution is respected (Ghorbani-Manqari, 2025). Artificial intelligence, which makes processes "easier" and "faster," is inherently inconsistent with the requirements of serious criminal adjudication. Its prohibition therefore functions as a safety mechanism against hasty executions.

3.2.3. *Continuous Monitoring of Algorithms to Eliminate Discriminatory Bias*

Even if artificial intelligence is transparent and remains under human supervision, a technical problem known as "algorithmic drift" persists. A system that is fair today may become discriminatory in the following year because of changes in input data or social conditions (Vaccaro, 2019). Digital justice is not a static condition but a dynamic process requiring continuous "maintenance" and "monitoring." Oversight cannot be entrusted to software manufacturers that possess a direct financial interest.

Structural Strategy: An independent interbranch body should be established, comprising senior Supreme Court judges, data-science and artificial-intelligence specialists, representatives of the Bar Association or Lawyers' Centre, and sociologists.

Its responsibilities should include periodically testing all judicial software, determining whether algorithms have developed biases against women or religious and ethnic minorities, and issuing either a licence for “continued operation” or an order for the “immediate suspension” of defective systems. The Centre for Monitoring the Implementation of the Judicial Transformation should serve as the committee’s executive arm and publish quarterly transparency reports for the public.

Operational Strategy: A reporting portal should be created within the Adl Iran system so that lawyers and researchers can report “suspicious algorithmic behaviour.” This would constitute “participatory oversight.” If ten lawyers report that a system is biased in criminal maintenance cases, the supervisory committee should be legally required to review the relevant code. The legal community would thereby become a network of “digital-justice monitors.”

3.3. *Technical and Structural Strategies*

Just as the state and the judiciary allocate funds for the construction of courthouses and associated institutions, they must invest in the twenty-first century in constructing the “digital infrastructure of justice.”

3.3.1. *Creating a National Court-Livestreaming Portal with Anonymisation Capabilities*

The conflict between the “publicity of proceedings” and the “protection of privacy” in cyberspace is among the most significant challenges confronting judicial transparency. The solution lies neither in completely blocking access nor in the unrestricted dissemination of information, but in establishing a system of “filtered transparency” through emerging technologies. A dedicated centralised platform with the following capabilities is therefore proposed.

Transition from General-Purpose Platforms to a Dedicated Centralised Portal: Instead of using general platforms such as Skyroom in a fragmented manner, the judiciary should design a dedicated national portal in which artificial intelligence performs the role of a “broadcast supervisor.” The publication of a daily searchable list of public hearings, combined with graduated levels of access, including comprehensive access for authenticated journalists and researchers and observer access for the public, would enable integrated content management and prevent the unauthorised dissemination of hearing links.

Real-Time Blurring Technology to Protect Identity: The technical core of this approach would involve the use of artificial-intelligence and facial-recognition algorithms to blur or pixelate automatically the faces and alter the voices of defendants, complainants, and witnesses, while leaving the images of public officials, including judges and prosecutors, unobscured. Such technology would permit compliance with the principle of publicity while protecting human dignity and personal reputation.

Introducing a “Time Delay” as a Safety Mechanism: As in the live transmission of sporting events, a short delay, such as two minutes, should be introduced into public broadcasts of online hearings to address security and ethical risks. During this interval, a “broadcast supervisor,” whether a human operator or an artificial-intelligence system capable of processing words, could monitor the content and activate a mute or “bleep” function where unexpected events occur, including insults or the disclosure of confidential information. This would ensure that transparency does not become public humiliation.

Dynamic Watermarking to Prevent Unlawful Dissemination: A viewer-specific identifier, such as a national identification number or IP address, should appear faintly and move across the broadcast image. This would create a powerful deterrent against unlawful recording and selective editing. By enabling the rapid identification of individuals who publish court recordings on social media, this technology would enhance observer accountability and prevent court proceedings from becoming sensational online content.

3.3.2. *Increasing the Dedicated Bandwidth of the Justice Network to Prevent Disconnection*

Internet disruption or instability in a virtual court is equivalent to depriving the defendant of the right of defence and “expelling the defendant from the hearing.” Because the state is responsible for providing the infrastructure of adjudication, four principal strategies are proposed.

Creating a Dedicated Tunnel within the “National Information Network”: Court audio and video data should be transferred from the public internet to an isolated, high-speed internal network based on fibre-optic infrastructure. This would ensure image quality and very low latency while minimising the risk of cyber intrusion, in line with the programmes of the

Centre for Monitoring the Implementation of the Judicial Transformation ([Center for Monitoring the Implementation of the Judicial Transformation, 2024](#)).

Applying Quality-of-Service Rules and “Priority for Judicial Traffic”: Where the public internet is used, operators should be required to prioritise court data packets. Adjudication is a “vital public service,” and its data should receive the same priority in internet traffic that an ambulance receives on the road.

Making Court-Hearing Data Free of Charge as a Measure of Economic Justice: To reduce inequality and implement paragraph 9 of Article 3 of the Constitution concerning the elimination of unjust discrimination, the Ministry of Information and Communications Technology should be required to exempt complainants, defendants, and lawyers from all data charges incurred when participating in court hearings.

Provision of “Backup Internet” and “Mirror Servers”: To guarantee “availability” as a key component of cybersecurity, court branches should be equipped with modems capable of automatically switching to cellular internet. Mirror servers should also be established in data centres located in different provinces so that, if the central server fails, hosting of the hearing can be transferred without interruption.

3.3.3. *Multi-Stage Biometric Authentication for Access to Virtual Courts*

Because criminal proceedings concern life, liberty, and reputation, the reliability of “identification” should approach 100%. The technical solution is to move beyond traditional usernames and passwords and establish “live biometric authentication.” The system must ensure that the person seated before the monitor not only “knows the password” but “is the authorised person” and, most importantly, is a “living human being” rather than a mask or recorded video ([Omotoye, 2021](#)). The most serious contemporary security threat is the use of artificial intelligence to generate synthetic faces. To counter this threat, the court case-management system should include a live-biometric-authentication module.

3.3.4. *Establishing Specialised Electronic-Court Branches with Standardised Equipment*

One reason electronic proceedings have failed in certain cases is the attempt to conduct virtual hearings in “traditional rooms.” The judge sits behind a desk covered with paper files, sunlight reflects from a window onto the monitor, the laptop webcam is poor, and air-conditioning noise echoes through the microphone. Such an environment undermines the solemnity of the court. The technical solution is to redesign judicial architecture and create “studio-courts.”

Specialised electronic branches should not resemble administrative offices; they should be designed as “live-broadcast studios.” “Judicial solemnity” must be reproduced in cyberspace ([Jain & Chaudhary, 2021](#)). When a judge appears with a dark image and distorted audio, the defendant’s confidence in the “authority of justice” diminishes. The studio-court restores this visual authority.

A judge is a legal professional, not an information-technology engineer. In a traditional court branch, the office manager performs administrative tasks. Electronic branches require a new institutional position known as the “technical branch manager.” This person should sit beside the judge, outside the camera frame, and perform the following functions:

- Managing internet connections and resolving technical problems experienced by the parties.
- Displaying documents on screen at the judge’s direction.
- Managing waiting rooms and organising groups of lawyers.
- Monitoring security alerts and identity verification.

The Centre for Monitoring the Implementation of the Judicial Transformation emphasises the need to improve employees’ digital literacy ([Center for Monitoring the Implementation of the Judicial Transformation, 2024](#)). In practice, however, judges should not be occupied with “muting and unmuting microphones.” Their attention must remain entirely focused on “justice,” while the technical burden is assumed by a specialist assistant.

3.4. Comparative Study and International Experience

Leading jurisdictions within the common-law tradition, including Canada and Australia, and the Romano-Germanic tradition, including France, are moving toward a “hybrid model” in which technology is treated as a “facilitator” rather than a “substitute.” Comparative analysis is essential for the Iranian legislature as it continues to implement and develop the Judicial Transformation Document in the field of electronic criminal proceedings.

3.4.1. Online-Court Experience in Australia and Canada: The Hybrid Model

Australia and Canada, as common-law jurisdictions characterised by extensive territory and dispersed populations, have been pioneers in the use of technology to improve access to justice. Their experience nevertheless demonstrates that, following the COVID-19 pandemic, they have undertaken an intelligent return to “physical presence in sensitive cases.”

In the Australian states of New South Wales and Victoria, the traditional concept of the court has changed. Instead of eliminating the physical courtroom, these jurisdictions have “distributed” it (Rossner et al., 2021). Under this model, the judge remains physically present in the courtroom to preserve the solemnity and formality of the proceedings, while other participants, including lawyers, witnesses, and defendants, may connect from different locations. A central feature of Australian law is the clear distinction between “procedural hearings” and “substantive hearings.” Case-management hearings, extensions of detention, and notices of representation are presumed to occur online. Hearings involving serious offences and witness testimony are presumed to occur in person. Australian superior courts have repeatedly emphasised that “assessing witness credibility” through a monitor is difficult and that a court should not refuse a defence request for the witness to appear physically merely on grounds of efficiency (Rossner et al., 2021). This is precisely the missing element that should be incorporated into Iranian law: the “priority of accurate fact-finding over procedural speed.”

Canada possesses an even richer body of experience. Following the COVID-19 pandemic, Canadian courts faced a large number of requests to continue “Zoom proceedings.”

In the well-known case of *R. v. Kahsai* (2023), an Ontario court issued a decision that has been regarded as an important international standard. The defendant argued that online proceedings had prevented effective communication with counsel. The court held that although technology is useful, the “right to a fair trial” includes the right to “immediate and private communication” with counsel, a right not fully realised through the Zoom platform (Netolitzky, 2024).

Current Canadian practice is moving toward “hybrid adjudication.” The complainant and the defendant attend court physically, whereas an expert witness, such as a forensic physician with limited availability, may participate online. This model balances “saving the expert’s time” with “respecting the defendant’s defence rights.” Canada’s principal lesson for Iran is that proceedings need not be treated as a binary choice between entirely online and entirely physical formats; an intelligently designed combination is possible.

3.4.2. The Council of Europe’s CEPEJ Approach to the Ethics of Artificial Intelligence in Adjudication

In 2018, the Council of Europe and its European Commission for the Efficiency of Justice adopted a historic instrument entitled the “European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems.” This was the first comprehensive international instrument to recognise the dangers of the “algorithmic judge” and establish a framework for controlling them. It now serves as an important foundation for European policy and legislation (Mihajlović, 2025). The Charter is based upon five fundamental principles that every intelligent judicial system should respect. Examination of these principles demonstrates that concerns raised in this article, including black-box opacity and discrimination, are global.

The first is the “principle of respect for fundamental rights.” Artificial intelligence must not be designed solely to achieve “efficiency.” An algorithm that increases speed but restricts defence rights should not be used. Justice takes priority over speed. This principle corresponds directly to the present article’s concern with preserving the principles of criminal law in electronic proceedings.

The second is the “principle of non-discrimination.” It directly addresses the problem of “biased data.” The Charter emphasises that states must audit every algorithm before deployment to ensure that it does not discriminate against vulnerable groups.

The third is the “principle of quality and security.” Judicial data must be stored on secure servers. Public cloud services should not be used indiscriminately for processing confidential judicial files. This principle corresponds to the proposed use of a national judicial intranet in Iran.

The fourth is the “principle of transparency, impartiality, and intellectual fairness.” This is the most important principle for addressing the “black-box” problem. The defendant has the right to know whether artificial intelligence has been used in the case and, if so, to understand its logic. The concept of “explainability” emerges from this principle.

The fifth is the “principle of user control,” which corresponds to the “human-in-the-loop” principle. The Charter provides that the judge must always possess the power to “override” an artificial-intelligence recommendation and must not be compelled to accept the machine’s conclusion (Mihajlović, 2025).

The Charter classifies artificial-intelligence tools into four categories:

Encouraged: Tools for searching judicial precedent, anonymising judgments, and managing schedules.

Neutral: Automated text-generation tools, subject to supervision.

Subject to Strict Caution: Tools for predicting case outcomes and calculating the risk of recidivism.

Prohibited: Tools that replace the judge’s conscience (Mihajlović, 2025).

Iran’s Judicial Transformation Document should adopt a similar classification. All forms of artificial intelligence should not be treated alike. Using artificial intelligence to transcribe a judgment may be highly beneficial, whereas its use to determine punishment should fall within the categories of “strict caution” or “prohibition.”

3.4.3. *French Rules on the Publicity of Proceedings Conducted by Videoconference*

The French legal system, as a leading jurisdiction within the civil-law tradition and a historical influence on Iranian law, has adopted a cautious and “human-rights-centred” approach to electronic proceedings. Whereas some common-law jurisdictions moved toward internet livestreaming, France adopted a different model described as the “physical extension of the courtroom,” seeking to preserve publicity while protecting privacy and judicial dignity (Peloso, 2024).

During the COVID-19 pandemic, the French government issued an ordinance authorising courts to conduct hearings online without the defendant’s consent. The French Bar challenged the ordinance, and the matter was referred to the Constitutional Council. In January 2021, the Council issued a landmark decision holding that the “compulsory use of videoconferencing in serious criminal proceedings, even during a public-health emergency, was unconstitutional.” It reasoned that the defendant’s physical presence before the judges forms part of the “right of defence,” which the state may not remove on grounds of “public health” or “technology” (Peloso, 2024).

The lesson for Iran is that technological efficiency has a boundary, and that boundary is determined by constitutional principles. Iran should not disregard the right to presence in serious offences merely to reduce transportation costs.

3.4.4. *The Jurisprudence of the European Court of Human Rights on Virtual Proceedings*

The European Court of Human Rights in Strasbourg is the final interpreter of the European Convention on Human Rights. Article 6 of the Convention, which guarantees the right to a fair trial, bears substantial similarity to Article 35 of the Iranian Constitution. The Court’s judgments concerning videoconferencing have created an international standard for assessing the legitimacy of online courts in terms of compliance with criminal-justice principles. Several significant cases are considered below.

A. *Marcello Viola v. Italy*: The Equivalence Standard

This 2006 case is a foundational authority concerning electronic proceedings. Mr Viola, a mafia leader, was tried by videoconference because of security risks. He complained that the procedure was unfair. The Court held that videoconferencing does not inherently violate human rights, provided that it serves a legitimate purpose, such as security, order, or efficiency, and satisfies the condition of equivalence. The defendant must be able to see and hear the court in substantially the same manner as if physically present (Ažubalytė & Titko, 2022).

B. Sakhnovskiy v. Russia: The Right to Confidentiality

In this 2010 case, a Russian defendant was tried by videoconference. He sought to consult with his lawyer, but prison guards were present in the room and the microphone remained open.

The Court held that Article 6 of the Convention had been violated. It reasoned that the right to legal representation includes the right to “confidential communication.” If videoconferencing technology cannot provide a secure and private line for lawyer–client communication, its use is unlawful (Ažubalytė & Titko, 2022).

C. Grigoryevskikh v. Russia: Responsibility for Technical Failure

In this case, the court’s internet connection repeatedly failed, and the defendant could not hear the witness’s testimony. The judge disregarded the problem and proceeded to judgment. The Court held that the state is responsible for the infrastructure and that failure to provide a stable connection does not excuse the violation of defence rights (Ažubalytė & Titko, 2022). In Iran, where failure of the case-management system prevents counsel from submitting a brief or presenting a defence, the defect should constitute a ground for reopening the proceedings or quashing the judgment. A judge cannot simply state that “the system failed and the defendant was unfortunate.” Responsibility for system failure rests with the state.

4. Conclusion

The introduction of communication technologies and intelligent algorithms into criminal proceedings constitutes more than a change of instruments; it represents a profound transformation in the “nature and psychology of adjudication.” This study demonstrated that reducing the court from a solemn physical institution to a “videoconference link” creates risks of emotional blindness, psychological distancing, and the weakening of the principles of presence and confrontation. At the same time, transferring judicial logic to machines exposes fair trial to the dangerous phenomena of “black-box justice” and hidden bias, directly violating the requirement that judgments be reasoned and undermining the human independence of the judge. Technology must not become the “actor of adjudication”; it must remain an assistant placed at the service of human dignity and the fundamental principles of criminal law. The appropriate response to this crisis is the adoption of a “human-centred hybrid model.” The legitimacy of electronic criminal proceedings at the trial stage depends upon their optional character for the defendant and the guarantee of effective defence. Internet disconnection in a virtual hearing is equivalent to expelling the defendant from a physical courtroom. The provision of dedicated infrastructure, including a judicial tunnel within the National Information Network and priority treatment for judicial data traffic, should therefore be regarded not as a convenience but as an undeniable sovereign obligation. The conflict between publicity and privacy in cyberspace can be resolved only through centralised platforms equipped with “filtered-transparency” technologies, including real-time blurring and delayed broadcasting. In dealing with artificial intelligence, the “human-in-the-loop” principle and the incorporation of “deliberate friction” into judicial software are necessary to restore the judge from the status of a passive operator to that of a courageous and accountable decision-maker. Ultimately, electronic criminal adjudication can become a new manifestation of fairness only when software code and internet bandwidth do not undermine equality of arms and when the spirit of adjudication remains alive within its digital form. Otherwise, this transition will amount to nothing more than the mechanisation of injustice.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

- Akhundi, M. (2015). *Understanding Criminal Procedure*. Dourandishan Publications.
- al-Hilli, J. i. a.-H. (1994). *Shara'i al-Islam fi Masa'il al-Halal wa al-Haram* (Vol. 4). Ismailian Institute.
- Amiri, A. (2023). *Criteria for Evaluating Judges' Conduct and Performance in the Judges' Disciplinary Prosecutor's Office*. Tasir Publications.
- Asadi, M. (2024). *Principles of Fair Trial in Islam, Contemporary Human Rights, and Iranian Laws*. Hekmat Gostar Publications.
- Ashouri, M. (2023). *Criminal Procedure* (8th ed.). Organization for Researching and Composing University Textbooks in the Humanities (SAMT).
- Ažubalytė, R., & Titko, I. (2022). Remote Criminal Trial—Fair Trial? *International Comparative Jurisprudence*, 8(2).
- Bazgir, Y. (2010). *Substantive Decisions of the Supreme Court in Civil and Criminal Matters*. Javidaneh Publications.
- Beiki Shouraki, M., & Fallah, M. R. (2024). Necessary Changes in Judicial Structure, Organization, and Institutions for Implementing Electronic Proceedings. *Quarterly Journal of Cyberspace Legal Studies*, 10(8), 30-40.
- Brayne, S. (2020). *Predict and Surveil: Data, Discretion, and the Future of Policing*. Oxford University Press.
- Center for Monitoring the Implementation of the Judicial Transformation, D. (2024). *Judicial Transformation and Excellence Document: The Second Step of Judicial Transformation*. Majd Publications.
- Donoghue, J. (2020). The Rise of Digital Justice: Courtroom Technology, Public Participation and Access to Justice. *Modern Law Review*, 80(6), 995-1025.
- Ghafouri, M. R. (2013). *Judicial Reasoning in the Two Major Formalist and Realist Legal Systems*. Majd Publications.
- Ghane, R., & Zarei, T. (2022). Improving Fair Trial Performance by Identifying and Removing Existing Barriers to the Development of Electronic Proceedings. *Quarterly Journal of Legal Civilization*, 5(12), 289-317.
- Gholamlou, J. (2019). *Conviction of the Innocent: An Interdisciplinary Approach to Criminal Evidence*. University of Tehran Press.
- Ghorbani-Manqari, M. (2025). *Capital Punishment and Strategies for Its Mitigation in the Legal System*. Amouzad Publications.
- Hayat Poursofii, M. (2021). *Electronic Proceedings in Iranian Criminal Law*. Sanjesh va Danesh Publications.
- Hungerford-Welch, P. (2024). *Criminal Procedure and Sentencing*. Routledge.
- Jain, R., & Chaudhary, S. (2021). The Renaissance of Virtual Courts: Towards the Digital Age. *International Journal of Law Management & Humanities*, 4(3), 5722.
- Keykha, M. R., & Ehsanifar, A. (2023). *Electronic Proceedings in Iran's Judicial System and the Use of Artificial Intelligence in Electronic Adjudication* Second International Conference on Jurisprudence, Law, and Religious Research.
- Khaleghi, A. (2024). *Criminal Procedure* (11th ed.). Shahr-e Danesh Institute of Legal Research.
- Khaloui Tafti, S. S., & Aghaabbasi, R. (2021). The Importance and Role of Electronic Proceedings in Judicial Adjudication. *Journal of Research and Studies in Islamic Sciences*, 3(28), 105-118.
- Kim, B.-J. (2025). AI Governance in the Context of the EU AI Act. *IEEE Access*.
- Mansourabadi, A., & Foroughi, F. (2016). *Criminal Procedure*. Mizan Publishing.
- Mihajlović, A. (2025). Efficiency of Justice—Importance of the CEPEJ as the Legacy of the Council of Europe. *Journal name*, 344-355.
- Moazenadegan, H. A., & Roustae, N. (2017). Electronic Proceedings in Confronting Cybercrime: Challenges and Requirements. *Judiciary Law Journal*, 81(100), 165-191.
- Mousavi, S. M. Y. (2016). *Jurisprudential Foundations of the Authority of Judgments Issued by an Authorized Judge*. Jurisprudential Center of the Pure Imams.
- Netolitzky, D. J. (2024). A Legion of Misshapen Cogs: Pseudolaw in Canadian Criminal Proceedings and Amicus Requirements. *Alberta Law Review*, 62, 710.
- Omotoye, K. A. (2021). *Facial Liveness Detection in Biometrics: A Multivocal Literature Review* International Conference on Information Systems and Management Science.
- Park, S. (2025). Theodor W. Adorno and Limits of Digital Positivism. In *Dialectic of Digital Enlightenment: Reclaiming Radical Philosophy for Our Times* (pp. 199-219). Springer Nature Switzerland.
- Peloso, C. (2024). Equality of Arms and Digital Discovery in Criminal Proceedings. In *La Justice pénale numérique en France et au Royaume-Uni* (pp. 203-220). Éditions Panthéon-Assas.
- Rahnama, Z., & Zafari Kurehtash, A. (2025). *The Role of Artificial Intelligence in Transforming the Criminal Justice System: From Criminal Investigations to the Execution of Imprisonment Sentences*. Raj Publications.
- Reiling, D., & Contini, F. (2022). E-Justice Platforms: Challenges for Judicial Governance. *IJCA*, 13.
- Rossner, M., Tait, D., & McCurdy, M. (2021). Justice Reimagined: Challenges and Opportunities with Implementing Virtual Courts. *Current Issues in Criminal Justice*, 33(1), 94-110.
- Schwarz, D. (2025). *AI-Powered Lawyering: AI Reasoning Models, Retrieval-Augmented Generation, and the Future of Legal Practice* (Paper Series, Issue).
- Seibert-Fohr, A. (2022). *Discourses on Judicial Independence* (A. Petfat, Trans.). Judiciary Research Institute Publications.
- Shahpouri, T., & Bashiriyeh, T. (2019). The Approach of Iran's Modern Criminal Procedure Legislative System Based on Labeling Theory. *Quarterly Journal of Legal Research*, 22(87), 275-302.
- Skundric, A. (2023). The Principle of Equality of Arms in Criminal Proceedings. *CRIMEN*, 228.
- Tadin, A. (2021). *History of Criminal Law and Its Developments: Including Persian Translations of Ancient Legal Codes*. Mizan Publishing.
- Vaccaro, M. A. (2019). *Algorithms in Human Decision-Making: A Case Study with the COMPAS Risk Assessment Software* Proceedings of the MIT Student Research Conference,

- Williams, R. J. (2021). Taking a Shot: Access to Justice, Judging and eCourt. *Family Court Review*, 59(2), 278-293.
- Wischmeyer, T. (2019). Artificial Intelligence and Transparency: Opening the Black Box. In *Regulating Artificial Intelligence* (pp. 75-101). Springer International Publishing.
- Zekos, G. I. (2022). Robo-Justice. In *Advanced Artificial Intelligence and Robo-Justice* (pp. 347-415). Springer International Publishing.