Sarhad Journal of Legal Studies
ISSN: 3106-7441 (Print) 3106-745X (Online)
January-June 2026, Vol. 02, No. 01, [42–57]
Published: 30th April 2026
Publisher: Sarhad Institute of Legal Studies, SUIT
https://journal.suit.edu.pk/index.php/sjls
RESEARCH PAPER

Judicial Oversight in the Age of AI: Can the CJEU Effectively Review Automated Risk Assessments?

Syed Shaharyar [1*]

ABSTRACT

The European Union's security architecture is undergoing a profound algorithmic turn, transitioning from reactive law enforcement to preemptive, risk-based border control. Instruments like the European Travel Information and Authorisation System (ETIAS) and the upgraded Europol mandate increasingly rely on Automated Risk Assessments (ARA) and Machine Learning to flag high-risk individuals before a crime is committed. This article critically examines whether the Court of Justice of the European Union (CJEU) possesses the epistemic competence to effectively review these opaque, probabilistic determinations. The paper argues that the CJEU's traditional administrative law standards, specifically the deferential manifest error of assessment test and the human in the loop safeguard, are structurally inadequate for the age of AI. The technical opacity of Black Box algorithms, combined with the proprietary nature of risk indicators, creates a blind spot in judicial protection that threatens the essence of Article 47 of the Charter of Fundamental Rights. By analyzing recent jurisprudence and the emerging AI Act, this article proposes a normative shift from a substantive review of outcomes to a procedural review of algorithmic design. It advocates for a new techno-judicial standard of scrutiny, necessitating the reversal of the burden of proof, strict explainability mandates for high-stakes adjudication, and the appointment of court-mandated technical experts. Ultimately, the article posits that without these procedural innovations, the CJEU risks becoming a rubber stamp for a Technological Leviathan, leaving the fundamental rights of data subjects without an effective remedy.

Keywords: Automated Risk Assessment (ARA), Judicial Review, CJEU, Artificial Intelligence, Article 47 CFREU, ETIAS, Algorithmic Accountability.

INTRODUCTION

The architecture of European security is undergoing a silent but seismic constitutional shift. For decades, the Area of Freedom, Security and Justice (AFSJ) was predicated on a model of retroactive law enforcement: a crime was committed, an investigation was launched, and suspects were identified based on specific, individualized evidence. Today, this causal logic is being rapidly supplanted by a predictive paradigm. We are witnessing an Algorithmic Turn in European

[1] Research Assistant, Vrije Universiteit Amsterdam, Netherlands; shaharyargcu@gmail.com **(Corresponding)**

integration, where the objective is no longer merely to punish the guilty, but to identify and neutralize risks before they materialize (Vavoula, 2025). This shift is most visible in the evolution of the EU's information systems. The early iterations, such as the Schengen Information System (SIS II), operated on a deterministic logic of database matching, digitalized hit/no-hit searches against lists of known warrants or missing persons (Bellanova & Glouftsios, 2020). While efficient, these systems remained fundamentally reactive. In contrast, the new generation of interoperable tools, exemplified by the European Travel Information and Authorisation System (ETIAS), the upgraded Visa Information System (VIS), and the forthcoming Prüm II framework, operates on a probabilistic logic. These systems do not merely store data; they actively generate new knowledge through Automated Risk Assessments (ARA) (Amelung & Machado, 2025).

By cross-referencing vast quantities of personal data against screening rules and risk indicators, these algorithms assign a probability score to individuals, often labeling them as potential security threats based not on what they have done, but on who they resemble or how they behave. This transition marks the rise of Administrative Power by Design, where the code regulating border access and security clearance effectively acts as law, regulating behavior and restricting rights before any human official has exercised discretion (Sanchez Del Rio et al., 2016). The algorithm is no longer just a support tool; it has become a de facto decision-maker, exercising a form of pre-emptive power that challenges the traditional contours of EU administrative law (Ahmed et al., 2025).

The central tension of this new paradigm is the widening gap between the technical reality of these predictive systems and the procedural requirements of the Rule of Law. As the EU entrusts more of its sovereign core capabilities, border control, surveillance, and policing, to automated systems, a critical question arises regarding judicial oversight (Ahmed, 2026). The primary research question of this article is: Can the Court of Justice of the European Union (CJEU) perform effective judicial review over administrative decisions derived from opaque Automated Risk Assessments (Matheu-García et al., 2018).

This question is not merely procedural but constitutional. Article 47 of the Charter of Fundamental Rights (CFR) guarantees the right to an effective remedy and a fair trial. However, the efficacy of this right is predicated on the equality of arms, the ability of the defense to understand, challenge, and rebut the evidence against them. In the context of AI, where decisions may be driven by Black Box neural networks or proprietary algorithms protected by trade secrets, the reasoning behind a decision becomes epistemically inaccessible to both the accused and the judge (Palmiotto, 2024). If a traveler is denied entry because an ETIAS algorithm flagged a correlation between their travel route and a specific payment pattern, how can a national court or the CJEU review the legality of that finding? Does the Court possess the epistemic competence to distinguish between a valid statistical correlation and a discriminatory proxy? If the CJEU cannot penetrate the *"Black Box,"* does judicial review become a mere formalistic exercise, rubber-stamping the technological truth produced by the machine?

To answer these questions, this article employs a doctrinal and critical methodology, analyzing the intersection of EU administrative law, fundamental rights jurisprudence, and the emerging regulatory framework for Artificial Intelligence. The analysis proceeds in four parts.

Section II ("*The Anatomy of Automated Risk"*) maps the technical landscape of the EU's new interoperable ecosystem, distinguishing between deterministic database checks and probabilistic AI tools to establish the precise nature of the legal challenge. Section III (*"The Current Standard")* critiques the existing standards of judicial review, specifically the manifest error of assessment test and the duty to give reasons (Article 41 CFR). It argues that these standards, developed for economic and scientific discretion, are ill-suited for the opacity of algorithmic decision-making.

Section IV (*"Re-Engineering Judicial Review"*) proposes a normative framework for a techno-judicial standard of scrutiny. Drawing on recent jurisprudence such as *Ligue des droits humains (Ligofnis)* regarding PNR data and OQ vs Land Hessen regarding automated credit scoring, it argues that the CJEU must move from a substantive review of outcomes to a procedural review of algorithmic design. This includes the necessity of explainability as a condition of legality and the introduction of burden-shifting mechanisms. Finally, Section V applies this framework to a stress-test case study of a High-Risk third-country national, demonstrating how the proposed standard would function in practice. Ultimately, the article concludes that without a rigorous update to its judicial toolkit, the CJEU risks failing in its mandate to protect fundamental rights in the digital age.

LITERATURE REVIEW

The intersection of artificial intelligence, automated decision-making, and judicial review in the European Union has attracted growing scholarly attention, yet the field remains fragmented across disciplines of public law, data protection, and computer science. This literature review maps the existing body of knowledge across four thematic clusters that directly inform this article's central inquiry: the governance of EU information systems, the doctrinal standards of judicial review, the emerging law of algorithmic accountability, and the normative critiques of automated risk assessments in border control. The foundational literature on EU large-scale information systems has undergone a significant evolution, moving from descriptive accounts of database architecture toward critical assessments of their constitutional implications. Early scholarship by Brouwer documented the progressive expansion of SIS and VIS, emphasizing the creeping erosion of the principle of purpose limitation as law enforcement access to originally migration-focused databases widened. Balzacq and Carrera subsequently situated these systems within a broader securitization framework, arguing that the AFSJ's information systems reflect a political logic of preemptive risk management systematically subordinates civil liberties to security imperatives.

More recently, Vavoula has produced the most doctrinally precise scholarship on the algorithmisation of EU border governance, critically examining how ETIAS and the interoperability framework shift the legal character of border decisions from individualized administrative acts to automated, probabilistic outputs. Jeandesboz, Alegre, and Vavoula's foundational report on ETIAS provides essential technical and legal analysis of the system's screening rules, establishing the analytical vocabulary, particularly the distinction between deterministic hit-list matching and probabilistic risk profiling, that this article adopts. Bellanova and Glouftsios have contributed critical infrastructure studies of SIS II, revealing how the politics of technological maintenance and fragility shape legal accountability in ways that traditional doctrinal analysis fails to capture. The more recent work of Amelung and Machado on Prüm II

extends this inquiry to cross-border DNA and biometric data exchange, underscoring the opaque contestations embedded within apparently technical policy decisions. A persistent gap in this literature is the insufficient engagement with judicial institutions: existing scholarships diagnoses the accountability deficit of interoperable systems but rarely models what an adequate judicial response would look like in operational terms.

The doctrinal architecture of EU judicial review has been extensively mapped by Craig, who traces the evolution of the manifest error of assessment standard from its origins in competition law, through Tetra Laval and Pfizer Animal Health, to its consolidation as the default posture in technical and scientific adjudication. Craig's analysis demonstrates that the Court's deference is not merely pragmatic but is grounded in a principled separation between legal legitimacy and technical expertise. Schwarze's seminal comparative work on European administrative law remains indispensable for understanding the structural choices the CJEU has made in calibrating intensity of review across different regulatory domains. Hofmann, Rowe, and Türk have provided the most comprehensive doctrinal synthesis, detailing how the duty to give reasons under Article 41 CFR operates as a structural prerequisite for judicial scrutiny. Covilla has more recently addressed the specific implications of algorithmic discretion for these traditional doctrines, arguing that the cognitive distance between a judge and a machine-generated recommendation constitutes a qualitatively new challenge for administrative law. Kochenov and Butler's institutional analysis of the CJEU's independence and epistemic capacity further contextualizes the institutional constraints under which algorithmic review must operate. The critical lacuna in this body of work is the absence of a concrete operational standard for review that accounts for the irreducible opacity of Black Box systems; existing literature identifies the problem but stops short of the normative design of a replacement doctrine.

Matheu-García et al.'s work on risk-based cybersecurity assessment frameworks, while focused on IoT certification, provides a methodological model for understanding how risk thresholds are operationally calibrated in ways that are rarely visible to legal scrutiny. The constitutional dimensions of predictive policing and pre-crime logic have been critically examined by Zedner, who argues that the shift from reactive to pre-emptive security fundamentally destabilizes liberal legal frameworks premised on the presumption of innocence and the requirement of individualized suspicion. Roeben's analysis of judicial protection as the meta-norm of the EU's judicial architecture provides the normative foundation for the claim that Article 47 CFR must be interpreted dynamically, expanding to meet new threats to procedural justice. Rabeharisoa and Paterson's work on techno-judicial imaginaries in the French criminal justice context offers a valuable comparative and socio-legal perspective on how courts construct epistemic authority in the face of opaque forensic technologies, a dynamic directly applicable to algorithmic evidence in the EU administrative law context. The combined body of this literature, while rich in diagnosis, has not yet produced a consolidated normative framework specifying the precise procedural and institutional reforms required to render CJEU review of Automated Risk Assessments effective. This article proposes to fill that gap.

METHODOLOGY

This article adopts a hybrid doctrinal and critical legal methodology, operationalized through three sequential analytical phases: doctrinal reconstruction, normative critique, and

prospective standard-setting. This multi-layered methodological design responds to the interdisciplinary nature of the inquiry, which spans EU constitutional and administrative law, data protection regulation, AI governance, and computational epistemology. Each phase draws on a distinct combination of sources and analytical techniques, as described below. The primary analytical layer is doctrinal legal analysis, which involves the systematic identification, interpretation, and synthesis of binding and persuasive legal materials within the EU legal order. The doctrinal method here is interpretive rather than merely descriptive: where existing doctrine produces results that are constitutionally incoherent in the algorithmic context, the analysis makes those tensions explicit and proposes reasoned alternative interpretations consistent with the Court's own established methodological canons, including purposive and systematic interpretation of fundamental rights provisions. The second analytical layer applies a critical legal methodology to expose the structural assumptions and distributional consequences embedded within existing judicial review doctrines. Specifically, this article employs a critical reading of the manifest error of assessment standard to reveal how epistemic deference, originally grounded in a reasonable division of competence between courts and expert agencies in the analog administrative state, is transformed into a mechanism of structural impunity when applied to algorithmic decision-makers. The third analytical layer is prospective and normative. Having established, through doctrinal analysis, where existing law fails, and through critical analysis, why it fails structurally, the article proceeds to design a reformed standard of judicial review that is both constitutionally grounded and operationally workable.

THE ANATOMY OF AUTOMATED RISK IN THE EU

To understand the challenge facing the CJEU, one must first dismantle the technical architecture of the EU's Security Union. The era of siloed databases, where the Visa Information System (VIS) and the Schengen Information System (SIS) operated in isolation, is effectively over. It has been replaced by the Interoperability Regulations (2019/817 and 2019/818), which create a mesh of interconnected data lakes. At the heart of this ecosystem lies the Common Identity Repository (CIR). The CIR does not merely store biographical data; it creates a super-identity for Third-Country Nationals (TCNs) by aggregating data from ETIAS, VIS, and the Entry/Exit System (EES). This aggregation is the fuel for Automated Risk Assessment (ARA). The most pertinent example for this study is the European Travel Information and Authorisation System (ETIAS) (Jeandesboz et al., 2017). Unlike traditional visa processing, which relies heavily on consular discretion, ETIAS is automated by default. Under Article 33 of the ETIAS Regulation, the system compares applicant data not just against hit lists (terrorists, criminals), but against screening rules. These rules are algorithms designed to identify specific risk indicators, combinations of age, education, travel routes, and disease risks, that statistically correlate with illegal immigration or high security risks. This is legally distinct from a SIS alert. A SIS alert is a factual assertion (*"This person is wanted"*). An ETIAS flag is a probabilistic assertion *("This person matches the profile of someone who might commit an offense"*).

Furthermore, the operational scope of Europol has expanded into this predictive domain. Europol's Innovation Hub and its expanded mandate allow for the processing of large datasets (Big Data) to train algorithms for Member States. This effectively nationalizes the output of EU-

level black boxes, complicating the chain of judicial accountability. The legal difficulty arises from the fundamental shift in reasoning employed by these systems (Vavoula, 2025). Traditional administrative law is built on causal reasoning: Person A is denied entry because they committed Act X. In contrast, modern Machine Learning (ML) and ARA operate on correlative reasoning: Person A is denied entry because they share data points X, Y, and Z with a reference group flagged as risky.

This introduces two distinct forms of opacity that the CJEU must contend with:

a. Proprietary Opacity (The Trade Secret): In systems like the PNR (Passenger Name Record), the specific criteria used to flag passengers are often classified to prevent circumvention. As seen in Ligofnis case, the Court struggles to demand transparency when the *"logic"* of the algorithm is itself a sensitive law enforcement technique.
b. Technical Opacity (The Deep Learning Black Box): While current systems like ETIAS use relatively transparent decision trees (if/then rules), the trajectory is toward Deep Learning. In Deep Learning models, the system teaches itself to identify patterns across thousands of variables. The resulting algorithm does not have a readable source code in the traditional sense; its logic is a weight-matrix of millions of parameters that even its developers cannot fully explain (Goodfellow et al., 2016).

If an algorithm denies a visa because of a complex, non-linear correlation between a traveler's IP address, payment method, and past travel history, there is no reason that a human judge can easily parse. The link is mathematical, not narrative. European legislators have attempted to mitigate this risk through the Human in the Loop (HITL) requirement, codified in Article 22 GDPR and reiterated in the ETIAS Regulation. The legal fiction is that the algorithm only makes a recommendation, and a human officer makes the final decision (Lazcoz & De Hert, 2023). However, this safeguard is increasingly viewed by scholars as illusory in the context of mass-scale processing, a phenomenon known as Automation Bias (Alon-Barkat & Busuioc, 2022).

a. The Epistemic Gap: The human officer at the ETIAS National Unit receives a hit notification. However, they often lack technical expertise to understand why the algorithm flagged the file, nor do they have the time to investigate the raw data deeply.
b. The Incentive Structure: There is a strong asymmetry in error costs. Overruling the AI and admitting a terrorist carries a massive professional and reputational cost. Rubber-stamping the AI and denying an innocent tourist carries a negligible administrative cost (Alon-Barkat & Busuioc, 2022).

Consequently, humans become a liability shield rather than a meaningful check. If the CJEU continues to treat these decisions as *"human"* decisions, it ignores the reality that the dispositive analysis was performed by code. Therefore, judicial review must penetrate the human layer and scrutinize the machine itself.

THE CURRENT STANDARD: JUDICIAL REVIEW'S BLIND SPOT

The primary doctrinal obstacle to effective oversight of AI is the standard of review itself. In EU administrative law, when the CJEU reviews complex technical, scientific, or economic

assessments made by EU institutions, it traditionally applies a limited standard of scrutiny known as the manifest error of assessment (Covilla, 2024). Originating from competition law cases like Tetra Laval and risk regulation cases like Pfizer Anima l Health, this doctrine establishes that the Court will not substitute its own assessment for that of the expert agency. Instead, it checks only whether the relevant procedural rules have been complied with, whether the facts have been accurately stated, and whether there has been no manifest error of assessment or misuse of powers.

This standard creates a dangerous paradox in the context of Automated Risk Assessments. In Tetra Laval, the complexity lay in economic forecasting, a field where judges can at least conceptually grasp the variables (market share, elasticity). In the context of a deep learning algorithm used by Europol or ETIAS, the complexity is of a different order, it is epistemically impenetrable. If an algorithm identifies a traveler as high risk based on a correlation of 500 variables, a judge cannot identify a manifest error because the reasoning is not linear. The error is not manifest (obvious); it is buried in the weighting of the neural network or the bias of the training data. Consequently, the Tetra Laval standard, when applied to AI, risks becoming a blank check, granting the algorithm a virtually unreviewable margin of discretion simply because its logic is too complex to be proven obviously wrong.

The second pillar of administrative accountability is the duty to give reasons, enshrined in Article 41(2)(c) of the Charter and Article 296 TFEU. The CJEU has consistently held that the administration must provide the reasoning in a clear and unequivocal fashion, allowing the person concerned to ascertain the reasons for the measure and the competent court to exercise its power of review. However, Black Box AI creates a fundamental tension with this requirement. Current explainable AI (XAI) techniques often provide post-hoc rationalizations rather than true causal explanations (Saeed & Omlin, 2023).

An ETIAS notification might tell an applicant, "You were denied because of your travel history and age." This identifies the input features but fails to explain the logic. It does not answer the crucial question: Why does my specific travel history combined with my age constitute a security threat? Meaningful judicial review requires counterfactual reasoning (If I had not visited country X, would I have been cleared?). Many sophisticated risk algorithms cannot provide this level of granularity. If the reasons provided to the court are merely a list of weighted variables, the duty to give reasons is formally satisfied but substantively hollowed out. The judge is left reviewing the inputs of the decision, not the rationality of the connection between the facts and the legal consequence.

Finally, the use of AI in national security and law enforcement exacerbates the tension regarding secret evidence. The CJEU has addressed this in the ZZ and Kadi jurisprudence, establishing that while full disclosure of national security intelligence is not always required, the essence of the grounds must be disclosed to ensure the equality of arms under Article 47 (Roeben, 2019). In the algorithmic context, the secret evidence is the algorithm itself. Agencies often refuse to disclose the source code or the specific risk indicators (as seen in the ligofnis PNR litigation), citing two reasons:

a. Security: Revealing the rules would allow criminals to game the system (circumvention).

b. Intellectual Property: The algorithm is a trade secret of the private vendor (e.g., the companies building ETIAS).

If the defense counsel cannot access the algorithm to test it for bias (e.g., proving that a high-risk flag is actually a proxy for racial profiling), the equality of arms is destroyed. The accused is fighting a mathematical assertion they cannot see, test, or question. Unlike Kadi case, where the accuser was a sanctioning committee, here the accuser is a proprietary formula. Without a mechanism to challenge the reliability of the tool itself, the adversarial process collapses into a Kafkaesque formality.

RE-ENGINEERING JUDICIAL REVIEW FOR THE AI ERA

The preceding critique demonstrates that the CJEU's existing standards for judicial review are structurally inadequate to address the epistemic opacity and systemic risks posed by Automated Risk Assessments (ARA). The solution is not to ban high-risk AI outright, which is politically and practically unfeasible, but to radically re-engineer the procedural and substantive standards of judicial scrutiny. This requires adopting a techno-judicial approach that shifts the focus from reviewing the outcome of an opaque decision to scrutinizing the governance, design, and interpretability of the algorithm itself (Haitsma, 2023).

The core of the proposed reform is the recognition that, for Black Box systems, the CJEU cannot reliably check the math, but it must check the governance. Judicial review must pivot from a reactive, ex-post review of individual decisions to a preemptive, ex-ante assessment of the system's design and deployment lifecycle. The EU AI Act, particularly its classification of AI systems used in migration, asylum, and border control as high-risk, establishes crucial procedural groundwork for this shift. Under the Act, high-risk systems are subject to stringent Fundamental Rights Impact Assessments (FRIAs) (Almada & Petit, 2022).

For the CJEU, the FRIA must be transformed from a bureaucratic checklist into a justiciable standard of legality. A decision based on an ARA should be considered ultra vires and invalid under EU law if the deploying agency failed to:

a. Identify and Mitigate Bias: Demonstrate how the training data was curated to prevent proxy discrimination (e.g., using residential areas as a proxy for ethnicity).
b. Establish Robustness and Accuracy: Provide independent audits and evidence showing the system's rate of false positives and false negatives under realistic operational conditions.
c. Define Human Oversight: Clearly delineate the specific steps a human reviewer must take to genuinely contest the algorithm's recommendation, moving beyond mere rubber-stamping (Ahmed et al., 2026).

The failure to conduct a methodologically sound FRIA, or the use of an ARA that demonstrably violates the Act's requirements on robustness and data quality, should constitute a manifest error of law by the administrative agency, thus triggering the Court's jurisdiction. This elevates compliance with technical standards into a constitutional precondition for the lawful use of high-risk AI (Ekeh et al., 2025). The reliability of any ARA is determined by the quality and representativeness of its training data. The CJEU must extend its scrutiny deep into the data supply

chain, looking at whether the data inputs themselves are lawful under the Law Enforcement Directive (LED) and the AI Act (Wachter et al., 2017). Concerns over Prüm II (the proposed expansion of automated data exchange) are particularly relevant. If national authorities feed biased, outdated, or contextually flawed data into a pan-European ARA system, the resulting risk assessment will be inherently discriminatory, creating what legal scholars term an algorithmic chain of illegality (Amelung & Machado, 2025).

The CJEU should establish a requirement that agencies submit Data Quality Statements to the court in the event of an appeal. The judicial task then becomes reviewing whether the agency took all reasonable steps to ensure the accuracy and representativeness of the data used for the specific risk calculation, focusing on whether data points are being used to predict attributes (like terrorist risk) for which they were never collected. The most direct normative intervention the CJEU can make is to enforce a strict interpretability mandate for all high-stakes automated decisions that directly restrict fundamental rights. This flows directly from the requirements of Article 47 (effective remedy) and Article 41 (duty to give reasons).

The duty to give reasons cannot be satisfied by simply listing the factors considered. The CJEU must demand counterfactual explanations, the ability for the agency to state precisely what change in the input data would have resulted in a different outcome. In a case involving an ETIAS denial, the agency must go beyond stating, "Your travel history was a factor." It must state: "The high-risk score resulted from the combination of your recent travel to Country A, your payment method X, and your age bracket. Had you used payment method Y, your score would have fallen below the high-risk threshold."

If technology, due to its reliance on Deep Learning or technical opacity, cannot provide a clear, non-technical counterfactual explanation to the individual and the reviewing judge, then its use must be deemed ultra vires for applications that restrict fundamental rights. This implies a functional ban on non-interpretable Black Box AI in high-stakes law enforcement adjudication, reserving it only for low-stakes, internal intelligence-gathering purposes (Ahmed, 2024). The CJEU's jurisprudence on the Passenger Name Record (PNR) in Case C-817/19 Ligue des droits humains (Ligofnis) offers a crucial doctrinal hook. In this judgment, the Court demanded that the criteria used for automated processing must be clear and precise. This requirement can be read not only as a demand for clarity in the statutory definition of a risk but also in the technical implementation of the algorithm. If an algorithm's logic is a non-linear network of millions of weights and biases, it is definitionally not clear and precise (Ulbricht, 2018). Extending the Ligofnis principle provides the CJEU with a constitutional basis to mandate Simplicity and Transparency by Design for all high-risk ARA deployed in the AFSJ. The Court can effectively state that legal precision cannot be outsourced to mathematical imprecision.

Since the current adversarial framework is inadequate for challenging complex algorithmic logic, the CJEU must adopt institutional and procedural reforms to level the equality of arms. The most impactful procedural change is the reversal of the burden of proof. In a traditional judicial review, the applicant challenging an administrative decision bears the burden of proving the manifest error of the administration. In the AI context, this is impossible due to the information asymmetry (Kochenov & Butler, 2021). Therefore, once the applicant establishes a prima facie

case that they were subject to an automated decision which negatively impacted their rights, and they demonstrate that the reasoning remains opaque, the burden of proof must shift entirely to the administrative agency. The agency (e.g., Europol, ETIAS National Unit) must then prove the following to the Court:

a. Technical Validity: That the algorithm is robust, accurate, and free of systemic bias.
b. Causal Necessity: That the specific factors leading to the decision were relevant and necessary to achieve the stated legal objective (e.g., border security).

This shift compels agencies to maintain audit trails and transparency reports, fundamentally re-aligning the incentives toward accountable system design. Judges cannot be expected to become computer scientists overnight. The CJEU and national courts of reference must gain necessary epistemic competence. This requires institutional reform:

a. Court-Appointed Technical Experts: The CJEU should establish a permanent roster of independent technical experts (Amicus Curiae Technicus). These experts, bound by strict confidentiality and subject to ethical oversight, would be tasked with auditing algorithms, analyzing source code, and explaining the logic, bias, and uncertainty to the bench. They would transform the review from a legal argument into an evidence-based technical assessment (Dwivedi et al., 2019).
b. Specialized Judicial Chambers: The creation of specialized chambers within the CJEU (or the General Court) for data governance and AI would ensure that a core group of judges develops the continuous expertise needed to handle these complex cases, minimizing the reliance on generalized administrative law principles) (Pollman, 2016).

The core dispute between judicial protection and national security often revolves around Access to Source Code. While blanket public disclosure is impractical due to security and IP concerns, the Court must develop a protected mechanism for disclosure, drawing lessons from ZZ and Kadi. The Court could implement a procedure where the source code and the training data are disclosed in camera and under strict secrecy oaths only to the Amicus Curiae Technicus and potentially a highly vetted defense counsel (Papadaki, 2019). This model balances the security necessity of secrecy with the fundamental right to contest the evidence, providing the defense with the ability to indirectly challenge the technical reliability of the algorithm without compromising national security operations.

CASE STUDY: THE "HIGH-RISK" TRAVELLER

To illustrate the practical necessity of the proposed reforms, this section constructs a stress test scenario. This composite case study synthesizes elements from the Ligofnis litigation and the operational mechanics of the ETIAS Central System, demonstrating the friction between algorithmic probability and individual rights. Elena X is a 29-year-old software engineer and a national of a visa-exempt Latin American country. She applied for an ETIAS travel authorisation to attend a tech conference in Berlin. She has no criminal record, no prior immigration violations, and is not listed in any SIS II or Interpol database. However, her application triggers a hit in the ETIAS Central System. The hit is not generated by a watchlist match, but by the ETIAS Screening

Rules (Article 33). A specific algorithmic risk indicator has flagged her profile based on a correlative pattern:

a. Travel History: Recent short stays in three specific jurisdictions known for loose cryptocurrency regulations.
b. Digital Behavior: Access to encrypted messaging platforms associated with cyber-crime (data harvested via interoperability with Europol's large data sets).
c. Demographic Profile: Female, age 25–30, with a background in computer science.

The algorithm, trained on historical data of cyber-crime syndicates, calculates a 78% probability that Elena fits the profile of a *"high-risk"* facilitator of cyber-fraud.

The file is forwarded to the ETIAS National Unit (ENU) in Germany for manual processing. The officer receives a notification on their screen: RISK CODE 44-B (Cyber-Facilitation Risk). Recommendation: DENY. Crucially, the officer does not see the underlying logic. They do not know that the crypto-jurisdiction variable was the deciding factor. Under pressure to process hundreds of applications daily and fearing the reputational risk of admitting a potential cyber-criminal, the officer succumbs to Automation Bias. They validate the hit without meaningful investigation. Elena receives a standard denial notification: *"Refused Entry. Reason: Security Risk. See Article 37(1)(c) of Regulation 2018/1240."* She has no idea why she is considered a risk, making it impossible for her to draft a factual rebuttal. Elena appeals the decision before the Administrative Court of Berlin, which eventually stays proceedings and sends a preliminary reference to the CJEU. The central question is: Does a refusal based on an opaque risk indicator violate the essence of the Right to an Effective Remedy (Art. 47 CFR)?

Case under the current standard approach as follows. The German authorities argue that the ETIAS screening rules are classified for security reasons. They provide a general statement that the system is reliable and that a human officer made the final decision. The Court, applying the Tetra Laval standard, looks for a manifest error. Since the Court cannot see the algorithm, it cannot find an obvious error. It defers to the *"broad discretion"* of the administration in security matters. The denial is upheld. Elena is effectively barred from the EU based on a statistical guess she cannot disprove.

Under the standard proposed in Section IV, the CJEU and the national court would apply a rigorous three-step scrutiny i.e. the Court acknowledges that Elena has no criminal record and that the reasoning (Security Risk) is insufficient for a defense. The burden of proof immediately shifts to the ETIAS National Unit to prove the validity of the risk assessment. The Court orders a protected disclosure of the specific Screening Rule used (Rule 44-B) to a court-appointed algorithmic auditor (Amicus Curiae Technicus). The expert discovers that the training data for Rule 44-B was heavily skewed towards a specific cyber-crime operation from five years ago that exclusively used female couriers. The demographic profile variable acts as a proxy for gender, and the travel history correlation is weak (many legitimate tech workers visit those jurisdictions). The Court applies the Explainability Threshold. It asks: Is there a causal link between Elena's travel and criminal intent? The agency admits it has no specific intelligence in Elena, only the probabilistic match. The Court rules that a mere statistical correlation (78% similarity to past

criminals) is insufficient to restrict the fundamental right of movement and the presumption of innocence.

The Court annuls the decision. It rules that administrative decisions restricting rights cannot rely on logic that cannot be explained to a judge. Risk indicators must show a specific, individualized threat, not just a general statistical resemblance to a risky profile. This case study demonstrates that without the Techno-Judicial toolkit (burden shifting, technical audit, causal requirement), the judicial review is a hollow shell. With it, the Court restores the rule of law, protecting the individual against the tyranny of the average (Rabeharisoa & Paterson, 2024).

CONCLUSION

This article began with an interrogation of the algorithmic turn in European security, a shift as significant as the removal of physical borders three decades ago. We have traversed the technical anatomy of the EU's interoperable ecosystem, from the deterministic logic of the Schengen Information System to the probabilistic, black box predictions of ETIAS and the new Europol mandate. The investigation reveals a disturbing trajectory: the European Union is rapidly constructing an administrative power by design, where the sovereign capacity to define risk, grant access, and deprive liberty is increasingly delegated to opaque automated systems.

The diagnostic findings of this research are stark. The current judicial toolkit of the CJEU, forged in the era of analog bureaucracy, is suffering from a crisis of obsolescence. The manifest error of assessment standard, designed to respect the discretionary expertise of economists and scientists, has mutated into a shield for algorithmic unaccountability. When applied to Deep Learning models whose internal logic is mathematically indecipherable, this deferential standard effectively creates a lawless zone at the heart of the Area of Freedom, Security and Justice (AFSJ). We have seen that the human in the loop (Article 22 GDPR) is, in the context of high-volume border control, largely a legal fiction, a procedural fig leaf that fails to mitigate the cognitive force of Automation Bias.

Consequently, a profound asymmetry has emerged. The EU administration is armed with big data and predictive capability, while the individual, and crucially, the reviewing judge, is left in a state of epistemic blindness. If the Court continues to treat algorithmic output as a neutral technical fact rather than a contestable administrative decision, it risks hollowing out the essence of Article 47 of the Charter. The right to an effective remedy cannot exist where the evidence is a trade secret and the accuser is a proprietary formula. Beyond the doctrinal mechanics, this shift poses an existential challenge to the European model of the Rule of Law (Rechtsstaat). The integration of unexplainable AI into the sovereign core of the state threatens to transition the EU towards an Algorithmusstaat, a polity governed by statistical correlation rather than legal causation. In a traditional Rechtsstaat, administrative action derives its legitimacy from its adherence to published laws and its susceptibility to reason-giving. The citizen obeys the decision because it can be justified. In an Algorithmusstaat, legitimacy is derived from efficiency and accuracy. The citizen is expected to obey the decision because the machine is statistically likely to be correct.

This article argues that the CJEU must resist this transition. The Court must recognize that Information Technology is no longer just a tool of administration; it is the administration itself. Therefore, the technical specifications of these systems, their error rates, their training data, their explainability parameters, are not merely engineering details; they are constitutional questions. We are witnessing the necessity for the Constitutionalisation of IT. Just as the CJEU once elevated general principles of law (proportionality, legal certainty) to constitutional status to control the expanding powers of the EEC, it must now elevate technical due process to constitutional status to control the expanding powers of the Digital Union. Technical robustness is not just an IT requirement; it is a precondition for the legality of administrative action. A system that generates false positives at a rate that disproportionately affects a protected group is not just buggy; it is unconstitutional.

To prevent the calcification of this technological leviathan, this paper has proposed a concrete normative framework for the CJEU. The Court must abandon its deferential posture and adopt a standard of strict Techno-Judicial scrutiny for any automated system that impacts fundamental rights. The Court must establish a red line: Nulla decisio sine ratione (No decision without a reason). If an AI system is so complex that it cannot provide a counterfactual explanation for its output, if it is a true black box, it is ipso facto incompatible with the Charter when used for high-stakes adjudication. The efficiency of Deep Learning cannot trump the transparency required by the Rule of Law. The CJEU's ruling in Ligofnis regarding clear and precise criteria must be interpreted as a ban on uninterpretable AI in law enforcement.

The presumption of regularity that administrative acts typically enjoy must be suspended for opaque automated decisions. Once a prima facie grievance is raised, the burden must shift to the state to prove, via audit logs and impact assessments, that the algorithm is reliable, unbiased, and operating within its legal mandate. The citizen cannot be asked to reverse-engineer a secret algorithm to prove their innocence. The Court must admit its own lack of technical expertise and institutionalize the role of the Amicus Curiae Technicus. Justice in the 21st century requires a dialogue not just between judges, but between jurists and data scientists. Without this interdisciplinary bridge, the Court will remain forever one step behind the technology it seeks to regulate (Imam & Ahmed, 2025).

The stakes of this debate extend to the legitimacy of the European project itself. The EU has positioned itself globally as the regulatory superpower of the digital age, championing a human-centric approach to AI (as evidenced by the AI Act). However, this regulatory ambition will ring hollow if the EU's own internal security agencies are permitted to operate standardless black boxes that violate the very rights the Brussels Effect seeks to export. If the CJEU fails to impose rigorous oversight, we risk a bifurcation of European law: a highly protected sphere for commercial data (under the GDPR/AI Act) and a lawless sphere for security data, where the exigencies of counterterrorism and migration control justify the suspension of procedural due process. The high-risk traveller described in our case study, Elena X, is not a marginal figure. She represents the future subject of EU law: profiled, risk-scored, and managed by interoperable databases. If the Court of Justice cannot offer her an effective remedy because it is too deferential

to challenge the magic of the machine, then the Court ceases to be a guardian of the Treaties and becomes a spectator to the rise of automated power.

The path forward requires judicial courage. The CJEU has a history of bold, transformative jurisprudence, from *Van Gend en Loos to Schrems*. The challenge of the AI era demands a similar leap. The Court must declare that in the European Union, no algorithm is above the law. It must assert that the convenience of prediction can never displace the necessity of proof. We are at a critical juncture. The infrastructure is being built; the code is being written. The black box is closing. It is up to the Court of Justice to pry it open, ensuring that the future of European security remains illuminated by the principles of justice, transparency, and human dignity. The age of AI does not require the abandonment of the Rule of Law; it requires its robust reinvention.

REFERENCES

Ahmed, S. S. (2024). Mastering the Digital frontier: the intersection of generative AI and human rights in the digital age. *UCP Journal of Law & Legal Education*, *2*(2), 73–94. https://doi.org/10.24312/ucp-jlle.02.02.271

Ahmed, S. S. (2026). Cross-Border surveillance and the right to privacy: legal remedies in the age of 5G and LOT. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.6000814

Ahmed, S. S., Haider, S., & Javed, M. S. (2026). AI Literacy as a Core Competency: Should Prompt Engineering for Lawyers be a Mandatory Course? *Pakistan Journal of Law, Analysis and Wisdom*, *5*(3), 1–13. https://pjlaw.com.pk/index.php/Journal/article/view/v5i3-01-13/v5i3-01-13

Ahmed, S. S., Javed, M. S., & Haider, S. (2025). Algorithmic Discrimination and the Law: Regulating Bias in AI Decision-Making. *Pakistan Journal of Humanities and Social Sciences*, *13*(4), 220–229. https://doi.org/10.52131/pjhss.2025.v13i4.3086

Almada, M., & Petit, N. (2022). The EU AI Act: Between product safety and Fundamental rights. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4308072

Alon-Barkat, S., & Busuioc, M. (2022). Human–AI interactions in public sector decision making: "Automation bias" and "Selective adherence" to algorithmic advice. *Journal of Public Administration Research and Theory*, *33*(1), 153–169. https://doi.org/10.1093/jopart/muac007

Amelung, N., & Machado, H. (2025). Dancing in the Dark: Policy transformations through obfuscating contestations in the case of Prüm II. *Università Degli Studi Di Roma "Unitelma Sapienza."* https://doi.org/10.15166/2499-8249/854

Bellanova, R., & Glouftsios, G. (2020). Controlling the Schengen Information System (SIS II): the infrastructural politics of fragility and maintenance. *Geopolitics*, *27*(1), 160–184. https://doi.org/10.1080/14650045.2020.1830765

Case C-12/03 P, Commission v Tetra Laval BV [2005] ECR I-00987. Retrieved from < https://curia.europa.eu/juris/document/document.jsf?text=&docid=81100&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=4841105>.

Case C-634/21, *OQ v Land Hessen (Schufa)*, Judgment of 7 December 2023, EU:C:2023:948. Retrieved from < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62021CJ0634>.

Case C-817/19, *Ligue des droits humains v Conseil des ministres* (PNR), Judgment of 21 June 2022, EU:C:2022:491. Retrieved from < https://curia.europa.eu/juris/document/document.jsf;jsessionid=30A1658C04750DE6AED

9D786C635F77A?text=&docid=261282&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=4811260>.

Case T-13/99, Pfizer Animal Health SA v Council [2002] ECR II-03305. Retrieved from < https://curia.europa.eu/juris/showPdf.jsf?text=&docid=47642&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=4842431>.

Charter of Fundamental Rights of the European Union [2012] OJ C326/391. Retrieved from < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT>.

Covilla, J. C. (2024). Artificial intelligence and administrative discretion: Exploring adaptations and boundaries. *European Journal of Risk Regulation*, *16*(1), 36–50. https://doi.org/10.1017/err.2024.76

Del Rio, J. S., Moctezuma, D., Conde, C., De Diego, I. M., & Cabello, E. (2016). Automated border control e-gates and facial recognition systems. *Computers & Security*, *62*, 49–72. https://doi.org/10.1016/j.cose.2016.07.001

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kar, A. K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., . . . Williams, M. D. (2019). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *57*, 101994. https://doi.org/10.1016/j.ijinfomgt.2019.08.002

Ekeh, A. H., Apeh, C. E., Odionu, C. S., & Austin-Gabriel, B. (2025). Automating legal compliance and contract management: Advances in data analytics for risk assessment, regulatory adherence, and negotiation optimization. *Engineering and Technology Journal*, *10*(01). https://doi.org/10.47191/etj/v10i01.26

Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. In *MIT Press eBooks*. https://dl.acm.org/citation.cfm?id=3086952

Haitsma, L. M. (2023). Regulating algorithmic discrimination through adjudication: the Court of Justice of the European Union on discrimination in algorithmic profiling based on PNR data. *Frontiers in Political Science*, *5*. https://doi.org/10.3389/fpos.2023.1232601

Imam, M. J., & Ahmed, S. S. (2025). The role of Generative Artificial intelligence in Judicial Decision-Making Process. *UCP Journal of Law & Legal Education*, *3*(1), 112–137. https://doi.org/10.24312/ucp-jlle.03.01.305

Jeandesboz, J., Alegre, S., & Vavoula, N. (2017). European Travel Information and Authorisation System (ETIAS): Border management, fundamental rights and data protection. *Dépôt Institutionnel De L'Université Libre De Bruxelles (Université Libre De Bruxelles)*. http://hdl.handle.net/2013/ULB-DIPOT:oai:dipot.ulb.ac.be:2013/264396

Joined Cases C-402/05 P and C-415/05 P, Yassin Abdullah Kadi and Al Barakaat International Foundation v Council and Commission (3 September 2008) [2008] ECR I-6351. Retrieved from < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62005CJ0402>.

Kochenov, D. V., & Butler, G. (2021). Independence of the Court of Justice of the European Union: Unchecked Member States power after the Sharpston Affair. *European Law Journal*, *27*(1–3), 262–296. https://doi.org/10.1111/eulj.12434

Lazcoz, G., & De Hert, P. (2023). Humans in the GDPR and AIA governance of automated and algorithmic systems. Essential pre-requisites against abdicating responsibilities. *Computer Law & Security Review*, *50*, 105833. https://doi.org/10.1016/j.clsr.2023.105833

Matheu-García, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., & Baldini, G. (2018). Risk-based automated assessment and testing for the cybersecurity certification and labelling of

IoT devices. *Computer Standards & Interfaces*, *62*, 64–83. https://doi.org/10.1016/j.csi.2018.08.003

Palmiotto, F. (2024). When is a decision automated? A taxonomy for a fundamental rights analysis. *German Law Journal*, *25*(2), 210–236. https://doi.org/10.1017/glj.2023.112

Papadaki, M. (2019). Substantive and Procedural Rules in International Adjudication: Exploring their Interaction in Intervention before the International Court of Justice. In *Nomos Verlagsgesellschaft mbH & Co. KG eBooks* (pp. 37–64). https://doi.org/10.5771/9783845299051-37

Pollman, T. (2016). Introduction to essays on technology in courtrooms and judicial chambers. *Legal Writing: The Journal of the Legal Writing Institute*, *21*, 1–3. https://legalwritingjournal.scholasticahq.com/article/25152

Rabeharisoa, V., & Paterson, F. (2024). Non-Manipulable Things? Maintaining a Techno-Judicial imaginary on sealed biological samples in the French criminal justice. *Engaging Science Technology and Society*, *9*(3). https://doi.org/10.17351/ests2023.1329

Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) [2018] OJ L236/1. Retrieved from < https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R1240>.

Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226. Retrieved from < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1240>.

Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 establishing a framework for interoperability between EU information systems in the field of borders and visa [2019] OJ L 135, 27 and Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration [2019] OJ L 135, 85, or more simply in footnotes as (EU) 2019/817 and (EU) 2019/818. Retrieved from < https://eur-lex.europa.eu/eli/reg/2019/818/oj/eng>.

Roeben, V. (2019). Judicial Protection as the Meta-norm in the EU Judicial Architecture. *Hague Journal on the Rule of Law*, *12*(1), 29–62. https://doi.org/10.1007/s40803-019-00085-3

Saeed, W., & Omlin, C. (2023). Explainable AI (XAI): A systematic meta-survey of current challenges and future opportunities. *Knowledge-Based Systems*, *263*, 110273. https://doi.org/10.1016/j.knosys.2023.110273

Ulbricht, L. (2018). When Big Data Meet Securitization. Algorithmic Regulation with Passenger Name Records. *European Journal for Security Research*, *3*(2), 139–161. https://doi.org/10.1007/s41125-018-0030-3

Vavoula, N. (2025). The future of digitalisation in EU law enforcement: enhanced exchanges of personal data, privatisation and algorithmisation. *Università Degli Studi Di Roma "Unitelma Sapienza."* https://doi.org/10.15166/2499-8249/851

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated Decision-Making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, *7*(2), 76–99. https://doi.org/10.1093/idpl/ipx005