RESOLUTION No. 615/2025, of March 11, 2025

Establishes guidelines for the development, use, and governance of artificial intelligence solutions within the Judiciary.

The PRESIDENT OF THE NATIONAL COUNCIL OF JUSTICE, in the exercise of his legal and regimental attributions,

CONSIDERING that Resolution No. 332, of the National Council of Justice (NCJ), dated August 21, 2020, establishes guidelines on ethics, transparency, and governance in the production and use of artificial intelligence in the Judiciary;

CONSIDERING the rapid pace of advancements in artificial intelligence technologies, particularly regarding algorithms powered by large language models that interact with users and generate automated solutions;

CONSIDERING the indispensability of specific regulations for the use of generative artificial intelligence techniques within the Judiciary, ensuring full transparency and publicity, so that its application aligns with fundamental ethical values, including human dignity, respect for human rights, non-discrimination, due process, proper justification and reasoning of judicial decisions, accountability, and responsibility.

CONSIDERING the importance of fostering the autonomy of Courts in implementing innovative technologies while promoting practices that ensure ethical, responsible, and secure innovation when adopting artificial intelligence tools;

CONSIDERING the potential risks associated with generative artificial intelligence, including threats to sovereignty, information security, privacy, and data protection, as well as the risk of amplifying biases and discrimination

CONSIDERING that the use of generative artificial intelligence to assist in the production of judicial decisions requires transparency, as well as the necessary oversight, review, and human intervention by the judiciary;

CONSIDERING that Resolution No. 332/2020 was designed with a focus on computational solutions aimed at supporting procedural management and enhancing the effectiveness of judicial services available at the time of its drafting, and recognizing the need to update this framework to encompass new technologies, particularly those known as generative artificial intelligence;

CONSIDERING the opinion issued by the Permanent Commission on Information Technology and Innovation of the National Council of Justice in the

Administrative Control Procedure No. 0000416-89.2023.2.00.0000, which underscored the importance of proper governance in the use of artificial intelligence, particularly generative artificial intelligence, within the Judiciary;

CONSIDERING the need to ensure that the development and deployment of artificial intelligence models in the Judiciary adhere to ethical principles of transparency, predictability, auditability, and substantive justice;

CONSIDERING that artificial intelligence solutions must be audited with regard to information security, data protection, performance, robustness, reliability, prevention of biases, correlation between inputs and outputs, and compliance with legal and ethical standards;

CONSIDERING the importance of fostering collaboration and sharing information on the use of artificial intelligence in the Judiciary to ensure transparency and effectiveness in applying these technologies;

CONSIDERING the need to respect the prerogatives of the Public Prosecutor's Office, the Public Defender's Office, the legal profession, and other stakeholders within the justice system;

CONSIDERING the suggestions received from judges, other stakeholders in the justice system, civil society, experts, and public and private institutions for updating Resolution No. 332/2020, presented during the public hearing held from September 25 to 27, 2024

CONSIDERING the report of the Working Group on the Regulation of Artificial Intelligence in the Judiciary, established by the NCJ Ordinance No. 338 of November 30, 2023, entrusted with conducting studies and presenting proposals for regulating the use of generative artificial intelligence systems;

CONSIDERING the decision issued by the Plenary of the National Council of Justice in the judgment of the Procedure for Normative Acts No. 0000563-47.2025.2.00.0000 during the 1st Extraordinary Session, held on February 18, 2025;

DECIDES:

CHAPTER I
DEFINITIONS AND FOUNDATIONS FOR THE USE OF AI- BASED TECHNOLOGIES WITHIN THE JUDICIARY

Art. 1 This Resolution establishes norms for the development, governance, audit, monitoring, and responsible use of solutions employing artificial intelligence (AI) techniques within the Judiciary, aiming at promoting technological innovation and the efficiency of judicial services in a safe, transparent, equitable, and ethical manner, benefiting users while strictly observing their fundamental rights.

§ 1 The governance of artificial intelligence (AI) solutions must respect the autonomy of the courts, allowing for the development and implementation of local innovative solutions, tailored to the specific contexts of each court, provided that the audit, monitoring, and transparency standards established by this Resolution are observed, without prejudice to the National Council of Justice's oversight within the scope of its competencies.

§ 2 The audit and monitoring of AI solutions shall be conducted using criteria that are proportional to the solution's impact, ensuring that systems remain practically and accessibly auditable or monitorable without requiring unrestricted access to source codes, as long as mechanisms for transparency and oversight of data usage and automated decisions are effectively implemented.

§ 3 Transparency in the use of AI shall be promoted through clear indicators and public reports that communicate the use of these solutions in a comprehensible and straightforward manner, ensuring that users are informed of AI usage where applicable, without compromising the efficiency or integrity of court proceedings and judicial decisions.

§ 4 The courts shall prioritize the collaborative development of AI solutions, promoting interoperability and the sharing of technologies, code, databases, and best practices with other bodies of the Judiciary.

§ 5 The National Council of Justice (CNJ) may establish incentive mechanisms, such as public recognition, awards, or the prioritization of resources and investments in innovation, for courts that, among other criteria established by regulation, adopt collaborative/cooperative practices in the development of AI solutions.

Article 2
The development, governance, auditing, monitoring, and responsible use of artificial intelligence (AI) solutions by the Judiciary shall be based on the following principles:

I - Respect for fundamental rights and democratic values;
II - Promotion of the well-being of court users;
III - Technological development and encouragement of innovation in the public sector, with an emphasis on collaboration between courts and the National Council of Justice to enhance the efficiency of judicial services, while respecting the autonomy of courts to develop solutions tailored to their specific needs;
IV - The centrality of the human person;
V - Human participation and supervision at all stages of the development and implementation cycles of solutions that adopt artificial intelligence techniques,

unless such technologies are used as auxiliary tools to increase efficiency, automate purely accessory or procedural judicial services, and provide decision-making support;
VI - Promotion of equality, diversity, and fairness in decision-making;
VII - Development of secure solutions for internal and external users, including the identification, classification, monitoring, and mitigation of systemic risks;
VIII - Protection of personal data, access to information, and respect for judicial confidentiality;
IX - Curation of data used in the development and improvement of artificial intelligence, adopting secure, traceable, and auditable data sources, preferably governmental, while allowing the use of private sources provided they meet the security and auditability requirements established in this Resolution or by the Judiciary National Artificial Intelligence Committee;
X - Raising awareness and disseminating knowledge about solutions adopting artificial intelligence techniques, with continuous training for their users on their applications, operational mechanisms, and risks;
XI - Assurance of information security and cybersecurity.
XII - the transparency of audit reports, algorithmic impact assessments, and monitoring.

Article 3

The development, governance, auditing, monitoring, and responsible use of artificial intelligence (AI) by courts shall be guided by the following principles:

I - Justice, fairness, inclusion, and the prevention of abusive or unlawful discrimination;
II - Transparency, efficiency, explainability, contestability, auditability, and reliability of systems that employ artificial intelligence techniques;
III - Legal certainty and information security;
IV - The pursuit of efficiency and quality in the delivery of judicial services while ensuring fundamental rights;
V - Due process of law, the right to a full defense, the principle of adversarial proceedings, the physical presence of the judge, and the reasonable duration of proceedings, ensuring full respect for the prerogatives and rights of stakeholders in the justice system;
VI - the prevention, precaution, and control of effective measures for mitigating risks arising from the intentional or unintentional use of solutions that employ artificial intelligence techniques.
VII - Effective, periodic, and appropriate human supervision throughout the lifecycle of artificial intelligence, taking into account the degree of risk involved, with the possibility of adjusting this supervision based on the level of automation and impact of the solution employed.

VIII – the offering, by courts and their training institutions, of continuous education for judges and court staff on the risks of automation, algorithmic biases, and critical analysis of AI-generated outcomes.

Article 4
For the purposes of this Resolution, the following definitions apply:

I - Artificial Intelligence (AI) System: a machine-based system that, with varying levels of autonomy and for explicit or implicit objectives, processes a set of provided data or information with the aim of generating likely and coherent outcomes in the form of decisions, recommendations, or content, which may influence the virtual, physical, or real environment.
II - Lifecycle: A series of phases encompassing the design, planning, development, training, retraining, testing, validation, deployment, monitoring, and any subsequent modifications or adaptations of an artificial intelligence system, including its termination, which may occur at any of the aforementioned stages, as well as the assessment of its impacts after deployment;
III - Sinapses: A computational solution designed to store, test, train, distribute, and audit artificial intelligence models, available on the Digital Judiciary Platform - PDPJ-Br;
IV - Artificial Intelligence System Developer: A natural or legal person, whether public or private, who develops or commissions an artificial intelligence system with the purpose of making it available on the market or applying it to a provided service, under their own name or brand, either for a fee or free of charge;
V - User: A person who uses the AI system and controls its functionalities, where control may be regulated or limited depending on whether it is external or internal to the Judiciary;
VI - Internal User: A member, staff, or collaborator of the Judiciary who develops or uses the intelligent system, potentially classified into different profiles according to their role and area of expertise;
VII - External User: an individual outside the Judiciary who interacts directly with the Judiciary's AI system, including lawyers, public defenders, prosecutors, members of the Public Prosecutor's Office, experts, technical assistants, and the general public under its jurisdiction.
VIII - Distributor: A natural or legal person, whether public or private, who makes an AI system available and distributes it for operation by a third party, either for a fee or free of charge;
IX - Generative Artificial Intelligence (Generative AI or GenAI): an AI system specifically designed to generate or significantly modify, with varying levels of autonomy, text, images, audio, video, or software code, in addition to statistical models and learning patterns derived from trained data.
X - Preliminary Assessment: The process by which the developing or contracting court evaluates an AI system prior to its use or deployment in PDPJ-Br, with the aim of classifying its risk level and fulfilling the obligations established in this Resolution;

XI - Algorithmic Impact Assessment: The continuous analysis of the impacts of an AI system on fundamental rights, including the definition of preventive measures, damage mitigation strategies, and actions to maximize positive impacts, without violating the industrial and intellectual property rights of the AI solution used;
XII - Judiciary National Artificial Intelligence Committee: A committee with a plural composition, aimed at assisting the National Council of Justice in the implementation, enforcement, and oversight of this Resolution, always engaging in dialogue with the courts and civil society;
XIII - Illegal or Abusive Discriminatory Bias: A wrongfully discriminatory outcome that creates, reproduces, or reinforces biases, whether derived from the data or its training process;
XIV - Privacy by Design: The preservation of data privacy from the inception of any new AI project or service throughout its entire lifecycle, including the anonymization and encryption of confidential data;
XV - Privacy by Default: The adoption of a high level of data confidentiality as the default standard;
XVI - Prompt: A natural language command used in generative AI to execute a specific task;
XVII - Auditability: The ability of an AI system to be subjected to an evaluation of its algorithms, data, design processes, or outcomes;
XVIII - Explainability: A clear understanding, whenever technically possible, of how the AI "decisions" are made;
XIX - Contestability: The possibility of questioning and reviewing the results generated by the AI.

CHAPTER II
FUNDAMENTAL RIGHTS

Article 5

In the development, deployment, and use of artificial intelligence solutions in the Judiciary, courts shall ensure their compatibility with fundamental rights, particularly those established in the Constitution of the Republic or in treaties to which the Federative Republic of Brazil is a party.

§ 1 The compatibility assessment with fundamental rights must take place at all stages of the lifecycle of the artificial intelligence solution, including development, deployment, use, updates, and any retraining of the systems and their data.

§ 2 Courts must implement continuous auditing and monitoring mechanisms to ensure that AI solutions remain compliant with fundamental rights and to make adjustments whenever incompatibilities are identified.

§ 3 In the event of reports or indications of violations of fundamental rights, the Brazilian Bar Association (OAB), the Public Prosecutor's Office, and other legitimate entities shall be granted access to algorithmic impact assessments and the right to petition the Committee to assess the need for requesting audits and other forms of oversight.

Article 6
The adoption of applications that incorporate artificial intelligence models must aim to ensure legal certainty and contribute to the Judiciary's adherence to the principles outlined in Article 3.

Sole Paragraph
Courts and AI developers shall be responsible for creating internal guidelines to ensure that AI solutions comply with the principles established in Article 3, with appropriate mechanisms for supervision and periodic review.

Article 7
Data employed in the development or training of artificial intelligence models must be representative of legal cases and observe precautions regarding judicial secrecy and the protection of personal data, in accordance with Law No. 13,709, of August 14, 2018 (General Data Protection Law - LGPD).

§ 1 Representative data are those that adequately reflect the diversity of situations and contexts within the Judiciary, avoiding biases that could compromise fairness and justice in decision-making.

§ 2 Data must be anonymized whenever possible, and it is a mandatory measure for confidential data or data protected by judicial secrecy, in accordance with the best practices for data protection and information security.

§ 3 Courts must implement mechanisms for data curation and monitoring, ensuring compliance with data protection legislation and the periodic review of data processing practices.

Article 8
Judicial decisions based on artificial intelligence tools must ensure equality, prevent abusive or unlawful discrimination, and promote plurality, guaranteeing that AI systems assist in fair judgments and contribute to eliminating or minimizing the marginalization of individuals and judgment errors arising from biases.

§ 1 Preventive measures must be implemented to avoid the creation of discriminatory biases, including the continuous validation of AI solutions and the auditing or monitoring of their suggested decisions throughout the entire lifecycle of the application, to ensure that AI solutions remain in compliance with the principles of fairness, plurality, and non-discrimination, with periodic reports assessing the impact of the solutions on fair, impartial, and efficient judgment.

§ 2 If a discriminatory bias or an incompatibility of the artificial intelligence solution with the principles established in this Resolution is identified, the necessary corrective measures shall be adopted, including temporary suspension (whether immediate or scheduled), correction, or, if necessary, the definitive elimination of the solution or its bias.
§ 3 If the removal of discriminatory bias is not possible, the artificial intelligence solution must be discontinued, with the consequent cancellation of its project registration in Sinapses. The preparation of a report detailing the measures taken and the reasons justifying the decision must be carried out, which may be submitted to independent review for further study, if applicable.

CHAPTER III
RISK CATEGORIZATION

Article 9

Courts must evaluate the risk level of Artificial Intelligence solutions, taking into consideration the categorization and criteria outlined in this Chapter and in the Risk Classification Annex, including factors such as the potential impact on fundamental rights, model complexity, financial sustainability, intended and potential uses, and the amount of sensitive data used.

§ 1 The evaluation shall be conducted by the court that develops or contracts the solution, preferably during the testing and approval phase or, in the case of low-risk applications, at the beginning of the internal deployment of the AI solution. This evaluation must follow clear guidelines and objective criteria to ensure uniformity in risk assessment, which shall be published on the Sinapses platform prior to the solution's availability on PDPJ-Br.

§ 2 The Judiciary National Artificial Intelligence Committee may establish the risk assessment guidelines and criteria referred to in § 1, after hearing the courts, developers, and civil society.

§ 3 The Judiciary National Artificial Intelligence Committee may, either ex officio or upon a substantiated request, determine the reclassification of the risk level of a particular solution, as well as mandate, with justification, an algorithmic impact assessment, when such a measure is deemed proportional, while respecting, as much as possible, the autonomy of the courts.

Art. 10. The Judiciary shall not develop or use the following solutions, for they pose excessive risks to information security, the fundamental rights of citizens, or the independence of judges:
I - Solutions that do not allow human review of the data used and the results proposed throughout their training, development, and usage cycles, or that create an absolute reliance on the proposed outcome by the user, without the possibility of modification or review;

II - Solutions that assess personal traits, characteristics, or behaviors of individuals or groups of individuals, to evaluate or predict the commitment of crimes or the likelihood of recidivism in the justification of judicial decisions;
III - Solutions that classify or rank individuals based on their behavior, social status, or personal traits, to assess the plausibility of their rights, the issue being adjudicated, or their testimonies;
IV - The identification and authentication of biometric patterns for emotion recognition.

§ 1 Courts must implement continuous monitoring mechanisms to ensure compliance with these prohibitions and oversee the development of AI solutions to prevent the unintentional use of prohibited technologies.

§ 2 Any AI solution that, during its use, falls under the prohibitions of this article must be discontinued, with documentation in Sinapses of the reasons and measures taken, for assessment by the Judiciary National Artificial Intelligence Committee, in order to prevent similar cases.

Article 11
AI solutions are considered high or low risk, as applicable, based on the techniques developed and used for the purposes and settings described in the Risk Classification Annex of this Resolution.

§ 1 High-risk solutions must undergo regular auditing and continuous monitoring processes to oversee their use and mitigate potential risks to fundamental rights, privacy, and justice.

§ 2 The categorization set forth in the Risk Classification Annex for high-risk solutions shall be reviewed at least annually by the Judiciary National Artificial Intelligence Committee, as provided in Article 16, I, of this Resolution, to ensure that the classification of high-risk settings remains up to date and continues to meet legal and ethical requirements.

§ 3 Low-risk solutions must be monitored and reviewed periodically to ensure they remain within those parameters and that any technological or contextual changes have not altered this classification.

CHAPTER IV
ON GOVERNANCE MEASURES

Art. 12. The developing or contracting court shall establish internal processes designed to ensure the security of artificial intelligence systems, including at least:
I - measures to ensure transparency regarding the use and governance of AI systems, including the publication of reports detailing the systems' functionality, purposes, the data processed, and supervision mechanisms;

II - the mitigation and prevention of potentially illegal or abusive discriminatory biases through continuous monitoring, analysis of outcomes, and the correction of any deviations, ensuring the periodic review of AI models.
III - the development of governance mechanisms to ensure the continuous monitoring of AI systems, including the appointment of individuals or internal committees responsible for overseeing compliance with security and transparency guidelines, as well as for analyzing reports and recommending improvements.
IV - the directive to prioritize the development of interoperable solutions that can be shared and integrated across different judicial bodies, avoiding redundancy and ensuring efficiency in the use of technological resources.
V - the requirement that only open-source or commercial solutions allowing flexibility to adapt to local contexts shall be employed, provided that security, transparency, and personal data protection guidelines are respected.
VI - the recommendation that AI solutions be managed following product management practices, including defining requirements, developing, testing, implementing, providing support, and continuously improving, with regular reviews to ensure these solutions evolve and associated risks are mitigated.
VII - the guideline to encourage the development of application programming interfaces (APIs) that enable interoperability for direct communication with the technological systems of other public institutions operating within the Justice structure, ensuring speed, security, and data integrity.
VIII - access for the Brazilian Bar Association (OAB), public advocacy, the Public Prosecutor's Office, and Public Defender's Offices, as applicable, to audit and monitoring reports, as well as to the parameterization throughout the lifecycle of AI-based solutions, in accordance with this Resolution.

Art. 13. Before being deployed in production, solutions that adopt high-risk artificial intelligence models must implement the following governance measures:

I - whenever technically possible, use training, validation, and testing data that are adequate, representative, and balanced, with appropriate statistical properties in relation to the affected individuals, taking into account specific characteristics and elements of the geographical, behavioral, or functional context in which the high-risk AI system will be used.
II - record automated sources and the degree of human supervision that contributed to the results generated by AI systems, ensuring they are subject to regular audits and continuous monitoring.
III - providing a clear and plain-language explanation of the objectives and intended outcomes of the ai model's use, ensuring these can be understood by users and supervised by judges;
IV - providing documentation in plain language, in a format appropriate to each ai agent and the technology used, explaining the system's functionality and the decisions involved in its development, covering all relevant stages of the system's lifecycle and updated whenever the system evolves;

V -using tools or processes for the automatic recording of the system's operations, enabling periodic evaluation of its accuracy and robustness, the detection of potential discriminatory outcomes, the implementation of risk mitigation measures with attention to adverse effects, and the identification of any malicious or improper use of the system;
VI - Measures to mitigate and prevent discriminatory biases, as well as management and governance policies to promote social and sustainable responsibility;
VII - The adoption of measures to enable explainability, whenever technically feasible, of the results produced by AI systems, as well as measures to provide proper information in plain and simple language that allows the interpretation of their results and functioning, while respecting copyright, intellectual property, and industrial and commercial confidentiality, ensuring the minimum transparency required to comply with the provisions of this Resolution.

Art. 14. The developing or contracting court must carry out an algorithmic impact assessment of solutions classified as high-risk in accordance with the provisions of Article 11 of this Resolution.
§1. The algorithmic impact assessment shall consist of a continuous process carried out in compliance with the technical guidelines and requirements previously established by the Judiciary National Artificial Intelligence Committee, including regular audits, continuous monitoring, periodic reviews, and the adoption of corrective actions when necessary.
§ 2. The preparation of the impact assessment should, whenever possible, include public participation, particularly from representatives of the Brazilian Bar Association (OAB), the Public Prosecutor's Office, and the Public Defender's Office, even if in a simplified manner.
§3. The findings of the impact assessment, including any corrective actions taken, shall be made public and available on the Sinapses platform through clear and accessible reports, ensuring comprehension by judges, court staff, and the general public.

CHAPTER V
ON SUPERVISION AND IMPLEMENTATION

Art. 15. The Judiciary National Artificial Intelligence Committee is hereby established.

§ 1. The Committee shall be composed of 14 (fourteen) full members and 13 (thirteen) alternates, divided by category, and appointed by an act of the President of the NCJ, from the following sources:

I - Two NCJ Councilors, both full members, with at least one of them being a member of the Permanent Commission on Information Technology.

II - Two auxiliary judges and two staff members with experience in NCJ-related matters;
III - Two judges, one representing the Federal Justice Council and one representing the Superior Council of Labor Justice.

IV - Four appellate judges, including one representative from a State Court of Justice, one representative from a Regional Federal Court, one representative from a Regional Labor Court, and one representative from an Electoral Court;
V - Two representatives from judicial training schools, one from the National School for the Training and Improvement of Judges (ENFAM) and one from the National School for the Training and Improvement of Labor Judges (ENAMAT).
VI - Four judges, selected from nominations by AMB, ANAMATRA, and AJUFE.
VII - Two representatives from the Brazilian Bar Association (Ordem dos Advogados do Brasil - OAB);
VIII - Two representatives from the Public Prosecutor's Office;
IX - Two representatives from the Public Defender's Office.
X - Two representatives from civil society, preferably with recognized expertise or a strong professional background in the fields of artificial intelligence, information technology, AI governance, and human rights.

§ 2. The presidency of the Committee, which shall have the casting vote, shall be held by the Councilor elected by the NCJ Plenary, while the vice-presidency shall be held by the other Councilor.

§ 3. The members referred to in items I to VI shall have both voice and voting rights, while those referred to in item VII and beyond shall have the right to speak but not to vote within the Committee.

§ 4. In cases of proven urgency, measures may be issued by the President of the Judiciary National Artificial Intelligence Committee, ad referendum of the full composition of the Committee.

§ 5 The decisions, statements, or proceedings of the Judiciary National Artificial Intelligence Committee may be submitted to the Plenary of the National Council of Justice, either ex officio or upon request, in accordance with Article 98 of its Internal Regulations. In the exercise of its original jurisdiction, the Plenary may decide, ratify, modify, assume jurisdiction over, or archive acts, proceedings, or matters related to the competencies assigned to the Committee under this Resolution.

§ 6 For the appointments provided for in § 1, the President of the NCJ may request nominations from relevant authorities or representative entities. The final appointment of full or alternate members in each category, as well as their replacement, when necessary, shall be at the President's discretion to ensure representation within the same category.

Art. 16. The Judiciary National Artificial Intelligence Committee shall have the following responsibilities:

I - to assess the need for updating the risk categorization criteria referred to in Article 11 and set forth in the Risk Classification Annex of this Resolution, based on objective criteria and in accordance with international best practices;
II - to reclassify certain systems contracted or developed by the courts, in accordance with § 3 of Article 9 of this Resolution, with due justification and the publication of a technical reclassification report, either ex officio or upon request.
III - to establish rules and business guidelines for the Sinapses system, including governance, transparency, audit, and monitoring standards;
IV - to consolidate governance standards and mapping of known and unknown risks, enabling the continuous definition and reassessment of the appropriate risk level for each application scenario, in consultation with courts, external experts, and civil society;
V - to recommend that the NCJ establish and implement agreements and cooperation arrangements with other national and international entities, aiming at the continuous improvement of AI systems and the incorporation of global best practices.
VI - to assess the advisability of using, ex officio or upon request, AI solutions available on the market, whether free or paid, that may be utilized by judges and court staff in the exercise of their judicial duties under a private license, particularly considering the conditions for the use of personal data and training data, security criteria, and the level of risk associated with the applications, while establishing additional governance and monitoring rules if necessary, in accordance with this Resolution.
VII - to monitor the training and education provided by the courts to their judges and staff, as well as to request or suggest that the National School for the Education and Training of Judges (ENFAM) and the National School for the Education and Training of Labor Judges (ENAMAT) develop curricular guidelines and initiatives aimed at training and education in artificial intelligence.
VIII - to mandate the execution or establish the minimum frequency for conducting audits and monitoring actions of artificial intelligence solutions, as well as to regulate the deadlines for the preparation of reports and their registration on the Sinapses platform;
IX - to define and implement standardized technical audit protocols, ensuring that all AI systems used by the Judiciary are audited prior to implementation and periodically thereafter, whenever possible;

X - To establish minimum transparency standards, including the requirement for detailed documentation and the publication of regular impact and performance reports, in accordance with this Resolution.

§ 1. The periodic evaluation referred to in item I, which may be included in the report provided for in Article 18 and published, shall address, in addition to other points deemed relevant for the administration of justice, the reasonable duration of proceedings, and the protection of fundamental rights:

I - A general analysis of the solutions registered in the Sinapses platform and those discontinued, discarded, or prohibited during the current year, with the publication of reports that may include conclusions and recommendations;
II - The necessary alignment with legislation and the normative acts of the National Council of Justice, especially regulations concerning data protection and the use of artificial intelligence;
III - An analysis of new technologies and innovations that may influence the effectiveness and adequacy of existing regulations, including recommendations for regulatory adjustments.
IV - To identify situations where the existing regulations prove insufficient to control the risks associated with the use of artificial intelligence within the Judiciary, and to propose measures to address gaps.

§ 2. The prohibition or limitation on the use of solutions based on large-scale language models (LLMs) and other generative artificial intelligence systems (GenAI), as referred to in item VI of the main provision of this Article, shall be guided by actual non-compliance or a well-founded risk of non-compliance with the guidelines established in § 3 of Article 19 of this Resolution. Such measures may include limiting the use of specific tools to low-risk solutions or determining provisions regarding data usage, while ensuring the possibility of revisiting any previously made decision if the conditions or terms of use of the solution are modified.

§ 3 National or foreign companies that provide storage, processing, digital intermediation, or artificial intelligence services to the Judiciary, or that operate platforms with a direct impact on the exercise of Brazilian jurisdiction, must fully comply with judicial decisions issued in Brazil and act in accordance with national legislation, observing the following:

a) Courts shall adopt continuous monitoring mechanisms to identify any non-compliance with judicial decisions by these companies, reporting such violations to the competent authorities for appropriate measures;

b) Contracts signed with technology companies must include contractual clauses requiring compliance with Brazilian legislation and judicial decisions, expressly providing for the possibility of contract termination and the application of penalties in case of non-compliance.

Art. 17. To support the assessment of updates to the risk categorization criteria, the Judiciary National Artificial Intelligence Committee shall consider the guidelines set forth in this Resolution, in addition to the following criteria:

I - Proven negative impact on the exercise of fundamental rights and freedoms or access to essential services;
II - High potential for material or moral harm, duly measured, including direct or indirect illegal or abusive discrimination;
III - Significant impact on individuals belonging to vulnerable groups, taking into account their social, economic, and cultural conditions;
IV - Irreversibility or difficulty in reversing potential harmful outcomes of the solution, particularly in cases directly affecting substantive or procedural rights, or causing significant automated activity in judicial proceedings;
V - A documented history of civil or administrative liability due to potential violations of the moral or substantive rights of external users by the artificial intelligence solution, duly analyzed in technical reports.
VI - Low levels of transparency, explainability, and auditability of the solution, with the adoption of objective criteria that hinder or prevent its control, supervision, and review by potentially interested parties;
VII - High levels of identifiability of data subjects, especially when processing involves the combination, matching, or comparison of data from multiple sources, with direct impact on privacy and personal data protection.

§ 1. The risk assessment shall be accompanied by performance indicators and audit or monitoring reports to ensure the effectiveness of risk mitigation measures.

§ 2. If an AI solution demonstrates low transparency or explainability, the responsible parties must promptly adopt corrective measures, including discontinuing the solution if corrections prove unfeasible.

Art. 18. The Judiciary National Artificial Intelligence Committee shall prepare a detailed report of its annual evaluation, which shall include:

I - The methodologies and criteria applied in the evaluation of artificial intelligence solutions;
II - The results of audits, monitoring activities, and algorithmic impact assessments conducted;
III - Updates to the risk categorization criteria listed in the Risk Classification Annex of this Resolution, if applicable;
IV - Recommendations for addressing identified flaws or improving the artificial intelligence solutions in use, as identified in audits, monitoring activities, or evaluations;
V - An overview of the state of generative artificial intelligence usage within the Brazilian Judiciary.

§ 1. The Committee shall publish the report and make it available to the general public, ensuring transparency in the evaluation and monitoring of AI solutions used in the Judiciary.

§ 2. The Committee may propose extraordinary reviews at any time if significant technological changes or new information warrant a reassessment of the risks associated with the AI solutions in use.

§ 3. The Committee shall ensure that all documents produced under this Resolution are available in accessible formats, promoting inclusion for persons with disabilities and other vulnerable groups while ensuring full transparency.

CHAPTER VI
ON THE USE AND PROCUREMENT OF LARGE LANGUAGE MODELS (LLMs) AND OTHER GENERATIVE AI SYSTEMS (GenAI)

Art. 19. Large Language Models (LLMs), Small Language Models (SLMs), and other generative artificial intelligence systems (GenAI) available on the internet may be used by judges and Judiciary staff in their respective activities as tools to support case management or assist in decision-making, in compliance with information security standards and the provisions of this Resolution.

§ 1. Courts shall preferably provide, enable, and monitor access to the models and solutions referred to in the main provision for use by judges and Judiciary staff.

§ 2. When the court does not offer a corporate artificial intelligence solution specifically trained and tailored for use in the Judiciary, judges, staff, or Judiciary collaborators may directly acquire a solution through a private subscription or registration, provided the guidelines set forth in § 3 of this Article are met.

§ 3. The direct procurement for private or individual use of large-scale language models (LLMs) and other generative artificial intelligence (GenAI) systems available on the global computer network, for functional activities within the Judiciary, shall be subject to the following conditions:

I - Users must undergo specific training and capacity-building programs on the limitations, risks, and the ethical, responsible, and efficient use of LLMs and generative AI systems in their activities. The courts and their training schools shall be responsible for promoting ongoing training for judges and Judiciary staff;
II - The use of these tools shall be supportive and supplementary, serving as mechanisms to assist decision-making. Their use as autonomous instruments for judicial decision-making is strictly prohibited without proper guidance, interpretation, verification, and review by the judge, who shall remain fully responsible for the decisions made and the information they contain;
III - Companies providing LLM and generative AI services must comply with data protection and intellectual property policy standards in accordance with applicable legislation. The processing, use, or sharing of data provided by Judiciary users, as well as data inferred from such data, is prohibited for training, improvement, or any other purposes not expressly authorized;
IV - The use of private or externally developed LLMs and generative AI systems for processing, analyzing, generating content, or making decisions based on confidential documents or data protected by judicial secrecy is prohibited, in accordance with applicable legislation. Exceptions are permitted only when the data has been properly anonymized at the source or when technical and procedural measures are implemented to ensure the effective protection and security of such data and its subjects.
V - The use of private or externally developed LLMs and generative AI systems is prohibited for purposes classified in this Resolution as excessively risky or high-risk, in accordance with Articles 10 and 11.

§ 4. The Judiciary National Artificial Intelligence Committee shall draft and periodically update a best practices manual in plain language to guide judges and court staff on the proper, ethical, and efficient use of LLMs and generative AI systems. The manual shall cover aspects such as their potential, limitations, recommended configurations, risks, appropriate and prohibited use cases, guidelines for critically interpreting results, and correcting potential errors or inconsistencies.

§ 5. Courts and their training schools, in alignment with the guidelines of the National Council of Justice, the National School for the Education and Improvement of Judges (ENFAM), and the National School for the Education and Improvement of Labor Judges (ENAMAT), shall promote continuous training programs to ensure the proper and responsible use of LLMs and generative AI systems by judges and Judiciary staff, as well as to keep them updated on the evolution of these technologies and their implications for the justice system.

§ 6. When generative AI is used to assist in drafting judicial acts, this fact may be mentioned in the text of the decision, at the judge's discretion. However, the internal system of the court must automatically register such use for statistical, monitoring, and audit purposes.

§ 7. In the case described in § 2 of this Article, any judge or manager who procures an artificial intelligence solution from the market for use in their Judiciary activities, or whose team includes staff or collaborators using such solutions, must periodically provide information to the local Judicial Oversight Office regarding its use, in accordance with applicable regulations.

§ 8. The Oversight Offices shall consolidate the information received pursuant to § 7 of this Article and submit it to the Judiciary National Artificial Intelligence Committee, which will use it for the purposes set forth in Article 25 of this Resolution.

Art. 20. The procurement of large-scale language models (LLMs), small-scale language models (SLMs), and other generative artificial intelligence (GenAI) systems by the courts shall comply with the following guidelines:

I - The contracted company must commit to complying with the laws in force in Brazil, including Lei Complementar No. 35 of March 14, 1979 (Foundational Law of the National Judiciary - LOMAN), the General Data Protection Law, Law No. 9,279 of May 14, 1996 (Intellectual Property Law - IPL), and this Resolution;
II - The use of data provided by Judiciary users for training purposes shall comply with the regulations established by the General Data Protection Law (LGPD) and cannot be used for purposes other than those expressly authorized, with continuous monitoring to ensure compliance with data protection and intellectual property guidelines;\
III - Contracting courts and their training schools, along with the judiciary and its staff, are responsible for providing training to internal users of LLMs and generative AI systems on the limitations, risks, and ethical, responsible, and efficient use of these solutions prior to their use in professional activities;
IV - The use of these tools shall be limited to an assisting and supporting role, and their use as autonomous instruments for judicial decision-making is prohibited without proper guidance, interpretation, verification, and review by the judge, who shall remain fully responsible for the decisions made and the information contained therein;
V - The use of LLMs and generative AI systems to process, analyze, generate content, or support decision-making based on confidential documents or data protected by judicial secrecy is prohibited, except in the cases provided for in Article 19, § 3, IV of this Resolution.
VI - It is forbidden to use private or non-judiciary LLMs and generative AI systems for purposes classified in this Resolution as excessively high-risk or high-risk, as defined in Articles 10 and 11;
VII - Contracted companies must safeguard the confidentiality of information shared by contracting courts, comply with and demonstrate the adoption of up-to-date security standards aligned with state-of-the-art practices, and may be required to undergo external audits or provide periodic reports on data security and compliance;

VIII - Contracted systems must provide updated documentation and bibliographic references, whenever available, in accordance with the intended use of their results;
IX - Contracted systems must adopt privacy by design and privacy by default mechanisms, including options for non-storage or deletion of the history of questions and prompts, and may be required to submit reports with clear indicators to assess their implementation and compliance.
X - The procurement of artificial intelligence services or solutions by the courts shall consider financial and budgetary aspects throughout their entire lifecycle, particularly in development, implementation, and maintenance.

Sole Paragraph. The use of confidential data or data protected by judicial secrecy for training artificial intelligence models is prohibited, except when such data has been previously anonymized at the source.

Art. 21. Electronic judicial process systems that employ artificial intelligence solutions must display, on their main interface, the list of models in use, their versions, registration codes in Sinapses, and the date of the latest update of this information.

§ 1. This information shall be reviewed and updated at least every twelve months or whenever significant changes are made to the models or their versions.

§ 2. Products automatically generated by artificial intelligence solutions must record the use of AI in the system's activity logs using appropriate and clearly identifiable tags for statistical, monitoring, and auditing purposes.

CHAPTER VII

TRANSPARENCY AND REGISTRATION IN SINAPSES

Art. 22. Any artificial intelligence model adopted by

the Judiciary must comply with the data governance rules applicable to their own computational systems, the Resolutions and Recommendations of the National Council of Justice, the General Data Protection Law, Law No. 12,527/2011 (Freedom of Information Act - LAI), intellectual property rights, and judicial secrecy.

§ 1. Compliance with these rules must be contractually ensured and enforced through continuous monitoring and, when necessary, audits focused on the protection of data, intellectual property, and the transparency of the AI models adopted.

§ 2. The use of artificial intelligence models within the Judiciary must be documented by periodic reports that demonstrate compliance with data governance guidelines, particularly for sensitive data, transparency, and the protection of intellectual property.

§ 3. The AI models that are adopted must include explainability mechanisms, whenever technically feasible, ensuring that their decisions and operations are understandable and auditable by judicial operators.

Art. 23. Judicial offices involved in artificial intelligence projects must:

I. Notify the National Council of Justice through the Sinapses platform about the conclusion of research or studies, the beginning of development, and the deployment of the AI solution, as well as its objectives and intended outcomes;
II. Promote efforts to operate under a collaborative model, discouraging parallel development by a court when an initiative shares identical and compatible objectives and outcomes with an existing AI model or system in another court;
III - The deposit of the source code, databases, and other components of the AI solution may be waived whenever copyright and intellectual property protection licenses restrict their public sharing. In such cases, the court must specify the systems, engines, databases, LLMs, and other elements used in the AI solution, along with their respective versions and providers.

Art. 24. AI solutions, whether under development or already adopted within the Judiciary, must be registered in the Sinapses platform, which will present a catalog of AI systems adopted by the Brazilian Judiciary, organized according to the solution's risk categorization as outlined in the Risk Classification Annex of this Resolution.

§ 1. The public summary of the algorithmic impact assessment referred to in Article 14 of this Resolution must also be included in Sinapses when the solutions are classified as high risk.

§ 2. The public summary may exclude sensitive, confidential, or proprietary data, ensuring the protection of privacy and the confidentiality of information.

§ 3. The court responsible for low-risk solutions must register them in the Sinapses platform before deployment into production, including the minimum information required, such as the solution's purpose, whether it is a proprietary or collaborative creation, whether the tool is contracted or internally developed, and a description of its objectives.

§ 4. For high-risk solutions, registration in the Sinapses platform may be completed after preliminary studies but must necessarily occur before the development begins.

§ 5. The information registered must be supplemented and updated as the solution evolves, with mandatory updates required for each new phase or significant version of high-risk solutions.

§ 6. The National Council of Justice shall provide the Sinapses Platform with the necessary infrastructure to receive registrations made by the courts, while exempting the deposit of large databases or models protected by intellectual property rights.

Art. 25. The National Council of Justice shall publish, on a dedicated section of its website, a list of applications that adopt artificial intelligence techniques, either developed or used by Judiciary offices, including a clear and concise description in plain language and an indication of the respective risk level, along with accessible explanations regarding the implications of the risk classification.

§ 1. The information must be periodically updated, with mandatory revisions every twelve months or whenever significant changes occur in the applications, such as software updates, changes in the risk level, or discontinuation.

§ 2. The list must clearly indicate the criteria used for risk classification, as well as any instances of discontinuation or suspension of application use.

§ 3. The National Council of Justice may remove discontinued or suspended applications from the catalog, provided that such removal is publicly communicated with justification.

CHAPTER VIII
QUALITY AND SECURITY

Art. 26. The data adopted in the development of artificial intelligence solutions should preferably come from public or governmental sources and shall undergo quality curation, particularly when developed internally, always in compliance with the guidelines of the General Data Protection Law.

§ 1. Secure sources for obtaining data are those that employ mechanisms for data validation and curation, ensuring accuracy, balance, integrity, and reliability. When data from non-governmental sources is adopted, a rigorous verification of the data's quality and security must be conducted.

§ 2. The use of data from non-governmental sources shall be allowed only when governmental data is insufficient or inadequate for the specific purpose of the artificial intelligence solution, provided that such data is validated in accordance with the criteria established in this article.

§ 3. Solutions procured by courts must contractually guarantee compliance with the guidelines of the General Data Protection Law.

§ 4. Entities shall collect only the data strictly necessary for training and shall not retain datasets without a clear purpose or proper storage control.

Art. 27. The system must prevent any alteration to the data received before its use in the development workflow of artificial intelligence solutions. This should be ensured through mechanisms such as version control, tokens, and audit and monitoring logs that guarantee data integrity and traceability.

§ 1. A copy of each dataset used in relevant versions of the models developed must be retained, ensuring that the data can be audited and reviewed whenever necessary.

§ 2. Copies of the datasets must be securely stored, employing encryption and access controls, in compliance with the guidelines of the General Data Protection Law, to safeguard against unauthorized access and other information security risks.

§ 3. If long-term retention of all datasets for relevant system versions becomes unfeasible due to their size, the court may establish a deletion plan for these files, in accordance with a timeline suitable to the algorithmic impact of the solution. However, the dataset previously used must be retained for at least one year after its obsolescence or modification.

Article 28. The storage and operation of artificial intelligence solutions, whether hosted in proprietary data centers, cloud service providers, or accessed through APIs (application programming interfaces), must ensure the isolation of data shared by the court. This should be achieved using appropriate security mechanisms, such as encryption and environment separation.

§ 1. The segregation must ensure that the court's data cannot be accessed, manipulated, or used by unauthorized third parties, safeguarding the privacy and security of the information.

§ 2. Cloud service providers and APIs must comply with Brazilian legislation, including the General Data Protection Law (LGPD), and adopt best practices in information security to protect the court's data.

§ 3 The use of cloud services and APIs for data storage, processing, and sharing within the Judiciary shall only be permitted through providers that meet mandatory minimum security and privacy standards, including:

I ‑ compliance with the General Data Protection Law (LGPD);

II - international information security certifications, in accordance with the guidelines of the National Committee;
III - adoption of robust encryption for data in transit and at rest;
IV - transparency in the policy for the retention, processing, and disposal of judicial data.

Art. 29. Data stored during the development and implementation of artificial intelligence solutions must be effectively safeguarded against risks of destruction, alteration, loss, unauthorized access, or unauthorized transmission through appropriate technical and administrative measures.

§ 1. Data protection measures must include the implementation of encryption, permission-based access control, regular audits, and monitoring to identify and mitigate potential security threats.

§ 2. Data protection practices must comply with the General Data Protection Law (LGPD) and applicable information security regulations, ensuring data privacy and integrity.

§ 3. Continuous and proactive monitoring tools, along with incident prevention measures, must be adopted to ensure a swift response to any attempted data security breaches.

Art. 30. In cases where the use of artificial intelligence solutions occurs directly through websites, applications, or APIs (application programming interfaces) that utilize shared data to feed the central repository or for training or (re)adjustment of the model, the sharing of data held by the Judiciary is prohibited, except when such data has been anonymized or pseudo-anonymized at the source, in compliance with the General Data Protection Law (LGPD) and best data security practices.

§ 1. Anonymization at the source is defined as the technical process of eliminating the possibility of a direct or indirect association between personal data and an identifiable natural person, conducted before the data is transmitted or processed by the AI solution.

§ 2. Mechanisms for auditing and control must be implemented to verify and ensure compliance of AI solutions with data protection regulations, particularly in the use of data for training or readapting artificial intelligence models.

Art. 31. The storage and operation of artificial intelligence models must take place in environments that comply with recognized information security standards, as outlined in this article.

Sole Paragraph. Best practices that comply with the provisions of the main section of this article include:

I - strict access controls, encryption of data both at rest and in transit, and the implementation of vulnerability management policies in storage and operational environments;
II - periodic audits and continuous monitoring mechanisms to ensure conformity with recognized security standards, providing adequate protection against unauthorized access, integrity failures, and other threats to information security;
III - the establishment of a data governance policy aimed at:
a) Continuously educate the team on information security practices, personal data protection, and privacy.

b) eliminating non-anonymized personal data from data repositories (data lakes, data warehouses, or data lakehouses) after model training is completed, in compliance with Art. 26, § 4, and Art. 27, § 3, of this Resolution.
c) Maintaining only tokenized data strictly necessary for the model, securely storing the latest approved datasets in locations that adhere to information security standards, in accordance with Art. 26, § 4, and Art. 27, § 3, of this Resolution;
d) Implementing data governance and curation processes to ensure data quality and security;
e) Conduct continuous monitoring and, when necessary, audits on models under testing and approved models to ensure compliance with security standards, personal data protection, and privacy.
f) Ensuring the functionality of models throughout the entire lifecycle of AI solutions and removing them once they become unnecessary or obsolete.
IV - adopting internationally recognized standards as a reference, whenever possible, such as ISO/IEC (International Organization for Standardization /International Electrotechnical Commission) 42001, the ISO/IEC 27000 series, and those issued by NIST (National Institute of Standards and Technology), or their successors, in addition to applicable local regulations.

CHAPTER IX
ON USER CONTROL

Article 32. The intelligent system shall ensure the autonomy of internal users by employing models that:

I - promote increased efficiency, accuracy, and quality in activities, without limiting the users' ability to act;
II - allow for a detailed review of the content generated and the data used in its preparation, ensuring that users have access to the assumptions and methods employed by the artificial intelligence in its formulation, without any obligation to adhere to the solution presented by the artificial intelligence, and guaranteeing the possibility of corrections or adjustments.

Sole Paragraph. Under no circumstances may the AI system restrict or replace the final authority of internal users.

Article 33. External users must receive clear, accessible, and objective information about the use of AI-based systems in the services provided to them. The information should use simple language to ensure non-specialized individuals easily understand it.

§ 1. The information described in the main provision of this article must emphasize the consultative and non-binding nature of the proposed solution presented by artificial intelligence. A competent authority must always review and issue the final decision, exercising human oversight over the case.

§ 2. Courts must communicate the use of AI through appropriate channels, such as system notices, informational materials, and explanatory guides. These resources should help external users understand the functioning, limitations, and objectives of intelligent systems within the Judiciary.

§ 3. The decision to communicate the use of AI in judicial decisions rests with the signatory, in accordance with § 6 of Article 19 of this Resolution.

§ 4. Courts must periodically provide educational materials to help external users understand the use of AI in judicial processes. These materials should clarify that AI systems play a supporting role and do not replace human decision-making authority.

Article 34. Computational systems used within the Judiciary must include human supervision and allow the competent judge to modify any output generated by artificial intelligence, whenever necessary, in compliance with Article 32 of this Resolution.

CHAPTER X
ON THE RESEARCH, DEVELOPMENT, AND IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE SERVICES

Article 35. Teams tasked with researching, developing, and implementing computational solutions that use artificial intelligence must prioritize diversity and representativeness. They should include individuals with varied gender and ethnic profiles, as well as diverse experiences and educational backgrounds.

§ 1. Teams must ensure representative participation, as much as possible, during the stages of planning, data collection and processing, model building, verification, validation, and implementation, covering both technical and business-related areas.

§ 2. Courts may waive the diversity requirements outlined in this article through a reasoned decision. Justifications may include, among other factors, the unavailability of qualified professionals within the court staff or the need to ensure efficiency and speed for short-term solution implementation.

§ 3. Teams must be interdisciplinary and include professionals from Information Technology, Law, and other relevant fields. Their scientific knowledge should contribute to the research, development, or implementation of intelligent systems within the Court.

Article 36. Studies, research, education, and training in artificial intelligence must be conducted in a manner that ensures fairness and impartiality, and must:

I - uphold the dignity and freedom of individuals or groups involved, avoiding any form of discrimination, harassment, or exclusion;
II - prevent activities that may pose risks or cause harm to humans, such as unsafe testing, manipulation of sensitive data without consent, or the indiscriminate or malicious use of data that could undermine fairness in decision-making;
III - identify and eliminate biases or prejudices that could compromise the objectivity or impartiality of the research or its results.

Article 37. Once courts finalize the research and begin developing solutions using artificial intelligence models, they must register the initiative in Sinapses, as outlined in Article 23 of this Resolution, and ensure its continuity as long as it remains useful for judicial activities.

§ 1. Courts must terminate the activities described in this article if a reasoned decision determines that the initiative fails to comply with the principles established in this Resolution or other applicable judicial regulations, and its adjustment is deemed unfeasible.

§ 2. Courts that intend to use artificial intelligence models applying facial recognition or biometric analysis techniques classified as high-risk applications, as defined in the Risk Classification Annex, item AR5, must obtain prior authorization from the Judiciary National Artificial Intelligence Committee. They must also submit a plan demonstrating compliance with fundamental rights, personal data protection, and the mitigation of potential discriminatory biases, particularly regarding race, social status, or geographic location of residence.

Article 38. Artificial intelligence models may use commercial tools or open-source solutions that:

I - facilitate their integration or interoperability with the systems used by Judiciary bodies, enabling efficient and secure information exchange;

II - create a collaborative development environment where different courts and institutions can contribute to the advancement of appropriate solutions;
III - ensure greater transparency by making processes and algorithms accessible for auditing, monitoring, and review by authorized experts or, upon request, by civil society;
IV - promote cooperation with other sectors and areas of the public sector, as well as civil society, fostering joint initiatives for the development and implementation of artificial intelligence solutions;
V - ensure the protection and security of the data used, particularly the data for which the Judiciary is responsible, by adopting measures to prevent unauthorized access and preserve the integrity of the information;
VI - ensure technological independence, avoiding reliance on a single provider or technology.

CHAPTER XI
ON AUDIT AND MONITORING

Article 39. Any computational solution implemented by the Judiciary that uses artificial intelligence models must ensure full transparency in accountability, aiming to ensure a positive impact for end-users and society.

§ 1. Accountability shall include:

I - the names of those responsible for executing the actions and for accountability reporting;
II - the costs involved in research, development, implementation, communication, and training;
III - the existence of collaborative and cooperative actions between public sector agents or between these agents and private sector entities or civil society;
IV - the intended results and those actually achieved;
V - evidence of effective disclosure regarding the nature of the service offered, the techniques used, system performance, and risks of errors;
VI - evidence that the information listed above has been disclosed in an accessible format and simple language, through appropriate channels, with regular updates, allowing public interaction to address questions and provide suggestions.

§ 2. The accountability report must be published through an official channel and may be subject to external audit by decision of the Court or the Judiciary National Artificial Intelligence Committee, as applicable.

Article 40. The development or use of intelligent systems that do not comply with the principles and rules established in this Resolution and other applicable regulations shall be monitored by the Judiciary National Artificial Intelligence Committee, without a disciplinary nature.

Sole Paragraph. Monitoring may indicate the need for an audit regarding inappropriate practices, misuse of data, or lack of transparency. Any identified noncompliance or discrepancies may be reported by the Committee to the competent authority for appropriate measures.

Article 41. The Judiciary National Artificial Intelligence Committee shall establish an audit and monitoring protocol for artificial intelligence models and solutions in use within the Judiciary.

§ 1. The Committee will define the methodology for conducting audits, considering risk identification, the establishment of safeguards (protective measures), and the documentation produced.

§ 2. To carry out audit and inspection activities, the Committee may propose to the President of the National Council of Justice the creation of technical committees or working groups, which must include qualified members with expertise in areas related to artificial intelligence auditing.

§ 3. Monitoring will consist of a simplified set of activities, including analysis, verification, and the adoption of best practices for data, process, and product management, to ensure the regular operation of AI-based solutions and their continued compliance with the guidelines of this Resolution.

§ 4. If non-compliance is identified, the Committee will set a deadline for correction, based on the severity and impact of the non-compliance.

Article 42. Judiciary bodies must report all adverse events related to the use of artificial intelligence solutions to the Judiciary National Artificial Intelligence Committee.

§ 1. Adverse events refer to incidents that cause negative impacts on system operations, data security, or service delivery.

§ 2 The communication of adverse events must be carried out within 72 (seventy-two) hours after their identification, including a description of the incident, its causes, and the corrective measures taken.

§ 3. The Committee will review the submitted information and may recommend corrective actions as necessary.

CHAPTER XII
FINAL PROVISIONS

Article 43. Judiciary bodies may establish technical cooperation agreements with other institutions, whether public or private, or with civil society, to collaboratively develop artificial intelligence models, provided that the provisions of this Resolution are observed.

§ 1. Technical cooperation agreements must include provisions that define the responsibilities of each party regarding data protection and the confidentiality of shared information.

§ 2. Partner institutions must ensure that the data used in the collaboration comply with the requirements of the General Data Protection Law and the security standards established by the National Council of Justice.

§ 3. Judiciary AI solutions must be developed with the objective of making their applications available on the **PDPJ-Br platform**. If necessary, they may be adapted to meet the platform's technical requirements.

Article 44. The provisions of this Resolution do not exclude the application of other norms within the Brazilian legal framework, including, but not limited to, federal, state, and municipal laws, as well as international treaties and conventions ratified by the Federative Republic of Brazil.

Article 45. The provisions of this Resolution also apply to artificial intelligence projects and models already under development or implemented in the courts, provided that already established acts are respected.

Sole Paragraph. Courts shall have a period of twelve months to adapt their projects and models, whether under development or already implemented, to the new provisions established in this Resolution, starting from its publication.

Article 46. NCJ Resolution No. 332, dated August 21, 2020, is hereby revoked as of the effective date of this Resolution.

Article 47. This Resolution shall enter into force 120 days after its publication.

RISK CLASSIFICATION ANNEX

The following purposes and contexts are considered high-risk for the development of artificial intelligence solutions designed to perform or support users in carrying out the following ancillary activities:

HR1 - Identifying profiles and behavioral patterns of natural persons or groups of natural persons, except when classified as low-risk or controlled situations according to objective criteria established;

HR2 - Assessing the adequacy of evidence and its evaluation in contentious jurisdiction cases, whether documentary, testimonial, expert, or of other types, especially when such evaluations can directly influence judicial decisions;

HR3 - Investigating, evaluating, classifying, and interpreting facts as crimes, criminal offenses, or infractions, except for solutions intended solely for routine tasks in criminal enforcement and socio-educational measures;

HR4 - Formulating conclusive judgments about the application of legal norms or precedents to a specific set of concrete facts, including the quantification or qualification of damages suffered by individuals or groups in criminal or non-criminal cases;

HR5 - Performing facial or biometric identification and authentication to monitor the behavior of individuals, except when used solely to confirm the identity of a specific individual or for duly justified public security activities, always ensuring compliance with fundamental rights and the continuous monitoring of such solutions.

The following purposes and contexts are considered low-risk for the development of artificial intelligence solutions designed to perform or support users in carrying out the following ancillary activities:

LR1 - Executing routine procedural acts or tasks that support judicial administration by extracting information from systems and documents. This includes classifying and grouping data and processes, enriching registries, certifying and transcribing procedural acts, summarizing documents, among other purposes related to procedural and operational management, provided that a human supervisor oversees these activities.

LR2 - Detecting decision-making patterns or deviations from such patterns, as well as identifying relevant qualified precedents, provided that artificial intelligence is used as a supporting tool. This usage must not replace human evaluation of cases and should be intended solely for internal court support and the standardization of case law.

LR3 - Providing judges with decision-making support through management reports and analyses using legal analytics techniques, integrating relevant information sources or detecting decision-making patterns. The solution must not replace human evaluation and must not make moral judgments about evidence, profiles, or individual behaviors;

LR4 - Producing supporting texts to facilitate the drafting of judicial acts, provided that the judge supervises and finalizes the document based on their instructions, especially decisions on preliminary matters and substantive issues;

LR5 - Enhancing or formatting a previously human-performed activity, provided that the substantive result remains unchanged, or performing a preparatory task for another activity classified as high-risk.

LR6 - Conducting statistical analyses for judicial policymaking, provided that continuous human supervision is ensured, especially to prevent biased conclusions;

LR7 - Transcribing audio and video to assist judges, with the final review carried out by a responsible individual.

LR8 - Anonymizing documents or their display, particularly to ensure compliance with privacy and data protection regulations.