Scientific
Journal of
**Applied
Social and
Clinical
Science**

ARTIFICIAL INTELLIGENCE IN THE BRAZILIAN JUDICIARY: THE EUROPEAN EXPERIENCE AS A REFERENCE

Adriana Barrea
Judge of the Court of Justice of the State of São Paulo in the Courts – Civil of Campinas. Studying specialization in Judicial Management: High Performance Judiciary, from the National School of Training and Improvement of Magistrates (ENFAM), and specialist in Digital Law from ENFAM and in Social Service, Ethics and Human Rights from UNYLEA.

Camila Henning Salmoria
Judge of the Court of Justice of Paraná, member of the 5th Appeal Panel; Master's student in Law, Efficiency and Justice System, at the National School of Training and Improvement of Magistrates (ENFAM) and specialist in Digital Law at ENFAM; student in Artificial Intelligence by: ``Universidade Positivo`` (UP); gender researcher in the collective. Post-graduation professor at EMAP /Faculdade Pan-americana.

Abstract: The objective of this article is to analyze the EU AI ACT, identifying its potential for improving Brazilian regulation for the Judiciary, Resolution 332 of the CNJ (NATIONAL COUNCIL OF JUSTICE). Through a deductive methodological approach, employing indirect research based on bibliographic and documentary review, the study analyzes the European regulatory model, drawing a comparison with the Brazilian system, identifying possibilities for improvement. The EU AI ACT analysis reveals that the European regulatory model is more comprehensive and robust than the Brazilian one and reveals that CNJ (NATIONAL COUNCIL OF JUSTICE) Resolution 332 can be improved in a series of aspects. In conclusion, the study finds that there are great opportunities to improve CNJ (NATIONAL COUNCIL OF JUSTICE) Resolution 332 with the adoption of models brought by European regulation.

Keywords: artificial intelligence, regulation, Judiciary, Brazil, European Union, CNJ (NATIONAL COUNCIL OF JUSTICE) Resolution 332

INTRODUCTION

According to the statistics panel, until July 31, 2023[1], 82,574,093 cases are being processed in Brazil.

With the implementation of the electronic process, Courts across the country undertake initiatives that contribute to the delivery of judicial provision more quickly.

Codex is a national platform developed by the Court of Justice of Rondônia in partnership with the National Council of Justice (CNJ (NATIONAL COUNCIL OF JUSTICE)), consisting of a procedural database that contains texts in structured data. Currently, there are 171 million processes stored, downloaded and in progress.

Thus, there is Big Data in the sphere of the judiciary that can serve as a basis for multiple research, from panels and management reports to the measurement of data aimed at implementing public policies and improving judicial services provided to the population.

In the meantime, the advancement of technology drives the need for public resources to be better managed. This is to recognize that the implementation of artificial intelligence will contribute to the provision of jurisdiction in a faster and more efficient way in resolving disputes aimed at social pacification.

The regulation of Artificial Intelligence (AI) has become a crucial issue as its presence and influence extends across diverse sectors of society. The need to establish clear criteria for its use has driven a series of regulatory efforts around the world. Among these initiatives, the recent approval, by the European Parliament, of a comprehensive set of guidelines to regulate AI stands out. This regulation has been the subject of considerable interest due to its thoroughness and breadth.

In Brazil, although there is still no specific legislation aimed at the comprehensive regulation of AI systems, the National Council of Justice (CNJ (NATIONAL COUNCIL OF JUSTICE)) established, in 2020, Resolution 332, which preliminarily addressed the issue within the scope of the Judiciary. However, with technological advances and the emergence of text-generating AI systems, a more in-depth review of this regulation becomes imperative.

The purpose of this article is to examine the extent to which European regulation can contribute to the improvement of CNJ (NATIONAL COUNCIL OF JUSTICE) Resolution 332. The first chapter performs a comprehensive analysis of AI regulation in different parts of the world, contextualizing

---

1 BRAZIL. CNJ (NATIONAL COUNCIL OF JUSTICE). Painel analytics. Available on the website: <https://paineisanalytics. CNJ (National Council of Justice). jus.br/single/?appid=9e4f18ac-e253-4893-8ca1-b81d8af59ff6&sheet=b8267e5a-1f1f-41a7-90ff-d7a2f4ed34ea&lang=pt-BR&theme=IA_PJ&opt=ctxmenu,currsel&select=language,BR>. Accessed on: 05 Oct. 2023.

both the European and Brazilian approaches. The second chapter is dedicated to examining the innovations brought about by the European regulatory model, with a specific focus on its applicability to the model established by Resolution 332. Finally, the third chapter examines the points of convergence between the resolution and the European act, evaluating the possibilities for improving national legislation.

THE REGULATION OF AI IN THE WORLD

The report prepared by the Law Library of Congress offers a comprehensive overview of AI regulation around the world. This study covers both legislations already approved and those in the approval process, both by countries and international organizations, as long as they have legal effects[2].

The 1981 Council of Europe (CoE) Convention represents the first international treaty on the protection of personal data, having entered into force in 1985. Currently, several countries already have some type of regulation relating to AI[3] while others are still in the discussion stages[4].

In some nations, normative texts address general aspects related to the development and commercialization of AI systems, establishing ethical guidelines, ensuring compliance with fundamental rights and providing authorities to supervise the progress of implemented systems.[5]. In other countries, regulation addresses issues such as payments, autonomous vehicles and the illegality of content produced by generative AI[6].

In Greece, for example, there are laws that establish registration or licensing requirements for certain AI systems, in addition to a project proposed in Canada on this topic. Furthermore, in countries such as Greece, Finland, Norway, Spain and Sweden, laws have been passed that address transparency, prevention of bias and assessment of the impact of the use of AI systems.

It must be noted that in the United Kingdom, a law was enacted authorizing the government to intervene in companies developing AI systems whose results could compromise the country's security. On the other hand, in Macau, there are tax benefits for companies that develop AI, which demonstrates the concern to value innovation.

It is concluded, therefore, that regulatory perspectives around the world are diverse, taking into consideration, several factors, such as the reality of each country and the nature of the services provided (whether public, on digital platforms or economic). However, these perspectives converge in the observance of fundamental rights and respect for the user, based on the self-determination of information, interfacing with the legislation that protects the personal data of those subject to jurisdiction.

EUROPEAN AI REGULATION

On July 14, 2023, the European Parliament approved the preliminary text of the

2 UNITED STATES OF AMERICA. Library of Congresss. **Regulation of artificial intelligence around the world**. Available on the website: <https://hdl.loc.gov/loc.law/llglrd.2023555920>. Accessed on: 14 Oct. 2023.
3 Argentina, Belarus, China, Denmark, Egypt, Estonia, Finland, Greece, Hungary, Iceland, Kazakhstan, Kyrgyzstan, Lithuania, Macau, Mauritius, Norway, Peru, Poland, Portugal, Qatar, Republic of Ireland, Russian Federation, Saudi Arabia, Serbia, Slovak Republic, Spain, Sweden, Taiwan, United Arab Emirates, United Kingdom and Uzbekistan.
4 Argentina, Belgium, Brazil, Canada, Chile, Colombia, Costa Rica, Israel, Mexico, Panama, Philippines, South Korea, Thailand and the United Kingdom.
5 Argentina, Belarus, Egypt, Iceland, Kazakhstan, Peru, Portugal, Qatar, Republic of Ireland, Russian Federation, Saudi Arabia, Serbia, Uzbekistan, and proposed legislation in Brazil, Chile, China, Colombia, Costa Rica, Israel, Mexico, Panama, Philippines, Taiwan and Thailand
6 China, Estonia, Greece, Hungary, Lithuania, Poland, United Arab Emirates, United Kingdom and Uzbekistan and Kyrgyzstan.

regulation of AI systems. The project was proposed by the European Commission in 2020, but is only expected to become law in mid-2025. The wording will still be the subject of negotiations with the European Council and Member States[7].

Although it does not have legal status, the European Union Artificial Intelligence Act (EU AI ACT) has attracted significant attention as it stands out as one of the first global regulations on the subject. In addition to the impacts this legislation will have beyond the borders of the European Union, it is expected to serve as an inspiring model for other jurisdictions around the world, similar to what happened with the General Data Protection Regulation (GDPR).

The act appears with a dual purpose: to promote technological innovation and safeguard human rights. To achieve these objectives, the following general principles were established: human oversight, security, privacy and data governance, transparency, non-discrimination and social and environmental well-being.

It must be noted that the European regulation will have the force of law. Thus, due to its binding nature, intended for all bodies and sectors of society, both in Europe and in the global market, which makes the regulations robust and of respectable content.

AI REGULATION IN BRAZIL

In Brazil, inspired by the IA Act, project, number: 2338/2023 is being processed with points of contact with European regulation, among others, which deserve to be highlighted: the use of technology at the service of man, human intervention to supervise systems of artificial intelligence (rights of affected people); transparency in the use of AI (opacity of algorithms that result in unauditable decisions), respect for fundamental rights,

the gradation of risks and the importance of regulation as a means of promoting the advancement of technology.

However, according to the commission of jurists, the aforementioned project demands greater debate, including because Generative AI is highlighted, which is also pending regulation around the world.

CNJ (NATIONAL COUNCIL OF JUSTICE) RESOLUTION 332/2020

In Brazil, referring to the European Charter of Ethics on the Use of Artificial Intelligence in Judicial Systems and their environments, the National Council of Justice published Resolution 332, which represents an important milestone in the regulation of AI, especially for the Judiciary. Focusing on transparency and security, the resolution establishes basic guidelines for the development and use of artificial intelligence systems within the Judiciary, highlighting the principles of dignity, freedom and equity in decisions (art. 21).

This is why it is important to highlight that, given the absence of specific standards, in Brazil, Resolution CNJ (NATIONAL COUNCIL OF JUSTICE) 332/2020 constitutes a regulatory framework for the Judiciary that has been developing with the implementation of the electronic process and its use in all regions. of extensive territoriality.

It is worth noting that resolution CNJ (NATIONAL COUNCIL OF JUSTICE), 332/2020 is a normative act issued by the National Council of Justice, controlled by the Federal Supreme Court and with the force of law, in addition to being specifically intended for bodies of the Brazilian Judiciary. So much so that it does not require the robustness required by European regulations, although improvements are welcome.

The regulations also cover aspects of

7 FERRAREZI, T. European Parliament adopts position to regulate AI. Available on the website: https://www.migalhas.com.br/depeso/389455/parlamento-europeu-adota-posicao-para-regulamentar-a-ia Accessed on: Jun 9, 2023.

data governance, ethical parameters for the development and use of Artificial Intelligence; with a focus on compliance with Fundamental Rights. So much so that Resolution CNJ (NATIONAL COUNCIL OF JUSTICE) 332/2020 provides for "ethics, transparency and governance in the production and use of Artificial Intelligence in the Judiciary and provides other provisions.

In its "recitals", it highlights the following points:

1. AI systems must be used with agility and consistency for decision-making, in compliance with and compatibility with Fundamental Rights;

2. the decision that is supported by AI systems must meet ethical criteria, transparency, predictability, and the possibility of auditing, aiming to guarantee impartiality and substantial justice;

3. highlights the principles of preserving equality, non-discrimination, plurality, solidarity and fair judgment, with the primacy of means aimed at eliminating or minimizing oppression and marginalization of human beings;

4. there is concern about avoiding errors in judgment resulting from prejudice; taking into consideration, that the data used in machine learning processes needs to be auditable and capable of being tracked, from secure sources, preferably governmental, all to guarantee the principle of transparency;

5. AI systems need to respect the privacy of users, who are responsible for knowing and controlling their personal data;

6. the existence of responsible use of AI, aimed at protecting the user, promoting equality, freedom and

justice and, finally, human dignity.

In your art. 2nd, the resolution provides definitions about: algorithm, artificial intelligence model, synapses, user, internal and external user.

The art. 4th highlights respect for fundamental rights and makes reference to the LGPD regarding sensitive personal data.

The principles of non-discrimination and transparency are, covering the responsible use of AI, with the indication of the objectives and results intended by the systems, the documentation of identified risks and indication of information security and control instruments to combat them, are detailed in articles 7 and 8.

There is also mention of the importance of audit mechanisms and certification of good practices. So much so that art. 10 provides that AI systems developed by bodies of the Judiciary must be reported to the CNJ (NATIONAL COUNCIL OF JUSTICE), whose models must be on the Sinapses Platform.

Finally, the regulations outline governance rules for AI models, which must respect the Resolutions and Recommendations of the National Council of Justice, Law, number: 13,709/2018, and judicial secrecy.

The application programming interface (API) that allows its use by other systems is established in art. 12, as a response to the importance of innovation and its adaptation to the various digital platforms, highlighting the Judiciary as a public service space.

For the same reason, in article 24, there is a provision that AI models must preferably use open source software that facilitates their integration or interoperability between systems used by bodies of the Judiciary.

Article 25 establishes that AI models must ensure transparency in accountability. Furthermore, article 26 provides for the liability of users of AI systems in cases of non-

compliance with the principles and standards stipulated in the Resolution.

Since its promulgation in 2020, this resolution has witnessed a significant expansion of AI systems within the Judiciary.

In compliance with the provisions of Resolution 332 of the CNJ (NATIONAL COUNCIL OF JUSTICE), the Sinapses Platform (CNJ (NATIONAL COUNCIL OF JUSTICE)) was created, which acts as a repository of all Artificial Intelligence models in operation or in the development phase in Brazilian Courts. According to the data collected, by the year 2022, 111 Artificial Intelligence projects had been registered in 53 Courts, including Superior Courts, such as the STJ, STF and the CNJ (NATIONAL COUNCIL OF JUSTICE). Among these, 63 projects are in production (in use) and 42 are in the development phase on the aforementioned platform.

Regarding the ranking of AI models produced, the RO Court leads with 21 models, followed by the TJ RS, with 7, and the TJDFT, with 5 models.

The topics covered by AI models are diverse and include petition classifiers, systems for generating draft sentences in electoral accountability, chatbots to clarify doubts from jurisdictions, models to assist in the screening of repetitive demands, class and subject recommendations for filed petitions, identification and unification of ongoing demands with the same fact and legal thesis, facilitating the indexing of documents for the transition from physical to digital format, generation of auxiliary texts in the preparation of minutes and verification of the presence of an injunction in the petition initial.

It is important to highlight that the motivation underlying the creation of Artificial Intelligence models is diverse, including increasing productivity (in terms of volume and time), innovation, improving the quality of services, reducing costs, better customer service citizen, the acceleration of judicial processes and the prevention of rework.

Among the projects, 21 tools were subjected to technical monitoring, 39 underwent legal and/or administrative review, and 38 had their training data reviewed to detect possible biases[8], which guarantees the transparency and accountability of AI systems.

EUROPEAN AI REGULATION INNOVATIONS

In Brazil, Resolution 332 of the National Justice Council (CNJ (NATIONAL COUNCIL OF JUSTICE)) constitutes a crucial milestone in the regulation of AI. When comparing this Brazilian resolution with the legislation in force in Europe, we realize that, although both have the common objective of promoting the safe development of AI systems, ensuring transparency and protection of fundamental rights, the European model stands out for its scope and substantial detail. European regulation introduces innovative approaches to overseeing artificial intelligence systems, which must serve as an inspiring model for other jurisdictions around the world.

RISK GRADATION

The EU AI ACT uses an innovative and pragmatic approach to assessing the risk associated with AI systems, with a taxonomy of actors and legal assets for gradation. By identifying who will be the user or recipient of an AI system and which legal asset is being protected in that context, it is possible to assess the risk more precisely and propose proportionate regulations.

Actor classification plays a key role in

8 BRASIL. CNJ (NATIONAL COUNCIL OF JUSTICE). Painel analytics. Available on the website: <https://paineisanalytics. CNJ (National Council of Justice).jus.br/single/?appid=9e4f18ac-e253-4893-8ca1-b81d8af59ff6&sheet=b8267e5a-1f1f-41a7-90ff-d7a2f4ed34ea&lang=pt-BR&theme=IA_PJ&opt=ctxmenu,currsel&select=language,BR>. Accessed on: 05 Oct. 2023.

assessing risk in AI regulation, as different systems are intended to be used by different audiences and contexts. Therefore, risk assessment must be personalized according to who uses the technology, who it is intended for and what legal interests are involved.

This is why the regulation mentions the rights of people affected or exposed to AI systems.

The European regulatory model is built on an understanding of AI risk. Systems with high risk are subject to much stricter regulation. Within this model, four risk levels were established: low, medium, high and unacceptable.

Low-risk AI systems, such as spam filters and video games, are permitted without significant restrictions, but with suggested codes of conduct (art. 69).

Those classified as limited risk include systems such as chatbots, emotion identifiers and biometric verifiers, for which the duty of information and transparency is required (art. 52)[9].

Those systems that have the potential to affect security or fundamental rights are considered high risk (art. 6), especially in the areas of education, work, immigration, as well as in the legislative and judicial branches. These systems are subject to stricter regulation.

In the last level, there are systems considered to pose an unacceptable risk (art. 5) and, therefore, prohibited, due to the fact that they are considered a threat to people. This group includes systems that perform cognitive-behavioral manipulation of vulnerable people or groups, social scoring, and real-time and remote biometric identification systems, such as facial recognition, biometric categorization systems based on sensitive data, predictive policing systems and emotion identifiers when used in the workplace, by educational institutions, or at borders[10].

The risk gradation approach adopted by the EU AI ACT based on the taxonomy of actors may prove to be extremely relevant for the National Council of Justice (CNJ (NATIONAL COUNCIL OF JUSTICE)) when regulating AI in the context of the Brazilian judicial system. By identifying the users, recipients and legal assets involved, it becomes possible to more accurately assess the risk associated with a given AI system. This, in turn, allows the definition of proportional regulatory approaches, adapted to the particularities of each system.

One of the main advantages of this approach is its adaptability, which is in line with the rapid pace of technological advancement. This means that the evaluation and regulation of AI systems can be carried out with greater precision and agility, thus ensuring more precise, balanced and up-to-date regulation. The specific rights and values involved in legal proceedings are also protected, ensuring that regulations are always aligned and updated with constantly evolving technological changes.

COMPLIANCE OBLIGATION

The EU AI ACT stands out by establishing the obligation for suppliers of high-risk AI systems to have compliance terms, ensuring that an assessment has taken place and ensuring compliance (art. 19). The regulation establishes two distinct procedures, depending on the type of system (Annex III): one for internal control (Annex VI) and another conducted by an independent body (Annex VII).

---

9 EDWARDS. L. **Expert explainer: The EU AI Act proposal**. Available on the website: <https://www.adalovelaceinstitute.org/resource/eu-ai-act-explainer/>. Accessed on: Oct 5, 23.

10 FEINGOLD. S. FEINGOLD, S. About artificial intelligence, trust is a must, not a nice to have," one lawmaker said. #AI. Available on the website: <https://www.weforum.org/agenda/2023/06/european-union-ai-act-explained/>. Accessed on: August 27, 2023.

In the first procedure, vendors are empowered to internally assess the compliance of their high-risk AI systems. This involves verifying that the quality management system complies with established requirements, thoroughly analyzing the technical documentation associated with the system and confirming that the design and development process complies with defined standards.

In the second procedure, based on the Assessment of the Quality Management System and Technical Documentation, the assessment is carried out by a notified body, which determines whether the quality management system and technical documentation follow pre-determined requirements. If the AI system is compliant, a European Union technical documentation assessment certificate will be issued. Any modifications to the quality management system or the list of covered AI systems must be communicated and, if necessary, reassessed.

On the other hand, the CNJ (NATIONAL COUNCIL OF JUSTICE) Resolution does not establish an obligation of compliance, limiting itself, in its articles 4 and 5, to stating general principles to guide developers, together with audit mechanisms and good practices (art. 8, V).

Inspired by the European model, the CNJ (NATIONAL COUNCIL OF JUSTICE) could establish specific quality and safety standards to be met by developers and suppliers of AI systems, requiring Courts to issue declarations of compliance to indicate that their systems have been evaluated and meet the established requirements. European regulations allow for the periodic review and updating of compliance requirements (art. 84), following technological advances. Resolution 332 could incorporate similar provisions to regularly review and update compliance requirements, thereby ensuring their continued relevance and effectiveness.

Additionally, in line with European regulation, Resolution 332 could include clauses that allow controlled exceptions to conformity assessment in exceptional circumstances, especially when public security or other fundamental interests are at stake (art. 6, 3, and Annex III of the EU AI Act).

The compliance obligation is aligned both with the concern for transparency and with ensuring the protection of citizens' fundamental rights. By incorporating this standard, the CNJ (NATIONAL COUNCIL OF JUSTICE) would also be ensuring these concepts to the AI systems of the Brazilian Judiciary.

SANDBOX

The term: "Sandbox" is an English term that, when applied in a technological context, represents an isolated and controlled environment where AI systems can be run and tested under strict supervision. This approach ensures that any issues are identified and corrected before the technology is widely implemented, avoiding negative impacts on the external environment.

With regard to testing for the use of AI systems, the EU AI ACT establishes the creation of "sandboxes" (art. 53), which are regulatory testing environments with the purpose of boosting innovation and competitiveness. Furthermore, the European regulation commits to flexible supervision and promotes international cooperation. The European Union defines specific eligibility criteria and selection procedures for participants in the "sandbox", encouraging the participation of small and medium-sized companies, as well as startups.

On the other hand, the CNJ (NATIONAL COUNCIL OF JUSTICE) Resolution focuses mainly on ethical supervision and compliance with ethical regulations applied to AI systems used in the Brazilian Judiciary. Currently, the

8

only control mechanism provided is related to systems in operation, when it explicitly requires a "record of adverse events" (art. 27).

The European experience with the "sandbox" can provide valuable lessons to the CNJ (NATIONAL COUNCIL OF JUSTICE) on how to create a regulatory environment conducive to the safe and ethical development of AI systems in the context of the Brazilian judiciary, promoting cooperation between courts. This knowledge may be particularly relevant as the CNJ (NATIONAL COUNCIL OF JUSTICE) seeks to implement a technological innovation that involves the collaboration of all Brazilian courts.

EUROPEAN-INSPIRED IMPROVEMENT OPPORTUNITIES

CNJ (NATIONAL COUNCIL OF JUSTICE) Resolution 332 has several points of contact with the EU AI ACT, in some of which the solutions adopted by the European model would complement and improve the model adopted by the CNJ (NATIONAL COUNCIL OF JUSTICE).

TRANSPARENCY

A major concern related to AI systems concerns opacity, both in technological and procedural terms. There are also concerns about the lack of transparency in the decisions made by AI systems, requiring the implementation of mechanisms to verify compliance with the rules and guarantee the protection of fundamental rights. Transparency emerges as a point of convergence between the CNJ (NATIONAL COUNCIL OF JUSTICE) and the European Union, with an emphasis on promoting responsible disclosure and clarity in communication.

With regard to transparency, it is observed that the CNJ (NATIONAL COUNCIL OF

JUSTICE) promotes "responsible disclosure" (art. 8, I), without going into specific details, and does not impose any notification obligation on user or recipient parties. On the other hand, the EU AI ACT stipulates that the parties involved must be informed about the use of AI systems, taking into consideration, the sensitivity of the data and emphasizing clarity in communication (art. 13).

Regarding risk documentation, there is a convergence between the two, as both the CNJ (NATIONAL COUNCIL OF JUSTICE) (art. 8, II) and the European Union recognize the importance of identifying and documenting the risks associated with AI, providing clear information on security measures and control. However, the EU AI ACT is more thorough in establishing specific requirements for instructions for use, requiring concise, complete, correct and clear information for users, while Resolution 332 does not address these details.

Both requirements that the parties involved have knowledge about the use of technology and its structure are aligned with the substantive dimension of guaranteeing due legal process, a right enshrined in public international law and recently recognized in a decision by the Federal Supreme Court[11].

DATA GOVERNANCE

Europe ensured data protection as an autonomous fundamental right by recognizing it in Article 8 of the 2000 Charter of Fundamental Rights of the European Union, which came into force in 2009. In 2018, this protection was implemented and expanded by the GDPR. Since then, data governance has been one of the European Union's central concerns regarding technological advancement.

Data governance is concerned with the

11 BRAZIL. Federal Court of Justice. Direct Unconstitutionality Action Number: 6387 Precautionary Measure-Referendum. Rapporteur Minister Rosa Weber. Full Court. Judged on 05/07/2020. Electronic Justice Gazette, nº 270, Released on 11-11-2020, Published on 12-11-2020. Electronic Process.

procedures and practices that an entity establishes to manage its data effectively, securely, ethically and responsibly. It involves the collection, storage, processing, sharing, disposal, in short, all the steps that involve the processing and protection of data, ensuring both its quality and privacy and security.

With this in mind, the EU AI ACT determines that, when using data-based training techniques, high-risk AI systems must follow strict guidelines related to data sets. These sets must meet specific quality criteria and be managed according to good data governance practices. This includes collection, preparation, quality assessment, and consideration of potential biases that may affect safety and non-discrimination. Furthermore, datasets must be relevant, representative, error-free and complete, taking into consideration, the context of use of the AI system. In cases strictly necessary to monitor, detect and correct bias, providers may process special categories of personal data, with appropriate safeguards to protect fundamental rights.

Data governance also focuses on protecting data. Article 15 of the EU AI ACT addresses risk management and cybersecurity of high-risk AI systems in Europe. Specifically, paragraph 4 of this article addresses the resilience of these systems in the face of unauthorized attempts by third parties to disrupt their operation by exploiting system vulnerabilities. This highlights the importance of adopting appropriate cybersecurity measures.

The EU AI ACT also recognizes the need to address specific threats to AI, such as attempts to manipulate training data (known as "data poisoning"), the insertion of inputs intended to induce errors in the model (known as "adversarial examples"), and flaws in the model itself. This reflects the importance of protecting AI systems against sophisticated threats. Similarly, CNJ (NATIONAL COUNCIL OF JUSTICE) Resolution 332, in articles 13 to 16, already establishes basic guidelines regarding the origin of data, the protection of the training data set and the security of data and systems.

Data contamination controls and cybersecurity measures play an essential role in ensuring that high-risk AI systems in Europe operate reliably and securely throughout their entire lifecycle. They also serve to protect these systems against malicious attempts by unauthorized third parties to manipulate their behavior or performance.

Such principles and guidelines can serve as a model to improve AI regulation in Brazil, including CNJ (NATIONAL COUNCIL OF JUSTICE) Resolution 332. This ensures that AI systems used in the context of the Brazilian judiciary are resilient to cybersecurity threats and protected against data manipulation attempts and unauthorized behavior. Such measures are essential to ensure the reliability and integrity of AI in the justice system.

Considering the growing number of cyber-attacks targeting Courts and bodies of the Judiciary, the National Council of Justice (CNJ (NATIONAL COUNCIL OF JUSTICE)) has an urgent need to regulate data governance and cyber security. Research revealed that, in 18 months, from November 2020 to April 2022, Brazilian courts faced 13 hacker attacks[12].

With sensitive data, high-profile decisions and executive power at stake, the Judiciary is an attractive target. Cyberattacks impacted both state and federal courts, including higher bodies such as the TSE, STJ and STF. These incidents have not only resulted in service interruptions, but have also posed serious risks to data integrity, with reports of hackers

---

12 Reina, E. " Wave of hacker invasions into court technological structures."Available on the website: https://www.conjur.com.br/2022-abr-15/onda-invasoes-hackers-estruturas-tecnologicas-tribunais. Accessed on: october, 11, 2023.

altering decisions and redirecting legitimate funds to fraudulent accounts[13].

When the activity of the legal system is harmed, weaknesses emerge that undermine the credibility of justice and its structures. Therefore, it is crucial that the CNJ (NATIONAL COUNCIL OF JUSTICE) establishes rigorous and detailed standards and protocols to ensure that cybersecurity is treated as a priority, preserving public trust.[14].

EXPLAINABILITY

Ensuring explainability in the regulation of AI systems is crucial to ensure adequate understanding and effective oversight of their functioning. The CNJ (NATIONAL COUNCIL OF JUSTICE) establishes a fundamental guideline in article 19, requiring that systems that use AI models to support judicial decisions prioritize the explanation of the processes that led to a certain result, allowing effective supervision by the responsible magistrate.

In parallel, the EU AI ACT also recognizes the importance of explainability in AI systems, especially in relation to high-risk systems. The European model goes further by establishing, in article 8, that high-risk AI systems must be designed in a manner transparent enough to allow users to interpret the functioning and results of the system. Furthermore, the regulation requires AI systems to provide clear and comprehensive instructions for use, ensuring that they are relevant, accessible and understandable to users.

Transparency in AI systems is critical to ensuring these systems are properly understood and audited. The CNJ (NATIONAL COUNCIL OF JUSTICE) can adopt the principles of responsible disclosure and risk documentation to promote transparency in AI systems used in the Brazilian judicial system. Furthermore, the CNJ (NATIONAL COUNCIL OF JUSTICE) demonstrates a preference for the use of open source software for AI models in the Judiciary (art. 24), while the EU AI ACT provides for the right of market surveillance authorities to access the source code of data processing systems. High-risk AI, with safeguards to protect the confidentiality of information, including source code (art. 70).

With growing concern regarding the opacity of AI systems, known as "algorithmic black boxes "[15], the need to establish explainability requirements to ensure the security and reliability of these systems becomes evident. These requirements are recognized as fundamental guarantees, derived from the intersection between the rights to data protection and due legal process. A notable example is the case of SyRI, a risk analysis system implemented by the Dutch government in 2014 and discontinued in 2020 due to the model's lack of transparency and explainability. The opacity surrounding the

13 ALVES, R. S.; CARVALHO GEORG, M. A.; NUNES, R. R. Judiciário sob ataque hacker: fatores de risco para a segurança do processo decisório em sistemas judiciais eletrônicos. Transformação digital, ciberespaço e novas tecnologias da informação na Justiça. Available on the website: <https://www.enajus.org.br/anais/assets/papers/2022/sessao-03/judiciario-sob-ataque-hacker-fatores-de-risco-para-a-seguranca-do-processo-decisorio-em-sistemas-judiciais-eletronicos.pdf>. Accessed on: October 14, 2023.

14 ALVES, R. S.; CARVALHO GEORG, M. A.; NUNES, R. R. Judiciary under hacker attack: risk factors for the security of the decision-making process in electronic judicial systems. Digital transformation, cyberspace and new information technologies in Justice. Available on the website: <https://www.enajus.org.br/anais/assets/papers/2022/sessao-03/judiciario-sob-ataque-hacker-fatores-de-risco-para-a-seguranca- of-the-decision-making-process-in-electronic-judicial-systems.pdf>. Accessed on: October 14, 2023.

15 NUNES, Dierle José Coelho; ANDRADE, Otávio Morato de. The use of explainable artificial intelligence as a tool to understand automated decisions: possible way to increase the legitimacy and reliability of algorithmic models? June 20, 2023. Available on the website: <https://periodicos.ufsm.br/revistadireito/article/download/69329/61096/379227>. Accessed on: 14 Oct. 2023.

type of algorithm used [16] made it difficult for the court to analyze the arguments presented by the parties [17]. This landmark case highlights the critical importance of transparency and explainability in AI systems, especially in contexts that affect human rights and justice.

BIAS

The EU AI ACT comprehensively addresses the issue of bias control in high-risk AI systems, recognizing its critical importance in ensuring the accuracy, robustness and security of these systems. To achieve this objective, the regulation establishes several specific guidelines. First, it requires high-risk AI systems to be highly robust, capable of resisting both internal and external errors and failures, ensuring reliable functioning (Recital 50).

The regulation also recognizes the possibility of bias over time due to biased or outdated training data, especially in post-market continuous learning systems. To address this challenge, the regulation stipulates the need for mitigation measures that eliminate or minimize the risk of biased outputs influencing future system operations, ensuring fair and accurate evolution (Recital 50).

The principle of robustness is emphasized as a fundamental requirement, and the regulation highlights the importance of appropriate technical solutions to prevent or minimize undesired behavior in systems. This includes the ability to safely stop system operation when anomalies are detected. The EU AI ACT aims to protect the fundamental rights and safety of people who interact with high-risk AI systems by promoting a trustworthy and fair environment for artificial intelligence.

Both CNJ (NATIONAL COUNCIL OF JUSTICE) Resolution 332 and the provisions of the EU AI ACT seek to establish safeguards against discrimination and bias in AI systems. The CNJ (NATIONAL COUNCIL OF JUSTICE) focuses on ensuring diversity and equitable representation in the composition of teams that deal with AI systems, covering aspects such as gender, race, ethnicity, sexual orientation, among others (art. 20). Furthermore, it emphasizes the importance of diverse participation in all phases of the process, from planning to implementation.

On the other hand, the European Regulation addresses the issue of risk associated with certain AI systems, such as those that influence access to essential services such as credit and public benefits. It recognizes the potential for discrimination arising from the use of AI systems in these areas and seeks to mitigate these risks, especially in systems considered high risk. Imposing measures to ensure fairness and the absence of discrimination in contexts where AI systems can exert significant influence over people.

The quest to avoid biased systems became even more vital after the COMPASS case was released. The system has become one of the best-known cases of the risk of discrimination in an AI system. It was proven in this case that the error was not actually due to the algorithm, but to the data used in the development of the system, which was fed with information from heavily policed areas, distorting the statistics to over-represent the poor and minorities [18].

16 VAN BEKKUM, Marvin; BORGESIUS, Frederik Zuiderveen. Digital welfare fraud detection and the Dutch SyRI judgment. European Journal of Social Security, v. 23, n. 4, p. 323-340, 2021.

17 APPELMAN, Naomi; FATHAIGH, Ronan O.; VAN HOBOKEN, Joris. Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands. J. Intell. Prop. Info. Tech. & Elec. Com. L., v. 12, p. 257, 2021.

18 KIRKPATRICK, Keith. It's not the algorithm, it's the data. Communications of the ACM, v. 60, n. 2, p. 21-23, 2017. Available on the website: https://cacm.acm.org/magazines/2017/2/212422-its-not-the-algorithmits-the-data/fulltext. Accessed on: 26 June. 2022.

FACIAL RECOGNITION AND BIOMETRICS

As for facial recognition, both standards address the topic, however, with different approaches. The CNJ (NATIONAL COUNCIL OF JUSTICE) adopts a more restrictive approach in article 22, requiring prior authorization for the use of facial recognition systems. On the other hand, the EU AI ACT carries out a thorough analysis [19], considering the structure of the system, the purpose, period and location of data collection, in order to assess the risk of the system. Therefore, simple biometric verification systems are classified as medium risk, while real-time identification systems in public spaces are expressly prohibited (article 52).

One of the main safeguards to fundamental rights brought by the European model is creating the obligation for suppliers to always inform that the parties are interacting with an artificial intelligence system, except when the interaction is considered obvious to a reasonably informed person.

The issue of facial recognition for policing purposes has been widely debated and controversial [20], being one of the points that experts believe can still be modified in the final draft of the EU AI ACT.

Regardless of the final wording of the device, the approach adopted by the CNJ (NATIONAL COUNCIL OF JUSTICE), which analyzes the structure of the system, the purpose, period and location of biometrics collection, represents a more functional model of regulation than simply requiring prior authorization for any system, especially considering the speed of technological advancement.

Regulating the use of facial and biometric recognition is an urgent need for the CNJ (NATIONAL COUNCIL OF JUSTICE), as the technologies are already being developed and tested by the courts. The Court of Justice of the Federal District and Territories (TJDFT) has implemented the Amon and Saref projects to address different security and monitoring needs [21].

The Amon project is a facial recognition system that aims to identify the large volume of vectorized images that access TJDFT facilities [22]. This image processing mechanism aims to assist and contribute to the internal security of the Court. However, it is important to highlight that Amon, as a remote facial recognition system in public places, would currently be prohibited by current EU AI ACT legislation.

On the other hand, Saref is a Facial Presentation and Recognition System used to verify the obligation to periodically appear at the Sentence Execution Court, with the purpose of proving compliance with the measures imposed under the open regime. Saref employs a facial recognition algorithm for this task. This system is permitted, but is subject to strict compliance rules to ensure the security and privacy of the individuals involved.

HUMAN SUPERVISION

The increasing integration of Artificial

---

19 Recitals 18-21 and 33 address the use of biometric identification systems.

20 FEINGOLD. S. FEINGOLD, S. About artificial intelligence, trust is a must, not a nice to have," one lawmaker said. #THERE. Available at: <https://www.weforum.org/agenda/2023/06/european-union-ai-act-explained/>. Accessed on: Aug 27, 2023.

21 TJDFT. President of TJDFT meets with managers to monitor artificial intelligence projects. Available at: <https://www.tjdft. jus.br/institucional/imprensa/noticias/2023/abril/president-do-tjdft-reune-se-com-gestores-para-avamosar-projetos-sobre-inteligencia- artificial>. Accessed on: 15 Oct. 2023.

22 SANTANA MELO, J. S.; SERIQUE JUNIOR, L. F. S. " Artificial intelligence and massive data processing: a reality that has already reached the TJDFT." In: Judicial innovation: foundations and practices for a high-impact jurisdiction, coordinated by Fabrício Castagna Lunardi and Marco Bruno Miranda Clementino. Brasília: Escola Nacional de Formação e Improvement of Magistrates — Enfam, 2021.

Intelligence (AI) systems in various spheres of modern society has raised significant concerns about the need for human supervision of these technologies. While AI systems have demonstrated impressive potential to drive efficiency and innovation across a wide range of industries, there is also a growing awareness of the risks associated with using these systems, especially in contexts where automated decisions can affect individuals and communities. .

Human oversight plays a crucial role in ensuring that AI systems are used ethically, responsibly and transparently. It ensures that the results and operations of AI systems are consistent with legal and ethical principles, and mitigates potential biases and biases that may arise during the automated decision-making process. Additionally, human oversight helps promote public trust in AI systems by allowing complex issues to be interpreted and evaluated by qualified and experienced individuals.

In this context, understanding the importance of human oversight for AI systems is critical to ensuring that these technologies are implemented in an enhanced, ethical manner and in accordance with fundamental human values. Effectively integrating human oversight into AI systems contributes to building a technological environment that prioritizes transparency, equity and accountability, while leveraging the positive potential of these technologies for social and economic advancement.

Both article 19 of the CNJ (NATIONAL COUNCIL OF JUSTICE) and article 14 of the EU AI ACT highlight the importance of human supervision in the context of the use of Artificial Intelligence systems, especially in situations where high-risk systems are involved in making decisions that may affect the health, safety or fundamental rights of people.

Article 19 of the CNJ (NATIONAL COUNCIL OF JUSTICE) stipulates that computer systems that use AI models to aid in the preparation of judicial decisions must allow the explanation of the steps that led to the result and the supervision of the responsible magistrate. This highlights the need to ensure that the decision-making process remains understandable and subject to human oversight to preserve transparency and accountability.

Similarly, Article 14 of the EU AI ACT sets out specific measures to ensure effective human oversight of high-risk AI systems, including the implementation of appropriate human-machine interface tools. Furthermore, it emphasizes the importance that human supervision aims to prevent or minimize potential risks associated with the use of the AI system.

These provisions in both regulations reflect concern about the potential impact of AI systems on people's lives and rights, recognizing the need to ensure that the use of these systems is subject to appropriate human control and that critical decision-making is supported by human supervision and interpretation.

High-risk AI systems must be designed to enable effective supervision by humans throughout their entire operation cycle. This involves developing suitable human-machine interfaces to facilitate supervision. This oversight can be achieved through measures incorporated by the provider directly into the system before it is made available on the market, or through measures identified by the provider and implemented by the end user. It is critical that those charged with oversight can understand the capabilities and limitations of the system, monitor its operation, detect potential excessive dependencies on system outputs, correctly interpret those outputs, and make informed decisions, including the

ability to stop the system if necessary.

The high-risk AI system must be delivered to users in such a way that those responsible for supervision can carry out all these actions appropriately and proportionately to the circumstances, thus ensuring effective and safe supervision of the system.

CONCLUSIONS

In this article, we seek to provide an overview of some of the most current aspects of EU AI ACT regulation and the guidelines for the Use of AI within the Judiciary in Brazil, exploring both points of contact between European regulation and Resolution 332/2020 CNJ (NATIONAL COUNCIL OF JUSTICE) as to the extent to which both can contribute to expanding the debate and regulation of the use of AI systems around the world.

With the pandemic, there was an acceleration in the digitalization of processes, the virtualization of acts carried out and the expansion of electronic processes, the emergence of Justice 4.0, the Virtual Balcony, virtual hearings and good practices using technology in the service of judicial provision with the reduction of costs and greater effectiveness, which promotes the efficiency of Justice as a service.

Thus, regulatory perspectives around the world are diverse, taking into consideration, several factors, such as the reality of each country and the nature of the services provided (whether public, on digital or economic platforms), the users and the impacts the use of different technologies. However, these perspectives converge on the importance of respect for fundamental rights, for users, based on the self-determination of information and data, interfacing with legislation that protects all citizens.

We also realize that the use of artificial intelligence systems within the Judiciary highlights the principles of dignity, freedom and equity in decisions (art. 21), in line with the Federal Constitution and International Human Rights Treaties, both in Europe and America.

This is why it is important to highlight that, given the absence of specific standards in Brazil, Resolution CNJ (NATIONAL COUNCIL OF JUSTICE) 332/2020 constitutes a crucial regulatory framework for the Judiciary that has been developing with the implementation of the electronic process and its use in all regions of extensive territoriality.

The regulations also cover aspects of data governance, ethical parameters for the development and use of Artificial Intelligence; with a focus on compliance with Fundamental Rights. So much so that Resolution CNJ (NATIONAL COUNCIL OF JUSTICE) 332/2020 provides for "ethics, transparency and governance in the production and use of Artificial Intelligence in the Judiciary and provides other provisions.

The CNJ (NATIONAL COUNCIL OF JUSTICE) Resolution, inspired by the European Charter, met points of contact with the IA Act, highlighting the primacy of human rights, such as the right to privacy, autonomy, equality, impacts of the use of systems of AI in private, economic and social life.

In another turn, we highlight that EU AI ACT regulation seeks to equate technological advancement with fundamental rights and guarantees, using regulatory and experimental sandboxes, risk gradation, concern with minimizing bias, opacity and cyber-attacks as instruments.

Therefore, the EU IA ACT represents a dialogue box and an opportunity to expand the horizons of the CNJ (NATIONAL COUNCIL OF JUSTICE) Resolution, a normative act of great relevance that can contribute as an experiment to the world, due to the large amount of data, within the Judiciary, whose management has been a reference to

other countries. Furthermore, the National Council of Justice has been working on data governance, as the Judiciary represents a large Big Data in our country and, in the near future, will collect enough data to implement public policies aimed at improving judicial provision.

Finally, we highlight that this is a moment of great debate and involves dialogue with existing legal institutes, the values involved in creating super regulation, ready, current and flexible to meet the technological demands of society and what is to come.

REFERENCES

ALVES, R. S.; CARVALHO GEORG, M. A.; NUNES, R. R. Judiciário sob ataque hacker: fatores de risco para a segurança do processo decisório em sistemas judiciais eletrônicos. Transformação digital, ciberespaço e novas tecnologias da informação na Justiça. Available on the website: <https://www.enajus.org.br/anais/assets/papers/2022/sessao-03/judiciario-sob-ataque-hacker-fatores-de-risco-para-a-seguranca-do-processo-decisorio-em-sistemas-judiciais-eletronicos.pdf>. Acesso em: 14 out 2023.

APPELMAN, Naomi; FATHAIGH, Ronan O.; VAN HOBOKEN, Joris. Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands. J. Intell. Prop. Info. Tech. & Elec. Com. L., v. 12, p. 257, 2021.

BRASIL. CNJ (NATIONAL COUNCIL OF JUSTICE). Painel analytics. Available on the website: <https://paineisanalytics.CNJ (National Council of Justice).jus.br/single/?appid=9e4f18ac-e253-4893-8ca1-b81d8af59ff6&sheet=b8267e5a-1f1f-41a7-90ff-d7a2f4ed34ea&lang=pt-BR&theme=IA_PJ&opt=ctxmenu,currsel&select=language,BR>. Acesso em: 05 out. 2023.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 6387 Medida Cautelar-Referendo. Relatora Ministra Rosa Weber. Tribunal Pleno. Julgado em 07/05/2020. Diário da Justiça Eletrônico, nº 270, Divulgação em 11-11-2020, Publicação em 12-11-2020. Processo Eletrônico.

CNN. Europa lidera corrida para regulamentar a inteligência artificial. Available on the website: https://www.cnnbrasil.com.br/tecnologia/europa-lidera-corrida-para-regulamentar-a-inteligencia-artificial-entendacomo/#:~:text=Nesse%20contexto%2C%20a%20Lei %20de,meio%20ambiente%20contra%20efeitos%20nocivos%E2%80%9D. Acesso em: 09 de jun de 2023.

EDWARDS. L. Expert explainer: The EU AI Act proposal. Available on the website: <https://www.adalovelaceinstitute.org/resource/eu-ai-act-explainer/>. Acesso em: 05 de out de 23.

ESTADOS UNIDOS DA AMÉRICA. Library of Congresss. Regulation of artificial intelligence around the world. Available on the website: <https://hdl.loc.gov/loc.law/llglrd.2023555920>. Acesso em: 14 out. 2023.

FEINGOLD. S. FEINGOLD, S.On artificial intelligence, trust is a must, not a nice to have," one lawmaker said. #AI. Available on the website: <https://www.weforum.org/agenda/2023/06/european-union-ai-act-explained/>. Acesso em: 27 de ago de 2023.

FERRAREZI, T. Parlamento Europeu adota posição para regulamentar IA. Available on the website: https://www.migalhas.com.br/depeso/389455/parlamento-europeu-adota-posicao-para-regulamentar-a-ia Acesso em: 09 de jun de 2023.

KIRKPATRICK, Keith. It's not the algorithm, it's the data. Communications of the ACM, v. 60, n. 2, p. 21-23, 2017. Available on the website: https://cacm.acm.org/magazines/2017/2/212422-its-not-the-algorithmits-the-data/fulltext. Acesso em: 26 jun. 2022.

NUNES, Dierle José Coelho; ANDRADE, Otávio Morato de. O uso da inteligência artificial explicável enquanto ferramenta para compreender decisões automatizadas: possível caminho para aumentar a legitimidade e confiabilidade dos modelos algorítmicos? 20 de junho de 2023. Available on the website: <https://periodicos.ufsm.br/revistadireito/article/download/69329/61096/379227>. Acesso em: 14 out. 2023.

REINA, E. "Onda de invasões de hackers em estruturas tecnológicas dos tribunais." Available on the website: https://www.conjur.com.br/2022-abr-15/onda-invasoes-hackers-estruturas-tecnologicas-tribunais. Acesso em 11 out 2023.

SANTANA MELO, J. S.; SERIQUE JUNIOR, L. F. S. "Inteligência artificial e processamento de dados massivos: uma realidade que já chegou ao TJDFT." In: Inovação judicial: fundamentos e práticas para uma jurisdição de alto impacto, coordenado por Fabrício Castagna Lunardi e Marco Bruno Miranda Clementino. Brasília: Escola Nacional de Formação e Aperfeiçoamento de Magistrados — Enfam, 2021.

TJDFT. Presidente do TJDFT reúne-se com gestores para acompanhar projetos de inteligência artificial. Available on the website: <https://www.tjdft.jus.br/institucional/imprensa/noticias/2023/abril/presidente-do-tjdft-reune-se-com-gestores-para-acompanhar-projetos-sobre-inteligencia-artificial>. Acesso em: 15 out. 2023.

TUCCI, J.R.C. Recente regramento da inteligência artificial na União Europeia. Available on the website: https://www.conjur.com.br/2023-jun-23/paradoxo-corte-recente-regramento-inteligencia-artificial-uniao-europeia Acesso em: 09 de jun de 2023.

VAN BEKKUM, Marvin; BORGESIUS, Frederik Zuiderveen. Digital welfare fraud detection and the Dutch SyRI judgment. European Journal of Social Security, v. 23, n. 4, p. 323-340, 2021.

WILMERHALE. European Parliament Adopts Negotiating Position on the AI Act. Available on the website: <https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20230615-european-parliament-adopts-negotiating-position-on-the-ai-act>. Acesso em: 27 de ago de 2023.

ZIADDY, H. ZIADY, H. Europa lidera corrida para regulamentar a inteligência artificial; entenda como. Available on the website: <https://www.cnnbrasil.com.br/tecnologia/europa-lidera-corrida-para-regulamentar-a-inteligencia-artificial-entenda-como/>. Acesso em: 27 de ago de 2023.