ICNL Recommendations: Brazil AI Legislation

Digital <digital@icnl.org>

sex 10/06/2022 22:27

Para: CJSUBIA <CJSUBIA@senado.leg.br>;

1 anexo

Brazil AI Summary Analysis - FINAL.pdf;

Você não costuma receber emails de digital@icnl.org. Saiba por que isso é importante

To whom it may concern,

The International Center for Not-for-Profit Law (ICNL) is pleased to share the attached analysis of Brazil's AI regulations. The analysis, including recommendations, addresses concerns regarding human rights protections in the context of AI. This analysis is being provided as part of the call for public input.

ICNL welcomes this opportunity to provide comments in response to the Bills and remains available to answer questions and engage with the Commission of Jurists during the legislative drafting process.

Thank you,

ICNL's Digital Team
digital@icnl.org | www.icnl.org

ICNL

www.icnl.org
info@icnl.org

Summary Analysis

Brazil's Draft Laws on Artificial Intelligence

Introduction

In an effort to regulate artificial intelligence (AI), Brazil's Federal Senate introduced bills 5051/2019 and 872/2021 that include high-level principles to guide the use of AI. Meanwhile, Brazil's Chamber of Deputies introduced and approved Bill 21/2020 which sets forth ten articles that propose "foundations, principles, and guidelines for artificial intelligence development and application in Brazil."[1] On March 30, 2022, the Federal Senate established a Commission of Jurists that is tasked with drafting a comprehensive law based on the three Bills ("Bills").[2] The Commission has 120 days to submit a proposal to the Federal Senate. This initiative aligns with Brazil's 2021 National AI Strategy which recommends Brazil undertake regulatory action as one means of guiding ethical AI research, development, and innovation.[3]

These Bills set out principles that encourage innovation and AI-powered economic development in Brazil while acknowledging risks and offering broad guidance for a light-touch approach to regulating AI. While Bill 21/2020 establishes a risk-based management approach for regulation by differentiating between low and high-risk AI systems, encourages self-regulation, and establishes transparency rules to provide notice and other information about a system to users, the Bills, in totality, rely too heavily on the development of voluntary codes of conduct in the future. Similarly, the Bills make regular reference to the creation of rules in the future that would be implemented "only when absolutely necessary."[4] Simply put, the Bills, as currently drafted, lack the specificity required to adequately protect human rights in the development and deployment of AI systems.

[1] Bill 21/2020, Preamble.

[2] Senado Federal, "Brasil poderá ter marco regulatório para a inteligência artificial
Fonte: Agência Senado" (March 2022), https://www12.senado.leg.br/noticias/materias/2022/03/30/brasil-podera-ter-marco-regulatorio-para-a-inteligencia-artificial.

[3] Ordinance GM No. 4617 of April 6, 2021, Establishing the Brazilian Artificial Intelligence Strategy and its Thematic Axes, available at https://www.in.gov.br/en/web/dou/-/portaria-gm-n-4.617-de-6-de-abril-de-2021-*-313212172.

[4] Bill 21/2020, Article 6(I).

Following a review of the Bills,[5] ICNL is concerned that they are insufficiently precise to give regulators or the private sector notice as to the relevant risk factors and how to assess them in the context of AI development and use. Rather, the Bills provide considerable discretion to authorities to determine risk levels on a case-by-case basis, which could lead to inconsistent and arbitrary oversight and enforcement, and sets forth minimal regulatory requirements, focusing instead on self-regulation of the industry. Inconsistent oversight of AI systems that pose a substantial risk to rights and minimal authorities for enforcement will continue to leave Brazilian consumers and users vulnerable to human rights harms caused by unregulated AI systems.

To address these concerns, future iterations of the AI legislation in Brazil could improve upon the following aspects of the Bills:

- **Undefined terms:** The Bills do not provide definitions for important terms that are critical aspects of AI development and use. Without a common understanding of what these terms mean, it is impossible fully and universally evaluate the risks that an AI system may pose to human rights.
- **Vague guidance for risk-based management:** The Bills establish a risk-based management system for evaluating risks of AI systems. However, the Bills do not provide a set of factors or meaningful guidance for how to determine whether a system poses a lower or higher risk to human rights. Without such specific guidance, there is concern that risk-based management will be incomplete or will be implemented arbitrarily, thus increasing the risk of misuse leading to human rights abuses.
- **Over-reliance on self-regulation:** The primary method of mitigating the risk from the deployment of AI systems proposed in the Bills is self-regulation and adherence to seemingly voluntary codes of conduct. There is concern that unless the Bills contain stringent provisions, with government oversight and with penalties for non-compliance, Brazilians may not be adequately protected from the human rights impacts of higher risk AI systems and AI systems that are likely to pose an unacceptable risk to human rights will be used.
- **Insufficient transparency requirements:** One of the primary concerns regarding the development and use of AI is that there is a lack of transparency and explainability of algorithmic decision-making. The Bills include relatively few transparency requirements. As a result, it will likely be very difficult, if not impossible, to assess when AI systems violate laws, including legal safeguards protecting fundamental rights, cause discriminatory or otherwise harmful

[5] ICNL's review was based on an official English translation of the Bills.

results, or enable those tasked with overseeing the AI systems to correct errors in the algorithms.

Background on Artificial Intelligence

AI is a term that refers to a wide range of "processes and technologies enabling computers to complement or replace specific tasks otherwise performed by humans, such as making decisions and solving problems."[6] AI has already been rapidly deployed in a variety of contexts, such as law enforcement, healthcare, social media content moderation, and transportation with the goal of improving the speed, efficiency, and quality of regular tasks.[7] However, AI development and use can also negatively impact human rights by exploiting user data in ways that infringe upon privacy rights or by reinforcing historic biases, leading to discrimination against marginalized populations.[8] Due to is complexity and potential risks, civil society has increasingly advocated for AI regulation to ensure that domestic innovation and commercial interests do not come at the expense of human rights.

International Law

According to human rights law, States have obligations both to refrain from interfering with the exercise of rights and to promote the enjoyment of human rights. In the context of AI, this means that the State's development, adoption, or use of AI tools should not infringe upon the rights of impacted individuals and that the State should also adopt and enforce legislation to protect the rights of individuals from human rights harms caused by private actors.[9]

As the development and adoption of AI systems have accelerated in recent years, States have yet to fulfill their positive obligation to protect against harms. In September 2021, the UN High Commissioner for Human Rights Michelle Bachelet called for a moratorium on the sale and use of AI systems that pose serious risks to fundamental human rights until appropriate regulatory safeguards are put in place.[10]

To ensure protection of these and other rights, the UN Human Rights Council has recommended that States 1) adopt regulatory frameworks that mitigate the risks of AI systems on human rights and ban the use of high-risk AI systems until such regulatory

[6] U.N. General Assembly, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," A/73/348 (Aug. 2018), para. 3.

[7] CivicSpace.tech, "Artificial Intelligence & Machine Learning," available at https://www.civicspace.tech/technologies/machine-learning/.

[8] CivicSpace.tech, "Artificial Intelligence & Machine Learning," available at https://www.civicspace.tech/technologies/machine-learning/.

[9] U.N. General Assembly, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," A/73/348 (Aug. 2018), paras. 19-20.

[10] https://www.ohchr.org/en/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet?LangID=E&NewsID=27469

safeguards are adopted and enforced; 2) ensure that data privacy regulations are in place and enforced through independent, impartial authorities; 3) when AI systems do cause human rights harms, ensure that the victims have access to effective remedies; and 4) require adequate transparency and explainability of all AI-enabled decisions that significantly impact human rights.[11]

OVERVIEW OF IMPACTED RIGHTS

AI poses many risks to human rights. According to the United Nations Special Rapporteur (UNSR) for the promotion and protection of the right to freedom of opinion and expression, impacted rights include the rights to 1) freedom of expression, 2) privacy, 3) non-discrimination, and 4) effective remedy.[12] These rights are enshrined in the International Covenant on Civil and Political Rights (ICCPR) and the American Convention on Human Rights (ACHR), both of which Brazil ratified in 1992.

FREEDOM OF OPINION AND EXPRESSON: The right to hold opinions without interference and the right to freedom of expression, including the freedom to seek, receive and impart information and ideas, are guaranteed under Article 19 of the ICCPR. An example of how AI systems impact these rights is the use of algorithms for content prioritization and moderation by social media companies in ways that can significantly manipulate user opinions and can result in the takedown of posts from independent media sources, human rights defenders, and satirists. While private companies have a right to moderate content on their platforms as they see fit, their widespread use of AI on platforms that have become essential tools for seeking and receiving information online diminish the right to access information without undue restriction or censorship, and since these algorithms are not transparent, "individuals will often have their expression rights adversely affected without being able to investigate or understand why, how or on what basis."[13]

PRIVACY: The right to privacy is guaranteed by Article 17 of the ICCPR, which bars arbitrary or unlawful interference with "privacy, family, home, or correspondence." Article 17's right to privacy is closely linked to Article 19's right to freedom of expression because individuals who know or fear that their communications are being monitored are less likely to express themselves freely. The development and use of AI relies upon the mass collection and exploitation of data, including personal data that is gathered by private companies and data brokers without the informed consent of individuals, without appropriate data protection and security safeguards (e.g., encryption, data

[11] U.N. Human Rights Council, "The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights," A/HRC/48/31 (Sept. 2021), para. 59.
[12] U.N. General Assembly, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," A/73/348 (Aug. 2018).
[13] U.N. General Assembly, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," A/73/348 (Aug. 2018), para. 32.

minimization, anonymization), and without sufficient transparency for users and victims of privacy right breaches to scrutinize how the systems are collecting and using their data and hold those responsible accountable for harms.[14]

NON-DISCRIMINATION: The principle of non-discrimination underpins all other rights and is also guaranteed in Article 26 of the ICCPR. Pursuant to Article 26, "the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."

Algorithms that are intended to discern patterns in human behavior or appearances are likely to cause discriminatory impacts when they have been trained with or make decisions based off poor quality data, biased data, or incomplete data. For example, AI systems that are used for law enforcement purposes may have been trained using historical data of police patrols and arrests. However, if those patrols or arrests were conducted due to discriminatory policies and attitudes towards a particular racial group, the AI system will reinforce past injustices. The problem is not only limited to faulty data; research has indicated that eighty-five percent of AI systems "deliver erroneous outcomes due to bias in data, algorithms, or the teams responsible for managing them.[15] Exacerbating the problem is that the opacity of algorithms means biases can be difficult to discern. These underlying discriminatory impacts are particularly concerning when a system is used in governance processes or to deliver public services, whereby faulty outcomes can become an enormous roadblock to civic participation and access to necessities.

EFFECTIVE REMEDY: Article 2(3) of the ICCPR obligates states to provide individuals access to effective remedies when their rights have been harmed and to enforce the remedies that are granted. AI systems, particularly complex and technologically advanced systems, can interfere with this right when their use obscures the decision-making that caused the harm, making it difficult or impossible for individuals to establish a claim for liability.

OTHER RIGHTS: The analysis does not provide an exhaustive list of potential human rights harms. Depending on the AI system and how it is deployed, other rights may also be impacted. A human rights impact assessment is one tool that public and private

[14] U.N. Human Rights Council, "The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights," A/HRC/48/31 (Sept. 2021), paras. 12-14.

[15] Gartner, "Gartner Says Nearly Half of CIOs Are Planning to Deploy Artificial Intelligence" (Feb. 2018), https://www.gartner.com/en/newsroom/press-releases/2018-02-13-gartner-says-nearly-half-of-cios-are-planning-to-deploy-artificial-intelligence.

sector actors can use to identify and evaluate the potential human rights harms that are relevant to a particular AI system.[16]

Analysis

DEFINITIONS

UNDEFINED TERMS USED IN THE BILLS

ISSUE: Aside from a definition for the term "artificial intelligence," the Bills employ terms that are not defined in the context of AI. This does not provide adequate regulatory guidance or notice to the public as to how provisions may be interpreted.

ANALYSIS: Article 2 of Bill No. 21/2020 includes a definition for the term "artificial intelligence."[17] Although there is no standard industry definition for AI, the definition in the Bill generally captures the broad set of technologies and applications that are used in AI systems and aligns closely with the European Union's (EU) draft AI Act, which has been one of the only other attempts to comprehensively regulate AI.

However, none of Brazil's Bills define other relevant terms that impact the interpretation and future enforcement of the provisions. For example, Article 4(2) of Bill No. 5051/2019 attributes liability for damages resulting from the use of AI systems to the system's supervisor, but there is no definition for "supervisor" and no explanation for whether this refers to the individual(s) responsible for developing and training the AI system, the individual(s) overseeing its operation, or someone else entirely. Bill No. 21/2020 does not use the term "supervisor," but attributes liability to agents, without providing any indication for how the legal definition of agent should be interpreted in the context of an AI system. Bill No. 21/2020 also empowers a "competent entity" and relevant "sectoral bodies" to take actions with respect to AI regulation but does not define which entities or bodies have such authority.

By failing to define key terms, the draft Bills do not provide legislators, enforcement agencies, or the public with sufficient clarity as to the intended meaning of the provisions and can create confusion, particularly in the context of artificial intelligence which is a novel legislative topic with technical dimensions that are not commonly understood.

RECOMMENDATION: Define terms that impact the interpretation of the regulations to ensure clear and consistent enforcement.

[16] U.N. General Assembly, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," A/73/348 (Aug. 2018), paras. 53-54.

[17] Article 2: "For the purposes of this Law, an artificial intelligence system is defined as a system based on a computational process that, from a set of goals defined by humans, can, through data and information processing, learn to perceive and interpret the external environment, as well as interact with it, making predictions, recommendations, categorizations, or decisions, and utilizing, but not limited to, techniques such as: (I) machine learning systems, including supervised, unsupervised, and reinforcement learning; (II) systems based on knowledge or logic; (III) statistical approaches, Bayesian inference, research and optimization methods."

EXCLUDED TERMS AND DEFINITIONS

ISSUE: The Bills do not include terms that are relevant to the development and use of AI, the absence of which weakens the efficacy of regulatory oversight.

ANALYSIS: The Bills not only fail to define key terms, but they also fail to reference or describe key technical terms that underpin the development of an AI system. Such technical terms and definitions are important for evaluating risks and determining whether an AI system is effective and fit for purpose.

For example, the methods and quality of the data used for an AI system's training, testing, and validation have significant consequences for AI algorithms because AI systems learn from and discern patterns in the data. The data that trains the algorithms directly impacts the decisions and outputs of the algorithm. Faulty methods and poor-quality data could result in inherent biases and discriminatory impacts being built into the system, such as for women, persons with disabilities, and racial monitories.[18]

Yet, the terms "training," "testing," and "validation data" are not described or mentioned at all throughout the Bills. Without definitions or descriptions that would provide a more holistic picture of AI development, regulators are not fully equipped to assess the discriminatory risks a particular AI system poses to individuals based on their race, color, sex, language, religion, political opinions, as required by Article 26 of the ICCPR. The failure to provide a framework for AI that addresses the range of human rights risks and impacts leaves communities in Brazil vulnerable to intentional and unintentional harms when they interact with AI systems.

RECOMMENDATION: Identify the technical characteristics of AI that contribute to creating risks within an AI system and provide definitions that aid in conceptualizing regulatory requirements that better protect the rights of users and consumers.

EVALUATION OF RISKS

ISSUE: Article 6(III)[19] of Bill No. 21/2020 sets forth a "risk-based management" approach for the regulation of AI systems but does not provide relevant factors for determining whether a system is higher or lower risk. This creates a weak regulatory framework that does not adequately protect users and vulnerable communities from rights violations.

[18] AI Now Institute, "Disability, Bias, and AI" (Nov. 2019), pgs. 8-9, https://ainowinstitute.org/disabilitybiasai-2019.pdf.

[19] Article 6: "When regulating the artificial intelligence implementation, the State shall observe the following guidelines: . . . (III) risk-based management: the development and usage of artificial intelligence systems shall consider the specific risks and definitions of the need to regulate artificial intelligence systems, and the respective degree of intervention shall always be proportional to the specific risks offered by each system and the probability of occurrence of these risks, always evaluated in comparison with: (a) the potential social and financial benefits of the artificial intelligence system; and (b) the risks presented by similar systems that do not involve artificial intelligence, according to item V of this head provision."

ANALYSIS: The purpose of risk-based management for AI is to identify the systems that could cause the greatest harms in order to focus regulatory burdens and costs on the highest risk systems. Meanwhile, the framework for lower risk systems is flexible and lighter touch to allow for innovation in the industry. Given the multifaceted techniques for the development of AI and varied uses of AI systems, from automating routine operational tasks to making life changing decisions regarding medical care in hospitals, sentencing in courts, and surveillance for law enforcement, risk-based management has been seen as an appropriate and balanced approach for regulation. However, evaluating risks is not straightforward because there are many factors that might make an AI system higher or lower risk, from a system's initial design to its training and testing to its deployment in the real world.

Thus, legislation must set fairly clear guidelines so that regulators, the private sector, and the public are aware of the relevant factors to determine risk levels. Factors for assessing risk can include the degree of human control and oversight over a system, the number of end-users impacted, the number of rights at risk and the severity of the potential harm, the potential for misuse, the extent to which harms can be easily identified and remedied, and the scale of personal or sensitive data that must be collected and processed for the development or deployment of the system.[20]

Article 6 provides the only guidance for how Government authorities should evaluate the level of risks. It stipulates that Government intervention must be proportional to the degree of the risks compared to the probability of such a risk occurring. This vague guidance to balance probability with degree of risk does not lay out factors that are directly relevant to the unique concerns posed by AI development and deployment. Moreover, they do not provide any clarity regarding how the Government should determine whether an AI system poses a risk, what risks are at stake, and what aspects of an AI system would lead to a determination that the risk warrants heightened Government intervention.

Likewise, the Bills do not consider that some risks to fundamental human rights may warrant banning certain uses of AI altogether. There are no provisions that provide regulators guidance on when rights-based concerns outweigh commercial and economic interests.

In comparison, the EU has also proposed a risk-based management process for AI regulation. The EU's draft AI Act outlines the following risk levels: AI with minimal to no risk, AI with low risk but with specific transparency requirements, high-risk AI, and AI with unacceptable risks that are prohibited altogether (subject to certain loopholes).

[20] European Center for Not-for-Profit Law, "Evaluating the Risk of AI Systems to Human Rights from a Tier-based Approach" (March 2021), https://ecnl.org/sites/default/files/2021-06/Evaluating%20the%20Risk%20of%20AI%20Systems%20to%20Human%20Rights_ECNL%20proposal.pdf.

The EU's draft Act also lists specific categories of AI systems that qualify as high and unacceptable risks "to the health and safety or fundamental rights of persons." Pursuant to the EU's draft Act, AI systems used for law enforcement purposes, the operation of critical infrastructure, migration and border control management, and the administration of justice are examples of systems deemed to be high-risk applications, and thus require increased government intervention. Meanwhile, unacceptable AI systems are stated to be those that "have a significant potential to manipulate persons through subliminal techniques beyond their consciousness or exploit vulnerabilities of specific vulnerable groups."

The EU framework for defining and regulating risks of AI systems is not the only option for AI regulation, and experts as well as civil society organizations have proposed other models for regulation.[21] However, if Brazil decides to adopt a risk-based management approach, future legislation should provide clearer guidance on how regulators must evaluate and determine varying levels of risks.

RECOMMENDATION: Design a framework for assessing human rights risks for AI systems and stipulate the factors that regulators should assess when evaluating the level of risk in an AI system, including the factors that would lead to a determination that an AI system poses an unacceptable risk to human rights.

RELIANCE ON SELF-REGULATION

ISSUE: The Bills provide overarching principles that should guide AI regulation in Brazil, but they do not set forth concrete requirements for private and public sector entities to follow to mitigate the risks of AI. The reliance on what is called "self-regulation," does not give regulators sufficient oversight and enforcement powers to prevent against or respond to the human rights harms of higher risk AI systems.

ANALYSIS: Article 4 of Bill No. 21/2020 stipulates that one of the foundations for AI development and implementation is "the encouragement of self-regulation, through the adoption of codes of conduct and guides to good practices. . ." and that these codes and guides "may serve as indicative elements of compliance." Moreover, Article 6 does not mandate specific requirements for the development and use of "high-risk" AI and instead stipulates that the government may request information about the system, with no further oversight or enforcement mechanisms in place.

The principle of self-regulation trusts that companies and organizations will monitor their own compliance with ethical, safety, or other industry standards without

[21] For example, the European Center for Not-for-Profit Law has proposed that five levels of risk be defined to inform regulatory action. European Center for Not-for-Profit Law, "Evaluating the Risk of AI Systems to Human Rights from a Tier-based Approach" (March 2021), https://ecnl.org/sites/default/files/2021-06/Evaluating%20the%20Risk%20of%20AI%20Systems%20to%20Human%20Rights_ECNL%20proposal.pdf.

requiring oversight and enforcement from governments or other independent third-party mechanisms.[22] Self-regulation based on voluntary codes of conduct in the industry may be sufficient for some companies, particularly those that are concerned with upholding a trustworthy reputation. However, the consequence of self-regulation is that an industry's market interests can create incentives for companies to forego adherence to standards, and the lack of external oversight and enforcement means that the public cannot hold them to account for compliance failures.

While self-regulation, voluntary codes of conduct, and existing remedies through individual tort claims may appropriately address lower risk AI systems, self-regulation cannot adequately address the risks of systems that substantially impact human rights. Governments can better prevent and protect against harms through proactive measures to enforce transparency and risk mitigation rules. Moreover, self-regulation does not address the uses of AI that pose unacceptable risks to human rights regardless of the safeguards put in place – such applications of AI systems may require a government-imposed ban, which is not currently authorized in the Bills.

Throughout the three Bills, the importance of innovation and commercial competitiveness are frequently emphasized, and this priority is reflected in the premise of self-regulation and minimal government intervention. While economic development is a legitimate interest, the public also has a strong interest in ensuring that development and efficiency do not come at the cost of fundamental human rights, and the Bills do not institute adequate guardrails for AI systems that pose a higher risk to those rights, falling short of the Human Rights Council guidance on AI regulation.

The types of oversight and enforcement powers may include more robust transparency rules (discussed below), Government registration or licensing mandates, required use of certain digital security safeguards, and Government bans to block the use of AI systems with unacceptable risk in Brazil.

RECOMMENDATION: In the next draft legislation, include more robust oversight and enforcement powers for regulators, particularly for higher risk AI systems. A self-regulatory approach may be suitable for systems that are lower risk.

TRANSPARENCY REQUIREMENTS

ISSUE: The Bills recognize the importance of transparency in the development and use of AI, but the transparency requirements that are included in Article 5[23] of Bill 21/2020

[22] Dylan John Mencia, "Regulating Artificial Intelligence: Self-Regulation, State-Regulation, and Everything In-Between," *University of Miami Law Review* (Apr. 2019), https://lawreview.law.miami.edu/regulating-artificial-intelligence-self-regulation-state-regulation-in-between/.

[23] Article 5: "The principles for artificial intelligence development and application in Brazil are: . . . (V) transparency: the people's right to be informed in a clear, accessible, and accurate way about the use of artificial intelligence solutions, unless otherwise provided by law and observing commercial and industrial secrets, in the following cases: (a) on the fact that they are communicating directly with artificial intelligence systems, such as through conversation robots for

do not enable the public or regulators to fully scrutinize an AI system or understand the underlying performance of the system.

ANALYSIS: The inherent opaqueness of AI systems is the greatest challenge for public oversight of human rights impacts. As the European Commission has noted, "The lack of transparency (opaqueness of AI) makes it difficult to identify and prove possible breaches of laws, including legal provisions that protect fundamental rights, attribute liability and meet the conditions to claim compensation." [24] This opacity can be addressed by instituting transparency obligations for AI systems that ensure users are notified when they are engaging with certain types of AI systems and that enable the explainability[25] of the system so the functioning and performance of the system is less opaque. Essentially, transparency should be at the heart of any AI regulation.

Article 2 of Bill 5051/2019 and Article 2 of Bill 872/2021 both recognize the importance of transparency in the use of AI systems, but neither elaborate on this principle. Meanwhile, Article 5 of Bill 21/2020 provide more detailed obligations for AI systems. Although it includes a concrete requirement for notification when an individual is interacting with an AI system, they are more focused on notification rather than the explainability of the system, so they may not provide regulators or individuals who are interacting with an AI system with enough information about the system's performance and functioning. Furthermore, they do not seem to be tailored to different types of AI systems or the level of risk the system poses to rights.

One example of a transparency obligation is to require clear and accessible notification when a user is interacting with an AI system, with the type of notification differing depending on the technology and how it is used. Deepfake technology, which is powered by AI, may require certain types of notification requirements, whereas AI systems used for internal business operations may not require notification.

A second example of a transparency obligation is to require the disclosure of easily comprehensible information about the functioning and performance of higher-risk AI systems. This information can include the intended purpose of the system, information about the training, validation, and security of the system, and any intended use or foreseeable unintended misuse of the system that would pose risks to health, safety, and

personalized online service (chatbot), when using these systems; (b) on the identity of the natural person, when one operates the system autonomously and individually, or of the legal entity responsible for the operation of artificial intelligence systems; (c) on general criteria that guide the functioning of the artificial intelligence system, ensuring that commercial and industrial secrets are safeguarded, when there is a potential for a relevant risk to fundamental rights."

[24] European Commission, "White Paper on Artificial Intelligence – A European Approach to Excellence and Trust" (Feb. 2020), https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[25] "Explainability (also referred to as "interpretability") is the concept that a machine learning model and its output can be explained in a way that "makes sense" to a human being at an acceptable level." C3ai, "Explainability," available at https://c3.ai/glossary/machine-learning/explainability/.

human rights.[26] These requirements not only aim to notify that a system is being used, but also aim to address the issue of explainability so that laypersons are better able to understand and evaluate the system itself.

Another example is to require the operators of high-risk systems to maintain technical documentation about the system, monitor performance, and report to the relevant regulatory body. The intent of monitoring and reporting is to ensure regulators have enough information about an AI system to effectively intervene.

These examples are not exhaustive, and the Commission of Jurists could consider other options to ensure the public and regulators can

Transparency requirements should be an essential component of any AI legislation, and Brazil's Bills include constructive provisions that increase public awareness of when AI systems are being used. However, future iterations of AI legislation in Brazil should consider more robust transparency requirements so that the public and vulnerable communities can better understand the systems that impact their rights and so that regulators are well-positioned to assess and address risks when they arise.

RECOMMENDATION: In future versions of the legislation, ensure that there is robust enough transparency requirements so that regulators and the public can exert adequate oversight over higher risk AI systems.

Conclusion

By proposing these Bills and establishing a Commission of Jurists to draft comprehensive legislation, Brazil is undertaking a monumental task of regulating a sector that is increasingly complex, both in terms of the technology itself and the profound impacts on society and individual rights. Brazil is one of the first countries to consider comprehensive AI regulation, which is commendable, but it also means that there are few models from which legislators can learn and adapt. Thus, it is important to carefully consider the perspectives of AI technologists, human rights experts, ethicists, civil society leaders, and impacted communities to draft legislation that can effectively regulate the sector to mitigate harms and establish regulatory bodies and institutional expertise that enable consistent and robust enforcement.

ICNL welcomes this opportunity to provide comments in response to the Bills and remains available to answer questions and engage with the Commission of Jurists and civil society during the legislative drafting process.

[26] These examples are included in Article 13(3)(b) of the EU's draft AI Act.