UNIO - *EU Law Journal*. Vol. 10, No. 1, May 2024, pp. 54-69.

School of Law – University of Minho

Regulation of artificial intelligence in Brazil: examination of Draft Bill no. 2338/2023[1]

Ana Frazão[*]

ABSTRACT: This article aims to explore the challenges faced by Brazilian Draft Bill no. 2338/2023 in its purpose to implement risk-based regulation of artificial intelligence in Brazil. Based on the inspiration received from the European AI Act, the article describes the Brazilian classification of risks and its impacts for the regulation, the governance rules, the practical application of principles of prevention and precaution, and the administrative and civil liability.

KEYWORDS: Artificial intelligence – risk-based regulation – Brazilian draft.

[1] This paper is based on the lecture that the author had the honour of giving in October 2023 at the "*I Congresso Ibero-Americano de Direito e Tecnologias Digitais*", held at the University of Minho.

[*] Lawyer and Associate Professor of Civil, Commercial and Economic Law at the University of Brasília – UnB. Member of the Commission of Jurists appointed by the Brazilian Federal Senate to prepare the "*Anteprojeto de Marco da IA*" or "AI Framework Draft", which was presented as a bill by Senator Rodrigo Pacheco, President of the Brazilian Senate.

1. Initial considerations

The discussions surrounding the need to regulate artificial intelligence (AI) in Brazil reflect, in a way, the dilemmas that have been faced by legislators and regulators around the world. Among the main concerns are why and for what should AI be regulated, and then when and in what way.

In Brazil, there are many voices who argue that any regulation of AI would be premature, given how little we know about it and the risks of inhibiting innovation. In fact, this narrative is widely propagated by major economic agents in the sector, a sentiment echoed in the mainstream media.

Nonetheless, there are several legislative initiatives for the regulation of AI in Brazil, including the draft legislation prepared by the Committee of Jurists appointed by the Federal Senate for this purpose, which ended up being presented as a bill by Senator Rodrigo Pacheco, President of the Senate.[2]

In light of the aforementioned draft, as well as the debates that preceded it, this article aims to show how several of the dilemmas related to the regulation of AI were faced, as well as exploring the main solutions found, highlighting the inspiration received from the European AI Act.

To this end, the article will initially seek to explore the main foundations that justified the conclusion that AI needs to be regulated immediately. Then, in its second part, it will seek to demonstrate the structure of Draft Bill no. 2338/2023 and its most important points.

2. Why regulate AI? Discussions about risks in the Brazilian debate

2.1. Reasons to regulate AI

One of the main debates held in Brazil has concerned the desirability of regulating AI, especially if we take into account the argument that very little is known about it and therefore, we are not in a position to regulate the unknown.

This idea has been widely explored both in academia, as well as in politics and the press itself, with the aim being that of restricting – or at least delaying – regulation. The main argument is that, in the face of significant uncertainty, it is better not to intervene or to intervene little. In many cases, this position is intensified by insisting on the supposed trade-off between regulation and innovation, in order to highlight the risk that premature or undue regulation inhibits innovation.

It is not without reason that, before the draft presented by the Senate Committee of Jurists, there were other projects that proposed to regulate by "*not regulating*" AI in Brazil. These were excessively generic or principled initiatives, which did not provide specific duties for AI agents, limiting themselves to establishing general principles with little concreteness and which could be fulfilled by such agents with great malleability and in accordance with their own interests.

Meanwhile, the Draft Bill no. 2338/2023 was based on the premise that, despite the unquestionable degree of ignorance that still exists in relation to AI, there is already considerable mapping in literature and various empirical studies of several of its risks.

One such example is the issue of algorithmic discrimination, which has long ceased to be a mere fear. In fact, there is countless evidence that situations like this

[2] This refers to the Draft Bill no. 2338/2032 or PL no. 2338/2023.

have occurred repeatedly, with consequent and serious harm to the poor, women, black people, children, adolescents and other vulnerable groups.[3] This is particularly serious in countries like Brazil, which have countless highly vulnerable minorities.

To the various risks already mapped, there is also the added problem – identified by Stuart Russell[4] – that the predominant model of AI is a threat to the survival of human beings, as systems are programmed to fulfil their objectives at any cost, becoming blind and indifferent to the destruction they can cause to people.

This shows how much the use of AI planned for a certain objective – such as keeping the user connected to a certain platform and more engaged with the content presented to them – can come at the price of great harm, such as encouraging addictions, depression, social dysfunction, manipulation of people, extremism, polarisation of society and various other damages.

Such difficulties highlight the fact that technology is neither neutral nor necessarily good. It all depends on how it is used, and the care and safeguards put in place for its use. The problem is that, in the absence of regulation, technology has been chosen and put into use without any type of risk analysis or accountability by economic agents who have probably prioritised their interests to the detriment of the interests of consumers, society, and democracy itself.

It is not without reason that the European AI Act – which served as inspiration for the Draft Bill no. 2338/2023 – adopted a risk regulation model which is not incompatible with the rights regulation model, and seeks to ensure that AI systems are designed, developed, and have quality management that is effectively well-matched with its respective risks, given the need to protect the rights of those who will be affected by these systems.

It is worth highlighting that, even for uses considered high-risk, the requirements of the European proposal, as well as those of the Brazilian one, do not conflict – for the most part – with what should already be practiced by responsible companies, even more so in countries where legislation such as the General Data Protection Regulation (GDPR) or *Lei Geral de Proteção de Dados Pessoais* (LGPD) already exists: that is, where the use of quality databases, the establishment of documentation and registration procedures, guaranteeing adequate levels of transparency and human supervision, as well as robustness, accuracy and security are mandatory.

2.2. Necessary compatibility between the regulation of AI and incentives for innovation

Another important contribution of the Committee of Jurists was to demonstrate that regulation based on risks, like the European model, could not be considered an obstacle to innovation. In fact, by regulating the concrete obligations to be obligatory for AI agents – modulated according to the degree of risk – regulation can even be an important factor in encouraging innovation, by guaranteeing the necessary legal certainty.

It is for this reason that the Committee of Jurists started from the premise that the supposed trade-off between regulation and innovation must be rethought, bearing in mind that the lack of regulation may, to a degree, compromise the advancement

[3] Cathy O'Neil, *Weapons of Math Destruction. How big data increases inequality and threatens democracy* (United Kingdom: Crown, 2016).

[4] Stuart Russell, *Human Compatible. Artificial intelligence and the problem of control* (United States: Penguin Publishing Group, 2019).

of innovation, but can also create competitive advantages for large players that have already implemented their business models or that can bear the costs of regulatory changes in the course of their activities.

In other words, the absence of regulation, in situations like this, can be a factor in facilitating the entrenchment of powerful economic agents, hindering, or even preventing a healthy competitive dynamic, especially with regard to competition for markets.

After all, for new entrants and small businesses, the absence of regulation or regulatory instability can lead to very pernicious scenarios, as not everyone is able to undertake a project while the rules of the game are not minimally defined. On the other hand, it is difficult to structure new business models based on respect for the rights of those affected by AI systems if the market is dominated by large agents who do not adopt these precautions and, precisely for this reason, are not subject to its respective costs.

In this way, the Committee of Jurists was guided by the premise that the argument that ignorance can and should lead to regulatory retraction is not correct. Since there is already evidence to justify the regulation of AI, especially in cases of high-risks, the option should not be between regulating or not regulating, or between regulating more or less. The key is to regulate appropriately.

Contrary to the assumption that the regulation of AI is necessarily incompatible with innovation – an argument that is more ideological and linked to the defence of free markets than actually based on consistent empirical evidence – it was considered that adequate regulation can even encourage innovation, ensuring the legal security necessary to discipline the market and to encourage new entries and new business models.

In any case, even if this were not the case, innovation should only be considered positive when its benefits are achieved in proportion to the risks and damages they cause. That is, when there is legitimacy and reasonableness between the means and ends, and when prevention measures for the violation of fundamental rights and repair and mitigation of damages are observed.

Thus, if regulation is capable of preventing or containing predatory, exploitative or violative innovations of fundamental rights, as well as innovations that assume unnecessary, inappropriate, excessive or undesirable risks, which compromise not only individuals, but also society itself and the democracy, this is a price that must be paid.

Finally, the Draft Bill no. 2338/2023 is based on the premise that adequate regulation of AI is not incompatible with the initiatives and particularities of each economic agent: compliance can and should be valued, as long as the minimum material and procedural rules of hetero-regulation are observed, whose objective is precisely to ensure harmonisation between innovation and protection of fundamental rights.

3. The proposal for a regulation based on risk and the classification dilemmas

3.1. The initially proposed classification

Before going into the specific issue of risks, it is worth highlighting that Draft Bill no. 2338/2023 has an Article that, as it provides for the fundamental rights of people affected by AI systems, can be considered the backbone of the project:

"*Article 5. People affected by artificial intelligence systems have the following rights, to be exercised in the manner and under the conditions described in this Chapter:*

I – right to prior information regarding their interactions with artificial intelligence systems;

II – right to explanation about the decision, recommendation or prediction made by artificial intelligence systems;

III – right to contest decisions or predictions of artificial intelligence systems that produce legal effects or that significantly impact the interests of the affected person;

IV – right to determination and human participation in decisions regarding artificial intelligence systems, taking into account the context and state of the art of technological development;

V – right to non-discrimination and correction of direct, indirect, illegal or abusive discriminatory biases; and

VI – the right to privacy and protection of personal data, in accordance with the relevant legislation.

Single paragraph. Artificial intelligence agents will inform, in a clear and easily accessible way, the procedures necessary to exercise these rights."[5]

Given this scenario, the Draft Bill no. 2338/2023 proposes a tripartite classification of risks – excessive risks, high-risks and other risks –, assigning a specific regulatory model to the last two and prohibiting excessive risks, as seen in Article 14:

"*Article 14. There is an embargo on the implementation and use of artificial intelligence systems:*

I – that employ subliminal techniques that have the objective or effect of inducing a natural person to behave in a way that is harmful or dangerous to their health or safety or against the foundations of this law;

II – that exploit any vulnerabilities of specific groups of natural people, such as those associated with their age or physical or mental disability, in order to induce them to behave in a way that is harmful to their health or safety or against the foundations of this law;

III – by public authorities, to evaluate, classify or rank natural persons, based on their social behaviour or personality attributes, through universal scoring, for access to goods and services and public policies, illegitimately or disproportionately."

As one can observe, the Draft Bill no. 2338/2023 takes a very cautious approach to excessive risks, only considering as such those in relation to which there is already considerable convergence of national and foreign opinions in this regard. That is why, faced with the impasses inherent to continuous remote biometric identification in spaces accessible to the public, it adopted an intermediate solution, not considering such risk *a priori* as excessive, but providing additional requirements for its assumption:

"*Article 15. Within the scope of public security activities, the continuous use of remote biometric identification systems in spaces accessible to the public is only permitted when there is provision in specific federal law and judicial authorisation in connection with the activity of individualised criminal prosecution, in the following cases:*

I – prosecution of crimes punishable by a maximum sentence of imprisonment of more than two years;

II – search for victims of crimes or missing people;

III – crime in the act.

Single paragraph. The law referred to in the caput will provide for proportional and strictly necessary measures to meet the public interest, subject to due legal process and judicial control, as well as the principles and rights provided for in this Law, especially the guarantee against discrimination and the need for review of the algorithmic inference by the responsible public agent before taking any action against the identified person."

[5] From here onwards, direct quotations from the legislation are freely translated.

High-risks were defined by Article 17 of Draft Bill no. 2338/2023 in the following terms:

"*Article 17. High-risk artificial intelligence systems are those used for the following purposes:*
I – application as security devices in the management and operation of critical infrastructures, such as traffic control and water and electricity supply networks;
II – education and professional training, including systems for determining access to educational and professional training institutions or for evaluating and monitoring students;
III – recruitment, screening, filtering, evaluation of candidates, making decisions on promotions or terminations of contractual employment relationships, distribution of tasks, and control and evaluation of the performance and behaviour of people affected by such artificial intelligence applications in the areas of employment, worker management and access to self-employment;
IV – evaluation of criteria for access, eligibility, concession, review, reduction or revocation of private and public services that are considered essential, including systems used to evaluate the eligibility of natural persons for the provision of public assistance and security services;
V – assessment of the debt capacity of individuals or establishment of their credit rating;
VI – dispatch or establishing of priorities for emergency response services, including firefighters and medical assistance;
VII – administration of justice, including systems that assist judicial authorities in investigating facts and applying the law;
VIII – autonomous vehicles, when their use may create risks to the physical integrity of people;
IX – applications in the health sector, including those intended to assist diagnoses and medical procedures;
X – biometric identification systems;
XI – Criminal Investigation and Public Security, especially for individual risk assessments by the competent authorities, in order to determine the risk of a person committing infractions or recurrence, or the risk for potential victims of criminal offenses or to evaluate personality traits and the characteristics or past criminal behaviour of individuals or groups;
XII – analytical study of crimes relating to natural persons, allowing law enforcement authorities to search large sets of complex data, related or unrelated, available in different data sources or in different data formats, with the aim of identifying unknown patterns or discovering hidden relationships in the data;
XIII – investigation by administrative authorities to assess the credibility of evidence in the course of the investigation or prosecution of infractions, to predict the occurrence or recurrence of a real or potential infraction based on the definition of profiles of natural persons;
XIV – migration management and border control."

Finally, the last category is residual, to encompass all risks that are considered neither excessive nor high.

As can be seen, the risk classification was inspired by the European AI Act model, albeit with some adaptations. Unlike the European solution, which creates four categories of risks – unacceptable, high, limited, and minimal – the Brazilian solution emphasises excessive and high-risks, leaving all others in a residual category.

As will be shown later, the importance of classification is fundamental because it will be decisive in knowing the regulatory regime to which a given use of AI will be subject, with the distinction between governance regimes being striking, the severity of which is proportional to the intensity of the risk.

Among the important consequences of risk classification, differences regarding civil liability regimes can be mentioned: in cases of high-risk or excessive risk, it will be in the objective modality, while in other cases, it will be subjective with the

presumption of the agent's guilt causing the damage and the consequent reversal of the burden of proof in favour of the victim.[6] By proposing a taxonomy of excessive and high-risks, Draft Bill no. 2338/2023 was inspired by the European AI Act, not ignoring the objections already directed to this kind of risk classification model, under the argument that very generic segmentations – such as the uses of AI in areas of health and education – could "*sin*" by both excess and lack, especially in cases of misuse of technologies that were designed for legitimate purposes.[7] In fact, the European AI Act has been consistently subject to criticism, which focuses on the fact that the categories refer to broad fields of AI application, meaning that the magnitude of its effects can be wrongly estimated, and this could curb innovation and prevent the effectiveness of regulation itself, especially in the face of general AI or generative AI.[8]

More than that, it is argued that, in the way the risk classification was designed, the AI Act would fail to promote adequate protection for fundamental rights, the rule of law and even democracy.[9] Hence the numerous suggestions for reform that European doctrine is proposing to the AI Act Draft.[10]

However, Draft Bill no. 2338/2023 was based on the premise that, due to the necessary legal certainty that should guide AI agents, a precise and objective description of applications would be the most appropriate solution, especially in areas such as health and education that involve ultra-sensitive data, with great potential to cause undue discrimination.

Furthermore, linking the taxonomy to the type of use (or misuse) of the AI system could give rise to endless interpretative discussions, in addition to the fact that, in all applications related to excessive or high-risks, the strength of the precautionary principle should be enforced, considering that we are dealing with

---

[6] This is the wording of the Article 27, of the Draft Bill: "Article 27. The supplier or operator of an artificial intelligence system that causes property, moral, individual or collective damage is obliged to repair it in full, regardless of the system's degree of autonomy.
§ 1 When dealing with a high -risk or excessive -risk artificial intelligence system, the supplier or operator is objectively liable for the damage caused, to the extent of their participation in the damage.
§ 2 When it is not a high -risk artificial intelligence system, the guilt of the agent causing the damage will be presumed, applying the inversion of the burden of proof in favour of the victim."

[7] Asress Gikay, et al., "High-Risk Artificial Intelligence Systems under the European Union's Artificial Intelligence Act: Systemic Flaws and Practical Challenges", November 2, 2023. Available at SSRN: https://ssrn.com/abstract=4621605 or http://dx.doi.org/10.2139/ssrn.4621605.

[8] Part of the criticism against the European AI Act can be found in: Claudio Novelli, et al. "Taking AI Risks Seriously: a Proposal for the AI Act", *AI & Society*, Springer, vol. 38, no. 3 (2023), https://doi.org/10.1007/s00146-023-01723-z.; Kees Stuurman and Eric Lachaud, "Regulating AI. A Label to Complete the Proposed Act on Artificial Intelligence", January 12, 2022. Available at SSRN: https://ssrn.com/abstract=3963890 or http://dx.doi.org/10.2139/ssrn.3963890; Nathalie Smuha, et al., "How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act", August 5, 2021). Available at SSRRN> https://ssrn.com/abstract=3899991 or http://dx.doi.org/10.2139/ssrn.3899991.

[9] Nathalie Smuha, et al., "How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act".

[10] See Claudio Novelli, et al., "Taking AI Risks Seriously: a Proposal for the AI Act".; Jonas Schuett, "Risk Management in the Artificial Intelligence Act", European Journal of Risk Regulation, First View , 1 - 19, https://doi.org/10.1017/err.2023.1; LAUX, Johann Laux et al., "Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk", https://onlinelibrary.wiley.com/doi/full/10.1111/rego.12512; Nathalie Smuha, et al., "How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act".

uncertain scenarios with risks of irreversible or even catastrophic damage. In any case, it became very clear that any taxonomy effort is always precarious, and, for this reason, it needs to be subjected to alteration and reform mechanisms that are agile and efficient, following not only the evolution of the technology, but also the changes in the social perception about the risks. Therefore, as the legal taxonomy is only a preliminary proposal, any flaws and reductionisms must be subjected to appropriate correction and amendment procedures. Such concerns, added to the fear of the necessity to create tools to update the taxonomy, were the reasons why Draft Bill no. 2338/2023 sought to ensure a point of balance based on the European AI Act: while the legal text offers an initial taxonomy, reflecting the values that inspired the legislator, it already provides mechanisms for its updating without the need for legislative reform, as will be seen in the next section.

3.2. The strategic importance of the responsible authority for updating the risk classification

One of the main dilemmas faced by the Committee of Jurists was how to implement risk classification. To ensure flexibility, a first alternative would be for the classification not to be included in the legal text, although this could create many interpretive difficulties. From the point of view of legal security, the most advisable option would be for the legal text to already contain an *a priori* risk classification, but this could hamper its updating, which would be worrying given a technology that evolves so quickly.

The solution found, once again, sought to ensure a path of balance, like the path that had already been followed by the European AI Act: the legal text offers an initial classification of risks, but already provides the mechanisms so that the aforementioned classification can be updated without the need for legislative reform.

This was one of the reasons why the Draft Bill no. 2338/2023 considered the establishment of an authority responsible for applying the law to be indispensable, which would have, within its numerous responsibilities, to constantly update the risk classification.

Especially because it was aware of the political dimension related to the constitution of the aforementioned authority and the discussions arising from it – whether, for example, a new and transversal authority should be created or whether an existing authority could assume such a function – the Draft Bill no. 2338/2023 did not advance in the nature and specificities of the aforementioned authority. However, it is unequivocal that the existence of the competent authority can be considered a true "*touchstone*" of the project in relation to several issues, including risk classification and the need for its constant updating.

Here, two important Articles from the Draft Bill no. 2338/2023 deserve to be highlighted, which deal with the importance of authority for the functioning of regulation based on risk classification:

> "*Article 16. It will be up to the competent authority to regulate excessive risk artificial intelligence systems.*
> *(...)*"
> "*Article 18. The competent authority will be responsible for updating the list of excessive or high-risk artificial intelligence systems, identifying new hypothesis, based on at least one of the following criteria:*

a) the implementation is on a large scale, taking into account the number of people affected and the geographic extension, as well as its duration and frequency;
b) the system may negatively impact the exercise of rights and freedoms or the use of a service;
c) the system has a high potential for material and moral harm, as well as discrimination;
d) the system affects people from a specific vulnerable group;
e) the possible harmful results of the artificial intelligence system are irreversible or difficult to reverse;
f) a similar artificial intelligence system has previously caused material or moral damage;
g) low degree of transparency, explainability and auditability of the artificial intelligence system, which makes its control or supervision difficult;
h) high level of identifiability of data subjects, including the processing of genetic and biometric data for the purposes of uniquely identifying a natural person, especially when the processing includes combining, matching or comparing data from several sources;
i) when there are reasonable expectations of the affected party regarding the use of their personal data in the artificial intelligence system, in particular the expectation of confidentiality, such as in the processing of confidential or sensitive data.
Single paragraph. The update of the list by the competent authority will be preceded by consultation with the competent sectoral regulatory body, if any, as well as public consultation and hearing and regulatory impact analysis."

3.3. The importance of engaging artificial intelligence agents

The Draft Bill no. 2338/2023 also started from the premise that risk regulation must contain due responsiveness, with the necessary engagement of AI agents.[11] Consequently, several duties related to preliminary risk assessment were imposed on AI agents:

"*Article 13. Prior to being placed on the market or used in service, every artificial intelligence system will undergo a preliminary assessment carried out by the supplier to classify its level of risk, whose registration will consider the criteria set out in this chapter.*
§ 1 Suppliers of general-purpose artificial intelligence systems will include in their preliminary assessment the indicated purposes or applications, in accordance with article 17 of this law.
§ 2 There will be registration and documentation of the preliminary assessment carried out by the supplier for liability and accountability purposes in the event that the artificial intelligence system is not classified as high-risk.
§ 3 The competent authority may determine the reclassification of the artificial intelligence system, upon prior notification, as well as determine the carrying out of an algorithmic impact assessment to inform the ongoing investigation.
§ 4 If the result of the reclassification identifies the artificial intelligence system as high risk, carrying out an algorithmic impact assessment and adopting the other governance measures provided for in Chapter IV will be mandatory, without prejudice to possible penalties in the case of preliminary assessment fraudulent, incomplete or untrue."

As can be seen, the competent authority can order the reclassification of the AI system and carry out an algorithmic impact assessment, as well as applying penalties if it believes that the assessment was fraudulent, incomplete or untrue.

Another fundamental point of the Draft Bill no. 2338/2023 concerns the governance measures for high-risk AI systems, as described in its Article 20:

"*Article 20. In addition to the measures indicated in Article 19, artificial intelligence agents that provide or operate high-risk systems will adopt the following governance measures and internal processes:*

[11] Julia Black and Robert Baldwin, "Really Responsive Risk-Based Regulation", *Law and Police*, v. 32, no. 2 (2010): 181-231, doi: 10.1111/j.1467-9930.2010.00318.x.

I – documentation, in the format appropriate to the development process and the technology used, regarding the functioning of the system and the decisions involved in its construction, implementation and use, considering all relevant stages in the system's life cycle, such as the development stage design, development, evaluation, operation and discontinuation of the system;
II – use of automatic recording tools for the system's operation, in order to allow the assessment of its accuracy and robustness and to determine discriminatory potential, as well as the implementation of the risk mitigation measures adopted, with special attention to adverse effects;
III – carrying out tests to assess appropriate levels of reliability, depending on the sector and type of application of the artificial intelligence system, including robustness, accuracy, precision and coverage tests;
IV – data management measures to mitigate and prevent discriminatory bias, including:
a) evaluation of data with appropriate measures to control human cognitive biases that may affect data collection and organization, as well as measures to avoid the generation of biases due to problems in classification, failures or lack of information in relation to affected groups, lack of coverage or distortions in representation, depending on the intended application, as well as corrective measures to avoid the incorporation of structural social biases that can be perpetuated and expanded by technology;
b) composition of an inclusive team responsible for the design and development of the system, guided by the search for diversity.
V – adoption of technical measures to enable the explainability of the results of artificial intelligence systems and measures to make available to operators and potential impacted parties general information about the functioning of the artificial intelligence model used, explaining the logic and relevant criteria for the production of results, as well as, upon request from the interested party, providing adequate information that allows the interpretation of the results actually produced, respecting industrial and commercial secrecy.
Single paragraph. Human supervision of high-risk artificial intelligence systems will seek to prevent or minimise risks to the rights and freedoms of people that may arise from their normal use or from their use under reasonably foreseeable conditions of misuse, enabling those responsible for human supervision can:
I – understand the capabilities and limitations of the artificial intelligence system and properly control its functioning, so that signs of anomalies, dysfunctionalities and unexpected performance can be identified and resolved as quickly as possible;
II – be aware of the possible tendency to automatically trust or rely excessively on the result produced by the artificial intelligence system;
III – correctly interpret the result of the artificial intelligence system taking into account the characteristics of the system and the available interpretation tools and methods;
IV – decide, in any specific situation, not to use the high-risk artificial intelligence system or to ignore, cancel or reverse its result; and
V – intervene in the operation of the high--risk artificial intelligence system or interrupt its operation."

Reading the Article it shows that: (i) transparency and accountability were indispensable points, including with regard to the provision of additional documentation obligations, (ii) concerns about ensuring accuracy, robustness, precision and coverage of systems of AI and avoid discriminatory biases, (ii) the adoption of techniques to enable the explainability of the results of AI systems, and (iii) the intention to implement substantive and not merely formal human supervision, which presupposes broad knowledge on the part of supervisors of the functioning and limitations of AI systems, as well as the attribution to them of

the necessary skills, including for the purpose of intervening or suspending the system's functioning.

With regard to the Public Power, additional measures were also foreseen, such as those set out in Article 21 of the Draft Bill no. 2338/2023:

"*Article 21. In addition to the governance measures established in this chapter, public bodies and entities in the Union, States, Federal District and Municipalities, when contracting, developing or using artificial intelligence systems considered high-risk, will adopt the following measures:*

I – holding a prior public consultation and hearing on the planned use of artificial intelligence systems, with information on the data to be used, the general operating logic and results of tests carried out.

II – definition of system access and use protocols that allow recording who used it, for what specific situation, and for what purpose;

III – use of data from secure sources, which are accurate, relevant, updated and representative of the affected populations and tested against discriminatory bias, in accordance with Law No. 13.709, of August 14, 2018, and its regulatory acts;

IV – facilitated and effective guarantee to the citizen, before the public authorities, of the right to human explanation and review of decisions by artificial intelligence systems that generate relevant legal effects or that significantly impact the interests of the affected person, to be carried out by the competent public agent;

V – use of an application programming interface that allows its use by other systems for interoperability purposes, in accordance with the regulations;

VI – publication in an easily and accessible manner, preferably on their websites, of preliminary assessments of artificial intelligence systems developed, implemented or used by public authorities in the Union, States, Federal District and Municipalities, regardless of the degree of risk, without prejudice to the provided for in Article 43.

§ 1 The use of biometric systems by the public authorities of the Union, States, Federal District and Municipalities will be preceded by the publication of a normative act that establishes guarantees for the exercise of the rights of the affected person and protection against direct, indirect, illegal or abusive discrimination, The processing of data on race, colour or ethnicity is prohibited, unless expressly provided for by law.

§ 2 If it is impossible to eliminate or substantially mitigate the risks associated with the artificial intelligence system identified in the algorithmic impact assessment provided for in Article 22 of this Law, its use will be discontinued."

Special care was also given to the algorithmic impact assessment, considered essential in high-risk cases, as can be seen from Articles 22 to 26:

"*Article 22. The assessment of the algorithmic impact of artificial intelligence systems is the obligation of artificial intelligence agents whenever the system is considered high-risk by the preliminary assessment.*

Single paragraph. The competent authority will be notified about the high-risk system by sharing the preliminary and algorithmic impact assessments."

"*Article 23. The algorithmic impact assessment will be carried out by a professional or team of professionals with the technical, scientific, and legal knowledge necessary to produce the report and with functional independence.*

Single paragraph. It will be up to the competent authority to regulate the cases in which the performance or audit of the impact assessment will necessarily be carried out by a professional or team of professionals external to the supplier."

"*Article 24. The impact assessment methodology will contain, at least, the following steps:*

I – preparation;

II – risk cognition;
III – mitigation of the risks found;
IV – monitoring.
§ 1 The impact assessment will consider and record, at least:
a) known and predictable risks associated with the artificial intelligence system at the time it was developed, as well as the risks that can reasonably be expected from it;
b) benefits associated with the artificial intelligence system;
c) probability of adverse consequences, including the number of people potentially impacted;
d) severity of adverse consequences, including the effort required to mitigate them;
e) operating logic of the artificial intelligence system;
f) process and results of tests and assessments and mitigation measures carried out to verify possible impacts on rights, with special emphasis on potential discriminatory impacts;
g) training and actions to raise awareness of the risks associated with the artificial intelligence system;
h) mitigation measures and indication and justification of the residual risk of the artificial intelligence system, accompanied by frequent quality control tests;
i) measures of transparency to the public, especially potential users of the system, regarding residual risks, especially when involving a high degree of harm or danger to the health or safety of users, in accordance with Articles 9 and 10 of Law no. 8,078, of September 11, 1990 (Consumer Protection Code);
§ 2 In compliance with the precautionary principle, when using artificial intelligence systems that may generate irreversible or difficult-to-reverse impacts, the algorithmic impact assessment will also take into account incipient, incomplete or speculative evidence.
§ 3 The competent authority may establish other criteria and elements for preparing an impact assessment, including the participation of the different affected social segments, depending on the risk and economic size of the organisation.
§ 4 The competent authority will be responsible for regulating the frequency of updating impact assessments, considering the life cycle of high-risk artificial intelligence systems and the fields of application, and may incorporate best sectoral practices.
§ 5 Artificial intelligence agents who, after their introduction into the market or use in service, become aware of an unexpected risk that they pose to the rights of natural persons, will immediately communicate the fact to the competent authorities and to the people affected by the artificial intelligence system."
"*Article 25. The algorithmic impact assessment will consist of a continuous iterative process, carried out throughout the entire life cycle of high-risk artificial intelligence systems, requiring periodic updates.*
§ 1 The competent authority will be responsible for regulating the frequency of updating impact assessments.
§ 2 The update of the algorithmic impact assessment will also include public participation, based on a consultation procedure with interested parties, albeit in a simplified manner."
"*Article 26. Once industrial and commercial secrets are guaranteed, the conclusions of the impact assessment will be public, containing at least the following information:*
I – description of the intended purpose for which the system will be used, as well as its context of use and territorial and temporal scope;
II – risk mitigation measures, as well as their residual level, once such measures have been implemented;
III – description of the participation of different affected segments, if any, in accordance with § 3 of art. 24 of this Law."

As can be seen, with regard to algorithmic impact assessment, the Draft Bill no. 2338/2023 requires, among other requirements establishes as necessary: (i) notification of the competent authority about the existence of high-risk systems, including through sharing of preliminary and of algorithmic impact, (ii) the qualification and independence of the team responsible for the algorithmic impact assessment, including enabling the authority to regulate the cases in which it must be carried out by professionals external to the supplier, (iii) the methodological requirements to be observed in the evaluation, including for the purpose of explaining the forms of monitoring and mitigation; (iv) the need to clarify the operating logic of the AI system and its possible impacts on rights, especially in the face of discriminatory risks, and (v) transparency measures for the public.

The role of the competent authority is also fundamental, as it will not only be responsible for establishing other criteria, based on procedures that ensure popular participation – notably of groups affected by the AI system – but also regulating the frequency of updating assessments.

Knowing that the algorithmic impact assessment will hardly be able to predict, *ex ante*, all the impacts of the AI system, its preparation does not exempt agents from the duty to immediately communicate, to the competent authority and the affected people, any unexpected risk.

4. Radical uncertainties and the express acceptance of the precautionary principle

Given the adoption by the Draft Bill no. 2338/2023 of risk regulation, it was essential that the Committee of Jurists could deal with the problem of uncertainties, that is, everything that, unlike risk – which can be predicted and, consequently, becomes more susceptible to measurements, prognosis and statistical or probabilistic calculations, control and management – it cannot be predicted or calculated.

In this sense, the Commission of Jurists relied on the abundant literature that, like Taleb,[12] shows the importance of regulation considering that "*we don't know that we don't know*", in order to create more resilient ways of life. This is a convergent reflection with the stance of Kay and King,[13] when they warn of the need to consider uncertainties in regulatory decisions, in order to achieve more resilient solutions that can consider different scenarios – beyond those predicted as the most likely or possible – and even unimaginable.

Obviously, dealing with uncertainty is not easy. However, AI does not represent the first time that legislators and regulators have encountered this type of problem. In several matters, they have already had to face the challenge, an example being Environmental Law, in which the precautionary principle is intended precisely to deal with uncertainties, while the prevention principle is intended to deal with risks.

The delicate part of the precautionary principle is that, in several aspects, it ends up being incompatible with the idea of evidence-based regulation, as well as with regulatory impact analyses, especially in the form of cost-benefit analyses.[14]

[12] Nassim Nicholas Taleb, *A lógica do cisne negro. O impacto do altamente improvável*, trans. Marcelo Schild (Rio de Janeiro: Best Business, 2018).

[13] John Kay and Mervin King, *Radical Uncertainty. Decision-making beyond the numbers* (New York: W.W. Norton & Company, 2020).

[14] As Johathan Wolff explains, there are clear limits to the use of cost-benefit analyses when risks

After all, in the face of uncertainty, the premise is that there is not enough scientific evidence to guide the decision. On the other hand, regulatory impact analysis also does not adjust to uncertainties, as they only measure risks and, even so, with numerous deficiencies.[15]

It is for this reason that, as René von Schomberg[16] explains, the precautionary principle is precisely related to two crucial elements: alongside scientific uncertainty, the seriousness of the consequences. It is such circumstances that establish a rationale for action that substantially reduces the requirements for regulatory action.

In the same sense, Jale Tosun[17] points out that the most important aspect of the precautionary principle is precisely that of reducing the requirements for regulatory action, starting to take into account socially constructed perceptions regarding uncertainties and their differences in relation to risks. More than that, the precautionary principle implies, as taught by Ian Scoones and Andy Stirling,[18] a new moment to rethink the relationships between state protection, technical expertise and deliberative citizenship under uncertainty, requiring a new form of responsibility politics.

However, it is necessary to consider that precautionary measures are provisional in nature, since they need to be regularly reviewed when scientific information requires strengthening or even relaxation, such as in hypothesis in which scientific knowledge transforms uncertainties into risks and consensual levels of damage.

From this perspective, there is no question that some of the applications of AI fully meet the requirement of serious consequences. Without any intention of exhausting the topic, examples of autonomous weapons, biometric recognition and various technologies that can manipulate people and even subvert free will can be cited.

Even though there is still a considerable degree of uncertainty, the fact that it is possible to anticipate some serious scenarios that could result from the misuse of such technologies is already a strong reason for regulatory action. After all, in terms of the European Commission's synthesis,[19] precaution has to do with the idea that regulatory intervention can be legitimate even when the evidence is still incomplete or speculative, and even when the costs of regulation are high, for the simple reason that its main foundation is the idea that prevention is better than cure ("*better safe than sorry*").

---

and probabilities are unknown. Furthermore, cost-benefit analyses ignore issues of moral hazard and the political dimensions of introducing new technologies, which is why they cannot be applied in cases of radical uncertainty. See Johnathan Wolff, "Risk and Regulation of New Technologies", in *Risks and Regulation of New Technologies*, ed. Tsuyoshi Matsuda, Jonathan Wolff and Takashi Yanagawa (Singapore: Springer, 2021), 3-18.

[15] Rene von Schomberg, "The precautionary principle and its normative challenges", in *Implementing the precautionary principle. Perspectives and Prospects*, ed. Elizabeth Fisher, Judith S. Jones and Rene von Schomberg (Cheltenham, Edward Elgar, 2006), 23.

[16] Schomberg, "The precautionary principle", 23.

[17] Jale Tosun, *Risk Regulation in Europe. Assessing the Application of the Precautionary Principle* (New York: Springer, 2013), 41-42.

[18] Ian Scoones and Andy Stirling, "Uncertainty and the politics of transformation", in *The politics of uncertainty: Challenges of Transformation*, ed. Ian Scoones and Andy Stirling (London: Routledge, 2020), Kindle version.

[19] European Commission, "The Precautionary Principle: decision-making under uncertainty", https://ec.europa.eu/environment/integration/research/newsalert/pdf/precautionary_principle_decision_making_under_uncertainty_FB18_en.pdf.

This stance also rules out the argument that this type of regulation would be "*anti-scientific*", since in terms of the European Commission's analysis, what would be anti-scientific would be to ignore the multiple perspectives of uncertainties.

Hence why – in relation to the uncertainties arising from AI – the Committee of Jurists started from the premise that it cannot be demanded that the advancement of regulation depends, absolutely, on unquestionably robust scientific evidence. In fact, in this field, the very idea of broad scientific proof proves to be erroneous, since risks, value and knowledge are contingent and in development.

Strictly speaking, this reasoning, far from being restricted to specific spheres, such asAI, must be applied to all human and social issues, in relation to which it is increasingly difficult to base decisions or policies on previously known risks, disregarding the uncertainties. In the terms of Jens Beckert and Richard Bronk's warning,[20] it is characteristic of contemporary economies that decision makers are constantly confronted with fundamental uncertainties, which makes it impossible for such decisions to be just rational calculations.

Still, according to Jens Beckert and Richard Bronk,[21] the future cannot be understood as a statistical shadow of the past, so that, strictly speaking, we cannot know what the correct model of how the economy will be, just as we cannot predict the future by the fact that "*what does not yet exist cannot now be known*".

Exactly for this reason, it is necessary to recognise the problem of uncertainty once and for all and face it whenever the serious consequences of an uncertain future arise. In a world full of uncertainty, demanding complete and robust scientific evidence or risk calculations for regulatory action is simply making any type of regulation unfeasible, completely disregarding the complexity of the world.

Even the alleged "*trade-off*" between innovation and precaution needs to be put into perspective. For Andy Stirling,[22] for example, the ideas that using the precautionary principle for technology would be dangerous, arbitrary, irrational or even suppress innovation are mistaken. In fact, the precautionary principle should serve to guide innovation – making it compatible with people's well-being – and not block it.

On the other hand, the precautionary principle can also serve to slow down innovation, which, depending on the case, can also be positive, since innovation is not necessarily good. It is worth highlighting Acemoglu's[23] interesting observation regarding the use of the precautionary principle precisely for this purpose:

"*These considerations then suggest a "precautionary regulatory principle" – ex ante regulation slowing down the use of AI technologies, especially in domains where redressing the costs of AI become politically and socially more difficult after large-scale implementation. AI technologies impacting political discourse and democratic politics may be prime candidates for the application of such a precautionary regulatory principle.*"

As can be seen, Acemoglu argues that the precautionary principle should justify the slowdown of some AI applications that can generate serious consequences, as is the case with technologies that impact political discourse and democracy itself.

---

[20] Jens Beckert and Richard Bronk, "An Introduction to Uncertain Futures", in *Uncertain futures. Imaginaries, narratives and calculation in the Economy*, ed. Jens Beckert and Richard Bronk (Oxford: Oxford University Press, 2018).

[21] Beckert, "An Introduction".

[22] Andy Stirling, "Precaution in the Governance of Technology", in *The Oxford Handbook of Law, Regulation and Technology*, ed. Roger Brownsword, Eloise Scotford, Karen Yeung (Oxford: Oxford University Press, 2017).

[23] Daron Acemoglu, "Harms of AI", *NBER*, Working Paper 29247 (2021), doi: 10.3386/w29247.

For all these reasons, the Commission of Jurists started from the premise that invoking uncertainties as a pretext for regulatory inaction is a huge mistake. In many cases, the serious consequences that can arise from such uncertainties are the greatest and best grounds for regulation that pays attention to the precautionary principle. In cases like this, omission can be disastrous, which recommends a regulatory model that adjusts to different scenarios and is minimally resilient to unexpected events.

This is precisely why it was included in Article 24 of the Draft Bill no. 2338/2023, which deals with algorithmic impact assessment, § 2, according to which "*[i]n attention to the precautionary principle, when using artificial intelligence systems that may generate irreversible impacts or those that are difficult to reverse, the algorithmic impact assessment will also take into account incipient, incomplete or speculative evidence.*"

5. Final considerations

In a recent article, Margrete Vestager,[24] when explaining the reasons for the European AI Act, states that the objective of the legislation was to find a balance between power, responsibility, between innovation and trust and between freedom and security based on a simple guideline, which focuses on use of AI: the riskier the use, the stricter the obligations of the agents involved.

This was exactly the reasoning behind the Draft Bill no. 2338/2023 which, based on the example of the European AI Act, which was used as a model, also sought to create a regime of regulation based on risks and rights, based on a well-defined risk classification – to guarantee legal certainty – but which can be updated by the competent authority – to ensure the necessary flexibility.

Despite the robustness of the text, we are not unaware of the numerous challenges that will arise in the implementation of the regulation, if it is approved by the Brazilian Parliament, even given the responsiveness expected from the adopted regulatory model and the necessary fine tuning between the competent authority and agents of AI.

However, given the risks and uncertainties related to the use of AI, it became clear, after all the debates held in the Committee of Jurists, that such challenges would need to be assumed, given the need and urgency to regulate AI.

[24] Margrete Verstager, "How to think about AI policy", *Project Syndicate*, March 11, 2024, https://www.project-syndicate.org/magazine/europe-ai-regulation-focuses-on-uses-not-technology-by-margrethe-vestager-2024-03.