Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

4 October 2022

CIPL's Top Ten Recommendations for Regulating AI in Brazil

I. Introduction

The benefits of artificial intelligence (AI) to address a wide range of societal challenges and improve our way of living are undeniable. By enabling a suite of emerging technologies (including machine learning, computer vision and natural language processing), AI empowers public and private sector organizations to deliver improved services across a multitude of industries, including healthcare, automotive, agriculture, military, financial services, law enforcement, education and marketing. 25% of large enterprises in Brazil are already using AI[1] and a 2021 study by Embrapii, a Brazilian industrial research and innovation group, found that 76% of companies believe the use of AI tools will have a major impact on their competitiveness.[2] According to a report by the Brazilian Association of Software Companies (ABES) and the International Data Corporation (IDC), spending on AI in Brazil is expected to increase by 28% in 2022 at $504 million.[3] Moreover, use of AI technology presents many opportunities for small and medium-sized enterprises.

While light-speed progress in AI technology has resulted in numerous benefits for society and propelled business growth, it has also created concerns regarding a variety of potential legal, ethical and societal risks and challenges. One of the potential challenges facing organizations is how to ensure the responsible and accountable use of AI technology and balancing this use with data protection concerns and the right to privacy of individuals. The Centre for Information Policy Leadership (CIPL)[4] has been working on the issue of accountable AI for many years and has engaged with law and policy makers as well as government departments and data protection authorities on the development of a sensible and future-proof framework for enabling accountable AI. CIPL commends the Federal Senate of Brazil for setting up a special committee of legal experts (the "Senate Committee") to consider an appropriate framework to regulate AI in Brazil. To assist the Senate Committee in this effort, CIPL puts forward this short paper outlining key recommendations for regulating AI in Brazil. These recommendations are based on CIPL's international experience in the field of AI policy and regulation[5] as well as its prior work on AI issues in Brazil.[6]

II. Key Recommendations

1. Flexible and adaptable AI regime

Brazil's AI regime should be designed in a way that enables it to evolve and be flexible to changes in the AI ecosystem. AI is constantly developing and a regime that is overly prescriptive or inflexible runs the risk of creating a framework that either will quickly become outdated or inhibit innovation. Brazil can create a technology-agnostic and future-proof regime by regulating only key AI issues and risks and enabling responsible AI through a suite of other tools, as described in these recommendations. Indeed, such an approach is consistent with Brazil's 2021 AI strategy which recommends avoiding regulatory actions that may unnecessarily limit AI innovation, adoption and development.[7]

2. Regime that builds on existing legal frameworks

In building an AI regime, Brazil should build on existing legal frameworks and avoid duplicating or creating any conflicting requirements with these frameworks. For example, certain aspects of AI are already regulated by Brazil's data protection law (Lei Geral de Proteção de Dados (LGPD))[8], the Civil Framework for the Internet,[9] the Consumer Protection Code[10] and the Access to Information Law.[11] Duplicative or conflicting requirements with these regimes could result in inconsistent protections for individuals and uncertainty with respect to their rights. It could also create regulatory uncertainty for both regulated entities and regulators as well as costly and unnecessary compliance obligations for organizations.

3. Principles and outcomes-based regulatory approach that enables organizational accountability

To ensure the long-term success of its AI regime, Brazil should adopt a principles and outcomes-based regulatory approach that enables organizational accountability. Principles-based rules prescribe the outcomes that organizations must achieve but leaves how to achieve such outcomes to organizations' discretion. Accountability requires organizations to operationalize and translate these principles-based rules through appropriate and demonstrable policies, procedures, controls and governance to deliver compliance. Accountability also enables the adaptation of principles-based rules to specific industries, technological applications and differing levels of risk.

Brazil's AI regime should explicitly include an accountability obligation to ensure that organizations that develop and deploy AI technologies do so in a responsible way. Implementing accountability is a more effective alternative to prescriptive and rigid legal requirements that apply across the board to all AI applications regardless of the risk involved. Accountability is already globally recognized as a key building block for effective regulation and ensuring corporate compliance. It has become a central focus of many regulatory regimes, including data protection and privacy, anti-corruption, anti-money laundering, white collar crime and corporate fraud, export controls and sanctions and healthcare. Equally, in the AI space, accountability obligations can enable responsible AI innovation, promote trust in the AI ecosystem and facilitate the responsible collection and use of data for AI training, development and deployment. In Brazil, accountability is a key principle of data protection under the LGPD[12] and the approach to accountability under this regime could serve as one source of inspiration as Brazil works towards a framework for responsible AI.

It is important to understand what the elements of accountability are as accountable AI programs should be based on these elements. There are different approaches to breaking down accountability into its constituent parts. One approach that is gaining traction among organizations and regulators is the use of an accountability framework, such as the framework created by CIPL (see below). The elements within the CIPL Accountability Framework are drawn from similar accountability elements of other regulatory areas (see above), which makes it law-agnostic and applicable to the AI context. Brazil's AI regime might establish the specific elements and expected outcomes of accountability or Brazil's National Data Protection Authority – Agência Nacional de Proteção de Dados (ANPD) – or other appropriate regulator could elaborate on the elements of accountability in regulatory guidance to give steer to organizations as they build accountable AI programs in Brazil.

Accountability Element	Description
Leadership and Oversight	**Establishing leadership and oversight for the responsible use of AI**, including governance, reporting, buy-in from all levels of management and appointing appropriate personnel to oversee the organization's AI accountability program and report to management and the board.
Risk Assessment	**Assessing and mitigating the risks** that AI applications may raise to individuals, including weighing the risk of the AI use against its benefits.
Policies and Procedures	**Establishing internal written AI policies and procedures** that operationalize legal requirements and create concrete processes and controls to be followed by the organization, reflecting the identified risks, applicable law, regulations, industry standards as well as the organization's values and goals.
Transparency	**Providing transparency to stakeholders internally and externally** about the organization's AI practices, the rights of individuals in relation to their data and the benefits and/or potential risks of AI applications. This may also include communicating with relevant regulatory authorities, business partners and third parties about the organization's AI practices. Importantly, providing effective transparency in the AI context depends on the nature of the audience involved, which will inform the level and type of information to be provided.[13]
Training and Awareness	**Providing training for employees** to ensure awareness of the organization's AI practices. This ensures AI accountability is embedded in the culture of the organization.
Monitoring and Verification	**Monitoring and verifying (including in the pre-deployment testing phase of particular AI applications) the implementation and effectiveness of the AI accountability program and internal compliance** with the organization's AI practices and controls through regular internal or external audits and redress plans.
Response and Enforcement	**Implementing response and enforcement procedures** to address inquiries, complaints and internal non-compliance, and to enforce against acts of non-compliance with the organization's AI accountability program.

Figure 1 – CIPL Accountability Framework – Universal Elements of Accountability

4. Risk-based approach that considers risks and benefits of AI applications holistically

The risk-based approach to regulating AI is central to a robust principles and outcomes-based AI regime. The focus of such an approach assesses the risk of the impact of AI technology in the context of specific uses and applications rather than the risk of the technology in the abstract. Understanding the potential impact and any risk of harms of a specific AI application on individuals enables organizations to make risk-based decisions and implement appropriate controls and mitigations to minimize the risks involved in an AI project. By focusing on impacts and risks, organizations can determine how to allocate resources and ensure appropriate attention is paid to AI applications that pose higher risks. For example, use of AI to recommend songs or movies most likely warrants less scrutiny than AI applications used in cars to avoid hitting pedestrians or other vehicles, or the use of facial recognition technology in commercial applications. Moreover, Brazil's AI regime could provide non-exhaustive criteria to assist organizations in determining whether their AI applications pose a high risk to individuals. An AI framework might delineate specific categories, types and examples of harm to individuals which should be considered as part of an AI impact assessment process. Furthermore, to encourage risk assessments and mitigation of risks in AI applications as part of accountability, Brazil could consider crafting a framework that mandates more stringent requirements for only those AI applications that are likely to cause harmful or negative impacts on individuals.

Any risk assessment requirement in Brazil's AI regime should explicitly include assessing the benefits of a proposed AI application or the risks of not proceeding with the development or deployment of the AI application (reticence risk). This is just as important as focusing on the harm that may result from proceeding with the AI application. It also helps to ensure that the use of an AI application is proportionate to the desired outcomes. For instance, there could be high risks related to a specific AI system that may be overridden by compelling benefits to individuals and society at large. For example, AI provides huge

benefits when used to monitor content on online platforms in order to fight disinformation, which could outweigh the risks associated with processing the relevant personal data.

After conducting a risk-assessment for specific AI applications, organizations may find that the residual risk level is still too high. In such cases, organizations should have the possibility to consult with the ANPD or other relevant sectoral regulator regarding the application, revise the scope of the AI project to reduce the risks or abandon the project and consider alternatives. Brazil's AI regime should leave such assessments and determinations to organizations as they will be best placed to holistically assess the risks involved. Of course, under the accountability principle, organizations must be able to demonstrate their risk assessments and decision-making process on request by an appropriate regulator for enforcement purposes. Moreover, this flexible approach will ensure that Brazil's AI regime can apply universally to all AI applications.

There has been a trend in some regions, particularly in the EU, to ban specific applications of AI. For example, the use of facial recognition for law enforcement and surveillance or use of AI to infer emotions of a natural person. While there are legitimate concerns associated with the use of such AI applications, such concerns should be addressed through the use of risk assessments and on a case-by-case basis. There are circumstances where an outright ban on using AI to infer emotions would, for example, prevent the use of AI to detect whether an individual is suicidal and to enable an appropriate response and intervention to prevent the individual from harming themselves or others. The benefits of this use of AI might outweigh the risks and should potentially be permitted, albeit under strict conditions and safeguards. At the same time, use of AI to infer emotions of individuals to manipulate them or coerce specific behaviors that they might not otherwise engage in could be completely inappropriate and carry very high risks and should not be enabled. Each of these applications should be required to undergo a risk assessment and depending on the results a determination can be made as to whether to proceed with the proposed AI application. As such, with the exception of categorically harmful and nefarious AI applications that potentially warrant prohibition, Brazil should generally avoid banning any specific application of AI under its AI regime. Of course, there may always be some bad actors that proceed with negative uses of AI but an outright legislative ban will not stop these bad actors. However, it would certainly prevent potentially beneficial uses of AI.

5. Regime that incentivizes development and implementation of accountable AI practices, including technological solutions and Privacy Enhancing Technologies

As mentioned above, accountability enables the requisite flexibility for organizations to achieve compliance through risk-based, verifiable and enforceable controls and practices. AI accountability can be achieved through a variety of mechanisms, which is particularly important as many different organizations are innovating in the AI field from large multi-national companies to SMEs and start-ups to public research and academic institutions, government entities and other public sector bodies. Such mechanisms include, custom-made internal policies, programs and controls tailored to company size, structure and data processing activities. They could also include formal accountability and assurance schemes such as enforceable codes of conduct, certifications and standards (see below for more information on such formal accountability schemes). Finally, leading companies developing AI technologies are also increasingly investing in privacy enhancing technologies (PETs), including federated learning, differential privacy, use of synthetic or encrypted data for algorithmic training, etc.

Any regime regulating AI in Brazil should incentivize the development and implementation of accountable AI practices and technological solutions to address privacy and other concerns in the development and deployment of AI systems. Organizations should be encouraged to adopt such practices to enable their AI innovations in a responsible way while also ensuring compliance with any AI regime and appropriate protections for individuals. Over the last few years, CIPL has collected examples of such accountable AI practices in line with the elements of CIPL's Accountability Framework. CIPL provides a table of these practices at the end of this paper (see Appendix 1). CIPL does not recommend mandating any of these particular practices in an AI law directly as organizations will need to make risk-based determinations as to which accountability measures are appropriate in a given AI context. Of course, the ANPD or other appropriate regulator might illustrate in regulatory guidance examples of these best practices, including additional practices that develop over time in Brazil and globally, to assist organizations in making appropriate choices. Finally, CIPL will be embarking on a project to map out and analyze the most prevalent and promising PETs and will engage in global discussions with regulators and industry to ensure broader adoption and understanding of the potential of such technologies.

6. Regulatory co-operation and consistent interpretation of AI rules

Globally, many discussions are taking place concerning which regulatory body or bodies should be responsible for AI. In Brazil, the ANPD will have a big role to play as many AI applications involve the use of personal data. In addition, AI use is prevalent in many industry sectors, such as healthcare and financial services, and sectoral regulators will also have an interest in overseeing AI regulation in Brazil. Some nations have considered the establishment of a dedicated AI regulatory body. CIPL is of the view that oversight and enforcement of AI in Brazil should be performed by existing regulators, including the ANPD, and such regulators should work together through a regulatory hub or other cooperation forum (similar to the UK Digital Regulation Cooperation Forum[14]) to ensure consistent interpretation of AI rules, oversight and enforcement. Leveraging the AI expertise and competencies of existing regulators and avoiding a fragmented regulatory approach through regulatory coordination is critical to the success of any AI regime in Brazil.

7. Co-regulatory mechanisms enabling responsible AI innovation

Regulators are charged with carrying out a multitude of tasks under conditions of limited resources. Co-regulatory mechanisms such as AI assurance frameworks, certifications, codes of conduct and standards could help relieve some of the pressure regulators might face in carrying out their existing tasks on top of a new AI regime in Brazil. Such co-regulatory mechanisms are starting to proliferate in global AI markets. These include the UK Centre for Data Ethics and Innovation (CDEI) AI Assurance Framework,[15] the New South Wales AI Assurance Framework,[16] the U.S. Department of Commerce NIST AI Risk Management Framework, [17] the UK National Health Service (NHS) code of conduct for artificial intelligence systems [18] and ISO and IEEE standards for artificial intelligence.[19]

Certification schemes and codes of conduct involve the use of third-party certifiers or monitoring bodies, as well as dispute resolution providers that are associated with such schemes. These entities can play important front-line enforcement and oversight roles and remediate many issues before a regulator needs to step in. These entities review organizations compliance and accountability programs and ensure that they comply with the relevant standard to which they were certified. When necessary, they can suspend certifications and take other remedial actions against non-compliant organizations. The dispute resolution

functions of these schemes relieve regulators from the burden of dealing with large numbers of "easy" cases, allowing them to focus their enforcement attention on more important and strategic matters.

AI standards can help to establish baseline requirements for certain uses of AI that can be modified and improved over time as the AI ecosystem advances. Standards are often developed in multi-stakeholder processes and can be better designed through the involvement of a wide range of stakeholders rather than leaving their development to law and policymakers alone. Like certifications, standards bodies can help to ensure appropriate adherence to adopted standards which can result in a push towards uniformity across numerous aspects of the AI ecosystem. Moreover, co-regulatory mechanisms can help increase trust by demonstrating that an AI application meets certain criteria that have been set by a cross-sector of relevant industry experts and/or assessed by an independent body.

8. Modern approach to regulatory oversight

Regulators will have an important role to play in ensuring proper application of principle-based rules and co-regulatory frameworks. They also need to stay on top of AI technology developments and its latest applications. This requires a new approach to regulatory oversight that differs from traditional regulatory approaches and behaviors.

In order to enable responsible AI innovation and experimentation, Brazil's AI regime should encourage new and agile approaches to regulatory oversight. Regulators need to be ready and equipped with appropriate resources and skills to engage constructively on the topic of AI with industry and government bodies developing and using the technology.

In addition, they will need modern and agile regulatory oversight tools such as regulatory sandboxes, policy prototyping projects and data review boards, all of which play an important role in the AI regulatory toolbox.

(a) AI *regulatory sandboxes* provide supervised "safe spaces" for organizations to test innovative AI products, services, projects, or business models in the real world with real consumers. They can be used to help address and resolve some of the more challenging aspects of deploying AI applications against the backdrop of the prevailing legal requirements, particularly those that appear inconsistent or in tension with new technologies and business practices. Regulatory sandboxes ultimately provide an opportunity for accountable organizations and innovative regulators to work and learn together in a collaborative environment to enable the benefits of AI while ensuring the protection of individuals. Brazil has already adopted sandboxes in the insurance,[20] banking[21] and fintech[22] sectors. Brazil's AI regime should encourage the ANPD or other appropriate regulators to create a regulatory sandbox for the purpose of encouraging innovation in AI and machine learning. Such an approach was proposed by India in its draft Data Protection Act.[23] We have also seen efforts by data protection authorities to launch AI sandboxes. For example, in 2021, the Norwegian Data Protection Authority (Datatilsynet) launched a special regulatory sandbox for AI applications.[24] In addition, the Colombian government has developed a regulatory sandbox to promote Privacy by Design and Default in AI projects.[25] Finally, in Singapore, the Infocomm Media Development Authority (IMDA) and the Personal Data Protection Commission (PDPC) launched a sandbox for PETs to support businesses to pilot PET projects that address common business challenges.[26]

(b) *Policy prototyping programs* are collaborative pilot projects that mobilize a coalition of public and private actors. These programs are also regulatory innovation labs intended to enable the development and testing of a policy idea in the field of new and emerging technologies, including AI. Unlike regulatory sandboxes that are designed to test innovations against existing regulatory requirements, policy prototyping programs enable the testing of policies that have yet to be enacted. The policy idea to be tested can be inspired by a law that is being discussed, a self-regulatory instrument, a code of conduct, a set of industry guidelines, etc. Policy prototyping programs are also empirical programs that provide evidence-based policy input to policymakers either to improve existing governance frameworks or to inform new ones. One example of a successful policy prototyping project in the AI space is the Open Loop Project.[27] Open Loop projects have been deployed in Europe in the context of AI risk assessments and the envisioned policy approach of the proposed EU AI Act and in Singapore and Mexico on transparency and explainability.

The policy prototyping process typically involves selecting a group of participants (e.g. start-up AI companies) and asking them to apply policy prototypes (co-created normative frameworks on certain AI topics, like explainability or fairness, or risk assessment) to specific AI applications they have built and are deploying. Based on this application, the organization conducting the policy prototyping process can collect information about the participants' experience and test and evaluate the prototypes under real world conditions. These frameworks can be improved based on the lessons learned and ultimately inform the AI regulatory debate by delivering evidence based policy recommendations. The Brazilian government might consider engaging in policy prototyping projects to test any proposed AI rules in the market before adopting them in an AI regime for Brazil.

(c) *Data review boards* (DRBs) are helpful for both public and private sector organizations. In the AI context, they can be used to consider the impacts of a particular use of data in an AI application prior to its development, deployment or use. DRBs are standing committees (whose characteristics may be defined by regulators) convened according to certain risk indicators. They are intended to promote a thoughtful dialogue between an organization and key stakeholders that make up the data review board and consideration of risks and benefits in relation to high-risk AI projects. Data review boards may include data protection experts, lawyers, engineers, consumer advocates, academics and other stakeholders. Organizations can structure their DRBs in different ways depending on the goals for the DRB itself. For instance, internal DRBs can assist organizations in making decisions to minimize the risks involved in particular AI projects. DRBs that draw on the expertise of external stakeholders can be useful to build confidence and trust that the AI project underwent a thorough review process before deployment.[28] Brazil should consider encouraging the development and use of such boards in any AI regime it develops.

9. Liability

Liability for damages caused by AI systems and applications is a complex topic and one that is currently being debated in Brazil. There are a number of different actors involved in the development and deployment of AI, including developers, suppliers and users. It is important to remember that most AI systems are not developed as a standalone product or service that is released into the marketplace by a single entity. Many AI applications are the result of numerous entities building upon each other's efforts. For instance, an AI application that emerges from the open source community could have been the result of the efforts of hundreds or thousands of contributors.

How liability is apportioned for damages caused by AI systems and applications is a still a nascent area of law. Previous attempts in the proposed EU AI regime to apportion greater liability to AI developers than users have been met with much criticism and have now been de-emphasized. Developers have an important role to play in ensuring AI systems and algorithms function properly. However, it also falls upon users to ensure proper use of the system for lawful and appropriate purposes and in a way that does not create risks and harms to people and society. Liability is, therefore, distinct and shared and both parties need to ensure their respective compliance with any laws in the development and use of AI systems. At the same time, applying strict liability to every participant in the AI value chain would frustrate Brazil's aims of supporting a healthy ecosystem of innovators, experimenters, contributors, and entrepreneurs. Such a regime would apportion liability in an indiscriminate manner, without taking into account the level of contribution and the actual damage caused by each actor or their ability to control and internalize the risks involved in a given AI application. Moreover, in many cases, users of AI systems determine how that system is ultimately going to be deployed in a specific AI context and it will be up to the user to ensure that it undertakes a context specific risk assessment and mitigation exercise to minimize any AI system and application failures. In other words, specific risks cannot in all cases be mitigated by the decisions of developers of an AI system and, as such, they should not be held responsible in all cases.

Given that liability for damages caused by AI is untested territory and that there is not enough industry and regulatory experience in this area to date, CIPL recommends that Brazil take caution in formulating any rules on liability, including how such liability is apportioned, for damages caused by AI systems and applications at this premature stage. Moreover, there should be a concerted effort to monitor market developments and for regulators to work with legal experts, practitioners and representatives of AI developers, suppliers and users to engage in thoughtful discussions on this topic as AI use continues to proliferate in Brazil.

10. Multi-stakeholder process to crafting AI regime

In crafting an AI regime, Brazil should engage in a multi-stakeholder process and consult a wide variety of stakeholders on any proposed framework for regulating AI. Such a process has proven successful in the development of other legal frameworks in Brazil, including the Civil Framework for the Internet and the LGPD. A multistakeholder process should include consultation with ethicists, lawyers and legal scholars, data scientists, engineers, privacy and security experts, computer scientists, epistemologists, statisticians, AI researchers, academics, civil society, business leaders and public representatives. The Senate Committee should ensure that it engages and interacts with all stakeholders in thinking through key issues. Indeed, CIPL commends the Senate Committee for holding a range of domestic hearings and an international seminar between April and June 2022. CIPL encourages the Senate Committee to continue to have similar discussions throughout the remainder of 2022 and in 2023 as it progresses its agenda.

III. Conclusion

CIPL is grateful for the opportunity to provide input to the Senate Committee as it considers the development of an appropriate framework to regulate AI in Brazil. By considering and adopting CIPL's recommendations presented in this paper, Brazil will ensure that it creates a layered framework for AI that (1) enables an agile, technology-agnostic and future-proof regime that builds on existing legal standards and frameworks; (2) is risk-based and grounded on the holistic impact assessment of AI applications; (3) fosters innovation through organizational accountability; and (4) enables consistent and modern approaches to regulatory oversight.

If you would like to discuss this paper or require more information, please contact Bojana Bellamy, bbellamy@HuntonAK.com or Sam Grogan, sgrogan@HuntonAK.com.

Appendix 1 - Examples of Accountable AI Best Practices

The following table outlines examples of accountable AI activities undertaken by select organizations of different sectors, geographies and sizes based on the CIPL Accountability Framework and against each accountability element. The practices are not intended to be mandatory industry standards, but serve as specific examples that are calibrated based on risks, industry context, business model, size and level of maturity of organizations.

Accountability Element	Related Practices
Leadership and Oversight	• Public commitment and tone from the top to respect ethic, values, specific principles in AI development • Institutionalized AI processes and decision-making • Internal Code of Ethics rules • AI/Ethics/Oversight Boards, Councils, Committees (internal and external) to review risky AI use cases and to continuously improve AI practices • Appointing member of the Board of Directors for AI oversight • Appointing Responsible AI Lead/Officer • Privacy/ AI engineers and champions • Set up an internal interdisciplinary board/senior working group (e.g. Lawyer, Technical teams, Research, Business units, internal audit, procurement, public affairs, thought leadership) • Appointment of privacy stewards to coordinate others • Ensuring inclusion and diversity in AI model development and AI product teams
Risk Assessment	• Understand AI purpose and use case in business/ processes—for decision making, or input into decision, or other • Understand impact (benefits and risks) on individuals and society • Algorithmic Impact Assessment / Algorithmic bias—tools to identify, monitor and continuous test, including sensitive data in data sets to avoid human bias • Fairness assessment tools to ensure biases are tested for, identified and any anomalies are mitigated to avoid concept drift in algorithms • Ethics Impact Assessment • Broader Human Rights impact assessment • DPIA for high risk processing • Assessment needs to include the benefits vs. risks of the AI autonomy, and challenge if such autonomy is necessary • Consider anonymization techniques • Document trade-offs (e.g. accuracy—data minimization, security—transparency, impact on few—benefit to society) for high-risk processing as part of the DPIA • Data quality assessment via KPIs • Framework for data preparation and model assessment – assessed and used by data scientists – including feature engineering, cross validation, back-testing, validated KPIs by business, etc.

	• Establishing controls and implementing safeguards to mitigate risks and trade-offs; • Working agile in close collaboration between business and data experts to assess regularly the needs and results accuracy – squad also includes data analysts, data engineers, IT and software engineers to ensure that the model can be properly used • Developing standardized risk assessment methodologies, which take into account the likelihood and severity of risk factors on individuals and/or society, level of human oversight involved in individually automated decisions with legal effects as well as their explainability (according to the contextual factors of the AI decision) and auditability, etc.
Policies and Procedures	• High level principles for AI—how to design, use, sell • Adopting specific AI policies and procedures on how to design, use or sell AI; • Assessment questions and procedures • Accountability measures for 2 stages – training and decision taking • White, black and gray lists of AI use • Evaluate the data against the purpose—quality, provenance, personal or not, synthetic, in-house or external sources • Purpose and other contextual factors of AI determines how much human intervention is required • Level of verification of data input and output; • Check no bias or unfair discrimination in the operation or outcome throughout the entirety of AI lifecycles • Pilot testing AI models before release • Use of protected data (e.g. encrypted, pseudonymised or where useful synthetic data) in some AI/ML models • Use of high quality but smaller data sets • Where applicable federated AI learning models (data doesn't leave device), considering trade-off with data security and user responsibilities • Special considerations for organizations creating and selling AI models, software, applications • Due diligence checklists for business partners using AI tech and tools • Using external tools, guidelines, self-assessment checklists • Processes and procedures to receive and address feedback and complaints • Define escalation steps with regards to reporting, governance, risk analysis and handling, etc. • Reliability – process for the testing and verification of the reliability of the AI system documented and operationalized. • Exploring ways to anonymise, de-identify or tokenise data, or to use synthetic data to train AI models; • Baseline model (if possible explainable) to assess uplift of advanced ones (advanced models should be used only if needed, model decision/KPI should consider the model complexity to be avoided – under the Occam's Razor principle)

	• Ideation phase between all stakeholders (data scientists, business, final user, control functions etc.) where needs, outcomes, validations rules, maintenance, need for explainability, budget, etc. are discussed • Documenting the use of AI technologies, the categories of data used in connection with the technologies, the decision-making process, and the identified risks and mitigations • Application of privacy and security by-design in AI life cycle
Transparency	• Different needs for transparency to individuals, regulators, business /data partners and internally to engineers and, leadership at the different stages of AI lifecycle • Adequate disclosures communicated in simple, easy to understand manner • AI must be inclusive and thus also accessible and usable by those in special needs/disabilities • Explainability is part of transparency and fairness • Transparency trail: explainability of decision and broad workings of algorithm; more about the process than the technology; what factors and what testing to be fair; accountability for impact of decisions on a person's life; what extent of human oversight • Explain that it is an AI/ML decision, if possibility for confusion (Turing test) • Provide counterfactual information • Differentiated and flexible transparency—linked to context, audience/users, purpose of explainability and risk, severity of harm—prescriptive lists of transparency elements is not helpful • Understand customers' expectations and deploy based on their readiness to embrace AI—tiered transparency • From black box to glass box—looking at the data as well as algorithm /model; aspiration of explainability helps understand the black box and builds trust • Define criteria of deployment of AI technologies within the organization (e.g. usage scenarios) and communicate them to the user • Traceability trail to make the AI system auditable, particularly in critical situations • Model cards (short documents accompanying AI models to describe context in which model should be used, what is the evaluation procedure) • Data hub for transparency on data governance, data accessibility, data lineage, data modification, data quality, definition, etc. • Use of LIME, SHAP, etc. for interpretation
Training and Awareness	• Data scientist training, including how to avoid and address bias • Cross functional training – privacy professionals and engineers • Ad hoc and functional training • Fairness training to technology teams • Ethics training to technology teams • Uses cases where problematic AI deployment has been halted • Role of "Translators" in organizations, explaining impact and workings of AI
	• Capability for human in the loop—in design, in oversight, in redress • Capability for human understanding of the business and processes using AI • Capability for human development of software and processes

Monitoring and Verification	• Capability for human audit of input and output • Capability for human review of individual decisions with legal effects • Ongoing monitoring, validation and checks • Oversight committees even in design stage • Redress to a human, not to a bot • Monitoring the eco-system from data flow in, data process and data out • Reliance on different audit techniques • Counterfactual testing techniques • Version control and model drift, tracking of black box, algorithms by engineers • RACI models for human and AI interaction • Pre-definition of AI audit controls • Internal audit team specialized on AI and other emerging technologies • Processes must allow human control or intervention in the AI system where both technically possible and reasonably necessary • See the *Assertion-based Framework for the Audit of Algorithms*, Otto Koppius and Iuliana Sandu • Model monitoring (including back-testing and feedback loop) and maintenance process
Response and Enforcement	• Complaints-handling • Redress mechanisms and appropriate personnel for individuals to remedy AI decision • Feedback channel • Internal supervision of AI deployment

References

[1] Brazilian Software Market Scenario and Trends 2021, Brazilian Association of Software Companies (ABES), available at https://abessoftware.com.br/wp-content/uploads/2021/08/ABES-EstudoMercadoBrasileirodeSoftware2021v02.pdf at page 29.
[2] Brazil excels in the use of artificial intelligence, Chamber of Commerce Brazil-Canada, 26 April 2022, available at https://ccbc.org.br/en/publicacoes/news-ccbc/brazil-excels-in-the-use-of-artificial-intelligence/#:~:text=A%20survey%20conducted%20last%20year,major%20impact%20on%20their%20competitiveness.
[3] AEBS presents trends for the Brazilian software market in 2022, available at https://abessoftware.com.br/en/abes-apresenta-tendencias-para-o-mercado-brasileiro-de-software-em-2022/.
[4] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this paper should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.
[5] For information about CIPL's Project on Delivering Sustainable AI Accountability in practice, see https://www.informationpolicycentre.com/ai-project.html.
[6] See, for example, CIPL response to the Brazilian MCTIC's Consultation on a National AI Strategy for Brazil, January 2020, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/_english__cipl_response_to_mctic_consultation_on_ai_strategy__24_january_2020_.pdf (English) and https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/_portuguese__cipl_response_to_mctic_consultation_ai_strategy__24_january_2020_.pdf (Portuguese); Best Practices in the Use of AI in Brazil, CIPL contribution in Inteligência Artificial - Sociedade, Economia E Estado, available at https://www.livrariart.com.br/inteligencia-artificial-9786556149226/p.
[7] Brazil Ministry of Science, Technology and Innovation, Summary of the Brazilian Artificial Intelligence Strategy (EBIA), 2021, available at https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-summary_brazilian_4-979_2021.pdf.
[8] LGPD, Law No. 13,709 of August 14, 2018, available at http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.
[9] Civil Rights Framework for the Internet in Brazil, Law No. 12,965 of April 23, 2014, available at http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.
[10] Brazil Consumer Protection Code, Law No. 8078 of September 11, 1990, available at http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.
[11] Brazil Access to Information Law, Law No. 12,527 of November 18, 2011, available at http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2011/Lei/L12527.htm.
[12] Article 6(X), LGPD.
[13] To provide effective transparency in the AI context, organizations will need to consider the specific audience involved. For instance, information about the inner workings of algorithms may be inappropriate and not useful to individuals who challenge the results of an automated decision. In contrast, in the context of a regulatory investigation, it may be necessary to provide more detailed information about how an AI system works to a regulator. In addition, organizations will need to balance the provision of transparent information with the need to ensure that intellectual property and proprietary information remain appropriately protected. As such, it can be helpful to consider the different goals of transparency in the AI context (i.e. provision of information to specific audiences to achieve understandability, traceability, explainability, articulation of benefits or individual rights and

avenues for redress). By considering these factors and goals, organizations can make contextual decisions to ensure that the right level of information is provide to the specific audience involved.

[14] UK Digital Regulation Cooperation Forum, available at https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum.

[15] "The roadmap to an effective AI assurance ecosystem", Centre for Data Ethics and Innovation (CDEI), December 2021, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1039146/The_roadmap_to_an_effective_AI_assurance_ecosystem.pdf.

[16] New South Wales AI Assurance Framework, available at https://www.digital.nsw.gov.au/policy/artificial-intelligence/nsw-ai-assurance-framework.

[17] National Institute of Standards and Technology, U.S. Department of Commerce, AI Risk Management Framework, available at https://www.nist.gov/itl/ai-risk-management-framework.

[18] Code of conduct for artificial intelligence systems used by the NHS, available at https://www.gov.uk/government/news/new-code-of-conduct-for-artificial-intelligence-ai-systems-used-by-the-nhs.

[19] See, for example, ISO/IEC TR 24028:2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence, available at https://www.iso.org/standard/77608.html; IEEE P7007 Ontological Standard for Ethically Driven Robotics and Automation Systems, available at https://site.ieee.org/sagroups-7007/; IEEE Standard Model Process for Addressing Ethical Concerns during System Design, available at https://standards.ieee.org/ieee/7000/6781/.

[20] In 2020, the Superintendence of Private Insurance (SUSEP) launched a regulatory sandbox program for the Brazilian insurance sector. See "SUSEP Implements a Regulatory Sandbox Model in Brazil", July 2020, available at https://a2ii.org/en/news/a2ii-newsflash-susep-implements-a-regulatory-sandbox-model-in-brazil.

[21] In 2021 the Central Bank of Brazil set up a regulatory "sandbox" program seeking to stimulate innovation in the finance and payments market. See Sciaudone, C., "Brazilian innovators get to play in regulatory 'sandbox'", 15 March 2022, available at https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/brazilian-innovators-get-to-play-in-regulatory-sandbox-69251435.

[22] In 2020, the Securities and Exchange Commission of Brazil (CVM) launched a regualtory sandbox program to enable organizations to test innovative projects in the financial space. See "Brazilian Securities and Exchange Commission begins admission process of regulatory sandbox participants", Latin America Business Stories, November 2020, available at https://labsnews.com/en/news/economy/brazilian-securities-and-exchange-comission-begins-admission-process-of-regulatory-sandbox-participants/.

[23] See Draft Report of the Joint Committee on the Personal Data Protection Bill, 2019, published November 2021, available at https://acrobat.adobe.com/link/review?uri=urn%3Aaaid%3Ascds%3AUS%3Af030ad33-879d-4127-870a-9f055fbe2644#pageNum=1 at Section 40.

[24] Datatilsynet AI Regulatory Sandbox, available at https://www.datatilsynet.no/en/news/2021/sandbox-open-for-new-applicants/.

[25] Sandbox on privacy by design and by default in Artificial Intelligence projects, Columbian Superintendence of Industry and Commerce, available at https://globalprivacyassembly.org/wp-content/uploads/2021/07/B6.-SIC-Colombia-Sandbox-on-privacy-by-design-and-by-default-in-AI-projects.pdf.

[26] Singapore IMDA and PDPC Privacy Enhancing Technologies Sandbox, available at https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2022/IMDA-and-PDPC-launch-Singapore-first-Privacy-Enhancing-Technologies-Sandbox-as-they-mark-decade-long-effort-of-strengthening-public-trust.

[27] See "Introducing Open Loop, a global program bridging tech and policy innovation", available at https://ai.facebook.com/blog/introducing-open-loop-a-global-program-bridging-tech-and-policy-innovation/; and AI Impact Assessment: A Policy Prototyping Experiment, available at https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3772500_code715910.pdf?abstractid=3772500&mirid=1.

[28] For more information about Data Review Boards, please see Cate, F., Dockery, R., and Crosley, S., "Why data review boards are a promising tool for improving institutional decision-making", IAPP Privacy Perspectives, 28 February 2020, available at https://iapp.org/news/a/why-data-review-boards-are-a-promising-tool-for-improving-institutional-decision-making/.