Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

24 January 2020

CENTRE FOR INFORMATION POLICY LEADERSHIP RESPONSE
PUBLIC CONSULTATION ON A BRAZILIAN ARTIFICIAL INTELLIGENCE STRATEGY

The Centre for Information Policy Leadership (CIPL)[1] welcomes this opportunity to respond to the Department of Telecommunications of the Ministry of Science, Technology, Innovations and Communications (MCTIC) on its public consultation on a National Artificial Intelligence Strategy for Brazil. CIPL welcomes MCTIC's initiative to create such a strategy, especially in the context of Brazil's upcoming new data protection regime under the Lei Geral de Proteção de Dados Pessoais (LGPD).[2]

CIPL commends MCTIC for thinking deeply about the many aspects integral to a national AI strategy, as evidenced by the breadth of issues and international literature mentioned in the consultation document. Given CIPL's expertise in the data protection sphere, this response will comment on the priorities and objectives portion of the consultation generally and following this will focus specifically on the following thematic axes out of the eight being consulted upon:

- Legislation, Regulation, and Ethical Use
- AI Governance
- International Aspects

I. Priorities and Objectives

a. What substantial problems must be addressed with priority by an AI strategy?

Throughout the late 2010's, many countries started creating and developing national AI strategies. According to the Organization for Economic Cooperation and Development's Observatory of Public Sector Information, at least 50 countries have developed, or are in the process of developing, a national AI strategy.[3] As MCTIC correctly notes in the consultation, the objective of a national AI strategy is to enhance the development and use of AI technology and to address certain challenges posed by AI, including issues around transparency, responsible disclosure when using AI systems and ensuring that AI systems respect the Rule of Law, human rights, democratic values and diversity. CIPL welcomes MCTIC's recognition of the dual objective of an effective AI strategy to not only address the risks and challenges presented by AI technologies but also to enable innovation and beneficial use of data through AI technology.

[1] CIPL is a global data privacy and cybersecurity 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 submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] Lei Geral de Proteção de Dados Pessoais (LGPD), available at http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

[3] AI Strategies & Public Sector Components, Observatory of Public Sector Information, Organization for Economic Cooperation and Development, November 2019, available at https://oecd-opsi.org/projects/ai/strategies/.

Consideration of issues surrounding the protection of personal data as it relates to AI technology is key to the creation of an AI strategy that facilitates the responsible use of AI while also ensuring compliance with data protection law and policy. As a result, CIPL believes that in order for Brazil to create a robust national AI strategy, it must consider and address privacy and data protection issues in the AI context as a matter of priority.

CIPL has written extensively about key data privacy issues as they relate to AI through its project on "Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice".[4] The first report in this project, entitled "Artificial Intelligence and Data Protection in Tension"[5] details the widespread use, capabilities and remarkable potential of AI applications and examines some of the tensions that exist between AI technologies and traditional data protection principles. The second report in this project, entitled "Hard Issues and Practical Solutions"[6] provides concrete approaches to mitigating some of the key challenges outlined in the first report and details examples of best practices and tools that can be deployed today to foster a better future in which human-centric AI, privacy and the protection of personal data prosper. We recommend that MCTIC review these papers as it formulates its national AI strategy and, in particular, its stance as AI relates to data protection.

II. Legislation, Regulation, and Ethical Use

MCTIC correctly notes that there has been much discussion around the technological development of AI and also much exchange around the need to develop legal, regulatory and ethical parameters to guide the development of AI technology in a way that balances the protection of rights, including those surrounding privacy and data protection, with the ability of organizations to innovate and develop AI applications, including those which are not yet fully understood.

The consultation mentions a plethora of guidelines and resource documents that have been produced to dive deeper into the legal, regulatory and ethical aspects of AI, including significant initiatives at the EU level such as the International Conference of Data Protection and Privacy Commissioner's 2018 Declaration on Ethics and Data Protection in Artificial Intelligence[7] and the Ethics Guidelines for Trustworthy AI produced by the European Commission High-Level Expert Group on Artificial Intelligence.[8] CIPL responded to public consultations on both of these documents in 2019.[9] CIPL has also discussed many

[4] See CIPL Project on Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice, available at https://www.informationpolicycentre.com/ai-project.html.

[5] First AI Report: Artificial Intelligence and Data Protection in Tension, 10 October 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_te....pdf.

[6] Second AI Report: Hard Issues and Practical Solutions, 17 January 2018 (pre-published advanced copy), available at https://www.informationpolicycentre.com/cipl-second-ai-report-01172020.html.

[7] ICDPPC Declaration on Ethics and Data Protection in Artificial Intelligence, 23 October 2018, available at https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf.

[8] Ethics Guidelines for Trustworthy AI, European High-Level Expert Group on Artificial Intelligence, 8 April 2019, available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419.

[9] See Comments by the Centre for Information Policy Leadership on the International Conference of Data Protection and Privacy Commissioners Declaration on Ethics and Data Protection in Artificial Intelligence, 25 January 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_icdppc_declaration_on_ethics_and_data_protection_in_artificial_intelligence.pdf; and CIPL Comments on the EU Commission's High-Level

of the issues outlined in these guidance documents in greater detail by hosting roundtables around the world with regulators, policy makers, industry leaders and academics[10] and believes that many of the findings from these meetings are of direct relevance to MCTIC's points for discussion under this thematic axis.

a. How is it possible to address questions related to discrimination and bias in decisions made by autonomous systems?

While algorithmic bias and discrimination are key concerns surrounding automated decision-making, it is important to recall that humans themselves are rarely consistently rational, unbiased or even capable of explaining why they reach certain decisions. In the long run, AI has the potential to help identify, correct and avoid many of the irrational biases that affect human decision-making and any national AI strategy should recognize this and aspire for AI to do so. In the immediate term, however, there is much concern over placing the outcome of certain decisions solely in the hands of an automated system which may produce a discriminatory result, for instance due to bias in the underlying data.

There are many measures that can be taken today to address questions related to such algorithmic bias and discrimination:

- **Facilitate access to data, including sensitive data**: AI technologists have confirmed that in order to avoid bias, algorithms must be tested by reference to sensitive categories of data, such as gender, race and health. Denying access to or preventing the retention or use of such sensitive data makes it more difficult to detect and remedy bias and may further limit the ability to explain why the AI application is arriving at discriminatory conclusions. It is important to note, however, that where sensitive data is processed to prevent bias from occurring, appropriate protections, including masking, anonymization and pseudonymisation, and accountability safeguards will be of increased importance.

- **Develop techniques to identify and address the risk of algorithmic bias**: Many organizations today are developing techniques to specifically address the issue of discrimination in AI applications. For example, some organizations rely on counterfactual fairness testing. This technique checks for fairness in outcomes by determining whether the same result is achieved when a specific variable, such as race or gender, changes.[11] A 2019 report on "Perspectives on

Expert Group on AI's Draft Ethics Guidelines for Trustworthy AI, available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=57590 at pages 351-358.

[10] The events included CIPL/Singapore Personal Data Protection Commission (PDPC) Joint Interactive Working Session on "Accountable and Responsible AI" (16 November 2018, Singapore); Roundtable with European Regulators and Industry Participants on "Hard Issues in AI" (12 March 2019, London); Roundtable with the EU Commission High Level Expert Group on "Ethics Guidelines for Trustworthy AI" (27 June 2019, Brussels); Roundtable with Asian Regulators and Industry Participants on "Personal Data Protection Challenges and Solutions in AI" (18 July 2019, Singapore); Roundtable with the UK Information Commissioner's Office (ICO) on "AI Auditing Framework" (12 September 2019, London); CIPL/TTC Labs Design Jam on "AI Explainability" (3 December 2019, Cebu); and CIPL Industry Workshop on a European AI Regulatory Approach (14 January 2020, Brussels).

[11] See Model Artificial Intelligence Governance Framework, First Edition, Singapore Personal Data Protection Commission, January 2019, available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/Model-AI-Framework---First-Edition.pdf?la=en at page 15. "A decision is fair towards an individual

Issues in AI Governance" released by Google details other algorithmic fairness techniques designed to "surface bias, analyze data sets, and test and understand complex models in order to help make AI systems more fair". These include Facets, the What-If Tool, Model and Data Cards and training with algorithmic fairness constraints.[12] Accenture has developed its own fairness tool to "identify and remove any coordinated influence that may lead to an unfair outcome"[13] which it uses both internally with respect to its own AI projects, as well as externally, on client projects involving the deployment of AI applications to help clients address the fairness standard. IBM has also created several tools to address issues of ethics and fairness in AI, including AI Fairness 360, "a comprehensive open-source toolkit of metrics to check for unwanted bias in datasets and machine learning models, and state-of-the-art algorithms to mitigate such bias,"[14] as well as IBM Watson OpenScale, a tool for tracking and measuring outcomes of AI to help intelligently detect and correct bias as well as explain AI decisions.[15]

- **Data scientist training**: Organizations developing AI applications and tools have invested heavily in training their data scientists that are engineering these systems. Part of this training includes raising awareness about different sources and types of bias, instruction on how to avoid and address bias when creating algorithms and how to detect and test algorithms for bias prior to deployment.

- **Ethics review processes**: Many organizations already have or are considering data review boards or similar internal or external ethics or AI committees as a way to drive organizational accountability, foster responsible decision-making and ensure that new data uses uphold corporate and societal values. With respect to bias, one company through using such a process, decided not to deploy facial recognition in police vest cameras due to the discovery of ethical concerns around bias and inaccuracy that could not be satisfactorily mitigated.[16]

CIPL recommends that MCTIC acknowledge the potential problem of algorithmic bias and discrimination in the national AI strategy and further highlight that solutions to address this problem are currently being developed by industry, with a call for organizations to continue working on such solutions and sharing relevant knowledge with the AI community.

if it is the same in the actual world and a counterfactual world where the individual belonged to a different demographic group".

[12] To read more about these techniques, please see Perspectives on Issues in Ai Governance, Google, 2019, available at https://ai.google/static/documents/perspectives-on-issues-in-ai-governance.pdf.

[13] Tackling the Challenge of Ethics in AI, Rumman Chowdhury, Accenture, 6 June 2018, available at https://www.accenture.com/gb-en/blogs/blogs-cogx-tackling-challenge-ethics-ai.

[14] Kush R. Varshney, "Introducing AI Fairness 360," IBM Research Blog (19 September 2018), available at https://www.ibm.com/blogs/research/2018/09/ai-fairness-360/.

[15] "Manage AI, with Trust and Confidence in Business Outcomes," IBM, available at https://www.ibm.com/downloads/cas/RYXBG8OZ.

[16] "In a move rarely seen among tech corporations, [Axon] convened the independent board last year to assess the possible consequences and ethical costs of artificial intelligence and facial-recognition software. The board's first report, published Thursday, concluded that 'face recognition technology is not currently reliable enough to ethically justify its use' — guidance that Axon plans to follow." A Maker of Police Body Cameras Won't Use Facial Recognition Yet, for Two Reasons: Bias and Inaccuracy, Deanna Paul, 28 June 2019, available at https://www.washingtonpost.com/nation/2019/06/29/police-body-cam-maker-wont-use-facial-recognition-yet-two-reasons-bias-inaccuracy/.

b. Acknowledging that AI systems can be used in a variety of contexts, with different risk levels for the individuals' rights (e.g. automatized translations vs. medicine application), in which circumstances and contexts should human intervention be preserved in decisions made by AI systems?

One of the core attributes of AI in many settings is the ability to make decisions without human intervention. However, there justifiably exist concerns around handing over full decision-making authority to a machine where its decisional output can negatively impact the individual who is the subject of the decision. The LGPD attempts to address this issue through Article 20 which provides data subjects with the right to ask for a review of decisions made solely on the basis of automated processing of personal data which impacts their interests, including decisions that aim to define their personal, professional, consumer and credit profile, as well as any aspects of their personality.[17] Article 20(1) further requires data controllers to provide to data subjects, whenever so requested, clear and adequate information about the criteria and procedures used for automated decisions, subject to commercial and industrial secrecy. Article 20(2) notes that when such information is not provided due to commercial or industrial secrecy, the Brazilian data protection authority (Agência Nacional de Proteção de Dados – ANPD) can audit the data controller's practices concerning automated decisions.

It is important to note that the LGPD does not expressly provide individuals with a right to request human review of automated decisions but rather provides them with a more general right to review which may include human intervention but could also potentially be automated in nature.

CIPL believes that the methodology and tools used for the review of automated decision making processes, including any elements of human intervention, will vary depending on the risk and impact posed to the individual by the decision. For example, the use of facial recognition technologies by airlines to check boarding passes or by customs officials to allow individuals into a country produce very significant decisions as they affect an individual's freedom of movement. Where an incorrect decision is reached in such scenarios, human intervention will compose a critical element of providing sufficient redress. In contrast, if a smart display in a retail space presents an ad intended for retirees to a young professional on the basis of facial recognition within the smart display incorrectly identifying the age group of the individual, such a decision would not warrant immediate human intervention or potentially any intervention at all. Therefore, where a risk assessment of an automated decision-making process indicates a high risk to individuals, human intervention may be an important risk mitigation factor for organizations to consider.

With respect to Brazil's national AI strategy, CIPL recommends highlighting the importance of human intervention in AI contexts where the outcome of an automated decision implies a high risk of harm for the individual that is subject to it. The national AI strategy should also acknowledge that organizations are best placed, and should have the flexibility, to define any methodologies and elements of review based on risks identified to individuals resulting from specific data processing activities. Indeed, the national AI strategy should encourage the exploration and development of appropriate review mechanisms in different AI contexts by organizations, keeping in mind that the majority of AI decisions will not warrant any intervention and that other accountability measures and safeguards will adequately protect individuals. For example, algorithmic and ethical impact assessments and the implementation of appropriate mitigations before the deployment of an AI system, ongoing monitoring, validations and

[17] See LGPD, Article 20.

checks of the algorithm once deployed by the AI service provider and even automated redress mechanisms.

c. How is it possible to implement the explainability idea in AI systems?

Explainability falls under the broader concept of transparency in the context of AI. It is a way of providing transparency about the outcome of an AI decision or process. As noted in the Singapore Personal Data Protection Commission's Model AI Governance Framework, "[a]n algorithm deployed in an AI solution is said to be explainable if how it functions and arrives at a particular prediction can be explained".[18]

Explainability can be realized in AI systems in many ways. For example:

- **Implementing best practices to facilitate traceability**: Traceability requires documenting data inputs and other "data sets and processes that yield the AI systems' decision".[19] By creating and implementing best practices or codes of conduct regarding the collection, deployment and use of data, organizations can improve traceability. This can in turn foster explainability.

- **Develop and employ explainability tools and techniques**: We mentioned counterfactual fairness testing in response to a previous question as it relates to preventing and detecting bias. This technique is also useful to facilitate explainability as it checks for fairness in outcomes by determining whether the same result is achieved when a specific variable, such as race or gender, changes. If a different result is reached by an AI system when such a variable changes, then data scientists and AI engineers will be able to look more closely at why that is, not only to remedy the bias but also to be able to explain, at least in part, what is driving the algorithm to arrive at such a result.

- **Consider the human decision-making alternative**: Often, humans are unable to consistently explain their preferences for one option over another, and there are a number of situations where decisions are not completed in a transparent manner, such as loan or credit approvals or hiring decisions. While we may be able to subsequently ask for an explanation, this explanation at best will be logical, and almost certainly will not be technical or mathematical. Considering approaches to transparency in an offline world can be illustrative of what level and type of transparency to strive for when building AI systems.

- **Consider the audience and use case involved**: What explainability involves and looks like may differ depending on the audience involved. For example, an organization may need to explain an AI outcome to an individual that is directly and negatively impacted by a decision, a regulator in cases of investigation and enforcement or participation in regulatory AI sandboxes, business partners who are interested in utilizing the AI solution or even for purposes of internal explainability and transparency to an oversight board or senior leaders. All of these different audiences imply different types and requirements of explainability which should be fulfilled appropriately. Similarly, explainability may differ depending on the use case involved. For instance, full technical explainability in the context of fraud detection and prevention would not

[18] *Supra* note 11 at page 13.
[19] *Supra* note 8 at page 20.

be appropriate as it could allow fraudsters to circumvent the AI solution for fraud detection and prevention. However, technical details could be provided to regulators, in the event of an investigation, and to individual-facing entities, so they are able to provide information to individuals.

- **Consider alternatives where explainability is not feasible**: The concept of explainability is often challenged by the "black box" phenomenon. As noted by the Norwegian DPA, "the black box makes it practically impossible to explain how information is correlated and weighted in a specific process".[20] The black box can create surprising or unanticipated results with invisible or unintelligible reasoning, even for developers. In addition, AI systems develop and change as a result of additional inputs, so decisions may not be easily repeatable. Where it is not possible to explain an AI outcome to individuals as a result of the black box problem, other options that deliver meaningful information and empowerment of the individual should be considered, including human review of AI decisions where appropriate, redress mechanisms and feedback tools.

While explainability in AI can be achieved through many different avenues, it may not always be appropriate. It is important to recognize that disclosing too much information about an algorithm or an AI process may not only result in confusion and information overload for some individuals while helping others game the system, but may also threaten commercial intellectual property interests by disclosing trade secrets. Indeed, Article 20(1) of the LGPD states that any information provided by the data controller to data subjects about the criteria and procedures for automated decisions should be provided subject to commercial and industrial secrecy. While respect for the Rule of Law and individual rights is of the utmost importance, this must be balanced with a company's ability to innovate and protect its intellectual property rights associated with its AI applications and inventions.

As evidenced by the above measures, there are many ways in which explainability can be implemented in AI systems. Risk-based flexibility, within appropriate standards or regulatory parameters, for organizations to decide which methods are most appropriate to implement explainability is crucial given that AI applications differ widely from one context to another. This approach should provide the necessary combination of flexibility as well as appropriate certainty for organizations to effectively implement explainability.

In the national AI strategy, CIPL recommends that MCTIC mention some of the various ways that explainability can be implemented in AI systems and encourage organizations to develop further ways to facilitate explainability and transparency as it relates to AI outcomes. In addition, MCTIC should also highlight the importance of innovation and competition and how any disclosure of how AI processes work and how decisions are reached must be balanced against commercial IP rights and business interests. Finally, MCTIC should also highlight that risk-based flexibility, within appropriate standards or regulatory parameters, is crucial for the effective implementation of explainability in AI systems given the contextual nature of AI applications.

[20] Artificial Intelligence and Privacy, Datatilsynet (Norwegian Data Protection Authority), January 2018, available at https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf at page 19.

d. Does it make sense to consider the adoption of a general law to address AI or would specific updates to existing legislation would suffice?

Many countries are currently considering regulation around AI. Some nations caution against the regulation of AI technologies and believe the adoption of such laws should be limited. For example, at the beginning of 2020, the US Office of Management and Budget released draft guidance for the regulation of AI applications.[21] The guidance introduces 10 regulatory principles for US federal regulation of AI applications developed and deployed by the private sector, framed by an overall mandate to "avoid regulatory or non-regulatory actions that needlessly hamper AI innovation and growth."[22] Other nations are more in favor of AI regulation. For instance, the recently appointed President of the European Commission, Ursula von der Leyen noted that during her first 100 days in office she will "put forward legislation for a coordinated European approach on the human and ethical implications of Artificial Intelligence".[23] However, it appears now that this initiative is more likely to only take the form of a policy paper that will spell out different options for a legal framework on AI which may lead to formal proposals later in the year.[24] CIPL is currently writing a paper on this initiative and engaging in discussions with the European Commission on its proposal.

It is important to note that most of the data protection challenges identified in the AI context both predate AI and are posed by technologies other than AI. Therefore, AI-specific legal structures or regulations could fail to resolve the underlying issue, while at the same time potentially deny society the benefits of properly implemented AI. Additionally, any type of regulation that is not technology-neutral may overlap with or duplicate already existing (horizontal) regulations, which would be detrimental to legal certainty. Where AI regulation is unavoidable, it should be developed thoughtfully and with enough time to allow a variety of stakeholders to identify, articulate, and implement key principles and best practices.[25] In the short term, however, serving the goals of enhancing data protection will instead require technology-neutral solutions and tools that can be applied across a variety of situations and contexts.

To the extent that Brazil ultimately chooses to regulate AI technology, CIPL believes that lawmakers should approach AI legislation with regard to the following overarching principles:

[21] Memorandum for the Heads of Executive Departments and Agencies: Guidance for the Regulation of AI Applications, Office of Management and Budget, 7 January 2020, available at https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf.

[22] *Id.* at page 2.

[23] "A Union that Strives for More: My Agenda for Europe, Political Guidelines for the Next European Commission", Ursula von der Leyen, available at https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf, at page 13 ("In my first 100 days in office, I will put forward legislation for a coordinated European approach on the human and ethical implications of Artificial Intelligence").

[24] See "Europe's upcoming artificial intelligence rules, explained" Janosch Delcker, Politico.eu, 10 January 2020, available at https://www.politico.eu/pro/europes-upcoming-artificial-intelligence-rules-explained-european-commission/.

[25] "AI technology needs to continue to develop and mature before rules can be crafted to govern it. A consensus then needs to be reached about societal principles and values to govern AI development and use, followed by best practices to live up to them. Then we're likely to be in a better position for governments to create legal and regulatory rules for everyone to follow." The Future Computed, Microsoft (2018), available at https://blogs.microsoft.com/wp-content/uploads/2018/02/The-Future-Computed_2.8.18.pdf, at page 9.

- **Build on existing legal frameworks** – including horizontal and sector-specific laws – that already provide the baseline structures, requirements, tools and remedies for accountable governance and use of AI.

- **Adopt a principles-based and outcome-based regulatory approach** that is capable of adapting to the variety, and rapidly evolving nature, of AI-related technologies and the unique challenges of specific industries, avoids overly rigid and prescriptive rules, and enables organizations to operationalize these principles by developing accountable and risk-based AI practices that achieve identified outcomes.

- **Make a "risks/benefits balancing test" and contextual impact assessment** key tools to support the beneficial use of AI, avoid risk reticence and enable proper risk mitigation.

In addition, CIPL supports a layered regulatory approach to AI which in the Brazilian context means:

- Building on LGPD rules and making the LGPD an AI enabler through forward-thinking and progressive interpretation of the requirements by the ANPD;

- Leveraging and incentivizing accountable AI practices of organizations (see response to the consultation questions relating to AI Governance)

- Fostering innovative approaches to regulatory oversight (e.g. regulatory sandboxes and regulatory hubs where regulators of different disciplines with interests in AI can exchange views, resolve conflicts of law issues, etc.)

As MCTIC considers the question of whether a general law to address AI or updates to existing legislation is more appropriate, CIPL recommends that the national AI strategy call first and foremost for consideration of the rules contained within the LGPD and its intersection with AI technology. Indeed, the LGPD provides a good threshold of protection with respect to AI applications that process personal data and enshrines key principles and ethical values that are of particular relevance to solving the challenges posed by AI (e.g. fairness, transparency). Any AI-related policy or legislative effort should remain consistent with the LGPD and avoid duplicating what is already in place.

In addition, MCTIC should promote organizational accountability as a means of effective AI governance in the national AI strategy (see response to the consultation questions relating to AI Governance) and to the extent that Brazil pursues any form of AI regulation, call for such regulation to be technology neutral and principles- and outcomes-based. Moreover, Brazil's national AI strategy should promote innovative approaches to regulation including regulatory sandboxes (see response to the consultation questions relating to AI Governance) and policy prototyping initiatives.

Finally, MCTIC should call for consistency in the regulation of AI. AI is a global industry and having multiple, diverging and potentially conflicting regulatory regimes could impede beneficial uses of AI and disrupt Brazil's ability to participate in the global AI-based economy, while not providing individuals with meaningful protections.

e. What role can be played by codes of conduct, good corporate practice rules and voluntary standards?

- **Codes of Conduct and Certifications**: CIPL believes that codes of conduct, certifications and similar accountability schemes can play an important role in ensuring accountability of AI systems and their development should be promoted in Brazil's national AI strategy. For instance, creating codes of conduct regarding the collection, deployment and use of data can help improve traceability. This can assist with ensuring fairness, conducting audits and fostering explainability. Such schemes can also demonstrate due diligence in the context of AI service providers and enable organizations to transfer data responsibly, safely and efficiently where such entities possess a relevant certification or participate in a relevant code of conduct. The use of certifications and codes of conduct for the latter purpose is especially important as AI requires substantial amounts of data to perform optimally and, as a result, data must be able to flow and be distributed among different AI systems. The national AI strategy should also highlight that any proposed framework for codes of conduct or certifications must be agile and flexible to meet the demands of new technology given the pace of developments in the area of AI.

- **Good Corporate Practice Rules**: CIPL believes that good corporate practice rules are essential to achieving and operationalizing AI accountability within organizations and form the core of responsible and ethical use of AI applications. CIPL discusses AI accountability in detail in our response to the consultation questions relating to AI Governance.

- **Voluntary Standards**: In the same way that voluntary codes of conduct and certifications can ensure AI accountability, CIPL believes that voluntary, but enforceable, standards have an equally important role to play in this regard. Voluntary standards have proven useful across many areas of privacy and data protection, including data transfers and data security. CIPL recommends that MCTIC call for the development of voluntary, but enforceable, AI data protection standards in its national AI strategy which should be developed in collaboration with industry, regulators (including the ANPD), privacy professionals and other stakeholders. Such standards should be complementary to the existing legal framework in order to ensure legal certainty.

III. AI Governance

In the consultation, MCTIC notes that the debates on governance structures that promote methods and procedures to ensure that principles for the ethical use of AI are met are starting to evolve. CIPL believes that a governance structure based on the essential elements of accountability provides a flexible yet robust framework that enables innovative and responsible uses of AI and facilitates the implementation of all applicable data protection requirements or other privacy standards through a comprehensive privacy program.

a. How is it possible to assess if artificial intelligence systems, especially within the scope of the public sector, are achieving their objectives?

- **Organizational Accountability**: MCTIC highlights the importance of creating risk management, monitoring and supervision routines for the use of AI systems along their entire lifecycle. These processes are integral to the concept of organizational accountability. Indeed, guidance for implementing such processes that foster responsible and accountable AI deployment while still allowing for innovation both in technology and in the processes used to achieve data protection has already been developed in other countries including Singapore (through the Singapore Personal Data Protection Commission Model AI Governance Framework),[26] the United Kingdom (through the UK Information Commissioner's Office AI Auditing Framework) [27] and within the European Union (through the European Commission High Level Expert Group on AI Ethics Guidelines for Trustworthy AI).[28]

CIPL has been a proponent of accountability in data protection for many years and has written extensively on the topic.[29] CIPL's accountability framework which comprises the essential elements of accountability (i.e. leadership and oversight; risk assessment; policies and procedures; transparency; training and awareness; monitoring and verification; and response and enforcement) has been used to promote organizational accountability in the broader context of building, implementing and demonstrating comprehensive privacy compliance programs. Equally, as discussed in CIPL's second AI report,[30] this framework can also be used to help organizations in both the public and private sectors to develop, deploy and organize robust and comprehensive data protection measures in the AI context and to demonstrate accountability in AI.

CIPL recommends that in the national AI strategy, MCTIC emphasizes the importance of organizational accountability to achieving effective AI governance. Accountability has been codified in Brazilian data protection law (see Article 6(X) and Article 50 of the LGPD) and the requirements of the LGPD map to the essential elements of accountability mentioned above.

- **Regulatory Sandbox**: Another mechanism that can be used to assess if AI systems are achieving their objectives is through testing the system in an AI regulatory sandbox before its deployment into the wider marketplace. The regulatory sandbox is a supervised "safe haven" which encourages and supports innovation in ways which will comply with legislative and other requirements. Participation in the sandbox typically involves the establishment of a forum by a regulator where organizations can experiment and test innovative products, services, business

[26] See *supra* note 11 generally.

[27] AI Auditing Framework, UK Information Commissioner's Office, available at https://ico.org.uk/about-the-ico/news-and-events/ai-auditing-framework/.

[28] See *supra* note 8 generally.

[29] See CIPL white papers on The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society, 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf; Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability, 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf; and CIPL Accountability Q&A, 3 July 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_q_a__3_july_2019_.pdf.

[30] *Supra* note 6.

models and delivery mechanisms in a live market with a limited number of real consumers under the supervision of the regulator.

The regulatory sandbox concept originated within the financial services sector. Indeed, in June 2019, the Brazilian Ministry of Economy's Special Secretariat for Finance, the Central Bank of Brazil, the Securities and Exchange Commission of Brazil and the Brazilian Superintendence of Private Insurance announced their intent to coordinate and implement a regulatory sandbox regime in Brazil in response to the transformation taking place in the financial, capital markets and insurance sectors.[31] The announcement further notes that the regulatory sandbox will address distributed ledger technology, blockchain, bots and AI.

The regulatory sandbox is increasingly being adopted into the data protection sphere. For example, the UK Information Commissioner's Office launched a beta phase of its data protection regulatory sandbox in 2019.[32]

We are also seeing the regulatory sandbox being adopted into the AI sphere. The concept has been mentioned in several countries' national AI strategies. For example, in December 2017, the Finnish Ministry of Economic Affairs and Employment published a report on Finland's national AI strategy which notes that a framework which ensures the availability of data must be created and that a "regulatory sandbox" experimentation environment can be created as one way to encourage data sharing.[33] In addition, in December 2019, South Korea's Ministry of Science and ICT announced that it would be creating a regulatory sandbox in the country's national strategy for the development of artificial intelligence.[34]

AI regulatory sandboxes also appear to be mandated by new data protection laws around the world. For example, in Malta, specific legislation has paved the way for a regulatory sandbox for testing artificial intelligence against pre-determined functional outputs.[35] Furthermore, India's Personal Data Protection Bill which was recently introduced into Parliament includes a provision requiring the Indian data protection authority, for purposes of encouraging innovation in AI, machine learning or any other emerging technology in the public interest, to create a Sandbox.[36]

[31] Joint Communication by Comissão de Valores Mobiliários (Brazilian Securities and Exchange Commission) on the intent to implement a regulatory sandbox for the Brazilian finance, insurance and securities industry sectors, 13 June 2019, available at http://www.cvm.gov.br/noticias/arquivos/2019/20190613-1.html.

[32] Regulatory Sandbox (Beta Phase), UK Information Commissioner's Office, available at https://ico.org.uk/for-organisations/the-guide-to-the-sandbox-beta-phase/.

[33] Finland's Age of Artificial Intelligence, Ministry of Economic Affairs and Employment of Finland, December 2017, available at http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160391/TEMrap_47_2017_verkkojulkaisu.pdf?sequence=1&isAllowed=y at page 44.

[34] South Korea National Strategy for Artificial Intelligence, December 2019, available at https://www.msit.go.kr/cms/www/m_con/news/report/__icsFiles/afieldfile/2019/12/24/%EC%9D%B8%EA%B3%B5%EC%A7%80%EB%8A%A5%20%EA%B5%AD%EA%B0%80%EC%A0%84%EB%9E%B5.pdf

[35] Malta Digital Innovation Authority Act, available at http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=12873&l=1.

[36] India Personal Data Protection Bill No. 373 of 2019, available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

CIPL recommends that MCTIC call for the creation of an AI regulatory sandbox by the ANPD in its national AI strategy, and that it looks to the experience of regulators and governments, both domestically and globally in establishing its own sandbox. CIPL has also written extensively about the regulatory sandbox in data protection[37] and MCTIC may find CIPL's work on the topic useful as it considers including the sandbox concept in its AI strategy.

b. Would it be useful to establish a requirement of preparing prior impact assessment reports regarding the use of AI in certain sectors?

Risk assessment is a core component of organizational accountability and a key requirement under modern day data protection laws. A common way of assessing the impact of a proposed data use is through a data protection impact assessment (DPIA). For example, under the EU GDPR, a DPIA is required in the context of automated decision-making which produces legal or similarly significant effects.[38] Indeed, in Brazil, Article 38 of the LGPD states that the ANPD may require a controller to prepare an impact report on the protection of personal data, including sensitive data, relating to its data processing. Such a report must contain, at least, a description of the types of data collected, the methodology used for collection and to ensure information security, as well as, the measures, safeguards and mechanisms adopted to mitigate the risks.

Such assessments may have additional value in the context of AI and some organizations are developing AI-specific DPIAs (or AI impact assessments), either as a supplement to the assessments required under data protection law or as an entirely separate assessment. Such AI impact assessments can structure the way that organizations assess issues of fairness, human rights, or other considerations in the deployment of new AI technologies. They can further help organizations build corporate values into their processes and will eventually provide a framework of pre-approved cases to set guides for assessing future innovations. In addition, such assessments may help organizations develop the documentation needed to provide effective transparency to regulators and individuals.

Importantly, any AI impact assessment must also include a process of balancing both the concrete benefits and risks of AI. 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 prevent terrorism, child abuse or other criminal behavior, which could outweigh the risk associated with processing the relevant personal data.

To further aid organizations in properly assessing the impact of AI and balancing benefits and risks, the so called "reticence risks" (i.e. what would the consequence to individuals and society be of not going

[37] Regulatory Sandboxes in Data Protection - Constructive Engagement and Innovative Regulation in Practice, 8 March 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_regulatory_sandboxes_in_data_protection_-_constructive_engagement_and_innovative_regulation_in_practice__8_march_2019_.pdf.

[38] GDPR, Article 22; see also GDPR, Article 35(1) ("Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data").

forward with a specific AI-related project due to potential risks?) should also be part of the assessment to ensure that all relevant factors are considered and inform the final decision.

Moreover, the development of sector-specific impact assessment frameworks should be further explored and promoted.

While CIPL believes that Brazil's AI strategy should mention and make reference to the importance of impact assessments in the AI context, CIPL cautions against a general requirement of preparing prior impact assessments for the use of AI in certain specified sectors. Under the GDPR, numerous and diverging national "black lists" of data processing from different EU data protection authorities that automatically require a DPIA have led to unrealistic and unmanageable expectations for organizations operating across the EU. In CIPL's view, any reference to risk or the risk-based approach in the context of AI applications outlined in the national AI strategy should be based on an approach that enables calibration of legal requirements and compliance measures to the actual risks to individuals associated with the AI application and context at hand. The LGPD is already quite prescriptive in that the ANPD has wide ranging authority to demand that a controller carry out an impact assessment.

The national AI strategy should further highlight that sector-specific impact assessment frameworks can assist organizations in addressing risks unique to certain sectors and should constitute a key part of an organization's risk assessment toolbox. However, there shouldn't be a default requirement to carry out a prior risk assessment on all AI applications in a certain sector as this could lead to thousands of risk assessments being conducted on AI technologies that pose little to no risk to individuals.

IV. <u>International Aspects</u>

a. Which international partners, be it government, companies, or research and educational institutions, should be engaged for the development of AI in Brazil?

As AI technologies impact many different stakeholders, areas of regulation and wider society, CIPL recommends that Brazil seek to work with many different international partners in developing the responsible use and deployment of AI. This could include international fora such as the Organization on Economic Cooperation and Development or regional groups such as the European Commission High Level Expert Group on AI or the Council of Europe Ad Hoc Committee on AI. It may also include international research institutions, universities and multinational corporations working on AI applications and initiatives.

CIPL has collaborated with many international stakeholders in discussing and formulating solutions to some of the most pressing and challenging issues in AI. These include global data protection authorities, law and policy makers, EU institutions, national governmental bodies, multinational organizations and academics. CIPL will continue to work on issues surrounding AI and in this regard welcomes the opportunity to respond to further consultations by MCTIC or otherwise engage with Brazil on key AI topics.

Conclusion

CIPL is grateful for the opportunity to respond to the Department of Telecommunications of the Ministry of Science, Technology, Innovations and Communications on its public consultation on a national artificial intelligence strategy for Brazil.

If you would like to discuss any of the comments in this paper or require additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com; Markus Heyder, mheyder@huntonAK.com; Nathalie Laneret, nlaneret@huntonAK.com; Sam Grogan, sgrogan@huntonAK.com; Matthew Starr, mstarr@huntonAK.com or Giovanna Carloni, gcarloni@huntonAK.com.