XXIV ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – XXIV ENANCIB

ISSN 2177-3688

GT 5 – Política e Economia da Informação

PARÂMETROS REGULATÓRIOS DE INTELIGÊNCIA ARTIFICIAL

ARTIFICIAL INTELLIGENCE REGULATORY PARAMETERS

William Henrique França – Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT), Universidade Federal do Rio de Janeiro (UFRJ)
Fabiana de Freitas Borges – Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT), Universidade Federal do Rio de Janeiro (UFRJ)
Gabriel Cunha Leal de Araujo – Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT), Universidade Federal do Rio de Janeiro (UFRJ), Fundação Getúlio Vargas (FGV)
Marco André Feldman Schneider – Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT), Universidade Federal Fluminense (UFF)

Modalidade: Trabalho Completo

Resumo: O impacto da Inteligência Artificial (IA) em todas as áreas da vida é tema de interesse das diversas ciências, dentre elas a Ciência da Informação. Como ocorreu anteriormente com o desenvolvimento de várias outras tecnologias de informação e comunicação (TICs), da escrita à Internet, sua regulação dificilmente acompanha a velocidade das transformações acarretadas por elas, para o bem e para o mal. A despeito desse atraso relativo, alguma regulação é sempre necessária, principalmente na medida em que se entende que sociedades democráticas devam estabelecer parâmetros racionais de uso dessas tecnologias, tendo em vista o bem comum como um valor superior ao bem corporativo, quando houver choque de interesses. E há, no caso da IA, como ocorreu e ainda ocorre com a imprensa, a radiodifusão de massa e a Internet. Tendo isso em vista, o objetivo deste estudo é compreender e apresentar o *status* do debate regulatório contemporâneo em torno da IA, mediante Análise de Conteúdo comparada entre seis jurisdições, atinentes à regulação da Inteligência Artificial, sendo quatro na América Latina (Argentina, Brasil, Colômbia e Uruguai), uma na América do Norte (Canadá) e a União Europeia (UE). As categorias de análise são definidas à luz da Ética da Informação. Como resultado, constata similitudes e diferentes abordagens sobre tópicos como responsabilidade, segurança e transparência. Aponta a necessidade de acompanhamento, sobretudo dos projetos brasileiro, canadense e uruguaio.

Palavras-chave: inteligência artificial; regulação de IA; ética da informação.

Abstract: The impact of Artificial Intelligence (AI) in all areas of life is a topic of interest to science, including Information Science. As previously occurred with the development of several other information and communication technologies (ICTs), from writing to the Internet, their regulation hardly keeps up with the speed of the transformations they brought about, for better or worse. Despite this relative delay, some regulation is always necessary, primarily as it is understood that democratic

societies must establish rational parameters for using these technologies, considering the common good as a higher value than the corporate good when there is a clash of interests. And there is, in the case of AI, as happened and still happens with the press, mass broadcasting, and the Internet. With this in mind, the objective of this study is to understand and present the status of the contemporary regulatory debate around AI, through Content Analysis comparing six jurisdictions relating to the regulation of Artificial Intelligence, four of which are in Latin America (Argentina, Brazil, Colombia, and Uruguay), one in North America (Canada) and the European Union (EU). The analysis categories are defined by considering information ethics. As a result, it finds similarities and different approaches to topics such as responsibility, security and transparency. It points out the need for monitoring, especially Brazilian, Canadian and Uruguayan projects.

Keywords: artificial intelligence; AI regulation; information ethics.

1 INTRODUÇÃO

A Inteligência Artificial (IA), ao desempenhar tarefas que exigiriam a capacidade cognitiva humana, mas com velocidade superior e a custos mais baixos, aumenta a produtividade, otimiza processos (D'Agostino, 2023; He; Degtyarev, 2023; França, 2022; Turing, 1950), produz emprego e desemprego. Dado o seu impacto em todas as esferas da vida e sua aparente imprescindibilidade naquilo que se tem chamado "transformação digital" da sociedade (OECD, 2020), estar atento ao debate regulatório internacional vai ao encontro do interesse dos agentes políticos e das instituições que protagonizam esse debate no Brasil.

Estudos como esta análise e os levantamentos da Acess Now (2024) e de Cantekin (2023) encontram-se na difícil tarefa de revisar propostas regulatórias na América Latina, onde se avolumam proposições e apensos[1] que se alternam entre pautas e arquivamentos. É possível que muitos projetos analisados não sejam aprovados ou sejam descartados diante de novas iniciativas, mas refletem os parâmetros regulatórios atuais da região (Acess Now, 2024).

Este estudo tem como objetivo proceder a uma Análise de Conteúdo comparada das leis, projetos e regulamentos com força de lei que versam sobre IA nas seguintes jurisdições: América Latina (Argentina, Brasil, Colômbia e Uruguai), América do Norte (Canadá) e União Europeia (UE).

1.1 Metodologia

Esta Análise de Conteúdo comparada é orientada pela sistematização feita por Moraes (1999). Para o autor, os procedimentos essenciais desse tipo de análise implicam a

[1] São propostas anexadas que passam a tramitar juntas ao projeto "principal" ou em tramitação nos parlamentos, por já estarem contempladas suas proposições ou pela semelhança de matéria e dispositivos.

categorização, a descrição e a interpretação (Moraes, 1999). O presente estudo tem caráter qualitativo, alinhando a pesquisa documental no âmbito de seis jurisdições estudadas à técnica de que trata Moraes (1999). Para a análise, foram definidas oito categorias: *segurança*, *interoperabilidade*, *transparência*, *privacidade*, *níveis de risco*, *inovação*, *responsabilidade* e *sanções*, interpretadas à luz da Ética da Informação. Dado que se trata de instrumentos jurídicos que visam regular o desenvolvimento e uso da Inteligência Artificial, essas categorias de análise se justificam por contemplar aspectos centrais no debate regulatório sobre IA no mundo: a proteção a direitos fundamentais dos indivíduos e coletividades impactadas por sistemas de Inteligência de Máquina.

A pesquisa documental teve como ponto de partida o levantamento da *Law Library of Congress EUA* (Cantekin, 2023). A escolha das jurisdições estudadas teve como critério o contingente populacional impactado: Brasil, Colômbia e Argentina, respectivamente, são os três maiores países da região; o Uruguai foi destacado por ocupar o terceiro lugar na América Latina em termos de preparação para a Inteligência Artificial, segundo o *Oxford Insights International Development Research Centre (IDRC)*[2]; o Canadá se destaca por ser o país com a maior concentração de especialistas em IA no mundo (Gil, 2019; Salomão Filho, 2017) e ter publicizado, desde 2018, a *Montreal Declaration*, documento principiológico para o desenvolvimento de IA responsável; e a União Europeia porque seus regulamentos devem ser observados por todos os países do bloco.

No âmbito de cada jurisdição, eventualmente, uma mesma categoria foi abordada em projetos distintos, de maneira semelhante. Nesses casos, com vistas à concisão, foi necessário sintetizar dispositivos de leis diferentes na mesma descrição, indicando, quando o caso, os projetos em que se encontram aquelas disposições.

No Quadro 1, para fins de assimilação pelo leitor, os projetos analisados estão em sequência alfabética. Na análise dos projetos da Argentina, *A* corresponde ao Projeto de Lei 1472-D-2023 *(Modificación Ley Nacional 25.467)*, *B* corresponde ao Projeto de Lei 2504-D-2023 *(Ley de Regulación y Uso de la Inteligencia Artificial en la Educación)* e *C* corresponde ao Projeto de Lei 2505-D-2023 *(Marco legal para la regulación del desarrollo y uso de la Inteligencia Artificial)*. No caso do projeto brasileiro, *D* corresponde ao PL 2338/2023. No caso

[2] A *Oxford Insights International Development Research Centre* publica o Índice de Preparação Governamental para a IA. Disponível em: https://oxfordinsights.com/ai-readiness/ai-readiness-index/. Acesso em 6 jun. 2024.

do Canadá, *E* corresponde ao *Bill C-27*. Na análise dos projetos da Colômbia, *F* corresponde ao projeto 59/2023 e *G* corresponde ao projeto 200/2023. Na análise das propostas europeias, *H* corresponde ao *General Data Protection Regulation (GDPR)* e *I* corresponde à *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence*.

2 DAS CATEGORIAS DE ANÁLISE E INDICADORES

A categoria *segurança* concerne à análise dos padrões de tratamento de dados pessoais empregados na aprendizagem algorítmica dos sistemas de IA, assim como às medidas de mitigação de riscos associadas ao uso de Inteligência de Máquina. Por outro lado, a *interoperabilidade* é um recurso que, observados os padrões de segurança estabelecidos, permite ao titular, pessoa autorizada ou autoridade competente, acessar, compartilhar ou recompilar dados por meio de ferramentas ou dispositivos externos para qualquer fim autorizado.

Segundo Bielby (2014), privacidade e transparência são temas de interesse desde a introdução da Ética da Informação no campo da CI, nos anos 1980 e início dos anos 1990. A *transparência* permite analisar a abordagem do legislador quanto ao funcionamento dos sistemas de IA, em aspectos como a obrigatoriedade ou não de notificar o usuário sobre a coleta e tratamento de dados, os critérios de tomada de decisão ou mesmo o início e a cessão da interação com o sistema. Por outro lado, a categoria analítica *privacidade* observa a atenção conferida pelo legislador ao direito humano fundamental, estabelecendo ou não mecanismos de revogação de consentimento, atualização ou eliminação de dados, assim como a eventual opção pela cessação da interação com um sistema de IA.

A análise dos *níveis de risco* dos sistemas de IA pode revelar diferentes classificações e abordagens quanto ao seu impacto sobre os indivíduos. Yoshua Bengio, diretor científico do *Mila-Quebec AI Institute*, argumenta pela regulação de sistemas de IA, independentemente do seu estágio. Segundo Bengio, um sistema de IA "pode ser perigoso mesmo agora se o projetarmos com objetivos maliciosos" (D'Agostino, 2023). Noutro norte, tem-se que a *inovação* é um processo contínuo e, aparentemente, irreversível, para o atendimento a demandas mercadológicas, estatais, sociais ou particulares que a IA propõe, sendo de interesse conhecer como as jurisdições estudadas orientam ou investem nesse processo.

Capurro (2017) reflete sobre as liberdades e responsabilidades na Era Digital. Nesse intuito, reproduz o preâmbulo da declaração de "Princípios Internacionais de Direitos Humanos sobre a Vigilância das Comunicações", segundo o qual o "setor privado assume a mesma responsabilidade [*que o Estado]* de respeitar os direitos humanos, em especial tendo em conta o papel fundamental que desempenha na projeção, desenvolvimento e difusão das tecnologias [...]" (Privacy International *et al.*, 2013 *apud* Capurro, 2017, p. 61, comentário nosso). Já a *responsabilidade* que cada país estudado atribui aos desenvolvedores e usuários tende a ser uma variável influenciada por aspectos políticos e culturais. Igualmente, as *sanções* que cada jurisdição prevê em razão daquelas responsabilizações tende a ser orientada pelos mesmos fatores.

O Quadro 1 relaciona as categorias aos respectivos indicadores. Os normativos analisados em cada jurisdição estão identificados por letras em sequência alfabética.

Quadro 1 – Categorias e Indicadores de Análise

Jurisdição	Categoria de Análise	Indicadores de Análise
Argentina	Segurança	1. Exige armazenamento de dados seguro contra acesso não autorizado ou uso indevido (*B* e *C*); 2. Exige sistemas de IA seguros que cumpram padrões éticos e de qualidade estabelecidos (*C*); 3. Exige monitoramento constante e avaliações periódicas quanto à qualidade, eficácia, adequação aos objetivos de ensino e impacto do sistema de IA na educação (*B*); 4. Estabelece Autoridade de Supervisão de IA (*C*); 5. Prevê proibição de IA de "risco inaceitável", que não comprovar medida de mitigação de riscos adequada (*C*); 6. Prevê criação de canal de denúncias à autoridade competente sobre sistemas de IA inadequados (*C* e *A*).
	Interoperabilidade	Não consta.
	Transparência	1. Exige identificar os sistemas de IA utilizados e informar o usuário impactado sobre o uso, o tipo e os critérios de aplicação dos dados coletados (*B*); 2. Exige clareza quanto ao funcionamento dos algoritmos (*B*), assim como limitações, riscos e precauções (*C*); 3. Exige documentação e divulgação do funcionamento dos algoritmos para fins de auditoria e avaliação de impacto (*C*); 4. Exige clareza quanto a tomadas de decisão e resultados gerados por sistemas de IA (*C*); 5. Exige autonomia do usuário para acessar, corrigir, eliminar ou solicitar interrupção do uso de dados pessoais por sistemas de IA (*B*); 6. Exige registro com especificações dos sistemas de IA, em todo o ciclo do seu funcionamento (*C* e *A*); 7. Possibilita usuários solicitarem explicações sobre decisões tomadas por sistemas de IA (*C*).
	Privacidade	1. Exige que sistemas de IA respeitem o direito à privacidade dos usuários impactados (*B* e *C*); 2. Exige autorização expressa dos titulares e seus responsáveis legais (se for o caso), antes da coleta e utilização de dados pessoais (*B* e *C*); 3. Orienta que o tratamento de dados pessoais por sistemas de IA esteja de acordo com as normas vigentes sobre o tema (*C*).
	Níveis de Risco	1. Estabelece níveis de risco "inaceitável", "elevado", "limitado" e "insignificante". Com exceção deste último, os demais têm impacto sobre direitos fundamentais ou a segurança dos indivíduos, exigindo-se medidas de mitigação compatíveis.

	Inovação	1. Exige melhorias contínuas nos sistemas de IA para incorporar avanços tecnológicos e atualizações curriculares (*B*); 2. Prevê colaboração entre instituições de ensino e pesquisa para a implementação de programas de formação e capacitação em IA em nível acadêmico e de mercado de trabalho (*C*); 3. Prevê cooperação da indústria, da sociedade e articulação internacional para a conformação de padrões, políticas e regulação de IA (*C*); 4. Prevê destinação de recursos e incentivos ou criação de fundo público-privado de investimento no âmbito acadêmico e industrial para o desenvolvimento de IA de interesse estratégico e social (*C*).
	Responsabilidade	1. Exige que os sistemas de IA garantam a não-discriminação, a segurança individual e coletiva, a autonomia dos indivíduos e a proteção do meio-ambiente (*A*); 2. Prevê criação de comissões e organismos para proceder à prova ética dos sistemas de IA (*C*); 3. Exige equidade, imparcialidade e inclusão (*B* e *A*), especialmente quanto às crianças e adolescentes (*B*); 4. Responsabiliza agentes de IA por danos em razão de erros de sistemas de IA e pelas consequências de suas ações e decisões (*C*); 5. Limita a utilização de IA em situações de emergência (*C*); 6. Estabelece a corresponsabilidade de usuários, exigindo que utilizem sistemas de IA conforme instruções técnicas, obrigando-os a reparação de danos causados a terceiros por uso indevido (*C*); 7. Exige seguro de responsabilidade civil entre agentes de IA e usuários, fornecido por seguradora autorizada para cobrir eventuais danos (à pessoa ou à propriedade), causados por erros de IA (*C*); 8. Prevê fomento à educação em IA para o uso responsável (*C*); 9. Exige avaliação constante para identificar e mitigar riscos (*C*); 10. Exige supervisão e regulação por autoridades competentes em educação e proteção de dados pessoais (*B*); 11. Exige que autoridades em educação promovam a capacitação de profissionais da área e alfabetização digital dos estudantes para o uso adequado dos sistemas de IA (*B*); 12. Prevê formação e capacitação em IA para profissionais, investigadores e estudantes (*C*).
	Sanções	1. Sistemas de IA de "risco inaceitável", que não comprovem medidas de mitigação de risco adequadas podem ser proibidos (*C*); 2. Prevê proibição, restrição ou multa quando o sistema de IA não for transparente e auditável, violar direitos humanos fundamentais, promover discriminação, representar risco de dano grave a pessoas ou ao meio ambiente, influenciar indevidamente na opinião dos indivíduos ou na tomada de decisões de caráter político (*C* e *A*).
Brasil	Segurança	1. Exige avaliação do sistema de IA para classificação do grau de risco antes da colocação no mercado; 2. Obriga avaliação contínua do impacto de sistemas de IA de alto risco, a ser realizada por técnicos e com participação pública; 3. Prevê supervisão humana sobre sistemas de IA de alto risco e intervenção em caso de danos relevantes à pessoa; 4. Prevê a comunicação de incidentes graves por parte dos agentes de IA à autoridade competente.
	Interoperabilidade	Não consta.
	Transparência	1. Assegura direito à informação prévia sobre interação com sistemas de IA; 2. Assegura direito à explicação sobre recomendação, previsão ou decisão tomada por IA; 3. Determina que agentes de IA explicitem para usuários os procedimentos, para fins de contestação de decisões e privacidade; 4. Exige informar pessoas expostas a sistemas de reconhecimento de emoções ou categorização biométrica sobre a utilização e o funcionamento do sistema no ambiente em que ocorrer a exposição; 5. Sistemas de IA destinados a grupos vulneráveis serão desenvolvidos de modo que essas pessoas consigam entender seu funcionamento e seus direitos; 6. A autoridade pública deve criar base de dados pública de IA.
	Privacidade	1. Assegura direito à proteção de dados, de acordo com a legislação vigente; 2. Assegura correção de dados incompletos, desatualizados ou inexatos, assim como direito de solicitar anonimização, bloqueio ou eliminação de

		dados desnecessários, excessivos ou tratados em desconformidade com a LGPD; 3. Proíbe sistemas de identificação biométrica à distância, exceto com previsão legal federal e autorização judicial.
	Níveis de Risco	1. Risco Excessivo: algumas práticas são vedadas e para outras deve haver legislação ou regulamentação específicas; 2. Alto Risco: medidas de governança mais rigorosas e supervisão humana para minimizar impactos, podendo interromper seu funcionamento.
	Inovação	1. Prevê que agentes de IA, individualmente ou em associações, formulem códigos e implementem programa de boas práticas; 2. Atribui à autoridade competente a promoção e a elaboração de estudos de boas práticas, além de ações de fomento e cooperação com outros países.
	Responsabilidade	1. Obriga que danos sejam reparados pelo fornecedor integralmente; 2. A responsabilização sobre dados relacionados ao consumo está sujeita ao Código de Defesa do Consumidor; 3. Prevê autoridade competente para fiscalização da lei, designada pelo Poder Executivo; 4. Veda a discriminação e determina correção de vieses discriminatórios.
	Sanções	1. Prevê sanções de advertência, multa limitada a cinquenta milhões de reais por infração, publicização da advertência, proibição ou restrição por 5 anos, suspensão parcial ou total, proibição de tratamento de algumas bases de dados.
Canadá	Segurança	1. Prevê o cargo de *Data Comissioner* para auxiliar na regulação das ações com IA; 2. Permite que presidente e ministros criem regulações sobre a IA e seu uso conforme necessário.
	Interoperabilidade	Não Consta.
	Transparência	1. O governo pode solicitar dados a qualquer momento para fins de auditoria ou contratar auditoria independente; 2. O governo pode solicitar publicação de relatórios de auditoria, medidas de melhoras e dados anonimizados a qualquer momento, exceto informação confidencial empresarial; 3. Obriga o provedor demonstrar como o sistema deve ser usado, os tipos de conteúdo, decisões e predições que ele pode fazer, as medidas de mitigação de problemas e outras informações adicionais prescritas pela regulação; 4. Exige manutenção de registros gerais e adicionais.
	Privacidade	1. Obriga que os dados sejam anonimizados; 2. O uso ou a posse de informação pessoal é considerada ofensa judicial, passível de punição.
	Níveis de Risco	1. Define 3 tipos de danos que as IAs podem causar: a) físico e psicológico a nível individual, b) dano à propriedade individual e c) perda econômica de um indivíduo; 2. Cria classificação de violação em 3 níveis: a) Violação Menor *(Minor)*, b) Séria Violação *(serious)* e c) Violação Severa *(Very Serious)*.
	Inovação	Não consta.
	Responsabilidade	1. A lei não se aplica a ferramentas de IA utilizadas pelo ministério da defesa, serviço de inteligência e outros setores estratégicos; 2. Responsabiliza pessoas e empresas que desenvolvem, desenham, tornam disponíveis e ou gerenciam operações com essas ferramentas; 3. O responsável pela IA deve ser o mesmo a avaliar se ela se configura como um sistema de alto impacto ou não e, caso for, deve ser quem deve propor soluções para mitigar os riscos; 6. Deve-se notificar ao governo se sistemas de alto impacto resultarem em material prejudicial; 7. Proíbe o uso de conteúdo gerado com vieses que possam prejudicar um indivíduo ou grupo; 8. Quando houver solicitado informações a agentes de IA para fins de auditoria, o governo não pode tornar pública esse tipo de informação, a não ser sob mandado judicial.
	Sanções	1. O governo pode cessar a prestação de serviço se houver indícios razoáveis de que o sistema pode causar dano eminente e grave; 2. A pessoa ou organização que for responsável pela IA e cometer alguma infração de acordo com as normas estabelecidas, pode ser obrigada a arcar com as multas que

		variam cujo limite é de 20 ou 25 milhões de dólares canadenses, a depender das receitas globais do infrator. 3. Prevê ações e sanções contra obstrução ou provimento de informação falsa ou enganosa;
Colômbia	Segurança	1. Toda decisão ou dado de IA é auditável, passível de revisão e de contestação e deve ser supervisionada (*F* e *G*); 2. Prevalência da inteligência humana; (*F* e *G*); 3. As políticas de cibersegurança devem passar pela Comissão de Tratamento de Dados e Desenvolvimento com a IA (*F*); 4. Os sistemas de IA não poderão ser usados como instrumentos armamentistas, exceto pela segurança nacional (*F*); 5. Observância dos princípios de desenho seguro das IAs (*F*); 6. Em todas as fases de implementação, deve-se analisar os riscos e a implementação deve ser contida em caso de risco e insegurança (*F*); 7. Integridade e confidencialidade da informação que poderá gerar algoritmos e criar programas de computador (*G*); 8. Desenvolvimento pautado através de evidência científica (*G*); 9. Exige publicação de avaliação dos riscos e impactos que os direitos fundamentais podem sofrer, antes de implantar tais sistemas (*G*); 10. Os usuários devem expressar seu consentimento para assumir os riscos (*G*); 11. Proíbe o uso de IA para menores de 18 anos (*G*); 12. Exige registro de modelos em plataformas de certificação (*G*).
	Interoperabilidade	Não consta.
	Transparência	1. Obriga responsáveis por sistemas de IA informar aos titulares dos dados utilizados o tratamento que lhes está sendo concedido e os resultados obtidos (*F* e *G*); 2. Exige transparência sobre as causas que dão origem a previsões, resultados ou decisões algorítmicas de IA (*F* e *G*).
	Privacidade	1. Cria a Comissão de Tratamento de Dados e Desenvolvimento com a IA (*F*); 2. Os titulares e herdeiros destes podem solicitar a retirada de seus dados, em prazo de até 5 dias (*F*); 3. Garantia da segurança da informação, respeitando sempre que o direito das pessoas à privacidade não seja violado (*F*); 4. Os sistemas precisam de permissão para uso de dados pessoais que possam gerar lucros e caberá indenização ao titular ou seus herdeiros em caso de uso sem consentimento (*F*); 5. Dados personalíssimos só poderão ser usados mediante autorização do titular (*F*); 6. Devem garantir anonimato em informações de caráter particular (*F*); 8. Proíbe reconhecimento facial para crimes graves sem decisão judicial (*G*); 9. Proíbe transferência de dados pessoais (*G*).
	Níveis de Risco	1. Inaceitável: afeta a segurança e os direitos humanos e fundamentais, Alto Risco: atividades suscetíveis de automatização e que podem limitar algum direito fundamental, Risco Limitado: uso de *chatbots* e robôs e Risco Nulo (*G*).
	Inovação	1. Estabelece a Política Sobre Crescimento Inclusivo, Desenvolvimento Sustentável e Bem-Estar (*F*); 2. Desenvolvimento da tecnologia orientada a considerações sociais e ambientais (*G*); 3. O Ministério das Tecnologias de Informação e Comunicação promoverá o desenvolvimento, utilização e implementação de IA e processos de automação para promover a educação, a ciência, a identidade cultural e a diversidade e facilitar processos dentro de entidades estatais para a organização da informação (*G*).
	Responsabilidade	1. O sistema deve prever detecção precoce, diagnósticos e o desenvolvimento de medicamentos e pode ser declarado de utilidade pública e interesse social (*F*); 2. Realização de controle sobre a veracidade dos dados e os resultados do sistema (*F*); 3. Responsáveis por sistemas de IA devem reparar danos materiais e imateriais (*F* e *G*); 4. Exige Registro Nacional da IA no Ministério de Ciência e Tecnologia (*F*); 5. Prevê responsabilidade ética e legal dos criadores e intermediários (*G*); 6. Obriga o setor público a prestar contas e criar mecanismos de supervisão em todas as fases que sejam auditáveis e rastreáveis (*G*); 7. Trabalhadores substituídos por sistemas de IA devem ser alocados em outro cargo por seis meses (*G*); 8. A Superintendência

		de Indústria e Comércio será a autoridade de proteção de dados, que implementará processos de auditoria de algoritmos, entre outras funções (*G*); 9. Proíbe discriminação e sistemas que atentam contra os direitos humanos e devem garantir a proteção e promoção da diversidade (*F* e *G*). 10. As pessoas que se sentirem prejudicadas podem pedir revisão, apresentar reclamação e pedidos de revogação (*G*); 11. Proíbe manipulação de comportamento, exploração de vulnerabilidades de pessoas ou grupos, habilitação de perfis para concessão de créditos, previsão de comportamento criminoso, reconhecimento de emoções, extração de imagens na Internet para base de reconhecimento facial, vigilância e identificação biométrica, categorização biométrica a partir de características físicas e sociais, realização de pontuação social ou reputacional, influência em eleitores e resultados de processos eleitorais, definições de sentenças judiciais, limitar liberdade de expressão (*G*). 12. Proíbe a divisão da sociedade e a promoção da violência (*G*)
	Sanções	1. A Superintendência de Indústria e Comércio adotará medidas e imporá sanções correspondentes ao Capítulo II do Título VII da Lei 1581 de 2012 (*G*).
União Europeia	Segurança	1. Exige sistema de governança, gestão de risco e de qualidade para IA de alto risco durante todo o ciclo de funcionamento (*I*); 2. Exige que sistemas de IA passem por avaliação e certificação de conformidade antes de serem colocados no mercado (*I*); 3. Sistemas de IA de alto risco que impliquem formação de modelos devem observar critérios de qualidade de dados de formação, validação e ensaio (*I*); 4. Exige que sistemas de IA de alto risco sejam rastreáveis, com registro automático de eventos (*I*); 5. Exige documentação técnica prévia dos sistemas de IA de alto risco com atualização constante para avaliação de conformidade (*I*); 6. Exige a possibilidade de supervisão humana eficaz sobre IA de alto risco (*I*); 7. Exige sistemas de IA de alto risco resilientes a erros, incoerências, especialmente em razão da sua interação com pessoas ou outros sistemas, e à intervenção de terceiros não autorizados que pretendam alterá-lo ou explorar vulnerabilidades (*I*); 8. Estabelece autoridade notificadora, organismos notificados identificados, organismos de avaliação de conformidade de países terceiros etc., e autoridade nacional competente para assegurar observância ao Regulamento e dirimir questões relativas aos sistemas de IA (*I*); 9. Cria o Conselho Europeu de Inteligência Artificial (*I*); 10. Cria base de dados de sistemas de IA de alto risco, no âmbito da UE (*I*); 11. Prevê monitorização dos sistemas de IA após sua colocação no mercado (*I*); 12. Exige que IA de alto risco se submeta à avaliação de conformidade por terceiros, quando represente risco de dano para a saúde, a segurança ou impacto adverso em direitos fundamentais (*I*).
	Interoperabilidade	Não consta.
	Transparência	1. Exige que sistemas de IA possibilitem a interpretação de seus resultados pelos utilizadores (*I*); 2. Exige disponibilidade de informações detalhadas sobre o sistema de IA (finalidade, desenvolvedor, capacidades e limitações etc.) (*I*); 3. Exige cientificar as pessoas que estão interagindo com IA, especialmente aquelas para fins de reconhecimento de emoções, salvo na hipótese de utilização para a prevenção de infrações penais (*I*); 4. Exige explicitar o uso de IA generativa (áudio, imagem e vídeo) (*I*); 5. Obriga fornecedores de IA de alto risco a fornecerem informações a autoridades competentes, incluindo registros automáticos (*I*).
	Privacidade	1. Exige medidas de anonimização e pseudonimização de dados (*I*); 2. Exige que autoridades competentes preservem informações comerciais e de propriedade intelectual e afins, no exercício de suas atividades (*I*).
	Níveis de Risco	1. Diferencia IA de alto risco (referidas no Anexo III) das demais (*I*).
	Inovação	1. Prevê *sandboxes* regulatórios controlados para desenvolvimento de sistemas de IA em conformidade com o Regulamento (*I*); 2. Prevê

		desenvolvimento de sistemas de IA em áreas de interesse público (*I*); 3. Prioriza pequenas empresas nos *sandboxes* regulatórios de IA (*I*).
	Responsabilidade	1. Exige registro para sistemas de IA de alto risco antes de serem colocados no mercado (*I*); 2. Proíbe sistemas de IA que empreguem técnicas subliminares que manipule o comportamento humano, que explore vulnerabilidade (idade, deficiência etc.) de pessoa ou grupo (*I*); 3. Proíbe autoridades públicas utilizarem IA para avaliação ou classificação de pessoas com base em seu comportamento social, características pessoais ou de personalidade (*I*); 4. Restringe a identificação biométrica em tempo real à busca direcionada de autor ou suspeito de infração penal específica ou de crianças desaparecidas, à prevenção de crime eminente ou de ataque terrorista, mediante autorização de autoridade competente (*I*); 5. Exige que utilizadores de sistemas de IA de alto risco utilizem-na conforme instruções do fornecedor e notifiquem-no caso considere que o sistema não observa os padrões de conformidade aplicáveis (*I*); 6. Exige que fornecedores, distribuidores e utilizadores de IA de alto risco mantenham todos os registros gerados automaticamente, quando estes estiverem sob seu controle, por período adequado à finalidade do sistema e às obrigações jurídicas a que estejam submetidos, especialmente se forem instituições de crédito (*I*); 7. Exige que fornecedores de IA comuniquem a autoridades competentes incidentes graves que constituam violação de obrigações referentes a garantia de direitos fundamentais (*I*); 8. Incentiva a adoção de Códigos de Conduta e a adoção de sistemas de IA que não sejam de alto risco (*I*); 9. Garante ao titular de dados o direito de não se sujeitar a decisões exclusivamente automatizadas, salvo se houver consentimento expresso, previsão em lei da UE (ou Estado-Membro) ou seja necessário para execução contratual entre o titular e o responsável pelo tratamento dos dados. Exceto no caso de previsão legal, o titular tem direito de intervenção humana e de contestação (*H*).
	Sanções	1. Prevê restrições, suspensão do registro ou do certificado emitido para um sistema de IA, em caso de descumprimento de requisitos de conformidade (*I*); 2. Prevê que mesmo os *sandboxes* regulatórios de IA podem ser suspensos até a sua conformação, se constatado risco de dano (*I*); 3. Prevê multas por desconformidade ou incumprimento de medidas impostas, que variam conforme o porte da empresa infratora (*I*).

Fonte: Elaboração própria (2024).

2.1 Da Análise

Sobre a Argentina, analisamos o projeto de *Modificación Ley Nacional 25.467* (*A*), a *Ley de Regulación y Uso de la Inteligencia Artificial en la Educación* (*B*) e o *Marco legal para la regulación del desarrollo y uso de la Inteligencia Artificial* (*C*). O projeto *A* altera lei vigente sobre ciência, tecnologia e inovação; os projetos *B* e *C* propõem novas leis. Em geral, as iniciativas argentinas têm forte apelo à responsabilidade e à transparência, tendo destaque, nessas categorias, doze e sete medidas, respectivamente. No que concerne à responsabilidade, oito medidas são estabelecidas no projeto *C*, quatro no *B* e duas no *A*. Em termos de transparência, *C*, *B* e *A* preveem cinco, duas e uma medida, respectivamente.

No Brasil, analisamos o PL 2338/2023 (*D*), em razão do Parecer[3] da relatoria da Comissão Especial do Senado. A transparência é a categoria com mais medidas impostas pelo projeto de lei, seguido por responsabilidade. Entre os indicadores de transparência que destacamos está a criação de base pública de IA e a comunicação de incidentes graves para as autoridades competentes. A supervisão humana é prevista em casos de alto risco ou de possíveis danos relevantes à pessoa. A privacidade é resguardada com os princípios da Lei Geral de Proteção de Dados (LGPD).

Quanto ao Canadá, estudamos o projeto *Bill C-27* (*E*), no que concerne à IA. Há pouco detalhamento na proposta. Níveis de risco são divididos em três categorias, mas sem especificá-los, propriamente, assim como não especifica tipos de danos causados por IA. Em termos de segurança, prevê que o presidente e ministros atuem sobre a criação de novas regulações para IA e institui o *Artificial Intellligence and Data Commissioner*, cuja função é assistir o governo no que se refere a regulação da IA. O projeto se destaca em tratar sobre privacidade, impondo a obrigatoriedade de anonimização dos dados e criminalizando o uso indevido de dados pessoais. Além disso, exige a manutenção de registros detalhados e notificação ao governo sobre impactos prejudiciais. Prevê responsabilização de desenvolvedores e gestores de IA por quaisquer problemas a ela relacionados. Enquanto sanções, prevê multas milionárias ao infrator.

Sobre a Colômbia, foram analisados dois projetos: o 59/2023 (*F*) e o 200/2023 (*G*). A segurança é a categoria em destaque nas duas propostas. O projeto *F* não trata sobre riscos nem prevê sanções, enquanto o projeto *G* aborda riscos, sanções e cita outra legislação aplicável para fins de penalidades. Ambas enfocam direitos humanos e impõem a inteligência humana sobre a das máquinas. A proposta *G* é mais específica em relação a proibições e riscos. Dentre elas, apenas o projeto *G* propõe medidas de proteção ao trabalhador em relação à IA.

Em 2023, o Parlamento do Uruguai apresentou o projeto de *Regulación de sistemas que utilizan inteligencia artificial*. Por ser proposta sucinta, que versa exclusivamente sobre a categoria transparência, dispensou-se sua inclusão no Quadro 1. Essencialmente, a lei exige que os usuários sejam notificados quanto à interação com um sistema de IA e obriga a adequada sinalização do conteúdo que tenha sido tratado com essa ferramenta. Em 2019, o

[3] Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9630164&ts=1718367328855&rendition_principal=S&disposition=inline. Acesso em 15 jun. 2024.

Uruguai já adotara documento estratégico para a utilização de IA no governo eletrônico. Anterior à popularização da IA generativa, o documento aborda tópicos essenciais, como a necessidade de prover IA transparente (em termos de algoritmo, utilização de dados etc.), que respeite direitos humanos e tenha como propósito a melhoria da qualidade de vida e a simplificação de processos com a IA (AGESIC, 2019). Também estimula o envolvimento do setor privado, academia e sociedade civil, com vistas a soluções inovadoras e eficazes que atendam às necessidades do governo e dos cidadãos e promova a cidadania digital e a governança eletrônica.

Os projetos na União Europeia têm maior apelo à segurança e à responsabilidade. Foram estudados o *General Data Protection Regulation (GDPR)* (*H*), onde se destaca uma das nove medidas de responsabilidade previstas no conjunto de normas europeias em estudo (veja-se indicador 9); a *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence*[4] (*I*), que prevê todas as doze medidas de segurança e oito das nove medidas de responsabilidade; e a *Proposal for a Directive of the European Parliament and of the Council*[5]. A Diretiva tem caráter regulamentador do projeto *I*, explicitando procedimentos em eventuais ações de danos morais causados por falhas na IA, razão por que não consta do quadro analítico. O *GDPR*, em seu Art. 22, trata sobre tomada de decisão individual automatizada. O projeto *I* não se aplica a autoridades públicas de país terceiro ou organizações no âmbito da UE, quando esses utilizem IA no contexto de acordos internacionais de cooperação policial e judiciária com a UE ou Estados-Membro.

3 CONSIDERAÇÕES FINAIS

Em se tratando de segurança, dentre os projetos analisados, a Argentina, o Brasil, a Colômbia e a União Europeia incluem disposições que exigem a supervisão humana sobre os sistemas. O Canadá não aborda esse tema. Ainda nesta categoria de análise, foi possível constatar que aquelas mesmas jurisdições instituem uma autoridade competente de fiscalização, enquanto o Canadá cria um cargo.

Na categoria responsabilidade, o estudo constatou que os projetos brasileiro, colombiano e europeu proíbem a identificação biométrica em tempo real em locais de acesso

[4] Proposta de Lei da Inteligência Artificial, que também altera determinados atos legislativos da União Europeia.
[5] Diretiva que adapta as regras de responsabilidade civil extracontratual para tratar sobre Inteligência Artificial.

ao público, salvo em casos previstos em lei, com decisão judicial. Nessa categoria, os projetos canadense e argentino não apresentam indicadores sobre esse tema. Por outro lado, Argentina, Brasil, Canadá e Colômbia responsabilizam desenvolvedores e provedores de IA por danos morais ou materiais causados em razão de erros de IA, sendo a Argentina a única a prever corresponsabilidade aos usuários, impondo igualmente a obrigação de reparar danos causados a terceiros. O projeto europeu, por sua vez, não trata da responsabilização, embora a proposta de Diretiva preveja procedimentos a serem observados em eventuais ações para fins de reparação de danos. No mesmo sentido, o projeto de Lei de Inteligência Artificial (*I*) não trata sobre vieses ou discriminação por falhas de IA. Argentina, Brasil, Canadá e Colômbia vedam expressamente.

Como os países analisados estão, em alguns casos, com mais de uma proposta em discussão ou em fase de ajustes, o acompanhamento e análise posterior, com os PLs consolidados ou as legislações aprovadas, se faz necessário. O Brasil é um caso em que muitas propostas foram apresentadas, mas é um substitutivo com inclusão de emendas ao PL 2338/23, que está em tramitação, no Senado.

O projeto regulatório do Canadá revelou-se incipiente, o que se explica, em parte, com o fato de que o projeto ainda está em construção. O Uruguai, igualmente, merece atenção em pesquisas futuras, pois desperta interesse de instituições de pesquisa, como a *Oxford Insights,* que constatou que o país é o terceiro na América Latina em termos de preparação para IA. Por outro lado, uma questão de interesse em futuras pesquisas seria compreender o cenário que o colocou em destaque na América Latina a ponto de empresas como a Microsoft tê-lo escolhido para sediar o seu primeiro laboratório de IA fora dos EUA.

Este estudo permitiu compreender como cada jurisdição estudada está propondo sua regulação para a IA, mas esta análise não é exaustiva. A depender do recorte estabelecido, um projeto pode ser incluído ou excluído das análises. Eventualmente, nos deparamos com a dificuldade de classificar um indicador ou outro em uma determinada categoria, uma vez que alguns poderiam ser alocados em mais de uma delas, simultaneamente, requerendo uma categorização flexível.

REFERÊNCIAS

ACCESS NOW (Estados Unidos). **Regulatory Mapping on Artificial Intelligence in Latin America**: regional ai public policy report. Nova York: Access Now, 2024. 90 p. Disponível em:

https://www.accessnow.org/wp-content/uploads/2024/07/TRF-LAC-Reporte-Regional-IA-JUN-2024-V3.pdf. Acesso em: 19 set. 2024.

AGESIC. **AI Strategy for the Digital Government**. Montevideo: [S.E], 2019. 16 p. Disponível em: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/ia-strategy-english-version/ia-strategy-english-version/ai-strategy-for. Acesso em: 03 fev. 2025.

ARGENTINA. Congresso. Senado. Projeto de Lei, de 2023. **Projeto de Lei 2504-D-2023 (Ley de Regulación y Uso de La Inteligencia Artificial En La Educación)**. Buenos Aires, 2023. Disponível em: https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2023/PDF2023/TP2023/2504-D-2023.pdf. Acesso em: 15 jun. 2024.

ARGENTINA. Congresso. Senado. Projeto de Lei, de 2023. **Projeto de Lei 2505-D-2023 (Marco legal para la regulación del desarrollo y uso de la Inteligencia Artificial).** Buenos Aires, 2023. Disponível em: https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2023/PDF2023/TP2023/2505-D-2023.pdf. Acesso em: 7 jun. 2024.

ARGENTINA. Congresso. Senado. Projeto de Lei, de 2023. **Projeto de Lei 1472-D-2023 (Modificación Ley Nacional 25.467)**, Buenos Aires, 2023. Disponível em: https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2023/PDF2023/TP2023/1472-D-2023.pdf. Acesso em: 7 jun. 2024.

BIELBY, J. Information Ethics I: Origins and Evolutions. Being Part One of a four part address of the history of Information Ethics. MA/MLIS. Affiliation: University of Alberta, 2014. Disponível em: https://www.linkedin.com/pulse/20140625225908-299816747-information-ethics-i-origins-and-evolutions/. Acesso em: 11 jun. 2024.

BRASIL. Senado. **Projeto de Lei do Senado Federal nº 2.338 de 2023**. Brasília: Senado Federal, 2023. Disponível em: https://www.linkedin.com/pulse/20140625225908-299816747-information-ethics-i-origins-and-evolutions/. Acesso em: 11 jun. 2024.

CANADÁ. Parlamento. Projeto de Lei. **Bill C-27.** Ottawa: House of commons, 2022. Disponível em: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading. Acesso em: 11 jun. 2024.

CANTEKIN, K. Regulation of Artificial Intelligence Around the World, Law Library of Congress (U.S.). **Global Legal Research Directorate**. Washington, D. C., 2023. Disponível em: https://www.loc.gov/item/2023555920. Acesso em: 7 jun. 2024.

CAPURRO, R. A Liberdade na Era Digital. In.: **Ética da Informação**: Perspectivas e Desafios. Maria Nélida Gonzalez de Gomez; Regina de Barros Cianconi (Orgs.). Niterói: Garamond, 2017. Disponível em: https://www.capurro.de/gonzalezdegomez.pdf. Acesso em: 10 fev. 2024.

COLÔMBIA. Congresso. Projeto de Lei. **Ley Estatutaria No. 200 del 2023 Cámara.** Bogota: congresso, 2023. Disponível em: https://www.camara.gov.co/inteligencia-artificial-1. Acesso em: 11 jun. 2024.

COLÔMBIA. Congresso. Projeto de Lei. **Proyecto de Ley n 059 de 2023.** Bogota: congresso, 2023. Disponível em: https://leyes.senado.gov.co/proyectos/index.php/textos-radicados-senado/p-ley-2023-2024/2964-proyecto-de-ley-059-de-2023. Acesso em: 11 jun. 2024.

D'AGOSTINO, S. 'AI Godfather' Yoshua Bengio: We need a humanity defense organization (entrevista com Yoshua Bengio). **Bullet of the Atomic Scientists**, 2023. Disponível em: https://thebulletin.org/2023/10/ai-godfather-yoshua-bengio-we-need-a-humanity-defense-organization/. Acesso em: 28 jan. 2024.

FRANÇA, William Henrique. **O uso do Twitter por Jair Bolsonaro durante a campanha eleitoral à Presidência da República em 2018**. 2022. 146 f., il. Dissertação (Mestrado em Comunicação) — Universidade de Brasília, Brasília, 2022. Disponível em: http://www.realp.unb.br/jspui/handle/10482/43710. Acesso em: 17 jun. 2024.

GIL, Marisa Adán. Canadá disputa liderança em inteligência artificial. **Época Negócios**, Rio de Janeiro, jul. 2019. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2019/07/canada-disputa-lideranca-de-pesquisas-em-inteligencia-artificial.html. Acesso em: 17 jun. 2024.

HE, Jingjie; DEGTYAREV, Nikita. AI and atoms: How artificial intelligence is revolutionizing nuclear material production. **Bulletin of the Atomic Scientists**, [S.L.], v. 79, n. 5, p. 316-328, 2023. Disponível em: https://thebulletin.org/premium/2023-09/ai-and-atoms-how-artificial-intelligence-is-revolutionizing-nuclear-material/. Acesso em: 26 jan. 2024.

MORAES, Roque. Análise de conteúdo. **Revista Educação**, Porto Alegre, v. 22, n. 37, p. 7-32, 1999.

OCDE. O Brasil na transformação digital: oportunidades e desafios. In: OCDE. **A Caminho da Era Digital no Brasil**. Paris: OECD Publishing, 2020. p. 1-26. Disponível em: https://www.oecd-ilibrary.org/economics/a-caminho-da-era-digital-no-brasil_0d4a61d4-pt;jsessionid=Kip733pUq4m9TGLApNbye_P6B9rsimfrNlgBRDAD.ip-10-240-5-70. Acesso em: 15 jun. 2024.

SALOMÃO FILHO. Por que o Canadá se tornou a Meca da Inteligência Artificial? **Revista Isto É Dinheiro**, [S.L], 2017 Disponível em: https://istoedinheiro.com.br/por-que-o-canada-se-tornou-a-meca-da-inteligencia-artificial/. Acesso em: 17 jun. 2024.

TURING, A. M. Computing Machinery and Intelligence. **Mind**, [S.L.]**,** Vol. 59, n. 236, p. 433–460, 1950. Disponível em: https://academic.oup.com/mind/article/LIX/236/433/986238. Acesso em: 9 jan. 2024.

UNIÃO EUROPEIA. Parlamento Europeu. Atos Legislativos nº 2016/679, de 2016. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**. Bruxelas, 25 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 16 jun. 2024.

UNIÃO EUROPEIA. Comissão Europeia. Projeto de Lei nº2021/0106. **Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.** Bruxelas, 2021. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206. Acesso em: 11 jun. 2024.

UNIÃO EUROPEIA. Comissão Europeia. Projeto de Lei nº 2022/0303. **Proposal for a Directive of the European Parliament and of the Council on Adapting Non-contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive)**. Bruxelas, 2022. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496. Acesso em: 11 jun. 2024.

URUGUAI. Cámara de Senadores. Projeto de Lei. **Regulación de sistemas que utilizan inteligencia artificial**. Montevidéu: Parlamento do Uruguai, 2023. Disponível em: https://parlamento.gub.uy/documentosyleyes/documentos/versiones-taquigraficas/senadores/49/1737/0/PDF. Acesso em: 20 set. 2024.