PARA FILTRAR AS FACES DA IA

Brasil, Canadá e países da Europa elaboram legislação para reduzir os riscos de mau uso de programas e aplicativos dessa área

Sarah Schmidt

Nos últimos meses, representantes do governo dos 27 países da União Europeia, do Canadá e do Brasil trabalharam intensamente para elaborar diretrizes para o uso seguro de programas e aplicativos que utilizam inteligência artificial (IA). O Parlamento europeu aprovou em junho a versão final de um projeto de lei, o AI Act. Caso seja aprovado pelos países-membros, talvez ainda neste ano, pode se tornar a primeira legislação sobre IA do mundo. No Brasil, ao menos quatro projetos de lei (PL) que procuram criar regras sobre o desenvolvimento, a implementação e o uso de sistemas de IA tramitam no Congresso Nacional e devem ser discutidos ainda em 2023.

A tarefa de estabelecer regras para controlar o uso dos programas desse tipo é complexa. A IA incorporou-se à ciência, ao sistema financeiro, à segurança, à saúde, à educação, à propaganda e ao entretenimento, na maioria das vezes sem que o usuário perceba. A regulamentação deveria estabelecer um equilíbrio entre reduzir os riscos de mau uso, evitar a discriminação de grupos minoritários da população e garantir privacidade e transparência aos usuários. Deveria também preservar o espaço da inovação, de acordo com os especialistas entrevistados para esta reportagem. Também não é possível prever todos os riscos que os usos dessas tecnologias podem trazer.

"Permanecer no território da incerteza de regulamentação pode ser prejudicial para os cidadãos", afirma a advogada Cristina Godoy, da Faculdade de Direito de Ribeirão Preto da Universidade de São Paulo (FDRP-USP). Ela é autora de um artigo publicado em outubro de 2022 na *Revista USP* sobre os desafios da regulação da IA no país. No final de setembro, ela deve apresentar em um congresso em Belo Horizonte os resultados iniciais de uma pesquisa sobre o uso de reconhecimento facial, um tipo de IA, para a concessão de empréstimos bancários.

No estudo, realizado no âmbito do Centro de Inteligência Artificial (C4AI) da USP, apoiado por IBM e FAPESP, 90% dos autores de 2,3 mil processos do Tribunal de Justiça do Estado de São Paulo (TJ-SP) não reconhecem os empréstimos aprovados por meio da biometria facial nos aplicativos dos bancos. "As pessoas alegam que não assinaram nenhum documento e não sabiam que estavam contratando o serviço", relata a pesquisadora. Os dados integram o Observatório Brasileiro de Inteligência Artificial, portal desenvolvido com o Núcleo de Informação e Coordenação do Ponto BR (NIC.Br), que deve ser lançado ainda neste ano.

O TJ-SP geralmente dá ganho de causa para os bancos por considerar que a biometria facial é uma forma segura de substituir a assinatura do cliente. Godoy discorda: "É uma tecnologia ainda com alto índice de erro". Para ela, outro problema é que pouco se sabe sobre como esses sistemas operam. "Não há clareza sobre qual empresa é contratada para prestar esse serviço, como ele foi desenvolvido, quais critérios adotam para atestar se é aquela pessoa ou não. Sem essas informações, é difícil para o cidadão contestar os bancos."

O grupo de Godoy também examinou sistemas de reconhecimento facial usados para identificar fraudes em descontos para estudante ou idosos no transporte público de 30 cidades brasileiras com mais de 1 milhão de habitantes. Na maioria delas (60%), o nível de transparência foi considerado muito baixo, já que os municípios não expunham como eram feitos a coleta e o tratamento das informações sobre os usuários de ônibus e trens nem quais parâmetros são usados para detectar fraudes. Os resultados foram publicados em novembro de 2022 nos anais da 11ª Brazilian Conference on Intelligent Systems, realizada em Campinas, interior paulista.

Godoy defende mais transparência nos programas de IA. Mas, para ela, não basta informar se os aplicativos estão usando as ferramentas: é preciso também explicitar como funcionam, como processam as informações e como tomam decisões. Essas informações ajudariam a evitar a discriminação contra grupos vulneráveis.

Um exemplo: pesquisadores da Universidade Federal do Rio Grande do Norte (UFRN) analisaram dados da Rede Observatório da Segurança, que monitorara dados de segurança pública em oito estados. Eles verificaram que 90% das 151 pessoas detidas no país em 2019 com base em câmeras de reconhecimento facial eram negras, como detalhado em um estudo publicado em julho de 2020 na revista *Novos Olhares*.

IMAGEM ALEXANDRE AFFONSO VIA MIDJOURNEY

Imagem gerada pelo programa de IA Midjourney para retratar o conceito de reconhecimento facial

"Ao serem treinados com bases de dados do passado e do presente, os programas de inteligência artificial podem muitas vezes reproduzir ou ampliar padrões de discriminação", avalia o advogado Bruno Ricardo Bioni, diretor da Associação Data Privacy Brasil de Pesquisa e membro do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, órgão consultivo da Autoridade Nacional de Proteção de Dados (ANPD).

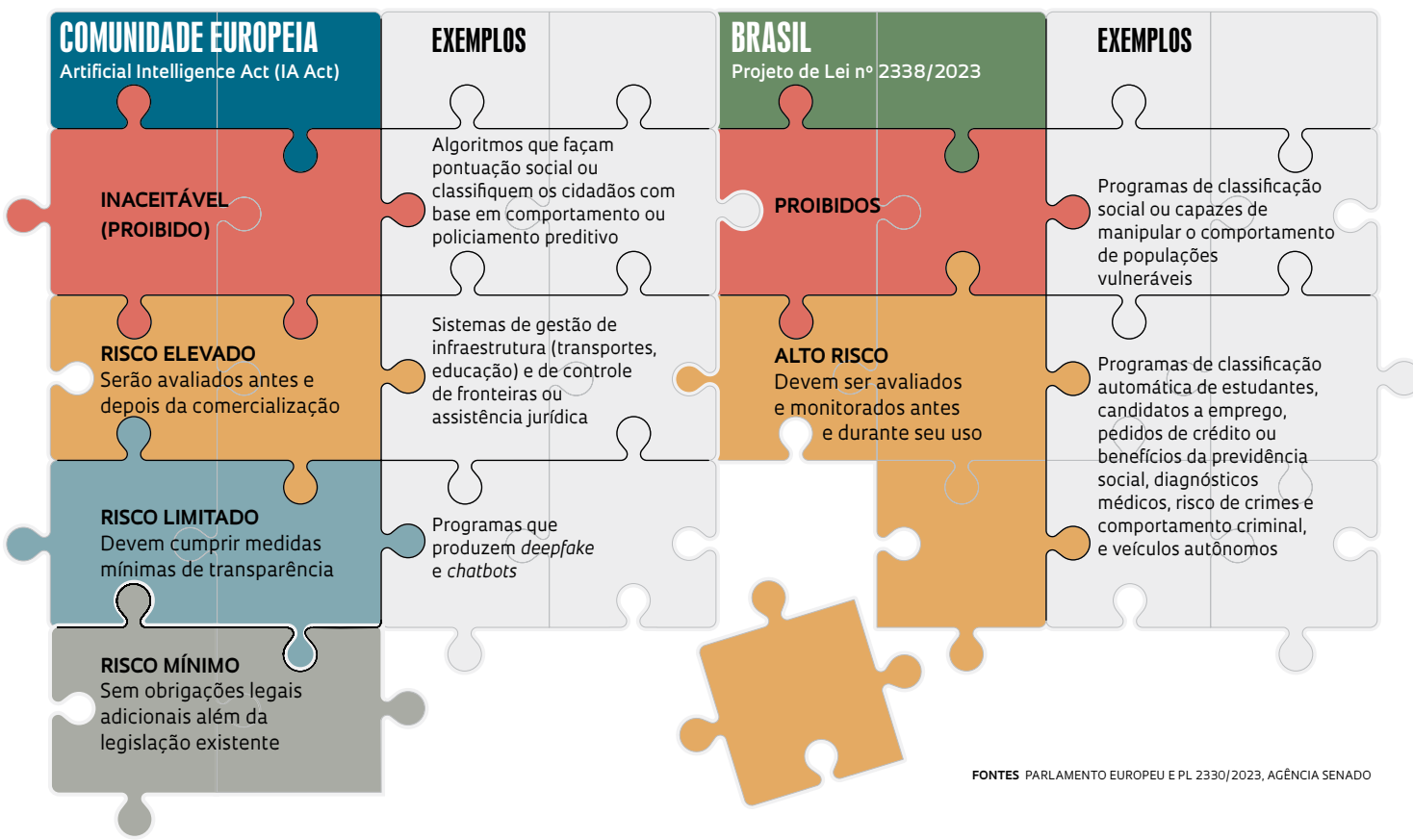
Bioni integrou a comissão de especialistas em direito digital e civil convocada pelo Senado Federal em março de 2022 para analisar os projetos sobre regulamentação de IA. Um deles, o PL 21/20, foi bastante criticado por ser muito genérico. Após nove meses de seminários e audiências públicas, a equipe de juristas apresentou um relatório de 900 páginas com conceitos e sugestões de princípios a serem seguidos. Cerca de 20 páginas serviram de base para outra proposta de PL, o 2338/23, apresentado em maio pelo senador Rodrigo Pacheco (PSD-MG), presidente do Senado. Em julho, o senador Jorge Kajuru (PSB-GO) solicitou ao Senado que os projetos de lei similares, como o 5691/19, o 21/20 e o 2338/23, tramitem juntos. "Agora, espera-se que neste segundo semestre o Parlamento possa avaliar esses projetos em conjunto, usando o 2338/23 como base, para aprovar uma regulamentação para o país", comenta Bioni.

"Não é possível conceber uma proposta de regulação que seja uma bala de prata, igualando a governança para todos os setores", observa o advogado. Segundo Bioni, a solução é criar uma regulamentação que classifique os sistemas de IA de acordo com níveis de risco, a abordagem adotada na legislação europeia, sobre a qual a proposta 2338/23 se estruturou.

O AI Act da União Europeia propõe que os sistemas de IA sejam transparentes, rastreáveis, seguros, não discriminatórios e respeitem a privacidade dos cidadãos, embora as formas de atingir esses objetivos ainda não estejam claras. Os programas também precisarão ser supervisionados por especialistas humanos, para evitar que decisões importantes sejam tomadas inteiramente por uma máquina. As aplicações serão classificadas de acordo com quatro categorias de risco: inaceitável e, portanto, sujeitas à proibição; alto; limitado, passíveis de regras mais brandas; e mínimo, sem obrigações legais adicionais além da legislação existente (*ver infográfico*). Os programas para os carros autônomos, por exemplo, estão na categoria de alto risco.

As aplicações de risco inaceitável incluem os programas de IA que classificam as pessoas com base em comportamentos ou policiamento preditivo para prever delitos. É o caso de algoritmos como o

OS NÍVEIS DE RISCO DA IA NA EUROPA E NO BRASIL



FONTES PARLAMENTO EUROPEU E PL 2330/2023, AGÊNCIA SENADO

AS PROPOSTAS EM ANÁLISE NO PAÍS

O projeto de regulamentação não menciona as IA generativas de uso geral, já que o trabalho dos juristas foi feito antes da liberação do ChatGPT, nem as usadas para criar *deepfakes*. Por isso, é provável que ainda passe por alterações em sua tramitação.

As aplicações que geram conteúdos sintéticos hiper-realistas, como as *deepfakes* de vídeo ou de áudio, são uma preocupação crescente devido à capacidade de gerar desinformação com conteúdos falsos, com potencial para prejudicar os processos democráticos nas eleições.

Um comercial recente de uma fabricante de veículos incluiu uma imagem gerada por *deepfake* da cantora Elis Regina, morta em 1982, cantando com a filha Maria Rita. Em julho, o Conselho Nacional de Autorregulamentação Publicitária (Conar) abriu um processo para investigar o direito de uso de imagem de Elis. A polêmica se estendeu ao Congresso Nacional: ao menos dois projetos de lei (3592/23, no Senado, e o 3614/23, na Câmara dos Deputados) propõem diretrizes para o uso de imagens e áudios de pessoas que já morreram por meio de sistemas de IA.

O advogado Antonio Carlos Morato, da Faculdade de Direito da USP, que pesquisa direito autoral e inteligência artificial, não vê a necessidade de leis específicas para esse tipo de uso: "Sem dúvida, é possível evitar que utilizações não autorizadas ocorram com o que já temos na Constituição Federal, Código Civil e Lei de Direitos Autorais. O Projeto de Lei n° 3614/23, por exemplo, pretende apenas detalhar o que já existe no texto atual do Código Civil".

Para ele, a autorização dos filhos para o comercial da cantora foi válida, uma vez que os direitos da personalidade (que incluem a imagem e a voz) já são protegidos pela Constituição Federal e pelo Código Civil, existindo a possibilidade de sua defesa por parentes até o quarto grau após a morte.

chamado Compas (sigla de Perfis de Gerenciamento de Infratores Correcionais para Sanções Alternativas), usado nos Estados Unidos para prever a chance de acusados voltarem a cometer crimes. Esses programas têm um viés preconceituoso ao indicar mais pessoas negras do que brancas como suspeitas de crimes. Sua transparência é baixa, já que o aplicativo é fornecido por uma empresa privada e seu código não é aberto.

As chamadas IAs generativas, que aprendem a produzir textos novos a partir da análise de padrões usados pelas pessoas para conectar palavras, ganharam uma seção nova na proposta, após a repercussão do ChatGPT, lançado em novembro de 2022. Elas deverão adotar medidas de transparência, deixando claro que seu conteúdo foi gerado por um sistema computacional inteligente, e serem programadas para evitar a criação de conteúdo ilegal nocivo, como fornecer a receita para fabricar uma bomba. Os de risco limitado, como os que criam imagens e conteúdos sintéticos, também precisam adotar requisitos de transparência.

No Brasil, a proposta 2338/23 segue uma lógica parecida, com dois níveis de grau de risco: o excessivo, cujas aplicações serão proibidas; e de alto risco, que deve ser avaliado e monitorado antes e durante seu uso. No primeiro se enquadram os algoritmos que exploram vulnerabilidades sociais ou promovem a classificação de pessoas por parte do Poder Público para acesso a bens e serviços públicos como benefícios sociais, entre outros. As aplicações de alto risco são softwares que podem tomar decisões em áreas como educação, filtrando o acesso às instituições de ensino, trabalho, classificando candidatos a vagas de emprego, saúde, realizando diagnósticos médicos, e previdência, concedendo benefícios de seguridade social, entre outros. Para evitar que o sistema de classificação fique engessado e possa acompanhar um ambiente tecnológico dinâmico, uma futura autoridade fiscalizadora, prevista no projeto, poderá reavaliar o risco de determinada aplicação.

"O PL nº 2338/23 é o mais completo, versando sobre a categorização dos riscos, e observou as tendências legislativas a respeito do tema, em especial as da União Europeia, e, quanto aos níveis de risco, constitui um detalhamento oportuno", avalia o advogado Antonio Carlos Morato, da Faculdade de Direito da USP.

"A proposta europeia com níveis de impacto diferenciados é um modelo interessante para servir de base para a discussão regulatória no país, mas é preciso ponderar que a realidade daqueles países é muito diferente da nossa", observa o cientista da computação Virgílio Almeida, da Universidade Federal de Minas Gerais (UFMG) e coordenador do Centro de Inovação em Inteligência Artificial para a Saúde (CIIA- Saúde), um dos Centros de Pesquisa em Engenharia (CPE) financiados pela FAPESP. "Aqui temos grandes desigualdades sociais e é preciso pensar em políticas públicas que avaliem e incentivem tecnologias automatizadas que não substituam trabalhadores menos qualificados, mas que promovam seu aprimoramento."

Em um artigo publicado em fevereiro na revista científica *IEEE Internet Computing*, ele, com os coautores, propõe um modelo de governança, que chama de corregulação. O governo estabeleceria diretrizes e políticas públicas, cabendo às empresas criar e seguir seu próprios mecanismos internos de governança. "As tecnologias de inteligência artificial mudam muito rapidamente e é difícil dar conta de todas essas transformações com apenas uma lei", pondera.

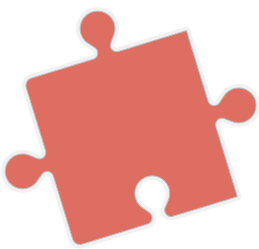
Fabio Gagliardi Cozman, coordenador do Centro de Inteligência Artificial da USP, alerta para o risco de as regras a serem criadas inibirem o empreendedorismo: "Uma regulamentação muito restritiva poderia impedir o desenvolvimento local da inovação e, no fim, as tecnologias teriam de ser importadas", observa.

INFOGRÁFICO ALEXANDRE AFFONSO / REVISTA PESQUISA FAPESP

Também preocupado com o impacto da regulamentação sobre a indústria nacional, o cientista político Fernando Filgueiras, da Universidade Federal de Goiás (UFG), defende: "A legislação deveria estar associada a mecanismos de incentivo à pesquisa e à indústria". Para Filgueiras, sem investimentos na pesquisa e indústria nacional, grandes corporações internacionais podem estar mais estruturadas para lidar com as possíveis sanções, enquanto as pequenas e médias empresas nacionais, com menos recursos, podem ficar para trás. A "Estratégia brasileira de inteligência artificial", que trata de questões éticas para o governo avançar na área, publicada em agosto de 2021 pelo Ministério da Ciência, Tecnologia e Inovação (MCTI), poderia, a seu ver, ser um documento complementar às regras a serem criadas. Mas, como ele observou em fevereiro de 2023 na revista *Discover Artificial Intelligence*, o documento do governo é genérico e não deixa claro como irá se movimentar nessa área e como pretende apoiar as pesquisas em universidades e empresas. Procurado, o MCTI não respondeu aos pedidos de esclarecimentos solicitados por *Pesquisa FAPESP*.

Cristina Godoy, da USP de Ribeirão Preto, observa que a proposta da União Europeia prevê uma avaliação do impacto da IA em pequenas e médias empresas, caso as medidas regulatórias fossem aprovadas, algo que não consta no documento brasileiro. "Conhecendo essa realidade, os governos podem calcular o quanto precisam investir para apoiar a inovação", afirma.

O AI Act prevê os chamados *sandbox* ou ambientes de teste de regulamentação, nos quais startups poderiam pôr à prova suas criações sem sofrer sanções ou multas. No Brasil, o PL nº 2338/23, do Senado, prevê ambientes regulatórios experimentais similares, igualmente fiscalizados por autoridade competente a ser definida. "Esses espaços dificilmente funcionarão de modo satisfatório sem uma visão estratégica do orçamento e das áreas prioritárias a serem apoiadas", alerta. Segundo ela, uma previsão de investimento em quais áreas de IA são mais relevantes pode tornar esse processo mais eficiente para as empresas se organizarem para participar da captação de recursos e, consequentemente, testarem depois seus produtos nesses ambientes *sandbox*. Ela apontou essa lacuna da estratégia nacional em seu artigo da *Revista USP*.



Outro desafio da regulamentação será a fiscalização das instituições públicas e privadas. Os europeus devem criar um órgão específico com essa finalidade. No Brasil, o projeto de lei prevê a constituição de uma autoridade regulatória que, a princípio, deveria dar conta de todas as áreas em que a IA possa ser aplicada. Ela deverá ser indicada pelo Poder Executivo. Especialistas ouvidos para esta reportagem veem uma movimentação da ANPD, que recentemente se tornou uma autarquia, para absorver essa função.

Godoy considera esse caminho arriscado. A permeabilidade das aplicações de IA, que estão em setores distintos da economia, tornaria a tarefa complicada se ela se concentrasse em apenas um órgão. "É difícil que ela reúna todas as expertises necessárias, passando da saúde à educação", diz.

Especialista nos impactos éticos e sociais da IA, Dora Kaufman, da Pontifícia Universidade Católica de São Paulo (PUC-SP), observa que a constituição de uma agência nacional de regulamentação talvez seja inviável e sugere que agências setoriais poderiam assumir essa missão – o Banco Central (Bacen) poderia cuidar do setor bancário e a Agência Nacional de Vigilância Sanitária (Anvisa) da saúde.

"Nos Estados Unidos não existe nem parece iminente uma regulamentação federal", ela comenta. "A autoridade e a responsabilidade pela regulamentação e governança de IA são distribuídas entre as agências federais." Os dois documentos que regem essa área – o "Blueprint for an AI bill of rights", da Casa Branca, e "NIST risk management framework", do Instituto Nacional de Padrões e Tecnologia – são de orientação voluntária, sem força de lei.

O cientista da computação André Carlos Ponce de Leon Carvalho, do Instituto de Ciências Matemáticas e de Computação (ICMC) da USP, em São Carlos, levanta outra dúvida: "Será que uma regulação nacional dará conta do problema ou os países precisarão de acordos internacionais, como foi feito com a energia nuclear?".

Os especialistas alertam que qualquer regulamentação precisará de um tempo de maturação para que os parlamentares conheçam melhor o assunto e outros setores da sociedade passem a participar dos debates. "A regulamentação prematura pode restringir a inovação e não proteger a sociedade", ressalta Kaufman. "O processo é tão importante quanto o resultado final." Como exemplos a serem lembrados, ela cita o Marco Civil da Internet, aprovado em abril de 2014 após discussões abertas que começaram em 2009, e o processo europeu de regulamentação da IA, cuja consulta pública começou em abril de 2021. ■

Os projetos e os artigos científicos consultados para esta reportagem estão listados na versão on-line.