



CÂMARA DOS DEPUTADOS

PROJETO DE LEI N.º 1.969, DE 2021

(Do Sr. Gustavo Fruet)

Dispõe sobre os princípios, direitos e obrigações na utilização de sistemas de inteligência artificial.

DESPACHO:

APENSE-SE À(AO) PL-21/2020.

APRECIÇÃO:

Proposição Sujeita à Apreciação Conclusiva pelas Comissões - Art. 24 II

PUBLICAÇÃO INICIAL

Art. 137, caput - RICD

PROJETO DE LEI Nº , DE 2021

(Do Sr. GUSTAVO FRUET)

Dispõe sobre os princípios, direitos e obrigações na utilização de sistemas de inteligência artificial.

O Congresso Nacional decreta:

Art. 1º Esta Lei dispõe sobre princípios, direitos e obrigações para sistemas de inteligência artificial - IA.

Art. 2º Para os fins desta Lei, considera-se:

I – usuário: qualquer pessoa natural ou jurídica, pública ou privada, que utiliza sistema de IA, exceto quando o uso ocorrer em atividades não profissionais;

II – sistema de IA: software desenvolvido com capacidade de, em vista de objetivos determinados por pessoa natural, gerar conteúdos, previsões, recomendações ou decisões que influenciam o ambiente em que interage;

III – provedor: pessoa natural ou jurídica, de direito público ou privado, que desenvolva sistemas de IA ou possua um sistema de IA desenvolvido com o objetivo de disponibilizá-lo no mercado ou utilizá-lo diretamente;

IV – dado biométrico: dado pessoal resultante de técnicas específicas de tratamento relacionadas a características físicas, psicológicas ou comportamentais da pessoa natural, que permitem a identificação dessa pessoa;



Assinado eletronicamente pelo(a) Dep. Gustavo Fruet

Para verificar a assinatura, acesse <https://infoleg-autenticidade-assinatura.camara.leg.br/CD216213500300>



V – sistema de reconhecimento de emoções: sistema de IA que identifica ou infere emoções e intenções da pessoa natural com base em dados biométricos.

Art. 3º Provedores que desenvolvem sistemas de inteligência artificial deverão observar a boa-fé e os seguintes princípios:

- I – responsabilidade e prestação de contas;
- II – explicabilidade;
- III – auditabilidade;
- IV – precisão;
- V – equidade.

Art. 4º Ficam vedadas a disponibilização para o mercado ou a utilização direta de sistemas de IA que:

I – empreguem técnicas subliminares que distorçam o comportamento de uma pessoa natural, de maneira a causar nelas ou em terceiros danos físicos ou psicológicos;

II - explorem as vulnerabilidades de grupos específicos de pessoas, seja em função da idade ou da condição física ou mental;

III – sejam usados, por parte do Poder Público, para aferir ou classificar a confiabilidade de pessoa natural baseando-se em seu comportamento social ou em práticas preditivas e que resultem em sistema de escore social de recompensas e punições;

IV – utilizem sistemas de identificação remota por meio de dados biométricos em tempo real e em espaços públicos para fins de segurança pública e atividades de investigação e repressão de infrações penais, a não ser:

- a) que vítimas de crimes em potencial sejam o alvo do sistema de IA, incluindo crianças perdidas;
- b) para a prevenção de uma ameaça específica, substancial e iminente para a vida ou segurança de pessoas naturais;
- c) para a prevenção de ações de terrorismo;



d) para a identificação, localização e persecução de suspeito de ofensa criminal punível com, no mínimo, pena de reclusão.

Art. 5º Provedores de IA que utilizam reconhecimento de emoções devem informar ao usuário pessoa natural, de forma destacada, a utilização desta técnica e permitir sua eventual desativação, a pedido do usuário.

Art. 6º A União criará uma lista de sistemas de IA de alto risco, que deverão ser certificados, diretamente pelo órgão público competente ou por terceiros credenciados.

§ 1º Na elaboração da lista referida no caput, levar-se-á em conta os riscos à saúde e à segurança, os impactos sobre direitos fundamentais do usuário, a probabilidade de ocorrência de incidente de segurança e a possibilidade de reversão do resultado danoso.

§ 2º A utilização de sistemas de IA de alto risco obrigam a implementação de um sistema de gerenciamento de riscos a ser estabelecido pelo órgão competente, que deve contemplar, pelo menos:

I – a identificação e análise dos riscos conhecidos e possíveis associados ao sistema de IA de alto risco;

II – a estimação e a avaliação dos riscos que podem potencialmente surgir quando o sistema de IA de alto risco é utilizado fora dos padrões;

III – a adoção de um programa de gerenciamento de riscos compatível e proporcional aos riscos envolvidos.

Art. 7º Caberá ao órgão competente mencionado no art. 6º a regulação e fiscalização do disposto nesta lei.

Art. 8º A infração desta lei ou das demais normas aplicáveis sujeitam os provedores de IA às seguintes sanções administrativas, aplicáveis pelo órgão competente, sem prejuízo das de natureza civil e penal:



I – advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até R\$ 50.000,00 (cinquenta mil reais) para pessoas naturais e de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração, após devidamente apurada e confirmada a sua ocorrência;

V - suspensão parcial ou total do sistema de IA a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

VI - proibição parcial ou total do exercício de atividades relacionadas a sistemas de IA.

Art. 9º Na aplicação das sanções serão considerados a natureza e a gravidade da infração, os danos dela resultantes para os usuários, a vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência específica.

Art. 10 Esta lei entra em vigor no prazo de 24 (vinte e quatro) meses após a data de sua publicação.

JUSTIFICAÇÃO

A inteligência artificial – IA – é uma tecnologia que veio para revolucionar a forma como interagimos com as máquinas. Seja no campo da saúde, com auxílio a cirurgias ou decisões no quadro clínico dos pacientes; seja na segurança pública, com a possibilidade de sistemas de reconhecimento facial; seja no trabalho, na administração da justiça; ou nos serviços de transporte. A IA veio para ficar.

Assinado eletronicamente pelo(a) Dep. Gustavo Fruet

Para verificar a assinatura, acesse <https://infoleg-autenticidade-assinatura.camara.leg.br/CD216213500300>



Por outro lado, embora as aplicações dessa tecnologia tenham enormes benefícios, há também riscos consideráveis. O tratamento automatizado de dados pode resultar, por exemplo, em discriminações ilícitas, técnicas abusivas de *geopricing* e *geoblocking*, reconhecimento facial e policiamento preditivo, que atentam contra direitos fundamentais. Tudo isso pode resultar, portanto, em sérios abusos nas atividades que exploram IA.

Por isso, é necessário, de um lado, que haja uma forte política pública de estímulo ao desenvolvimento da IA no Brasil, nos moldes do que foi feito, ainda que imperfeitamente, por meio da Estratégia Brasileira de Inteligência Artificial. Mas, de outro, é também imperioso que haja uma regulação sobre os atores de mercado de IA a fim de balizar e orientar o uso ético e resguardar o interesse público nas aplicações de IA.

Inspirados na proposta de regulação da IA da Comissão Europeia, a presente proposta legislativa procura justamente delinear os princípios, direitos e obrigações a serem seguidos pelos sistemas de inteligência artificial – IA – no Brasil.

Primeiro, consideramos como usuário de IA toda a pessoa natural ou jurídica, pública ou privada, que utiliza sistema de IA, exceto quando o uso ocorrer em atividades não profissionais. Diferente da proteção prevista aos titulares na Lei Geral de Proteção de Dados Pessoais, LGPD, que se restringe à proteção da pessoa natural, entendemos que se deve proteger não apenas a pessoa física, mas também a pessoa jurídica.

Nas definições de sistema de IA, dado biométrico e sistema de reconhecimento de emoções adaptamos noções semelhantes às da proposta europeia. O mesmo se deu na definição de provedor, que visa incluir pessoas que desenvolvem sistemas de IA ou que têm o objetivo de disponibilizá-lo no mercado ou utilizá-lo diretamente. Essa definição ampla de provedor pretende



estender a abrangência da incidência da proposta para toda a cadeia de desenvolvedores e comerciantes de produto e serviços que desenvolvem IA.

Quanto aos princípios aplicáveis aos provedores que desenvolvem sistemas de inteligência artificial, enumeramos os seguintes: (i) responsabilidade e prestação de contas, que aloca o dever de adoção de medidas eficazes e capazes de cumprir as normas atinentes ao mercado de IA; (ii) explicabilidade, que procura evitar a opacidade do provedor em oferecer explicações e justificar os resultados advindos da decisão algorítmica do sistema de IA; (iii) auditabilidade, que torna obrigatória a validação ou averiguação dos passos tomados pelo sistema de IA para alcançar os resultados pretendidos, inclusive para fins de fiscalização pelo Poder Público; (iv) precisão, de modo a evitar-se o falseamento de informações inseridas ou conclusões resultantes de sistemas de IA; e (v) equidade, a fim de se proibir tratamentos com vieses discriminatórios.

Umas das maiores preocupações da presente iniciativa foi o estabelecimento de limites para a utilização da IA. Especialmente quando tal uso colocasse em risco direitos fundamentais. Em tais casos, propusemos a vedação da disponibilização para o mercado em geral ou mesmo a utilização direta de sistemas de IA pelas próprias empresas, ainda que o produto de IA não fosse publicamente oferecido ao mercado, em algumas hipóteses.

A primeira dessas hipóteses é quando houvesse o emprego de técnicas subliminares que distorcessem o comportamento de uma pessoa natural, de maneira a causar nelas ou em terceiros danos físicos ou psicológicos. A economia comportamental é uma ciência que tem avançado muito nos últimos anos e, se usada indiscriminadamente, pode trazer prejuízos significativos à liberdade e autonomia privada das pessoas.



Em segundo lugar, vedamos o uso de sistemas de IA que visam à exploração das vulnerabilidades de grupos específicos de pessoas, seja em função da idade ou da condição física ou mental. De fato, a sociedade da informação e o uso intensivo da tecnologia tornam determinados grupos mais suscetíveis às manipulações de um sistema de IA, como crianças e idosos. Por isso, entendemos oportuna a restrição da amplitude do rol de possibilidades em que tais sistemas podem operar quando lidam diretamente com esse público.

Em terceiro, determinamos a proibição do uso de sistemas de IA, por parte do Poder Público, com a finalidade de aferir ou classificar a confiabilidade de pessoas naturais tomando como base o seu comportamento social ou por meio de mecanismos preditivos dos quais resultem um sistema de score social de recompensas e punições. A ideia é que o Estado não possa empregar sistemas de IA que utilizem elementos subjetivos e da personalidade dos cidadãos como forma de criar meios que instituem pontuações ou notas e que acarretem em ferramentas de recompensas e punições.

Por fim, estabelecemos restrições para sistemas de IA que lancem mão de mecanismos de identificação remota que utilizem dados biométricos, em tempo real e em espaços públicos para fins de segurança pública e atividades de investigação e repressão de infrações penais. O objetivo é impedir que, sob o pretexto de garantir a segurança pública à população, o Estado simplesmente promova a disseminação de câmeras de reconhecimento facial ou de sistemas que tratem dados biométricos em espaços públicos, de forma abusiva. Muitas vezes o Poder Público pode praticar monitoramento remoto para causas menores ou insignificantes, que não justificam a devassidão que essas tecnologias invasivas podem causar na vida do cidadão.

Em relação a esta última vedação, trouxemos algumas exceções. A primeira delas é o caso em que o alvo do sistema de vigilância são

Assinado eletronicamente pelo(a) Dep. Gustavo Fruet

Para verificar a assinatura, acesse <https://infoleg-autenticidade-assinatura.camara.leg.br/CD216213500300>



vítimas de crimes em potencial, incluindo crianças perdidas ou casos de sequestro, por exemplo. O segundo caso é o da prevenção a uma ameaça específica, substancial e iminente para a vida ou segurança de pessoas naturais. O terceiro engloba ações de contenção de terrorismo. Por óbvio, quando o risco for significativo e iminente, prevalecem o direito à vida e à integridade física das pessoas sobre o direito à proteção de dados e à privacidade. A quarta e última exceção é o caso em que se busca a identificação, localização e persecução de suspeito de ofensa criminal punível com, no mínimo, pena de reclusão. São casos de suspeitos mais perigosos, que justificam, mais uma vez, o uso de sistemas de IA invasivos para a preservação de direitos importantes.

Em todas essas hipóteses, o sopesamento entre a invasão da privacidade e os valores que se buscam defender justifica o uso de sistemas de IA que tratam dados biométricos em espaços públicos. Para estes casos, assim como na proposta de legislação europeia, propusemos que haja um critério de transparência máxima, para que a pessoa saiba exatamente o que esperar quando se deparar com esse tipo de IA.

Um dos problemas fundamentais é o da adoção de sistemas de IA que trazem um alto risco para a sociedade. Para estes casos, determinamos que a União deverá criar uma lista técnica que contemple sistemas de IA de alto risco, que deverão ser certificados diretamente pelo órgão público competente ou por terceiros credenciados.

O objetivo é criar um órgão ou atribuir a um órgão já existente da União uma estrutura que possa supervisionar e fiscalizar o cumprimento do disposto na presente proposta e a quem caberá, também, a criação dessa lista que compreenda os sistemas de IA de alto risco. Para a elaboração da lista de sistema de IA de alto risco, o órgão competente deve considerar, minimamente, os riscos à saúde e à segurança, os impactos sobre direitos fundamentais do



usuário, a probabilidade de ocorrência de incidente de segurança e a possibilidade de reversão do resultado danoso.

Estabelecemos, ainda, que a utilização de sistemas de IA de alto risco obriga a implementação de um sistema de gerenciamento de riscos a ser balizado pelo órgão competente, e que deve contemplar, pelo menos: (i) a identificação e análise dos riscos conhecidos e possíveis associados ao sistema de IA de alto risco; (ii) a estimação e avaliação dos riscos que podem potencialmente surgir quando o sistema de IA de alto risco é utilizado fora dos padrões; e (iii) a adoção de um programa de gerenciamento de riscos compatível e proporcional aos riscos envolvidos.

Quanto às sanções administrativas que poderão ser aplicadas pelo órgão competente, estão a da advertência, com indicação de prazo para adoção de medidas corretivas e a de multa simples, de até R\$ 50.000,00 (cinquenta mil reais) para pessoas naturais e de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração.

No que se refere aos valores das multas, os consideramos razoáveis, tendo em vista que a proposta de regulação da União Europeia define um valor de até 30 mil euros para pessoas naturais e de até 6% do faturamento bruto anual mundial da empresa, para os casos mais graves, e de 4% para casos menos graves. O percentual de faturamento previsto é o mesmo da LGPD.

Previmos também sanções de multas diárias, observado o limite total previsto para a multa simples, a publicização da infração após devidamente apurada e confirmada a sua ocorrência.

Por fim, propusemos também sanções de suspensão parcial ou total do sistema de IA a que se refere a infração pelo período máximo de 6

Assinado eletronicamente pelo(a) Dep. Gustavo Fruet

Para verificar a assinatura, acesse <https://infoleg-autenticidade-assinatura.camara.leg.br/CD216213500300>



(seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador, e de proibição parcial ou total do exercício de atividades relacionadas a sistemas de IA.

Reconhecemos a gravidade destas últimas medidas sancionatórias, mas as entendemos necessárias, tendo em vista que, assim como ocorre no Marco Civil da Internet e na Lei Geral de Proteção de Dados Pessoais, muitas empresas não faturam seus serviços em território brasileiro, tornando inócuas as sanções de multa, por exemplo.

Por fim, preceituamos que, por ocasião da aplicação das sanções administrativas, o órgão competente deverá levar em consideração a natureza e a gravidade da infração, os danos dela resultantes para os usuários, a vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência específica.

As possibilidades trazidas por sistemas de IA certamente trarão consideráveis benefícios para a economia e para a qualidade de serviços públicos e privados, com ganhos de produtividade e eficiência alocativa. Para que tenhamos um ambiente propício a esse desenvolvimento, com proteção ao cidadão e segurança jurídica, sem excessos regulatórios, é que apresentamos este projeto de lei.

Sala das Sessões, em de de 2021.

Deputado GUSTAVO FRUET

2021-3721



Assinado eletronicamente pelo(a) Dep. Gustavo Fruet
Para verificar a assinatura, acesse <https://infoleg-autenticidade-assinatura.camara.leg.br/CD216213500300>



LEGISLAÇÃO CITADA ANEXADA PELA
Coordenação de Organização da Informação Legislativa - CELEG
Serviço de Tratamento da Informação Legislativa - SETIL
Seção de Legislação Citada - SELEC

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018

Lei Geral de Proteção de Dados Pessoais
 (LGPD) ([*Ementa com redação dada pela Lei nº 13.853, de 8/7/2019*](#))

O PRESIDENTE DA REPÚBLICA

Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. ([*Parágrafo único acrescido pela Lei nº 13.853, de 8/7/2019*](#))

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

- I - o respeito à privacidade;
- II - a autodeterminação informativa;
- III - a liberdade de expressão, de informação, de comunicação e de opinião;
- IV - a inviolabilidade da intimidade, da honra e da imagem;
- V - o desenvolvimento econômico e tecnológico e a inovação;
- VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
- VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

- I - a operação de tratamento seja realizada no território nacional;
- II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou ([*Inciso com redação dada pela Medida Provisória nº 869, de 27/12/2018, convertida na Lei nº 13.853, de 8/7/2019*](#))

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

FIM DO DOCUMENTO