[B/Luz] Estudo IA - Comissão Senado

Fernando Bousso | Baptista Luz Advogados <fernando@baptistaluz.com.br>

sex 10/06/2022 11:51

Para: CJSUBIA <CJSUBIA@senado.leg.br>;

Cc: Odélio Porto Júnior | Baptista Luz Advogados <odelio@baptistaluz.com.br>;

1 anexo

BLUZ-v01-Comissão IA_2022.04.29_PR_V2.pdf;

Prezados, bom dia.

Encaminhamos anexa a nossa contribuição para a Comissão responsável pelo PL sobre IA.

Abraços,
Fernando | Odélio

b/luz

Fernando Bousso
/ Partner

Tel. +55 11 3040 7050
Cel. +55 11 99200 8587
baptistaluz.com.br

Regulamentos sobre IA nos EUA, União Europeia e China
–
Análise Comparada
(Baptista Luz Advogados)

Autores:
Dandara Ramos Silvestre da Silva
Ananda Fernandes Garcia
Matheus Botsman Kapustis
Fernanda Catão de Carvalho
Odélio Porto Júnior

Revisão Técnica:
Fernando Bousso
Paula de Moura Corte Real

SUMÁRIO

1) INTRODUÇÃO

Este estudo analisa as principais normas e projetos de lei sobre regulação de algoritmos de inteligência artificial (IA) nos Estados Unidos, União Europeia (EU), e China, para auxiliar a comissão de juristas instaurada pelo Senado na elaboração do projeto de regulação de IA para o Brasil.

2) METODOLOGIA

Este estudo foi desenvolvido sob um viés de direito comparado, com análise descritiva dos textos normativos em sua versão original e/ou traduzida para o inglês. Conjuntamente, foi realizada revisão da literatura científica sobre as normas e projetos de lei analisados.

3) NORMAS E PROJETOS DE LEI SOBRE IA – EUA, UE e CHINA

3.1) Estados Unidos

Atualmente, os Estados Unidos possuem diversos projetos de lei – tanto na esfera federal quanto na estadual – que buscam regular o desenvolvimento e o uso de inteligência artificial.[1] Por exemplo, para o ano de 2021, a Conferência Nacional das Legislaturas Estaduais (*National Conference of State Legislatures*) contabilizou 33 leis /projetos de leis estaduais que, em graus variados, regulavam o uso de IA.[2]

Apesar da abundância legislativa, alguns se destacam em decorrência do seu escopo e jurisdição. Na esfera estadual merece destaque o "*Automated Decision Systems Accountability Act*" apresentado ao Senado da Califórnia em dezembro de 2020. Já na esfera federal, destaca-se o "*Algorithmic Accountability Act*", apresentado à Câmera de Deputados do Congresso dos Estados Unidos em fevereiro 2022. Abaixo serão analisados em maior detalhe esses projetos de lei.

3.1.1. California - Automated Decision Systems Accountability Act

O "*Automated Decision Systems Accountability Act*" é um projeto de lei que busca implementar procedimentos a serem seguidos pelos órgãos do poder público na contração de bens ou serviços que envolvam o uso, licenciamento ou desenvolvimento de um sistema de tomada de decisão automatizado para aplicação de alto risco.[3]

De acordo com o projeto de lei, quando da abertura de licitação para contratação de bens ou serviços que utilizem decisões automatizadas, toda e qualquer agência do estado da California deve encorajar o fornecedor interessado a submeter relatório de análise de impacto do sistema de tomada de decisões automatizado.[4]

As seguintes informações devem estar contidas no relatório: (i) nome, fornecedor, versão do sistema de decisão automatizado e descrição dos seus recursos e limitações; (ii) descrição da finalidade do sistema de decisão automatizado; (iii) explicação completa de como o sistema de decisão automatizado funciona, a relação lógica entre inputs e outputs de dados, e como esses outputs se relacionam com a decisão tomada pelo

---

[1] NCSL. Legislation Related to Artificial Intelligence. 2021. Disponível em: <https://bit.ly/3P04Vi5>. Acesso em 02/05/2022.

[2] *Ibidem.*

[3] ESTADOS UNIDOS. Automated Decision Systems Accountability of 2021. Legislatura Estadual da California. Disponível em: <https://bit.ly/3FrghHM>. Acesso em 02/05/2022.

[4] *Ibidem*, artigo 12115.5.

sistema; (iv) descrição das medidas proativamente tomadas pelo fornecedor para a condução de testes de avaliação do sistema, para análise dos riscos à privacidade e das consequências resultantes de decisões imprecisas, injustas, ou discriminatórias que afetem pessoas físicas; (v) descrição dos possíveis impactos aos direitos civis dos afetados pelas decisões; (vi) descrição de quaisquer políticas internas que o fornecedor tenha adotado para identificar possíveis impactos negativos do sistema; (vii) descrição das melhores práticas adotadas pelo fornecedor com fins de evitar ou minimizar impactos negativos do sistema; e (viii) qualquer informação adicional solicitada pela agência contratante.[5]

Ainda, os fornecedores devem incluir em seu relatório de avaliação do sistema de decisão automatizada, a ser enviado ao Departamento de Tecnologia do governo da California, as seguintes informações:

> "qual o nível de acesso do público a explicações sobre as decisões tomadas pelo sistema, o que inclui a forma como o sistema toma decisões em termos compreensíveis para um leigo; qual a capacidade do fornecedor de corrigir ou invalidar os resultados obtidos; e como essas informações serão disponibilizadas ao público e quais são os procedimentos disponibilizados para correções ou invalidações."[6] (tradução nossa)

3.1.2. Algorithmic Accountability Act of 2022

No âmbito federal o projeto de lei de destaque nos Estados Unidos é o "*Algorithmic Accountability Act*", que busca regular de forma geral as atividades de empresas privadas no desenvolvimento, venda e uso de algoritmos de decisão automatizada.[7] Tendo, portanto, um enfoque mais amplo que o projeto de lei da Califórnia, que se limita a regular a contratação de sistemas automatizados.

Em síntese, o projeto de lei obriga que tanto as empresas responsáveis pela tomada de decisões automatizadas quanto as empresas que criaram a tecnologia conduzam análises de impacto referentes à eficácia, transparência e integridade do processo de tomada de decisão, bem como do sistema de inteligência artificial. De acordo com o "*Algorithmic Accountability Act,*" recairá sobre a Federal Trade Commission (FTC), agência regulatória federal para proteção da concorrência e dos direitos do consumidor, a obrigação de criar regulamentos específicos sobre o tema, tendo como base as diretrizes gerais estabelecidas pelo projeto de lei.

Atualmente, não existe uma única autoridade federal responsável por fiscalizar o uso de inteligência artificial por empresas. No entanto, diversas agências federais já se pronunciaram no sentido de invocar a sua competência para atuação em áreas específicas envolvendo IA, como o Consumer Financial Protection Bureau e a Equal Employment Opportunity Comission.[8]

Assim, caso o "*Algorithmic Accountability Act*" seja aprovado pelo Congresso, a FTC passará a exercer maior poder sobre o tema de inteligência artificial, uma vez que, além de criar regulamentações e diretrizes, ela terá competência para fiscalizar e executar o cumprimento das regras ali dispostas.[9]

---

[5] *Ibidem*.

[6] *Ibidem*, artigo 12116(a)

[7] ESTADOS UNIDOS. Algorithmic Accountability Act of 2022. Washington DC: United States Congress. Disponível em: <https://bit.ly/3LToLd4>. Acesso em 03/05/2022.

[8] GIBSON DUNN. Artificial Intelligence and Automated Systems Annual Legal Review. 2021. Disponível em: < https://bit.ly/37wMvoq>. Acesso em 03/05/2022.

[9] Seção 9(a), *Algorithmic Accountability Act* of 2022.

Apesar de ser de competência da FTC regulamentar a condução de análises de impacto do uso de inteligência artificial para a tomada de decisões automatizadas, o "*Algorithmic Accountability Act*" fornece os requisitos fundacionais das análises, conforme detalhado abaixo.

/ Revisão de processos já existentes

A Seção 4(a)(1) estabelece que no caso da criação de um novo processo de tomada de decisão automatizada, é necessário avaliar se existem outros processos anteriormente implementados para a tomada da mesma decisão. Com isso, a lei busca garantir uma efetiva melhoria nos processos, uma vez que as empresas se veem obrigadas a analisar as nuances dos processos anteriores de forma comparada (e.g., falhas, possíveis prejuízos, benefícios, finalidade etc.).

/ Consultas com terceiros interessados

A Seção 4(a)(2) solicita que na realização de avaliações de impacto do algoritmo, a empresa descreva eventuais consultas que realize com os stakeholders/terceiros interessados (por exemplo, sociedade civil, universidades, etc).

/ Testes e avaliações

A Secão 4(a)(3) estabelece a obrigatoriedade da realização de testes e avaliações dos possíveis riscos à privacidade e das medidas implementadas para mitigação e/ou eliminação desses riscos. De acordo com essa seção, tais testes devem ser baseados nas melhores práticas indicadas pelo National Institute of Standards and Technology (NIST), ou por outros órgãos competentes do governo dos Estados Unidos.

Ainda, a Seção 4(a)(4) estabelece a obrigatoriedade de realizar testes e avaliações referentes à performance do sistema e ao processo de tomada de decisões automatizadas. Especificamente, essa seção buscou destacar a importância da análise da existência de possíveis diferenças em performance que possam ser associadas à raça, cor, gênero, idade, deficiência, religião, e status familiar ou socioeconômico.

/ Treinamento de empregados

A Seção 4(a)(5) estabelece a realização de treinamentos com empregados e quaisquer terceiros envolvidos no processo de tomada de decisões automatizadas em relação a sistemas de decisão similares que tenham gerado impactos negativos nos consumidores.

/ Documentação

As Seções 4(a)(7), (10) e (12) dizem respeito às obrigações de manutenção de documentações referentes aos processos e sistemas de tomada de decisões automatizadas.

Dentre as informações a serem documentadas, destacam-se (i) a metodologia pela qual a empresa coletou as informações utilizadas; e (ii) a obtenção ou não de consentimento por parte dos consumidores para a coleta e o uso dos seus dados.[10]

Ainda, é necessário indicar, caso haja, eventual análise de risco do sistema de decisões automatizadas que ainda esteja em andamento.[11]

Finalmente, empresas devem documentar informações pormenorizadas sobre o descumprimento de qualquer requisito estabelecido pelo projeto de lei na Seção 4(a), registrando a causa desse descumprimento.[12]

---

[10] Seções 4(a)(7)(iii), *Algorithmic Accountability Act* of 2022.
[11] Seções 4(a)(10), *Algorithmic Accountability Act* of 2022.
[12] Seções 4(a)(12), *Algorithmic Accountability Act* of 2022.

/ Avaliação dos direitos dos consumidores
A Seção 4(a)(8) obriga que as empresas avaliem se os direitos dos consumidores estão sendo respeitados. Tais direitos incluem: (i) informações claras sobre o uso de sistema ou processo de tomada de decisões automatizado; e (ii) fornecimento de mecanismo para que o consumidor possa optar por não ter decisões sobre si realizadas de forma automatizada.

Ainda, essa avaliação deve incluir a análise do nível de transparência do sistema/processo e até que ponto o consumidor pode contestar, corrigir ou apelar uma decisão automatizada, ou efetivamente optar por não fazer parte do processo de tomada de decisões automatizadas.

/ Identificação de impactos negativos
A Seção 4(a)(9) estabelece a obrigatoriedade de identificar qualquer impacto negativo relevante que o sistema ou processo de decisão automatizada pode ter nos consumidores e analisar métodos de mitigação aplicáveis.

/ Melhorias no processo ou sistema
A Seção 4(a)(11) estabelece que na elaboração da avaliação de impacto do sistema devem ser identificados mecanismos para melhoria do sistema. Como exemplo, são citados quaisquer recursos, ferramentas, padrões, conjuntos de dados, protocolos de segurança, melhorias no fomento a participação dos stakeholders interessados nas consequências das decisões automatizadas, ou outros recursos que possam ser benéficos para melhorar o sistema nas seguintes áreas: (i) desempenho, incluindo precisão, robustez e confiabilidade; (ii) integridade, incluindo ausência de viés discriminatório; (iii) transparência, explicabilidade, contestabilidade e oportunidade de recurso; (iv) privacidade e segurança; (v) segurança pessoal e pública; (vi) eficiência e pontualidade; e (vii) custo.

Finalmente, o "*Algorithmic Accountability Act*" estabelece **(i)** a obrigatoriedade do compartilhamento dos relatórios referentes à condução de análises de impacto com a FTC;[13] **(ii)** a publicação por parte da FTC de relatório anual contendo informações agregadas e anonimizadas sobre tendências na tomada de decisões automatizadas e o estabelecimento de um repositório de informações onde consumidores e terceiros interessados possam revisar quais decisões críticas foram automatizadas pelas empresas;[14] e **(iii)** o fornecimento de verba à FTC para a contratação de 50 funcionários e a criação de um "*Bureau of Technology*" para fazer cumprir os dispositivos do projeto de lei e apoiar a FTC nos aspectos tecnológicos de suas funções.[15]

3.2) União Europeia

3.2.1) AI Act nº 52021

Após cerca de três anos de estudos e consultas públicas, em abril de 2021, a Comissão Europeia colocou em pauta a sua proposta de regulamentação sobre a utilização e desenvolvimento de sistemas de inteligência artificial, o Artificial Intelligence Act ("AI Act").[16] O Projeto de lei tem como principais objetivos garantir que os sistemas de IA colocados no mercado da União Europeia sejam seguros e respeitem a legislação em

[13] Seção 5, *Algorithmic Accountability Act* of 2022.
[14] Seção 6, *Algorithmic Accountability Act* of 2022.
[15] Seção 8, *Algorithmic Accountability Act* of 2022.
[16] UNIÃO EUROPEIA. AI Act - COM/2021/206. Comissão Europeia. 2021. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52021PC0206#footnote3> Acesso em: 02/05/2022.

vigor em matéria de direitos fundamentais e valores da União, além de, garantir a segurança jurídica para facilitar os investimentos e a inovação no domínio de IA.

/ Principais características

Uma das principais característica do AI Act é adotar uma abordagem baseada em risco mais complexa, trocando a categorização binária de risco (alto risco/sem risco) por uma abordagem mais refinada[17]. Para isso, realiza a diferenciação entre sistemas de IA que criam:

i) um risco inaceitável, sendo proibidos;
ii) um risco elevado, sendo sujeitos a maiores regras;
iii) um risco limitado, para os quais a proposta estabelece apenas a necessidade de transparência; e
iv) risco mínimo, incluindo os sistemas não cobertos pelos requisitos e salvaguardas do regulamento.

Portanto, observa-se que o AI Act adota um critério de proporcionalidade, ou seja, quanto maior o risco associado ao sistema, maiores serão as restrições e exigências aplicáveis. O AI Act também foi elaborado com base no sistema normativo para segurança de produtos da União Europeia.

O AI Act busca estabelecer uma coerência com outras legislações setoriais, sobretudo, a GDPR e a Carta de Direitos Fundamentais da União Europeia. Dessa forma, o projeto fornece regras básicas que se aplicam a todos os setores, evitando duplicação normativa, e minimizando encargos adicionais. Traz também regras baseadas em princípios abrangentes, o que permite uma maior adaptabilidade das disposições, garantindo que diversos setores sejam regulados pela legislação.

Destaca-se também a intenção da proposta em adotar uma linguagem tecnologicamente neutra para suas definições. Toma-se como exemplo a definição de sistema de IA, caracterizado como:

> "um programa informático desenvolvido com uma ou várias das técnicas e abordagens enumeradas no anexo I, capaz de, tendo em vista um determinado conjunto de objetivos definidos por seres humanos, criar resultados, tais como conteúdos, previsões, recomendações ou decisões, que influenciam os ambientes com os quais interage."[18]

Assim, a definição de sistema de IA é complementada pelo anexo I da proposta, que inclui uma lista de abordagens e técnicas de desenvolvimento de inteligência artificial, que poderá ser adaptada posteriormente em conformidade com as inovações tecnológicas.

/ Práticas Proibidas

Em seu **título II**, o AI Act estabelece uma lista taxativa de sistemas de AI cuja utilização é vedada. Adicionalmente, propõe restrições e salvaguardas para sistemas de identificação biométrica à distância para fins de segurança pública. Essas restrições são proporcionais aos riscos de violação aos direitos da União Europeia.[19] As práticas proibidas podem ser categorizadas em quatro categorias - duas relacionadas com a capacidade manipulativa de comportamentos, uma categoria relacionada com a

---

[17] Smuha, N. A., Ahmed-Rengers, E., Harkens, A., Li, W., MacLaren, J., Piselli, R., & Yeung, K. (2021). How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act. Disponível em <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991> p. 25. Acesso em: 29 /04/ 2022

[18] AI Act, art 3(1).

[19] Smuha *et al*, idem, p. 25.

realização de *scoring* social, e a última relacionada a sistemas de análise biométrica à distância, em tempo real e em espaços acessíveis ao público.[20]

No tocante as categorias de IA com **capacidade manipulativa** de comportamentos, a primeira proibição está relacionada aos sistemas de IA que empreguem técnicas subliminares que contornem a consciência de uma pessoa para distorcer substancialmente o seu comportamento de forma a causar danos físicos ou psicológicos de natureza individual.[21] Uma hipótese que pode exemplificar esse tipo de sistema de IA, seria a utilização frequências sonoras tocadas em um caminhão que manipulem os motoristas a dirigir de forma mais arriscada, sendo as tecnologias de IA utilizadas para maximizar tais efeitos sobre os condutores[22].

A outra categoria de sistema manipulativo proibido está relacionada a sistemas de IA que explorem vulnerabilidades associadas à idade ou deficiência física ou mental de um grupo específico de pessoas, de forma a causar danos físicos ou psicológicos a esses indivíduos.[23] Como exemplo, menciona-se a possibilidade de brinquedos com sistema de voz integrada que incentivem crianças a tomar comportamentos perigosos.[24]

O terceiro sistema proibido pela proposta está relacionado com a utilização de sistemas de AI para **classificação da credibilidade de indivíduos/ *scoring* social**, utilizados por parte de autoridades públicas ou em seu nome. A utilização de tais sistemas é vedada caso a classificação conduza a tratamentos prejudiciais ou desfavoráveis de pessoas ou grupos, em contextos não relacionados com os da coleta dos dados, ou que sejam desproporcionais em face do comportamento analisado. Neste ponto, cabe ressaltar que a proibição apenas afeta a utilização de sistemas de AI para *scoring* social por autoridades públicas, ou seja, a utilização por empresas privadas para a tomada de decisões - como recrutamento de candidatos a vagas de emprego e concessão de empréstimos – não são abrangidas por essa proibição.[25]

A última vedação estabelecida pelo AI Act é em relação a **sistemas de análise biométrica**[26] em tempo real[27] em espaços de acesso público, para fins de segurança pública. Cita-se como exemplo, a utilização de sistema de vigilância por vídeo em larga escala com software de reconhecimento facial integrado.[28] Tal vedação se refere à utilização da IA para fins de segurança pública, dessa forma, a utilização de sistemas de identificação biométrica para outras finalidades não é vedada (por exemplo, proteção da saúde pública).

Diferentemente das outras três proibições, a proposta explicita hipóteses nas quais esses sistemas biométricos podem ser utilizados, desde que certas condições sejam

---

[20] KOP, Mauritz. EU Artificial Intelligence Act: The European Approach to AI. Disponível em < https://futurium.ec.europa.eu/sites/default/files/2021-10/Kop_EU%20Artificial%20Intelligence%20Act%20-%20The%20European%20Approach%20to%20AI_21092021_0.pdf> p. 3. Acesso em: 29/04/2022.

[21] AI Act, arts 5(1)(a).

[22] VEALE, Michael; BORGESIUS, Frederik Zuiderveen. Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach. Computer Law Review International, v. 22, n. 4, p. 97-112, 202. Disponível em <https://www.degruyter.com/document/doi/10.9785/cri-2021-220402/html> Acesso em: 29/04/2022.

[23] AI Act, art. 5(1)(b).

[24] VEALE, *idem*.

[25] *Ibidem*, p. 28.

[26] O sistema de categorização biométrica é definido no art. 3(35) do AI Act como "*um sistema de IA concebido para classificar pessoas singulares em categorias específicas, tais como sexo, idade, cor do cabelo, cor dos olhos, tatuagens, origem étnica ou orientação sexual ou política, com base nos seus dados biométricos*".

[27] Um sistema de identificação biométrica à distância "em tempo real" é definido no art. 3(37) do AI Act como "um sistema de identificação biométrica à distância em que a recolha de dados biométricos, a comparação e a identificação ocorrem sem atraso significativo. Para evitar que as regras sejam contornadas, tal inclui não apenas a identificação instantânea, mas também a identificação com ligeiro atraso".

[28] VEALE, *idem.*

satisfeitas - entre elas a análise de prejuízo caso o sistema não seja utilizado, e a análise de proporcionalidade entre o uso do sistemas de AI e as implicações para os direitos e liberdades dos afetados. Atingidas tais condições a utilização de sistemas de análise biométrica em tempo real em espaços públicos poderá ocorrer – como, por exemplo, para a busca de vítimas de crimes, prevenção de ameaça iminente à segurança pública; ou para detecção, identificação e perseguição de suspeitos de crimes graves.

/ Sistemas de AI com alto risco associado

Após a listagem das tecnologias expressamente proibidas, o título III do AI Act é destinado à regulação dos sistemas de AI que podem gerar riscos altos para a saúde, segurança e direitos fundamentais. Esses sistemas são submetidos a uma série de regramentos específicos relacionados à documentação de registros, transparência, supervisão humana, e exatidão das decisões.

Os sistemas com alto risco associado podem ser categorizados em duas grandes categorias: **(i)** sistemas de IA concebidos para serem utilizados como componentes de segurança de produtos que estão sujeitos a regulamentações na área da saúde ou segurança (por exemplo, brinquedos, máquinas, dispositivos médicos);[29] e **(ii)** sistemas de IA autónomos que afetem direitos fundamentais mencionados no anexo III:

- identificação e categorização biométrica;
- gestão e operação de infraestrutura crítica (ex: transporte);
- formação educacional e profissional; que possa determinar acesso à educação ou profissionalização (ex: classificação em provas)
- emprego, gestão de trabalhadores e acesso ao trabalho (ex: software de recrutamento e seleção);
- acesso e usufruto de serviços e benefícios essenciais;
- aplicação da lei;
- migração, asilo e gestão de fronteiras; e
- administração da justiça e democracia.

A proposta impõe uma lista de obrigações aos fornecedores de sistemas de IA, entre elas a necessidade de implementação e documentação de um sistema de gestão de risco[30], que deve ser mantido durante todo o ciclo de vida do sistema. Devendo tal processo conter a identificação e análise de riscos conhecidos e previsíveis associados ao sistema de IA. Além da mera documentação, o fornecedor também deverá realizar testes, e adotar medidas adequadas para a eliminação ou redução dos riscos identificados.

Em adição a necessidade de estabelecimento de um sistema de risco, os sistemas de IA de alto risco que utilizem técnicas que envolvam o treino de modelos de dados devem estabelecer medidas de governança e gestão de dados que promovam resultados proporcionados e adequados. Entre as obrigações estabelecidas está a necessidade de garantir que conjunto de dados de treino, validação e teste atendam a critérios de qualidade, inclusive em relação à relevância, representatividade, precisão, integridade e propriedade específicas da área de aplicação.

Também em relação a garantia de **qualidade dos dados**, com o intuito de evitar a discriminação indireta que possa advir de decisões tomadas unicamente por sistemas de IA, o AI Act autoriza o tratamento de categorias especiais de dados para a detecção e correção de eventuais vieses discriminatórios[31]. Tendo em vista a restrição ao tratamento de tal categoria de dados disposta na GDPR, o AI Act criaria a isenção necessária para que os fornecedores de AI de alto risco utilizem dados sensíveis para o

[29] Ibidem, p. 6.
[30] AI Act, art. 9°.
[31] AI Act, art. 10°, (3).

reconhecimento de eventuais características relevantes, muitas vezes sensíveis, de indivíduos e comunidades impactados pela tecnologia.[32]

A necessidade de se implementar técnicas de **supervisão humana** nas tecnologias de IA de alto risco também são abordadas pela proposta. O artigo 14° estabelece que os sistemas devem incorporar ferramentas de interface que garantam a supervisão por seres humanos, procurando prevenir ou minimizar os riscos associados. Entre as funcionalidades que devem estar abarcadas nesses sistemas, encontra-se a possibilidade de permitir que o supervisor consiga detectar e resolver eventuais anomalias. Também o supervisor deve ter a capacidade de decidir as situações específicas nas quais o sistema deve ser utilizado, além de poder ignorar, anular ou reverter eventuais resultados gerados pelo sistema.

O AI Act também estabelece uma série de etapas[33] que devem ser seguidas para que os sistemas de IA de alto risco entrem no mercado. O desenvolvimento do sistema deve ser acompanhado de avaliações internas de impacto, feitas previamente a implementação (*ex ante*), e elaboradas por equipes multidisciplinares.

Por fim, os sistemas de IA de alto risco autônomos devem ser registrados antes do lançamento no mercado[34] em uma base de dados públicas, com o objetivo de permitir que as autoridades competentes, os utilizadores e outras pessoas interessadas verifiquem se o sistema cumpre os requisitos estabelecidos e possam exercer uma maior supervisão dos sistemas de IA que representam riscos elevados.

/ Sistemas de AI com risco limitado

Terminadas as disposições relacionadas aos sistemas de IA de alto risco, o título IV da proposta estabelece obrigações específicas de transparência aplicáveis a todos sistemas de IA que atendam aos critérios dispostos no título[35]. A primeira obrigação de transparência é direcionada aos fornecedores de sistemas de IA destinados a interagir com pessoas naturais, tais sistemas devem fornecer mecanismo de transparência que possibilitem que o usuário seja informado que estão interagindo com um sistema de AI, evitando que tais interações possam ser confundidas com interações humanas. Não sendo necessário a aplicação de tais mecanismos se o contexto da interação deixar claro ao usuário tratar-se de interação com uma IA, ou se o sistema for utilizado para prevenção de infrações criminais.

No mesmo sentido, o AI Act estabelece disposições de transparências para sistemas de IA destinados a produzir conteúdo sintéticos, descritos como "*conteúdos de imagem, áudio ou vídeo que sejam consideravelmente semelhantes a pessoas, objetos, locais, entidades ou acontecimentos reais e que, falsamente, pareçam ser autênticos e verdadeiros a uma pessoa*". [36] Os utilizadores desses sistemas devem divulgar que o conteúdo foi gerado ou manipulado artificialmente. [37]

/ Sistemas de AI com risco mínimo

---

[32] VEALE, *idem*.
[33] EUROPEAN COMISSION. Excellence and trust in artificial intelligence. Disponível em: < https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_en>. Acesso em: 29/04/2022.
[34] AI Act art. 51
[35] AI Act art. 52
36 AI Act art. 52 (3)
[37] O AI Act define em seu art. 3° (4) utilizador como " uma pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que utilize, sob a sua autoridade, um sistema de IA, salvo se o sistema de IA for utilizado no âmbito de uma atividade pessoal de caráter não profissional".

Por fim, é desenhada a categoria de sistemas de IA com risco mínimo, aos quais as regras estabelecidas pela AI Act não se aplicam devido ao baixo risco para os direitos ou segurança dos cidadãos.[38]

3.3) China

3.3.1. Internet Information Service Algorithmic Recommendation Management Provisions

No cenário regulatório chinês sobre algoritmos destaca-se a recente norma administrativa elaborada pela Administração do Ciberespaço da China (CAC) denominada "*Internet Information Service Algorithmic Recommendation Management Provisions*". O CAC é uma agência regulatória da internet chinesa, tendo competência para criar normas e fiscalizar questões relacionadas a controle de conteúdo online, concessão de autorização para funcionamento de serviços de notícias online, e temas de segurança da informação[39].

De forma geral, a regulação sobre algoritmos de recomendação de conteúdo dispõe sobre explicabilidade de algoritmos, controle de recomendação de conteúdo, prevenção de danos aos usuários, combate à disseminação de desinformação e vício online, manutenção da ordem social, proteção extra a grupos específicos, e vedação de discriminação de preços a usuários. Importante ressaltar que a regulação dá maior foco aos direitos do consumidor ou aos trabalhadores na esfera do direito civil, mas não nos direitos dos cidadãos na sua relação com o Estado.

Abaixo são analisados em maiores detalhes os temas listados acima.

/ Escopo da Regulação

A regulação se aplica ao uso de tecnologias de recomendação de conteúdo por meio de algoritmos, no contexto do fornecimento de serviços de informação na internet[40]. A recomendação algorítmica de conteúdo é definida, nos termos do artigo 2º da regulação como:

> "uso de modelo generativo ou sintético, modelo de recomendação personalizada, modelo de classificação e seleção, modelo de filtro de pesquisa, modelo de despacho e tomada de decisão e outras tecnologias algorítmicas para fornecer conteúdo de informação aos usuários". (tradução nossa)

/ Dever ético

O art. 4º traz um primeiro dever aos provedores de serviços de recomendação algorítmica, que consiste, em síntese, em um dever ético na sua utilização. Nos termos do artigo, tais provedores devem:

> "cumprir as leis e regulamentos, observar a moral e a ética social, respeitar a ética comercial e a ética profissional e respeitar os princípios do justo e da justiça, abertura e transparência, ciência e razão, sinceridade e confiabilidade."

Tal dever está previsto ao longo de toda a regulação, com obrigações específicas que incluem desde a vedação à discriminação até o combate ao vício.

---

[38] EUROPEAN COMISSION, *idem*.

[39] THOMSON REUTERS PRATICAL LAW. Glossary Cyberspace Administration of China (CAC). Disponível em: <https://tmsnrt.rs/3vHPYJY>. Acesso em: 14/04/2022.

[40] WEBSTER, Graham; CREEMERS, Rogier; e TONER, Helen. Translation: Internet Information Service Algorithmic Recommendation Management Provisions (Draft for Comment). DigiChina – Stanford University. Disponível em: < https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/>. Acesso em: 19/04/2022.

/ Auto supervisão e supervisão social

O art. 5º recomenda a autorregulação de organizações setoriais por meio de entidades representativas, com incentivo à elaboração de normas, padrões para adequação do uso de algoritmos e a criação de uma estrutura de supervisão. O mesmo artigo também determina que a supervisão social deve ser aceita pelas entidades.

Posteriormente, o art. 24 complementa o assunto ao dizer que os operadores devem instalar estruturas para reclamações de usuários, reclamações públicas e relatórios, e esclarecer fluxos de trabalho de manuseio e períodos de feedback.

/ Manutenção da ordem social

Ainda, a regulação condiciona o uso de algoritmos de recomendação à manutenção da ordem social, impondo aos provedores uma série de procedimentos para plataformas que tenham a capacidade de influenciar a opinião pública ou a mobilização social.

Tal caráter é visível do art. 6º, o qual prevê:

> "Os provedores de serviços de recomendação algorítmica devem manter as orientações de valor dominantes, otimizar os mecanismos de serviço de recomendação algorítmica, disseminar vigorosamente energia positiva e promover o uso de algoritmos para cima e na direção do bem.
> [...]
> Os provedores de serviços algoritmos não podem usar serviços de recomendação para o envolvimento em atividades que prejudiquem a segurança nacional, perturbem a ordem econômica e a ordem social, infrinjam os direitos e interesses legais de outras pessoas e outros atos proibidos por leis e regulamentos".

Tais aspectos gerais da ética e da manutenção da ordem social podem se entrelaçar. Verifica-se que ambos estão presentes no art. 8º, o qual afirma que "os provedores de serviços de recomendação algorítmica devem examinar, verificar, avaliar e checar regularmente mecanismos, modelos, dados e resultados de aplicativos algorítmicos, etc., e não podem estabelecer modelos algorítmicos que vão contra a ordem pública e os bons costumes, como levar os usuários a vício ou consumo de alto valor".

No mesmo sentido, o art. 11 afirma que os provedores devem apresentar informações em conformidade com as orientações de valor dominantes em segmentos-chave, como em primeiras páginas, telas principais e termos mais pesquisados.

/ Dever de segurança

Nos termos do art. 7º, os provedores de serviços de recomendação algorítmica devem cumprir sua responsabilidade primária pela segurança algorítmica. São listadas uma série de medidas técnicas a serem adotadas, como a revisão de ética tecnológica, o exame e verificação de disseminação de informações, dentre outras.

Vale ressaltar que o art. 23 estabelece a criação de um sistema de gerenciamento de segurança de algoritmos e de serviços de recomendação, considerando fatores como capacidade de mobilização social, categorias de conteúdo, escala de usuários, o grau de importância dos dados tratados na recomendação algorítmica etc.

/ Vedação a informações falsas, ilegais ou prejudiciais

Dentre as obrigações específicas há um dever relacionado a classificação das informações recomendadas. O art. 10 define que os provedores devem estabelecer normas internas para categorização das informações recomendadas (*tags*). Também veda a inserção de informações ilegais ou prejudiciais como palavras-chave para fins de recomendação de conteúdo.

Destacam-se os deveres de estabelecimento de bancos de dados a serem usados para identificar informações ilegais e prejudiciais, marcação com um indicador das informações para a sua disseminação e a interrupção imediata da transmissão de informação ilegal, com preservação dos registros relevantes e envio de relatório ao Departamento de Cibersegurança e Informatização.

No caso de algoritmos de recomendação que tenham "capacidade de mobilização", os art. 24 estabelece que os provedores devem se registrar previamente com o CAC, e fornecer à autoridade relatório de avaliação do algoritmo.

Ainda, a regulação também enfrenta a divulgação de notícias falsas (*fake news*). O seu art. 13 exige a obtenção de licença para os provedores de serviços de recomendação algorítmica que divulguem notícias na internet, e segue de forma a afirmar: *"Não podem gerar ou sintetizar informações de fake news, e não podem divulgar informações de notícias não divulgadas por unidades de trabalho no âmbito determinado pelo Estado."*

/ Autonomia do usuário

O art. 10 consolida o direito de autonomia do usuário ao dispor que os provedores devem aperfeiçoar mecanismos para intervenção manual e escolha autônoma do usuário para a recomendação de conteúdo.

A autonomia do usuário é reiterada pelo art. 17, o qual afirma que os provedores devem oferecer aos usuários a opção de não segmentar suas características individuais, ou fornecer aos usuários a opção de desligar os serviços de recomendação algorítmica. O artigo prevê, ademais, que os usuários devem ter a opção de escolher, revisar ou excluir *tags* inferidas ao seu usuário.

/ Direito de revisão e de petição

O art. 17 também prevê que, quando os algoritmos possuírem um grande impacto nos direitos e interesses dos usuários, os usuários terão o direito frente aos provedores à explicação e à responsabilização de acordo com a lei.

Nesse sentido, destaca-se que o art. 30 determina que indivíduos ou organizações que descobrirem atos que violem as obrigações previstas na resolução possam apresentar reclamação ou denúncia aos departamentos governamentais competentes.

/ Transparência

O art. 14 traz um dever de transparência por parte do provedor, de forma a vedar o uso de algoritmos para "registrar usuários falsamente, negociar contas ilegalmente ou manipular contas de usuários; ou para falsas curtidas, comentários, compartilhamentos, etc."

O art. 15 segue para vedar o uso de algoritmos para, dentre outros, a manipulação de listas de tópicos, classificações de resultados de pesquisa e outras intervenções na apresentação de informações, bem como a prática de atos que influenciem a opinião pública online.

O dever de transparência também é latente no art. 12, que prevê que os provedores devem otimizar a transparência e a compreensão da pesquisa, rankeamento, seleção, notificação por *push*, dentre outros, para evitar a criação de influência nociva sobre os usuários, ou gerar controvérsias ou disputas.

Por fim, o dever de transparência também se verifica no art. 16, o qual afirma que os prestadores "devem notificar os usuários de forma clara sobre a situação dos serviços de recomendação algorítmica que prestam, e divulgar os princípios básicos, propósitos

e motivos, mecanismos operacionais, etc., dos serviços de recomendação algorítmica de forma adequada".

/ Proteção da concorrência
O art. 15 proíbe que os provedores imponham restrições não razoáveis, obstruam ou destruam outros provedores de serviços de informações da Internet, bem como que realizem atos de concorrência monopolistas ou impróprios.

/ Crianças, adolescentes e idosos
Atenção adicional é dedicada a públicos específicos. Em relação às crianças e adolescentes, o art. 18 afirma que, sempre que os prestadores realizem serviços a esse público, devem cumprir com deveres de proteção e facilitar a obtenção de conteúdos informativos benéficos para a sua saúde física e mental, desenvolvendo modelos de forma adequada a sua compreensão.

Os prestadores, não podem, ainda, exibir a esse público conteúdo relacionado à insegurança, atos que violem a moral social, que tenham tendências nocivas ou outros que possam impactar a saúde física e mental desse público ou levar ao vício online.

No mesmo sentido, o art. 19 afirma que sempre que os prestadores de serviços de recomendação algorítmica prestem serviços a idosos, devem respeitar os seus direitos e considerar suas necessidades especiais. Ainda, prevê-se, para esse grupo, medidas relativas a telecomunicações e fraude online, e bem como a obrigação de tornar conveniente para os idosos o uso seguro de serviços de recomendação algorítmica.

/ Mercado de trabalho
No mesmo sentido, o art. 20 dispõe sobre o uso de algoritmos de recomendação no mercado de trabalho, afirmando, nesses casos, que os prestadores "devem proteger os direitos e interesses legais dos trabalhadores, como obter remuneração do trabalho, descanso e férias, etc., e estabelecer e aperfeiçoar algoritmos relacionados à entrada e alocação da plataforma, composição da remuneração e pagamento, tempo de trabalho, recompensas, etc.".

/ Consumidores
O art. 18, por sua vez, dispõe sobre a proteção dos consumidores, e afirma que, sempre que houver venda de produtos ou serviços a esse grupo, deve-se proteger os direitos do consumidor. Dessa forma, é vedado o uso de algoritmos para tratamento diferenciado injustificado em condições de negociação, como preços de negociação, e outras atividades ilícitas, com base nas tendências e hábitos dos consumidores e outras características semelhantes.

/ Sanções
Os artigos 23 e seguintes, por fim, indicam as autoridades responsáveis pelas fiscalizações e sanções para o descumprimento dos artigos da regulação, que incluem advertências, multas e suspensões, sem prejuízo da responsabilidade civil e criminal, a depender do artigo violado.

Conclui-se que a legislação chinesa está pautada nos pilares da ética, da autonomia do usuário, da segurança e da transparência, e, também, na da manutenção da ordem social. O tempo deverá mostrar como tais objetivos, alguns aparentemente opostos, irão ser compatibilizados pelo governo chinês.

Da mesma forma, deverão ser avaliadas quais das obrigações surtirão efeito, ou mesmo como serão monitoradas, e quais se mostrarão impossíveis de serem cumpridas. "Pode ser tecnicamente desafiador policiar o comportamento de um algoritmo que está

mudando continuamente devido a novos inputs"[41]. Será importante se atentar, também, sobre a maneira que o país lidará com eventuais entraves ao cumprimento da legislação.

Nesse meio tempo, segue oportuno acompanhar os desdobramentos decorrentes da inovação regulatória sobre a qual acima se discorreu.

3.3.2. Lei de Proteção de Dados Chinesa

A Lei Geral de Proteção de Dados da República Popular da China apresenta poucos pontos sobre regulamentação de decisões automatizadas/inteligência artificial.[42] Em seu artigo 73, o termo decisão automatizada é definido como:

> "as atividades de análise e avaliação automática de comportamentos pessoais, hobbies ou situação econômica, de saúde e crédito, entre outros, por meio de programas de computador e tomada de decisões."

O artigo 24 estabelece que no uso de sistemas de decisão automatizada devem ser garantidas: (i) a transparência; (ii) a imparcialidade; e (iii) a justiça no que diz respeito a esse tratamento de dados. Assim, são vedados tratamentos diferenciados injustificados que resultem, em por exemplo, alterações em preços de produtos com base em tais decisões.

Ademais, nos casos em que são utilizadas propagandas e comerciais baseados em decisões automatizadas, a lei determina que, em todas as situações, deve haver opções ao titular de dados para: (i) negar a utilização de seus dados pessoais; e (ii) recusar a propaganda/comercial como um todo. Os agentes de tratamento são obrigados a especificar o objetivo do tratamento de dados, e que os titulares podem recusar que seus dados sejam tratados exclusivamente a partir de decisões automatizadas, caso a decisão os impacte de forma significativa.

Por fim, o artigo 55 define a necessidade de elaboração de uma avaliação de impacto de proteção de dados para tratamentos envolvendo decisões automatizadas, previamente ao tratamento dos dados.

3.4) Brasil

3.4.1. Análise do modelo de responsabilização dos PLs brasileiros

Os projetos de lei que atualmente tramitam no Congresso Nacional já dispõem, em alguma medida, sobre a responsabilidade civil em inteligência artificial.

O PL n. 5051/2019, do Senador Styvenson Valentim (Podemos), determina no § 2º do art. 4º que a responsabilidade civil de danos decorrentes de sistemas de inteligência artificial será sempre do supervisor humano do sistema, embora não estabeleça o regime de responsabilidade civil aplicável em regra, ou seja, se objetivo ou subjetivo.

O PL n. 872/2021, do Senador Veneziano Vital do Rêgo (MDB), por sua vez, ainda não conta com disposições específicas sobre a responsabilidade civil em inteligência artificial. Há, no entanto, proposta de Emenda n. 17 ao projeto, de autoria do Senador Styvenson

---

[41] CONRAD, Jennifer. China Is About to Regulate AI—and the World Is Watching. Wired, Disponível em: <https://www.wired.com/story/china-regulate-ai-world-watching/>. Acesso em: 19/04/2022.

[42] CHINA. Personal Information Protection Law of the People's Republic of China. Congresso Nacional do Povo da República Popular da China. 2021. Disponível em: <http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm>. Acessado em: 02/05/2022.

Valentim, que também atribui a responsabilidade civil dos danos decorrentes de inteligência artificial ao supervisor do sistema. Mesmo na Emenda, não há disposições sobre o regime de responsabilidade civil aplicável.

Entre todos, o PL n. 21/2020, do Deputado Eduardo Bismarck (PDT), é o que apresenta as considerações mais descritivas sobre o tema. A Emenda n. 5 do Deputado Renildo Calheiros (PCdoB), aprovada em setembro de 2021, introduziu ao art. 6º do projeto o inciso VI, que passou a estabelecer, em regra, um regime de responsabilidade civil subjetiva para os agentes que atuam na cadeia de desenvolvimento e operação de sistemas de inteligência artificial, salvaguardando, entretanto, a aplicação do regime de responsabilidade civil objetiva para as relações de consumo (§ 3º), conforme o Código de Defesa do Consumidor.

Vale notar que há uma diferença no escopo dos projetos que impacta na responsabilização dos agentes. O PL n. 5051/2019 prescreve que os sistemas de inteligência artificial serão sempre auxiliares à tomada de decisão (art. 4º), requerendo, portanto, um supervisor humano. Essa mesma disposição é sugerida pelo Senador Styvenson Valentim na Emenda n. 17 ao PL n. 872/2021, embora o texto inicial do projeto não estabeleça qualquer recorte desta natureza. O PL n. 21/2020, por outro lado, reconhece sistemas de inteligência artificial por aprendizagem não supervisionada (inciso I, art. 2º) e estabelece um princípio de intervenção subsidiária para os sistemas de inteligência artificial (inciso I, art. 6º).

Dessa forma, enquanto os demais PLs enfocam uma abordagem, em certa medida, mais proibitiva e interventiva quanto à inteligência artificial, a adoção do princípio da intervenção subsidiária pelo PL n. 21/2020 permite que *qualquer agente que atue na cadeia do sistema de inteligência artificial* seja responsabilizado, e não apenas o supervisor do sistema.

Aliás, sobretudo no setor privado, a ótica de responsabilização do supervisor do sistema não pode se confundir com a responsabilização do empregado ou trabalhador subordinado a determinada pessoa jurídica. Nesse sentido, é acertado o art. 6º, inciso VI, § 4º, do PL n. 21/2020, pelo qual as pessoas jurídicas de direito público e de direito privado responderão pelos danos que seus agentes causarem a terceiros.

Embora se trate tão somente de uma reprodução da regra do art. 932, inciso III, do Código Civil, essa disposição assume relevância ante as discussões ocorridas com a regulamentação da LGPD, principalmente por órgãos públicos, nas quais houve a tentativa de responsabilizar estagiários e outros servidores – na qualidade de encarregados pela proteção de dados – pelos danos causados aos titulares das informações, levando a Autoridade Nacional de Proteção de Dados a manifestar-se especificamente contra essa tendência em diretrizes sobre o assunto.[43]

3.4.2 Quadro-resumo das normas analisadas

[43] "Daí decorre que não são controladoras as pessoas naturais que atuam como profissionais subordinados a uma pessoa jurídica ou como membros de seus órgãos. É o caso de empregados, administradores, sócios, servidores e outras pessoas naturais que integram a pessoa jurídica e cujos atos expressam a atuação desta. Nesse sentido, a definição legal de controlador não deve ser entendida como uma norma de distribuição interna de competências e responsabilidades. De forma diversa, trata-se de comando legal que atribui obrigações específicas à pessoa jurídica, de modo que esta assume a responsabilidade pelos atos praticados por seus agentes e prepostos em face dos titulares e da ANPD". ANPD. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Versão 2.0. Abr. 2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf>. Acesso em 04/05/2022.

Projeto/Lei	Jurisdição	Agente Responsabilizado	Regime de Responsabilidade	Mecanismo de análise de risco
PL n. 5.051/19	Brasil	Supervisor do sistema de IA	Indefinido	Indefinido
PL n. 872/21	Brasil	Supervisor do sistema de IA	Indefinido	Indefinido
PL n. 21/20	Brasil	Qualquer agente que atue na cadeia do sistema de IA	Em regra, subjetivo	Relatório de Impacto
Automated Decision Systems Accountability Act	California (Estados Unidos)	Órgão do poder público que contratar sistema de IA de alto risco	Indefinido	Relatório de Impacto
Algorithmic Accountability Act of 2022	Estados Unidos (lei federal)	Agentes responsáveis pelo desenvolvimento e tomada de decisão automatizada	A ser regulado pela Federal Trade Commission	Relatório de Impacto
AI Act n. 52021	União Europeia	Provedor do sistema de IA	Indefinido[44]	Relatório de Impacto
Internet Information Service Algorithmic Recommendation Management Provisions	China	Provedores de serviço de recomendação algorítmica	Indefinido	Relatório de Impacto
Lei de Proteção de Dados	China	Agentes de tratamento e pessoas responsáveis pelo sistema de IA	Em regra, objetivo	Relatório de Impacto

3.4.3. Direito Comparado - Sugestões para o Brasil a partir dos casos analisados

De forma geral, verifica-se que normas que regulam o uso de algoritmos de IA nos Estados Unidos, União Europeia e China apresentam um enfoque em estabelecer obrigações de análise de risco pelos desenvolvedores e agentes que irão utilizar essas tecnologias. Devendo a análise de risco ocorrer tanto na fase de desenvolvimento como de forma regular, quanto do uso de sistemas de IA.

[44] O regime de responsabilidade objetiva não é definido explicitamente no texto do projeto de lei do AI Act, mas sim em outra proposta regulatória do Parlamento Europeu (2020/2014(INL)), conforme resolução de 20 de outubro de 2020. UNIÃO EUROPEIA. Recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)). Parlamento Europeu. 2020. Disponível em: <https://bit.ly/3wfpsqx>. Acesso em: 01/05/2022.

Tal modelo regulatório baseado em risco é semelhante ao modelo atual da LGPD, inspirado na GDPR, que reconhece que a regulação tecnológica é uma questão complexa e que a imposição de obrigações aos agentes regulados deve ser proporcional aos riscos auferidos no caso concreto.

Modelo semelhante pode ser uma opção viável a ser adotada pelo projeto de lei a ser elaborada pela Comissão,

4) BIBLIOGRAFIA

ANPD. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Versão 2.0. Abr. 2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf>. Acesso em 04/05/2022.

CHINA. Personal Information Protection Law of the People's Republic of China. Congresso Nacional do Povo da República Popular da China. 2021. Disponível em: <http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm>. Acessado em: 02/05/2022.

CONRAD, Jennifer. China Is About to Regulate AI—and the World Is Watching. Wired, Disponível em: <https://www.wired.com/story/china-regulate-ai-world-watching/>. Acesso em: 19/04/2022.

ESTADOS UNIDOS. Algorithmic Accountability Act of 2022. Washington DC: United States Congress. Disponível em: <https://bit.ly/3LToLd4>. Acesso em 03/05/2022.

ESTADOS UNIDOS. Automated Decision Systems Accountability of 2021. Legislatura Estadual da California. Disponível em: <https://bit.ly/3FrghHM>. Acesso em 02/05/2022.

EUROPEAN COMISSION. Excellence and trust in artificial intelligence. Disponível em: < https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_en>. Acesso em: 29/04/2022.

GIBSON DUNN. Artificial Intelligence and Automated Systems Annual Legal Review. 2021. Disponível em: < https://bit.ly/37wMvoq>. Acesso em 03/05/2022.

KOP, Mauritz. EU Artificial Intelligence Act: The European Approach to AI. Disponível em < https://futurium.ec.europa.eu/sites/default/files/2021-10/Kop_EU%20Artificial%20Intelligence%20Act%20-%20The%20European%20Approach%20to%20AI_21092021_0.pdf> p. 3. Acesso em: 29/04/2022.

NCSL. Legislation Related to Artificial Intelligence. 2021. Disponível em: <https://bit.ly/3P04Vi5>. Acesso em 02/05/2022.

Smuha, N. A., Ahmed-Rengers, E., Harkens, A., Li, W., MacLaren, J., Piselli, R., & Yeung, K. (2021). How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act. Disponível em <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991> p. 25. Acesso em: 29 /04/ 2022.

THOMSON REUTERS PRATICAL LAW. Glossary Cyberspace Administration of China (CAC). Disponível em: <https://tmsnrt.rs/3vHPYJY>. Acesso em: 14/04/2022.

UNIÃO EUROPEIA. AI Act - COM/2021/206. Comissão Europeia. 2021. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52021PC0206#footnote3> Acesso em: 02/05/2022.

UNIÃO EUROPEIA. Recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)). Parlamento Europeu. 2020. Disponível em: <https://bit.ly/3wfpsqx>. Acesso em: 01/05/2022.

VEALE, Michael; BORGESIUS, Frederik Zuiderveen. Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach. Computer Law Review International, v. 22, n. 4, p. 97-112, 202. Disponível em <https://www.degruyter.com/document/doi/10.9785/cri-2021-220402/html> Acesso em: 29/04/2022.

WEBSTER, Graham; CREEMERS, Rogier; e TONER, Helen. Translation: Internet Information Service Algorithmic Recommendation Management Provisions (Draft for Comment). DigiChina – Stanford University. Disponível em: < https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/>. Acesso em: 19 abr. 2022.