Carta Idec nº 102/2022/Coex

São Paulo, 30 de junho de 2022

À COMISSÃO DE JURISTAS RESPONSÁVEL POR SUBSIDIAR ELABORAÇÃO DE SUBSTITUTIVO SOBRE INTELIGÊNCIA ARTIFICIAL NO BRASIL (CJUSBIA)
cjsubia@senado.leg.br

Ref. Consulta Pública - Contribuições escrita sobre inteligência artificial

Prezadas e prezados integrantes da CJUSBIA,

O Idec - Instituto Brasileiro de Defesa do Consumidor é uma associação de consumidores, sem fins lucrativos, independente de empresas, partidos ou governos. Fundada em 1987 em São Paulo/SP, sua missão é a defesa dos consumidores, na sua concepção mais ampla, representando-os nas relações jurídicas de qualquer espécie, promovendo a educação, a conscientização, a defesa dos direitos do consumidor e a ética nas relações de consumo, com total independência política e econômica. Desde a sua fundação, o Idec tem atuado na defesa do consumidor, com uma incidência ativa para a aprovação de importantes leis consumeristas, tais como o Código de Defesa do Consumidor, em 1990.

O Instituto tomou conhecimento de chamada pública para envio de contribuições à Comissão de Juristas no Senado e, considerando sua expertise no tema, envia contribuições a alguns dos tópicos dispostos nos eixos temáticos em discussão do Plano de Trabalho da CJUSBIA, com destaque especial ao item "*4.1 Regimes de responsabilidade civil*" e "*3.1 Deveres e responsabilidades: Transparência*".

O Instituto parabeniza o trabalho realizado até o momento pela Comissão e se disponibiliza a contribuir em outras oportunidades para a pauta, inclusive em outros processos de participação da sociedade civil, como por meio de audiências públicas.

SUMÁRIO

CONTRIBUIÇÕES DO INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR (IDEC) 2
1. Conceitos, compreensão e classificação de inteligência artificial 2
1.3. Por que e como regular 2

1.3.2. Diálogo das fontes e normas de transição; debate sobre a eventual necessidade de modificação de outras normas 2
2. Impactos da inteligência artificial 3
2.1. Contexto econômico-social e benefícios 3
2.2. Riscos 4
3. Direitos e deveres 7
3.1. Transparência; 7
3.2. Explicabilidade; 8
3.3. Revisão; 10
3.4. Direito à intervenção humana; 11
3.5. Correção de vieses; 11
3.6. Atributos do design técnico: segurança, robustez, resiliência, acurácia e confiabilidade; 12
3.7. Segredos comercial e industrial 12
4. Accountability, governança e fiscalização 13
4.1. Regimes de responsabilidade civil; 13
4.4. Auditoria; 16
4.5. Arranjos institucionais de fiscalização; 17

I. CONTRIBUIÇÕES DO INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR (IDEC)

Abaixo, o Idec selecionou alguns dos eixos temáticos submetidos à chamada para enviar suas contribuições:

1. Conceitos, compreensão e classificação de inteligência artificial

1.3. Por que e como regular

1.3.2. Diálogo das fontes e normas de transição; debate sobre a eventual necessidade de modificação de outras normas

A nova legislação sinalizará um importante marco de referência sobre inteligência artificial, mas que não é criada em um vazio normativo, de modo que não se deve olvidar de uma

interpretação compreensiva com outras leis existentes. Assim, qualquer legislação estará em diálogo com um complexo quadro legislativo: o ***Código de Defesa do Consumidor*** (CDC, Lei nº 8.078/1990) no tocante ao direito de consumidores; a Lei Geral de Proteção de Dados Pessoais (LGPD, Lei nº 13.709/18), quando envolver dados pessoais; o Marco Civil da Internet (Lei nº 12.965/14); o Código Civil (em especial seus dispositivos de responsabilidade e atividades de risco); a *Lei de Ação Civil Pública* (LACP, Lei nº 7.347/1985), no tocante à responsabilidade civil por violação a direitos difusos' além de diversas legislações setoriais como a *Lei de Cadastro Positivo* (Lei nº 12.412/11), normativas de saúde, financeiras, etc.

Enquanto normativa abrangente e ampla, o **direito dos consumidores** deve ser especialmente considerado no tocante à capacitação e proteção dos consumidores, como **guia interpretativo e principiológico**, além de suas normas específicas que devem ser respeitadas. Nesse sentido, será necessário concretizar e expandir os direitos do consumidor no uso da inteligência artificial, como os direitos de informação, de acesso a produtos e serviços seguros e de qualidade, dentre outros. Igualmente, implementar limitações claras no que respeita ao desenvolvimento, a implantação e a utilização da inteligência artificial, de modo a evitar a discriminação dos consumidores e situações de perigo e risco. Desta maneira, o pano de fundo da legislação deve centrar-se no utilizador das tecnologias e prever medidas de não-discriminação desses usuários (desde sua idade, do seu gênero, raça, das suas capacidades ou das suas características), a fim de garantir inovações com impactos positivos à sociedade.

Da mesma forma, o diálogo com a LGPD será central para uma legislação adaptada ao direito brasileiro, dado que grande parte das tecnologias baseadas em inteligência artificial são alimentadas por dados pessoais (seja em sua formação, no treinamento do algoritmo, ou na sua operação diária). Assim, a legislação de IA também deve ser formulada em consonância com os fundamentos e princípios estabelecidos na LGPD.

2. Impactos da inteligência artificial

2.1. Contexto econômico-social e benefícios

Os **consumidores** e usuários das tecnologias, que devem estar no centro da legislação, devem ser informados quando estão interagindo com uma IA e se é possível desativar ou restringir sua atuação, especialmente quando se trata de uma forma de personalizar um produto ou serviço.

Além disso, durante a criação, implementação e utilização de um sistema de IA, deve haver constante adequação dos processos de coleta e seleção de dados, medidas adequadas de segurança e proteção de dados, bem como mecanismos de ***feedback***[1], sempre considerando a

[1] UNESCO. **Recommendation on the ethics of artificial intelligence.** 2022

Lei Geral de Proteção de Dados (LGPD), seus princípios norteadores e o bem-estar dos usuários-consumidores.

No setor de saúde, o Parecer da Comissão do Ambiente, da Saúde Pública e da Segurança Alimentar, reitera o entendimento de que dados pessoais colhidos por sistemas de IA não poderão ser compartilhados com companhias de seguros ou similares para prática de discriminação na fixação dos preços, prática inclusive vedada pela regulação de saúde e de proteção de dados. [2]

2.2. Riscos

Para determinar o grau de risco presente em um sistema de IA, é necessário realizar uma **avaliação *ex ante* imparcial, regulamentada pela autoridade competente e baseada em critérios concretos e definidos**.[3]

Segundo o Livro Branco sobre Inteligência Artificial da Comissão Europeia, para serem consideradas de alto risco, as IAs devem preencher dois critérios cumulativos: (i) utilização em setores que, dadas as características tipicamente realizadas, se possa esperar riscos significativos e que (ii) sejam utilizadas de forma que possa gerar riscos significativos, critério que deve ser avaliado com base no impacto as partes afetadas. [4] Assim, são sistemas de alto risco, aqueles que, durante seu desenvolvimento, implantação ou utilização implicarem um risco significativo de prejudicar, ou de causar danos às pessoas, ou à sociedade.[5]

Assim, é obrigação das autoridades nacionais realizar uma lista não-exaustiva e cumulativa de setores, de utilizações e finalidades para **identificar as tecnologias de alto risco dos pontos de vista éticos, técnicos e jurídicos**. Também devem estabelecer e **supervisionar** a aplicação de medidas necessárias e adequadas para conter riscos decorrentes das IAs de alto risco.

Ainda segundo a Comissão Europeia, os requisitos obrigatórios para que as IAs de alto risco possam ser utilizadas, são: (i) dados de treino (conjunto de dados amplo); (ii) conservação de registos e de dados; (iii) prestação de informações; (iv) robustez e exatidão; (v) supervisão humana; (vi) requisitos específicos para determinadas aplicações de IA, tais como as utilizadas

[2] PARLAMENTO EUROPEU. **Parecer da Comissão do Ambiente, da Saúde Pública e da Segurança Alimentar.** Voto Relator Adam Jarubas. Parlamento Europeu, 2020

[3] PARLAMENTO EUROPEU. Relatório que contém recomendações à Comissão sobre o quadro dos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas. Voto Relator Ibán Garcia del Blanco. Parlamento Europeu, 2020.

[4] COMISSÃO EUROPEIA. **Livro Branco: sobre a inteligência artificial – Uma abordagem europeia virada para a excelência e a confiança.** 2020.

[5] PARLAMENTO EUROPEU. Relatório que contém recomendações à Comissão sobre o quadro dos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas. Voto Relator Ibán Garcia del Blanco. Parlamento Europeu, 2020.

para fins de identificação biométrica à distância. A Comissão determina ainda que os sistemas não classificados como de "alto risco", mas que preencherem os requisitos indicados de forma voluntária, deverão receber um selo de qualidade.[6]

Assim, uma abordagem baseada em riscos e no princípio da precaução passa pela mensuração de uma matriz de risco, incluindo tecnologias de IA consideradas inaceitáveis, de alto risco, risco moderado ou limitado e risco baixo ou mínimo. Devendo ser considerado para esta análise a potencial extensão dos efeitos adversos nos direitos humanos, na democracia e no Estado de direito; a escala e onipresença deste impacto; sua probabilidade de ocorrência; sua extensão temporal e a possibilidade de reversão dos danos; além de características da tecnologia como sua rastreabilidade, explicabilidade, processamento de dados, níveis de segurança, nível de automação e acessibilidade. Além do estabelecimento dos critérios para classificação do risco, essas escolhas devem ser feitas com ampla publicidade e participação social, tendo em vista que impacta a regulação específica sobre cada uso de IA e, portanto, o consumidor e utilizador final.

Nesse sentido, existem algumas tecnologias de vigilância que são simplesmente tão perigosas que inevitavelmente causam muito mais problemas do que resolvem. **Quando se trata de reconhecimento facial, reconhecimento de emoções, gênero, idade e outras tecnologias biométricas remotas que permitem a vigilância em massa e a vigilância direcionada discriminatória, o potencial de abuso é muito grande e as consequências muito graves.** Assim, pedimos pelo banimento total das referidas tecnologias de IA, uma vez que essas ferramentas são capazes de identificar, seguir, destacar individualmente e rastrear pessoas em todos os lugares que elas vão, minando nossos direitos humanos - incluindo os direitos à privacidade e à proteção de dados, o direito à liberdade de expressão, o direito à liberdade de reunião e associação (levando à criminalização de protestos e causando um efeito inibitório), e os direitos à igualdade e à não-discriminação.

Pedimos pelo banimento porque o uso dessas tecnologias constitui uma ameaça existencial aos nossos direitos humanos, não existindo mecanismos em nossas atuais estruturas legais para conter satisfatoriamente tais riscos aos nossos direitos fundamentais e liberdades civis.

Para as tecnologias consideradas de alto risco, isto é, quando há riscos significativos ou desconhecidos para os direitos humanos, democracia ou estado de direito, mas existem medidas que podem auxiliar na mitigação adequada desses riscos. Nestes casos, consideramos fundamental que essas tecnologias passem por processos de deliberações públicas, devendo ser aprovadas ou não pela autoridade competente. A tecnologia pode ser não aprovada, se considerada inaceitável, ou aprovada, podendo ser submetida a uma série de requisitos

[6] COMISSÃO EUROPEIA. **Livro Branco: sobre a inteligência artificial – Uma abordagem europeia virada para a excelência e a confiança.** 2020.

especiais de monitoramento *ex post*., como a apresentação pública de relatórios de impacto anuais.

Para dirimir os riscos, devem ser estabelecidos critérios para realização do relatório de impacto. Que deve conter, no mínimo, (i) uma descrição sistemática do sistema e suas finalidades, assim como os interesses legítimos em caso de coleta de dados; (ii) uma avaliação da necessidade e proporcionalidade do sistema de IA; (iii) uma avaliação dos riscos para os direitos e liberdades dos consumidores e (iv) as medidas previstas para dirimir e evitar os riscos.

Apesar dos possíveis benefícios da utilização de inteligência artificial, **não se pode afastar seu potencial discriminatório.** Embora a tecnologia muitas vezes seja vista sob a falácia da neutralidade e objetividade, toda a inteligência artificial é criada a partir de inputs humanos, inserida e executada em contextos discriminatórios e, portanto, sujeita aos seus vieses.

Dentre essas discriminações, pode-se destacar, a título exemplificativo, a população trans e não-binária. Essa preocupação foi levantada no Caso ViaQuatro[7], no qual o Idec questionou a utilização não-consentida e não-informada de reconhecimento facial para fins de direcionamento de publicidade em painéis digitais na linha 4 do Metrô de São Paulo. Esse tipo de tecnologia também classificava as pessoas entre "homens e mulheres", pressupondo uma separação binária[8] entre pessoas e atribuindo externa e automaticamente o gênero da pessoa, de modo a potencialmente gerar resultados errados e discriminatórios contra pessoas trans e não-binárias.

Sobre esse tema, sugere-se o parecer da Access Now no caso ViaQuatro[9] e o artigo "As implicações da construção binária do gênero para a realização de decisões automatizadas que impactam diretamente as pessoas trans e não-binárias" (de Maraísa Cezarino Rosa e Camila Leite Contri, presente no livro "TIC, Governança da Internet e Gênero - Tendências e Desafios, de 2022)[10].

Por fim, por este motivo, é necessário que se leve em conta essa preocupação com discriminação e que haja um esforço central de considerar os direitos humanos no desenvolvimento e na operacionalização de tecnologias. Para tanto, é necessário que haja diversidade nas pessoas responsáveis pela criação, implementação e por todos os processos de

[7] IDEC. Em ação do Idec, Justiça condena ViaQuatro por reconhecimento facial não consentido no Metrô de SP. 01 de maio de 2021. Disponível em: https://idec.org.br/release/em-acao-do-idec-justica-condena-viaquatro-por-reconhecimento-facial-nao-consentido-no-metro.

[8] CPDP Latam. **Facial Recognition Technology is Binary, People are not: A Human Rights Analysis. 14 jul. 2021**. Disponível em: https://www.youtube.com/watch?v=cgOvpWoIjmI

[9] Disponível em: https://www.accessnow.org/data-for-sale-in-brazil/

[10] Disponível em: https://cgi.br/publicacao/2-coletanea-de-artigos-tic-governanca-da-internet-e-genero-tendencias-e-desafios/.

efetivação dessas tecnologias, incluindo cientistas de dados, engenheiros, mas também profissionais ligados ao campo das ciências sociais.

3. Direitos e deveres

3.1. Transparência;

A regulamentação e as orientações relativas à **explicabilidade, auditoria, rastreabilidade e à transparência,** são essenciais para garantir a **confiança** dos cidadãos nessas tecnologias, bem como para facilitar o controle social e monitorar sistemas discriminatórios. Os **consumidores devem ser capacitados e devidamente protegidos,** frisa-se que as tecnologias devem centrar-se no utilizador e ser concebidas de forma que todos possam utilizá-las, independentemente da sua idade, gênero, capacidades ou das suas características.

O princípio à transparência é previsto no art. 5º, inciso V, do PL, porém, apenas em casos de: (a) comunicação direta com sistemas de IA, como *chatbot;* (b) identidade da pessoa física ou jurídica que estiver operando o sistema de IA; e (c) critérios gerais que orientam o sistema de IA. Esta abordagem limitada é contrária ao artigo 20 da LGPD, que, além do direito à revisão, também assegura aos consumidores o direito à "informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada", *sempre* que seus interesses foram atingidos.[11]

Assim, para que o direito à transparência seja cumprido em sua completude, os consumidores devem ser informados quando estão interagindo com uma IA e de seus direitos. Além disso, entendemos que os consumidores devam ter o direito de desativar ou restringir a atuação destes sistemas, especialmente quando se trata de uma forma de personalizar um produto ou serviço. Em relação às tecnologias voltadas ao setor de saúde, os pacientes devem saber, não apenas quando estão interagindo com um profissional humano e quando se trata de uma IA, mas também devem ter liberdade sobre esta interação e alternativas de igual qualidade caso estes prefiram. [12,13]

Os consumidores também devem ser informados sobre como seus dados estão sendo utilizados, quais os impactos gerados pelo sistema e como se opor ao processamento de seus dados, além de como contestar as decisões automatizadas (conforme explorado no item

[11] IRIS. Marco Legal da Inteligência Artificial Contribuições do IRIS à Comissão de Juristas do Senado. Instituto de Referência em Internet e Sociedade, 2022.
[12] UNESCO. **Recommendation on the ethics of artificial intelligence.** 2022
[13] PARLAMENTO EUROPEU. **Parecer da Comissão do Meio Ambiente, da Saúde Pública e da Segurança Alimentar.** Voto Relator Adam Jarubas. Parlamento Europeu, 2020

3.3). Nesse sentido, são diversos os casos em que os dados são coletados, e posteriormente tratados, sem qualquer justificativa aos consumidores. Como os casos de solicitação de biometria e CPF por redes farmacêuticas, que, por iniciativa do Idec, vêm sendo investigadas pela Secretaria Nacional do Consumidor (Senacon).[14] Isso porque, falta transparência no tratamento de dados sensíveis de saúde de seus usuários, visto que não é um dado necessário para prestação do serviço, gerando riscos à privacidade dos consumidores de forma desnecessária, além de não se ter sequer confirmação de se há utilização de inteligência artificial (por exemplo, na formação dos descontos), conforme apontado pelo Idec.[15]

Outro caso paradigmático em que o direito à transparência não foi observado foi na mudança da política de privacidade do aplicativo WhatsApp, anunciada em janeiro de 2021. Isso porque, a falta de informações claras, transparentes e do consentimento dos titulares de dados para o compartilhamento de dados entre empresas do grupo Meta acabam por dificultar aos consumidores a compreensão sobre o sentido e alcance dos termos contratuais para utilização do aplicativo. Nesse sentido, **considerando a alta complexidade e assimetria informacional dos sistemas de IA, a transparência não pode ser exercida de forma genérica ou complexa, assim as informações relevantes aos consumidores devem estar disponíveis de forma clara e objetiva.** Evidenciando a relevância do caso e a importância do direito à transparência, tais condutas vêm sendo investigadas pela Autoridade Nacional em Proteção de Dados (ANPD) e pelo Ministério Pública Federal (MPF).

Assim, as regras de consentimento para coleta de dados e o uso das ferramentas de inteligência artificial devem ser claras, simples e completas, e não ocultadas nos termos de serviço.

Ainda recomendamos que os responsáveis pela IA devem **tornar públicas as informações sobre as reclamações feitas por indivíduos ou grupos de afetados** sobre os produtos e serviços que estes ofereçam, além dos resultados destas reclamações, com o objetivo de garantir que não haja reparação apenas em casos específicos, mas sim nos próprios sistemas, **corrigindo erros** antes que o dano ocorra em grande escala.[16]

3.2. Explicabilidade;

A explicabilidade e transparência dos algoritmos gera **confiança aos consumidores**, o que auxilia na implementação e utilização destas tecnologias, além de permitir controle social sobre

[14] LONGUINHO, Daniella. Farmácias que pedem CPF para dar descontos serão investigadas pelo MJ. Agência Brasil, 17 nov. 2021. Disponível em: https://agenciabrasil.ebc.com.br/radioagencia-nacional/justica/audio/2021-11/farmacias-que-pedem-cpf-para-dar-descontos-serao-investigadas-pelo-mj. Acesso em: 14 jun. 2022.

[15] IDEC. Do CPF à biometria, qual é o limite da coleta de dados por empresas? 12 abr. 2021. Disponível em: https://idec.org.br/idec-na-imprensa/do-cpf-biometria-qual-e-o-limite-da-coleta-de-dados-por-empresas. Acesso em: 14 jun. 2022.

[16] COUNCIL OF EUROPE. **Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems.** 2020

elas. É essencial que esses sejam informados de forma adequada, compreensível, normalizada, rigorosa e acessível dos eventuais resultados, consequências e da própria existência dos sistemas algorítmicos.[17] Logo, o consumidor saberá como a tecnologia funciona e, caso necessário, como as **decisões podem ser verificadas, contestadas e corrigidas.**

Em casos em que não seja possível explicar por que motivo um modelo levou a um resultado ou decisão específicos, como é o caso dos algoritmos de "*black box*", outros princípios, como a **transparência, auditoria e revisão**, devem ser considerados para garantir a responsabilização. Ademais, o uso de IA que não permita explicabilidade sobre seu processo decisório não deve ser utilizado para tecnologias que apresentem risco médio ou moderado ao utilizador e não devem ser utilizados quando houver impactos para o consumidor, tendo em vista que o CDC prevê a obrigação de informação adequada e clara sobre as características, composição, qualidade, preço e riscos oferecidos, ou seja, a informação prestada ao consumidor deve ser feita de forma plena, não podendo ser dirimida por sistemas artificiais opacos.

Neste sentido, **a precificação também deve se basear em critérios claros e objetivos**, conforme o art. 6º, inciso III do CDC. Um exemplo de precificação discriminatória que deve ser regulada é a do aplicativo Tinder. Uma pesquisa conduzida pela Consumers International e pela Mozilla, e apoiada pelo Idec, revelou que os usuários do Tinder Plus, plano pago do aplicativo de encontros Tinder, estão sendo cobrados de forma diferente com base em suas características pessoais em diversos países do mundo. Ou seja, estão sendo "precificados" de forma oculta e discriminatória pelo aplicativo, principalmente em função da idade dos usuários.[18]

Ainda, deve-se considerar que um sistema explicável é aquele que permite a compreensão de como o *processo decisório* foi formado, isto é, quais os critérios são considerados para a tomada de decisão que impacta o consumidor. Não sendo suficiente, portanto, a simples apresentação dos dados utilizados como *input,* mas também as inferências, correlações e novas informações realizadas pela IA ao longo do tempo, além dos critérios e pesos diferentes usados para analisar esses *inputs*. É nesse sentido, que a pontuação de crédito, por exemplo, para ser explicável e transparente não deve apresentar somente quais os dados que o birô utiliza, mas também qual o peso de cada fator, quais as correlações que o sistema fez, quais as categorizações em que o consumidor se enquadra, em suma, por quê ele possui determinada pontuação. Todos estes deveres constituem o direito ao devido processo informacional, que deve garantir o controle regulatório e informacional sobre os sistemas de IA através da isenção,

[17] PARLAMENTO EUROPEU. **Parecer da Comissão do Mercado Interno e da Proteção dos Consumidores.** Voto Relatora Alexandra Geese. Parlamento Europeu, 2020.

[18] IDEC. Tinder pratica preços discriminatórios em diversos países, revela pesquisa. 08 fev. **2022. Disponível em:** https://idec.org.br/noticia/tinder-pratica-precos-discriminatorios-em-diversos-paises-revela-pesquisa. Acesso em: 13 jun. 2022.

informação, compreensão, revisão e prevenção. Ao mesmo tempo, o direito também visa garantir um conjunto de salvaguardas aos indivíduos. Portanto, o direito ao devido processo informacional deve ser assegurado ao consumidor, no uso de IA, ou a qualquer utilizador quando possa impactar direitos fundamentais.

A fim de preservar os direitos humanos, os provedores dos sistemas de IA devem apresentar às **configurações de privacidade de forma facilmente visível e inteligível,** a fim de facilitar o uso das tecnologias e garantir os direitos dos usuários e titulares de dados. A coleta de dados por padrão deve considerar apenas os **dados necessários e proporcionais à finalidade legítima em questão**. Além disso, qualquer aplicação de mecanismos para bloquear, apagar ou colocar em quarentena os dados do usuário, para, por exemplo, fins de segurança, deve ser acompanhada de garantias de devido processo e soluções rápidas, em caso de uso incorreto ou desproporcional dos dados.[19]

3.3. Revisão;

Qualquer pessoa deve ter o direito de se **desvencilhar, limitar ou mesmo recorrer de uma decisão automatizada que lhe seja desfavorável**[20]. Conforme o art. 20 da LGPD, os titulares dos dados têm direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses. Todavia, o PL 21/20, não traz normatizações em relação ao tão importante direito à revisão.

Deve ser garantido expressamente o direito à **revisão humana** dos sistemas automatizados que gerem impactos aos direitos fundamentais dos utilizadores e quando envolverem relações de consumo, reforçando e ampliando o direito previsto na LGPD. Nesse sentido, sugere-se a seguinte redação, semelhante à redação original da LGPD:

> *Art. xx. O titular dos dados tem direito a solicitar* ***revisão, por pessoa natural****, de decisões tomadas com base em tratamento automatizado de dados pessoais* ***que afetem seus interesses,*** *inclusive de decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.*

Recomenda-se, a fim de facilitar o direito à revisão, que, além de garantir que os revisores humanos permaneçam acessíveis e que o contato direto seja possível, os responsáveis pelas tecnologias também assegurem que os profissionais tenham conhecimento sobre normas de direitos humanos. Por fim, o direito à revisão deverá ser irrenunciável e deve ser acessível e facilmente exequível antes, durante e após a decisão.

---

[19] COUNCIL OF EUROPE. **Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems.** 2020

[20] PARLAMENTO EUROPEU. **Parecer da Comissão do Mercado Interno e da Proteção dos Consumidores.** Voto Relatora Alexandra Geese. Parlamento Europeu, 2020.

3.4. Direito à intervenção humana;

Para que uma IA seja confiável e centrada no ser humano, deve-se garantir um envolvimento adequado dos seres humanos, assim as tecnologias devem garantir a possibilidade de intervenção humana, inclusive de **anular decisões automatizadas.** Dessa forma, conforme já defendido anteriormente, qualquer pessoa singular ou coletiva deve ter o direito de se desconectar, limitar ou mesmo recorrer de uma decisão realizada com o recurso de IA que lhe seja desfavorável. [21]

Ainda na fase de **concepção**, devem ser impostas restrições operacionais aos sistemas de IA com o objetivo de evitar violações de direitos e impossibilidade de intervenções futuras. Além disso, os sistemas devem ser monitorados em tempo real e deve haver possibilidade de desativação automática por humano a todo momento. [22]

Em relação à saúde, recomenda a UNESCO, que **decisões finais sobre diagnóstico e tratamento devem ser sempre realizadas por humanos e em respeito aos direitos humanos**, ainda que auxiliados por sistemas de IA.[23] A revisão humana é um avanço necessário em relação à atual redação da LGPD, de modo a garantir com efetividade a salvaguarda de titulares de dados e usuários de IA. Isso porque a tecnologia não consegue entender contextos perfeitamente, tampouco conflitos éticos, além de frequentemente discriminar ilicitamente por meio de suas análises.

3.5. Correção de vieses;

Com o objetivo de garantir que erros, vieses e discriminações não ocorram (conforme mencionado no item "2.2. Riscos"), desde a fase de elaboração do sistema de inteligência, os atores responsáveis devem estar cientes dos riscos relacionados à qualidade, natureza e origem dos dados utilizados para treinar seus sistemas.

Para isso, deve-se utilizar uma base de dados de treino amplas, representativa e que abranja todos os cenários necessários para se evitar vieses e situações perigosas. Estes conjuntos de dados devem ser **verificáveis** pelas autoridades nacionais a fim de garantir o bom funcionamento dos sistemas de IA.

---

[21] PARLAMENTO EUROPEU. **Parecer da Comissão do Mercado Interno e da Proteção dos Consumidores.** Voto Relatora Alexandra Geese. Parlamento Europeu, 2020.
[22] COMISSÃO EUROPEIA. **Livro Branco: sobre a inteligência artificial – Uma abordagem europeia virada para a excelência e a confiança.** 2020
[23] UNESCO. **Recommendation on the ethics of artificial intelligence.** 2022

Ainda, caso a correção do viés não seja possível e dê causa a discriminações e desrespeito aos direitos fundamentais, ela deve ser descontinuada, assim como nos casos em que não a tecnologia seja opaca e não auditável, de modo em que não seja possível verificar a ocorrência de discriminação. Este é o posicionamento do Idec em relação ao uso de reconhecimento facial, identificação biométrica e outros mecanismos de vigilância em espaços públicos. Sobre esse tema sugere-se a carta aberta da campanha **#TireMeuRostoDaSuaMira**, que explica como estes sistemas de inteligência artificial violam direitos e liberdades das pessoas em sua essência, razão pela qual não devem ser utilizados para fins de segurança pública.[24]

3.6. Atributos do design técnico: segurança, robustez, resiliência, acurácia e confiabilidade;

Com o objetivo de tornar os sistemas de inteligência e armazenamento de dados mais seguros, os atores responsáveis devem configurá-los de forma a impedir qualquer acesso ilegal, no sistema ou uso indevido dos dispositivos, tanto por terceiros quanto por sua própria equipe, sob pena de responsabilização (conforme item 4.1 Regimes de Responsabilidade Civil).

Os valores éticos de equidade, exatidão, confidencialidade e transparência devem constituir a base da IA, contribuindo para que o sistema não gere resultados injustamente tendenciosos.[25]

Deve-se atentar especialmente à equidade nos usos de IA para perfilizações e classificações de indivíduos e grupos. Qualquer categorização nesse sentido deve se limitar a discriminações que sejam lícitas, isto é, que sejam baseadas em critérios razoáveis, de boa-fé e que guardem sentido lógico entre a situação específica do grupo/indivíduo e o impacto específico estabelecido. Nesse sentido, não são aceitas discriminações baseadas em gênero, raça e capacidades e características físicas ou mentais, devendo, ainda, ser garantido acesso equânime ao produto/serviço automatizado.

3.7. Segredos comercial e industrial

Devem ser estabelecidos níveis adequados de transparência no que se refere às compras públicas, a utilização, o desenho e os critérios e métodos básicos de processamento dos sistemas algorítmicos implementados tanto pelo setor privado quanto pelo setor governamental. **As estruturas legais de propriedade intelectual e de segredo comercial não podem ser utilizadas para impedir tal transparência, e o poder público e o setor privado devem evitar procurar explorá-las para este fim.**

---

[24] TIRE MEU ROSTO DA SUA MIRA. Carta Aberta. Disponível em: https://tiremeurostodasuamira.org.br/carta-aberta/. Acesso em: 01 de junho de 2022.

[25] PARLAMENTO EUROPEU. **Relatório que contém recomendações à Comissão sobre o quadro dos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas.** Voto Relator Ibán Garcia del Blanco. Parlamento Europeu, 2020.

Os níveis de transparência devem ser tão altos quanto possível e proporcionais à gravidade dos impactos adversos aos direitos humanos. O uso de sistemas algorítmicos nos processos de tomada de decisão que comportam altos riscos aos direitos humanos deve estar sujeito a padrões particularmente elevados no que diz respeito à explicabilidade dos processos e dos resultados.

Segundo recomendações sobre os impactos dos sistemas algorítmicos nos direitos humanos do *Council of Europe* (COE), os Estados devem, regularmente, conduzir avaliações de impacto sobre os direitos humanos, sendo que a confidencialidade ou segredos comerciais **não devem inibir a implementação de avaliações que visem identificar resultados adversos aos direitos humanos**.[26]

Nesse sentido, o uso de segredos comercial e industrial deve ser específico e residual, não podendo servir de obstáculo ao exercício de direitos (especialmente de transparência e explicabilidade) e ao monitoramento e avaliação do poder público.

4. Accountability, governança e fiscalização

4.1. Regimes de responsabilidade civil;

O uso de Inteligência Artificial por envolver uma complexa cadeia de atores, automações com resultados imprevisíveis, em virtude do aprendizado de máquina, podendo envolver impactos desconhecidos, discriminatórios e que coloquem o utilizador (e a sociedade) em risco, deve ser considerada uma atividade de risco. **Nesse sentido, em linha com o Código Civil[27], tecnologias que utilizem IA devem estar sujeitas à reparação de danos independente de culpa, pois implicam, por sua natureza, riscos aos direitos de outrem.**

Neste ponto, o Idec sugere a seguinte redação:

> Art. xx: responsabilidade: normas sobre responsabilidade dos agentes que atuam na cadeia de desenvolvimento e operação de sistemas de inteligência artificial devem, salvo disposição em contrário, se pautar na responsabilidade **objetiva e solidária, observando as disposições constantes da Lei nº 8.708, de 11 de setembro de 1990 (Código de Defesa do Consumidor) e da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil).**

[26] COUNCIL OF EUROPE. **Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems**. 2020

[27] Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. Parágrafo único. Haverá **obrigação de reparar o dano, independentemente de culpa**, nos casos especificados em lei, ou **quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem**"

Isto porque o desenvolvimento tecnológico impõe novos desafios, mas o direito brasileiro continua oferecendo respostas adequadas à questão da responsabilidade civil de agentes inteligentes. A novidade está, portanto, nos avanços tecnológicos e não nas soluções jurídicas.

Nesse sentido, o regime objetivo de responsabilidade - ou seja, independentemente de culpa - é o mais idôneo à tutela efetiva das vítimas[28]. Afirmar que as "*normas sobre responsabilidade dos agentes que atuam na cadeia de desenvolvimento e operação de sistemas de inteligência artificial devem, salvo disposição em contrário, se pautar na responsabilidade subjetiva*" destoa frontalmente dos regimes estabelecidos no ordenamento jurídico brasileiro, tanto no Código de Defesa de Consumidor quanto na Constituição Federal.

Em ***relações de consumo***, é induvidosa a aplicação do Código de Defesa do Consumidor. Aplicam-se, portanto, as normas relativas (i) à inversão do ônus da prova (art. 6º, inc. VIII, CDC) e (ii) à responsabilidade objetiva e solidária (arts. 12 e 14, CDC) da cadeia de fornecimento (incluindo os desenvolvedores de *softwares* ou algoritmos) pela reparação por danos (no caso, falta de segurança) decorrentes de fato ou vício/defeito do produto ou serviço, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos. Sendo considerado defeituoso aquele produto ou serviço que não fornece a segurança esperada.

Além das proteções especiais ao consumidor, a responsabilidade solidária e objetiva deve ser estabelecida para todo uso de IA, considerando que o utilizador final da tecnologia está em condição de vulnerabilidade e assimetria informacional perante à complexidade da cadeia de IA. Dessa forma, as tecnologias devem ser desenvolvidas, desde sua concepção, de forma segura, rastreável, rigorosa do ponto de vista técnico, fiável, ética, juridicamente vinculativa e devem estar sujeitas a controle e supervisão (conforme explorado no item 4.7), afinal todos os intervenientes na cadeia de desenvolvimento e de fornecimento de produtos e serviços podem ser judicialmente responsabilizados, em linha com as recomendações da Comissão Europeia sobre o quadro dos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas.[29]

Ou seja, mesmo em relações que não são de consumo, deve-se aplicar responsabilidade objetiva por danos causados com o uso da IA, tendo em vista a assimetria informacional e a atividade de risco, nos termos do art. 927 do Código Civil. Em ambos os casos, em se tratando de responsabilidade objetiva, aplica-se igualmente a disposição sobre inversão do ônus da prova (art. 373, §1º, Código de Processo Civil).

---

[28] TEPEDINO, Gustavo; DA GUIA SILVA, Rodrigo. Desafios da inteligência artificial em matéria de responsabilidade civil. **Revista Brasileira de Direito Civil-RBDCivil**, v. 21, n. 03, p. 61, 2019. Disponível em: https://rbdcivil.emnuvens.com.br/rbdc/article/view/465.

[29] PARLAMENTO EUROPEU. **Relatório que contém recomendações à Comissão sobre o quadro dos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas.** Voto Relator Ibán Garcia del Blanco. Parlamento Europeu, 2020.

Mais especificamente no caso do ***poder público***, a referida possibilidade de responsabilidade subjetiva é flagrantemente inconstitucional, uma vez que a Constituição Federal, em seu art. 37, § 6º[30], define expressamente que é objetiva a responsabilidade das pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos.

Nesse sentido, vale recuperar o entendimento apontado em nota técnica da Comissão de Proteção de Dados e Privacidade da OAB-RJ sobre o substitutivo ao PL 21/2020[31]:

> "*Não faz nenhum sentido que a lei oriente a criação pelo poder público de um regime de responsabilidade para a IA seja, abstratamente, menos protetivo do que o previsto para outros danos causados pela atividade humana.*
> *(...)*
> *Fica claro que a redação proposta pelo substitutivo para o inciso VI do art.6º. do PL 21/2020 é incompatível com a proteção constitucional – especialmente com a reparação integral –, com a sistemática da Responsabilidade Civil já existente no ordenamento jurídico brasileiro, vai no sentido oposto do debate internacional, além de não conseguir dar conta da complexidade do tema.*"

O regime de responsabilidade objetiva tão presente no ordenamento jurídico brasileiro é especialmente relevante nos casos de emprego de tecnologia de IA. Isso porque os problemas de transparência e, consequentemente os ônus de compreensão dos riscos, as dificuldades de detecção dos defeitos, de auferimento de culpa em cadeia de produção complexa e, ainda, de produção de provas são extremamente altos, considerando a opacidade dos sistemas de IA e seu desconhecimento perante à população em geral.

Assim, casos como falhas no reconhecimento de objetos no uso de automóvel autônomo que impliquem o atropelamento de um indivíduo podem ter sua atribuição de responsabilidades dificultadas em um regime de responsabilidade mais frouxo. O mesmo pode ocorrer na atribuição de responsabilidades no caso de invasão de uma casa com sistema inteligente de fechadura que apresentou falha, ou com o *hackeamento* de brinquedos inteligentes que deixem crianças em situação de perigo.

---

[30] **Constituição Federal, Art. 37.** A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte:
§ 6º As pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa.

[31] OAB-RJ. CPDP - Comissão de Proteção de Dados e Privacidade. Nota técnica da Comissão de Proteção de Dados e Privacidade da OAB/RJ: Substitutivo ao PL 21/2020. Disponível em: https://www.migalhas.com.br/arquivos/2021/9/2F0E0B7DA86433_NOTAIAOABRJ.pdf

Nesse sentido, a instauração de um regime de responsabilidade subjetiva causaria danos sem precedentes aos consumidores-cidadãos brasileiros ao impedir a "*efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos*", conforme art. 6º, VI do CDC, em violação também ao direito básico do consumidor de "*proteção da vida, saúde e segurança contra os riscos provocados por práticas no fornecimento de produtos e serviços considerados perigosos ou nocivos*" (art. 6º, I do CDC).

As falhas de segurança em sistemas de IA podem estar conectadas a diversos fatores, que vão desde problemas com a disponibilidade e qualidade dos dados até problemas de segurança da informação ou decorrentes da aprendizagem automática[32]. Esperar a compreensão do problema exato ocorrido, para, então, acionar o responsável subjetivo é ignorar a assimetria informacional presente e a vulnerabilidade do consumidor nas relações de consumo, bem como a vulnerabilidade do cidadão perante o Estado e perante práticas comerciais arriscadas. Podem dificultar até mesmo a atuação das autoridades de fiscalização, tendo em vista a opacidade do sistema de IA e a concentração de informações nos desenvolvedores e a consequente dificuldade de obtenção de provas.

Além das dificuldades *a posteriori* na reparação dos danos, a própria existência do regime subjetivo pode acarretar um mercado de produtos de IA inseguro, pois diminui os incentivos dos atores para monitorar a qualidade dos serviços e produtos dessa complexa cadeia de produção.

4.4. Auditoria;

Apesar da importância dos direitos de transparência e explicabilidade, em virtude da complexidade das tecnologias de IA, seu funcionamento e impacto não são, em geral, plenamente compreendidos pelo utilizador. Além disso, muitas dessas tecnologias terão impactos sobre grupos, comunidades, ou mesmo a sociedade como um todo, que não podem ser compreendidos ou mesmo vistos em uma dimensão individual, como costumam ser exercidos os direitos de transparência e explicabilidade. Considerando, ainda, as limitações que segredos empresariais e comerciais podem impor sobre as regras de transparência, é fundamental garantir que as tecnologias de IA sejam auditáveis.

Nesse sentido, as auditorias são mecanismos fundamentais para impedir e fiscalizar o mau funcionamento e impactos negativos da IA para a sociedade, além de potenciais impactos legais, sociais e éticos que os sistemas podem gerar.[33] Conforme recomendação da UNESCO, estas auditorias também devem identificar **impactos sobre os direitos humanos e garantias**

[32] European Commission, White Paper on Artificial Intelligence – A European approach to excellence and trust, COM(2020) 65 final, 2020. Disponível em: https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

[33] COUNCIL OF EUROPE. **Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems.** 2020.

fundamentais, especialmente os relacionados às pessoas em situação de vulnerabilidade. [34]

Dessa forma, é preciso estabelecer arranjos institucionais e fiscalizatórios que executem auditorias, com a atribuição de competência para autoridades, com profissionais especializados e capacitados para fiscalizar a tecnologia. Ademais, para IAs consideradas de alto risco, deve-se estabelecer a realização de auditorias periódicas e regulares pelo órgão competente, independente de motivação por denúncia. Para que as auditorias e fiscalizações sejam eficazes, as tecnologias devem disponibilizar seus algoritmos e conjuntos de dados, tanto os utilizados na elaboração do sistema, quanto os produzidos após sua utilização. [35]

4.5. Arranjos institucionais de fiscalização;

Dado o caráter multidisciplinar da IA, sua fiscalização deve envolver diversas autoridades. Deve-se estabelecer, assim como tem sido feito nas matérias de proteção de dados pessoais, diálogos e cooperações entre essas autoridades.

Nesse sentido, cita-se como exemplo a cooperação interinstitucional para investigação das mudanças de privacidade do aplicativo WhatsApp, do qual participaram: a Secretária Nacional do Consumidor (Senacon), o Conselho Administrativo de Defesa Econômica (Cade), a Autoridade Nacional de Proteção de Dados (ANPD) e o Ministério Público Federal (MPF). A cooperação justifica-se pelo envolvimento de diversos direitos, como direitos dos consumidores, direito à concorrência, privacidade e privacidade e proteção, além de outros.[36]

A fim de cumprir os direitos à informação e transparência é essencial que as empresas de tecnologia possam prestar informações, inclusive em relação aos algoritmos e conjuntos de dados utilizados ou produzidos, às autoridades públicas. [37]

---

[34] UNESCO. Recommendation on the ethics of artificial intelligence. 2022

[35] COMISSÃO EUROPEIA. **Livro Branco: sobre a inteligência artificial – Uma abordagem europeia virada para a excelência e a confiança.** 2020.

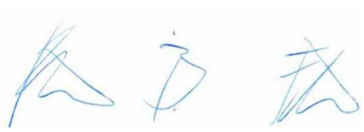
[36] Caso Whatsapp: proteção de dados dos usuários permanece ameaçada. **IDEC**, 2022. Disponível em: https://idec.org.br/noticia/caso-whatsapp-protecao-de-dados-dos-usuarios-permanece-ameacada. Acesso em: 13 de jun. de 2022.

[37] PARLAMENTO EUROPEU. **Relatório que contém recomendações à Comissão sobre o quadro dos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas.** Voto Relator Ibán Garcia del Blanco. Parlamento Europeu, 2020.

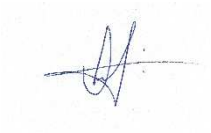
Certos de sua atenção, ficamos à disposição para contribuir com a CJUSBIA em outras oportunidades.

Carlota Aquino Costa Salgueiro de Souza
Coordenadora Executiva

Igor Rodrigues Britto
Diretor de Relações Institucionais
OAB/DF nº 54.565



Renato Barreto
Coordenador de Advocacy



Georgia Carapetkov
Gerente de Projetos e Programas

Camila Leite Contri
Advogada do Programa de
Telecomunicações e Direitos Digitais
OAB/SP nº 453.466

Juliana Oms
Advogada do Programa de
Telecomunicações e Direitos Digitais

Luã Cruz
Pesquisador do Programa de
Telecomunicações e Direitos Digitais