Brasília, 30 de junho de 2022

Exmo. Sr. Presidente Rodrigo Pacheco,

Exmo. Sr. Presidente da Comissão, Min. Ricardo Villas Bôas Cueva,

Exmo. Sr. Relator do Projeto de Lei, Sen. Eduardo Gomes,

Assunto: Contribuição à Comissão de Juristas responsável por subsidiar a elaboração de minuta de substitutivo para instruir a apreciação dos Projetos de Lei nº 5.051/2019, 21/2020, e 872/2021, que têm como objetivo estabelecer princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a aplicação da inteligência artificial no Brasil

A Coalizão Direitos na Rede (CDR) é uma rede de entidades que reúne 51 organizações acadêmicas e da sociedade civil em defesa dos direitos digitais, tendo como temas principais de atuação a defesa do acesso, liberdade de expressão, proteção de dados pessoais e privacidade na Internet. As entidades que integram o coletivo participaram ativamente da construção de políticas públicas de Internet de grande relevância para o Brasil, como o processo de discussão e elaboração do Marco Civil da Internet e de seu decreto regulamentador, bem como a Lei Geral de Proteção de Dados Pessoais (LGPD).

Por meio deste documento, a CDR apresenta suas contribuições à Comissão de Juristas responsável por subsidiar a elaboração de minuta de substitutivo para instruir a apreciação dos Projetos de Lei nºs 5.051, de 2019, 21, de 2020, e 872, de 2021, que têm como objetivo estabelecer princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a aplicação da inteligência artificial (IA) no Brasil.

1. Objeto a ser regulado

Na justificativa da versão original do Projeto de Lei 21/2020, apresentado pelo Deputado Eduardo Bismarck (PDT/CE), em fevereiro de 2020, fala-se em como as transformações causadas pela presença cada vez mais forte e mais espalhada da inteligência artificial fazem com que seja imperativa a necessidade de legislar sobre direitos e deveres envolvidos no desenvolvimento e uso dessas aplicações. A persistência do desafio que orientou o Projeto que viria a se tornar a principal referência na elaboração de um Marco Regulatório de Inteligência Artificial no Brasil, diligência que é o objeto desta consulta pública, é prova simultânea de sua complexidade e importância pública.

A combinação desses fatores significa que o debate deve ser aberto, plural, interdisciplinar, e contar com representação regional e multissetorial. O reconhecimento tardio dessa condição inerente é parte fundamental do necessário esforço coletivo representado pelas audiências e consultas da Comissão, razão pela qual elogia-se a iniciativa e apresentam-se contribuições.

A proposta de elaboração de um Marco Normativo para a Inteligência Artificial no Brasil precisa ser conduzida com o devido cuidado e a indispensável abertura à participação efetiva da sociedade civil. Isso porque, se a urgência aventada pela justificativa do PL 21/20 tem razão de ser, também é verdade que este mesmo Projeto foi alvo de incertezas basilares ao longo da sua apressada trajetória na Câmara dos Deputados.

A primeira questão que se impõe diz respeito à própria **definição de inteligência artificial** e, consequentemente, do **escopo de aplicação** da proposição. Consideramos que o amadurecimento do debate quanto ao objeto a ser regulado é ponto necessário para a compreensão quanto às razões, os princípios e os procedimentos envolvidos em tal regulação.

Ressalta-se que **não há uma definição consensual do que é inteligência artificial** e tampouco pode-se afirmar que essa seja a melhor terminologia para embasar um marco normativo que tenha como escopo as aplicações popularmente conhecidas como pertencentes a esse conjunto de tecnologias. A ausência de uma definição balizada é um dado no campo científico especializado e um ponto a ser considerado também pelo legislador. Não por acaso, foi questão repetidamente apontada em contexto de definições internacionais de valor normativo ou referencial, como nas Recommendation of the Council on Artificial Intelligence da OCDE[1], das Recomendações da UNESCO (2021)[2], e no debate em torno da elaboração e proposição do AI Act da União Europeia , marco proposto pela Comissão Europeia.[3]

Consideramos que os textos dos Projetos de Lei analisados nesta consulta pública não são exitosos em estabelecer uma definição funcional para fins legais. A definição proposta no Art. 2° do PL 21/20 parte de um diálogo direto com parte do conceito proposto pela OCDE em 2021, mas inclui elementos que prejudicam sua precisão e compreensão. É o que ocorre, por exemplo, ao estabelecer como critério a capacidade ampla e pouco objetiva de "aprender a perceber e a interpretar o ambiente externo, bem como a interagir com ele".

Consideramos **que a definição do objeto a ser regulado deve ser prontamente revisitada**, avaliando-se os benefícios em incluir uma definição do tipo, em primeiro lugar, e quais elementos e enfoques devem tomar parte dela, em caso afirmativo. Assim sendo, o debate envolve, prontamente, características macro do que se entende por IA e os riscos que os diversos usos podem ocasionar.

[1] Organização para a Cooperação e Desenvolvimento Econômico (OCDE). **Recommendation of the Council on Artificial Intelligence**. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.
[2] UNESCO. **Recommendation on the Ethics of Artificial Intelligence**. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000380455.
[3] Comissão Europeia. **Artificial Intelligence Act**. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

2. Aspectos concorrenciais e relativos à inovação

Um dos grandes potenciais das aplicações de inteligência artificial no mercado está na relação que as empresas têm com consumidores e com outras empresas. Por um lado, há um potencial positivo para a orientação de consumidores e usos de novas tecnologias por agências reguladoras e entidades sociais consumeristas. Por outro, especialmente em mercados nos quais o ambiente concorrencial já é desequilibrado, os sistemas de inteligência artificial podem resultar em uma maior concentração econômica e táticas agressivas de eliminação de concorrentes de menor porte. Exemplos são a coordenação para fixação de preços em um determinado setor, diante das possibilidades de rápida avaliação e ajuste das ofertas propiciada por aplicações de IA, ou o acesso a ferramentas tecnológicas capazes de influenciar o comportamento do consumidor e que sejam inacessíveis para pequenos competidores[4].

Esse problema se agrava em setores mercadológicos altamente digitais, nos quais já tradicionalmente se observam profundas dificuldades na tentativa de se atingir um ambiente concorrencial saudável, com uma crescente diminuição da entrada de novos agentes nestes mercados. O relatório *Investigation of Competition in Digital Markets* do Congresso dos EUA aborda esse ponto de maneira bastante detalhada[5].

Resumidamente, **uma empresa dominante encontra nos sistemas de IA uma poderosa ferramenta para não só preservar como aprofundar sua dominância em determinado mercado.** Por isso, foi extremamente salutar a inclusão no substitutivo da deputada Luiza Canziani dos incisos XIV e XV no art. 4º[6], que deverão ser mantidos. Entretanto, existem sérios riscos na inclusão

[4] ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **OECD Business and Finance Outlook 2021: AI in Business and Finance**. Disponível em: https://www.oecd-ilibrary.org/sites/3acbe1cd-en/index.html?itemId=/content/component/3acbe1cd-en.

[5] ESTADOS UNIDOS. **Investigation of Competition in Digital Markets - Majority Staff Report and Recommendations.** Disponível em: https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf.

[6] Art. 4º O desenvolvimento e a aplicação da inteligência artificial no Brasil têm como fundamentos: (...) XIV: a proteção da livre concorrência e contra práticas abusivas de mercado, na forma da Lei nº 12.529, de 30 de novembro de 2011; e XV – a harmonização com as Leis nºs 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), 12.965, de 23 de abril de 2014, 12.529, de 30 de novembro de 2011, 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), e 12.527 de 18 de novembro de 2011.

do inciso VI no art. 6º[7], que firma uma regra geral de responsabilidade subjetiva para o desenvolvimento e operação de sistemas de inteligência artificial, pelo menos na sua redação atual.

Isso porque um dos novos elementos que aplicações de inteligência artificial trazem para essa discussão são os argumentos de falta de culpa ou mesmo de qualquer ciência do comportamento anti-competitivo pelos sócios ou administradores das entidades empresárias que praticam esses atos, ao transferir a responsabilidade para decisões algorítmicas tomadas de forma automatizada. Considerando a relativa autonomia de alguns desses sistemas e a real possibilidade de inexistência de uma ordem explícita humana que leve ao comportamento irregular, essa alegação deve ser levada a sério. **É necessário proteger os consumidores e o sistema concorrencial ao mesmo tempo em que se estabelece regras previsíveis a ser seguidas pelos agentes empresariais, formulando um quadro regulatório não só em relação ao uso empresarial das tecnologias de IA, mas também sobre o seu desenvolvimento, estabelecendo restrições intencionais por *design* para evitar ações anticoncorrenciais dos algoritmos.**

A aplicação de leis concorrenciais tradicionais, como as do Sistema Brasileiro de Defesa da Concorrência, parece ser insuficiente para lidar com esses novos desafios, por estes muitas vezes não envolverem sequer uma ciência das empresas que estão engajadas em comportamentos anticompetitivos. É recomendável estabelecer critérios objetivos de infrações do sistema concorrencial relacionadas ao uso de IA.

Além disso, como recomendações posteriores à formulação do Marco Legal, os procedimentos de investigação existentes, do CADE ou de outros

[7] Art. 6º Ao disciplinar a aplicação de inteligência artificial, o poder público deverá observar as seguintes diretrizes: (...) VI – responsabilidade: as normas sobre responsabilidade dos agentes que atuam na cadeia de desenvolvimento e operação de sistemas de inteligência artificial deverão, salvo disposição legal em contrário, pautar-se na responsabilidade subjetiva e levar em consideração a efetiva participação desses agentes, os danos específicos que se deseja evitar ou remediar e a forma como esses agentes podem demonstrar adequação às normas aplicáveis, por meio de esforços razoáveis compatíveis com os padrões internacionais e as melhores práticas de mercado.

órgãos, precisam ser adaptados para os mercados digitais, com participação de figuras especializadas na análise de comportamentos algorítmicos[8].

Nesse mesmo sentido, a legislação brasileira concorrencial têm dispositivos abertos capazes de abarcar essas novas situações, mas seria imprescindível para um sistema eficiente também o detalhamento, que poderia também ocorrer regramentos infralegais, de como esses artigos se aplicariam nos mercados digitais e em caso de atos anticompetitivos originados em (ou com participação de) sistemas de inteligência artificial.

3. Bases de dados, direito autoral e mineração

A "mineração de textos e dados" é um processo que permite a análise computacional de um grande volume de dados e de textos para identificar novas informações, relações e correlações. Esta prática é essencial para o desenvolvimento das tecnologias de inteligência artificial e é parte intrínseca e inexorável do ecossistema de inovação. **Estabelecermos uma limitação que expressamente permita a mineração de textos e dados irá ampliar as possibilidades de inovação e trazer mais segurança jurídica para todos os negócios intensivos em dados.** Além disso, reforçará a presença do Brasil no grupo de países que já reconhecem esta necessidade e instituíram este direito em suas legislações, colocando-se à frente do processo de inovação em relação aos demais países.

Ressalta-se aqui que, quando fazemos referência à mineração de dados, estamos aludindo a dados de forma ampla e não exclusivamente aos pessoais, caso em que é preciso atentar para as normas da LGPD e outras setorias que tutelam o direito à privacidade e proteção de dados.

Isso significa tratar de dados e informações tuteladas por outros sistemas jurídicos. No entanto, há uma barreira de acesso e tratamento de informações principalmente nos direitos exclusivos de propriedade intelectual. Destacam-se os de direito autoral, que exigem a autorização do autor e, em boa parte dos

[8] Sobre as dificuldades de auditoria de sistemas de IA, ver: RAJI, I. D. *et al.* **Closing the AI accountability gap**. Em: FAT*'20: Proceedings of the 2020 Conference on Fairness, Accountability, dnd Transparency. ACM, 22 jan. 2020. Disponível em: http://dx.doi.org/10.1145/3351095.3372873.

casos, também remuneração ao titular, para o uso de textos, imagens, músicas, dentre outras obras intelectuais, inclusive bancos de dados que são utilizados nos processos de treinamentos de IA.

Cabe mencionar, a título de ilustração do impacto que a aplicação das normas de direitos autorais no caso da mineração de dados e textos, a iniciativa do imunologista Helder Nakaya. Ele utilizou uma série de fotos de cepas do protozoário Leishmania (causador da doença de chagas) para, por meio de inteligência artificial, criar um algoritmo capaz de identificá-lo utilizando microscópio comum, o que democratiza a possibilidade de identificação em laboratórios de menor sofisticação[9].

No caso em tela, havendo o entendimento de que a extração de informação de obra seja protegida por direito autoral, seria preciso tanto autorização quanto remuneração dos titulares para uso das as fotos do protozoário. Assim sendo, a pesquisa e a inovação em questão teriam grandes chances de ser inviabilizadas. Primeiro porque seria extremamente custoso e demorado encontrar todos os titulares das obras e, segundo, seria dispendioso licenciar o volume de obras necessárias para o aprendizado de máquina e criação do algoritmo de inteligência artificial.

Para mineração de bancos de dados, a lógica é outra. Dados, fatos e informações em si não são protegidos por direitos autorais, nem, de fato, por outras formas de propriedade intelectual. Contudo, justifica-se a exclusividade atribuída por direitos autorais quando formam um conjunto (de dados) que, pela sua seleção, organização ou disposição (Lei 9.610/98, art. 7°, XIII) contenham um mínimo de originalidade. Então, embora os dados não estejam sujeitos à exclusividade justificada pelos direitos autorais, os bancos ou base de dados o são.

O alcance da exclusividade atribuída ao titular das bases de dados pelos direitos autorais, que é de 1998, é extremamente amplo e carece de limitações para compatibilizá-la com outros direitos e políticas públicas essenciais. É neste sentido que o projeto aprovado na Câmara dos Deputados prevê "não violação

[9] AGÊNCIA FAPESP. **Técnica baseada em inteligência artificial permite detectar a doença de Chagas usando imagens de celular**. 30 maio 2022. Disponível em: https://agencia.fapesp.br/tecnica-baseada-em-inteligencia-artificial-permite-detectar-a-doenca-de-chagas-usando-imagens-de-celular/38741/.

do direito de autor pelo uso de dados, de banco de dados e de textos por ele protegidos, para fins de treinamento de sistemas de inteligência artificial, desde que não seja impactada a exploração normal da obra por seu titular" (art. 5°, VIII, PL 21-A/2020).

Vale reforçar que a mineração de dados e textos fora do escopo de aplicação das normas de direitos autorais não viola os padrões internacionais de proteção à propriedade intelectual, estabelecidos nos tratados firmados no âmbito da Organização Mundial de Propriedade Intelectual (OMPI). Prova disso é que diversos sistemas legais pelo mundo, notavelmente de países e regiões que apresentam bons índices de desenvolvimento tecnológico, já estabeleceram flexibilidades para possibilitar essa mineração de textos e dados, geralmente por meio de limites e exceções de direito autoral.

Exemplos são as regras da Diretiva 2019/790 da União Europeia[10] ou as reformas das leis de Direito Autoral no Japão[11] realizadas desde 2009. Entretanto, conforme pesquisa "Research Exceptions in Comparative Copyright" publicada em maio de 2022, o Brasil permanece com uma das legislações mais restritivas do mundo nesse aspecto, gerando um ambiente de insegurança jurídica para pesquisadores e empresas que trabalham com tecnologias de inteligência artificial.

Por último, e considerando a importância de proteção de artistas e criadores em geral, sublinhamos que a mineração de obras protegidas por direitos de autor não implica na fruição ou proveitos destas obras, tampouco na sua disponibilização ao público ou aproveitamento econômico das obras em si. Assim, a mineração de dados e textos não acarreta em qualquer prejuízo aos autores nem concorrência ao filme, música, livro e/ou texto científico de onde as informações e dados serão extraídos.

[10] DIRETIVA (UE) 2019/790 DO PARLAMENTO EUROPEU E DO CONSELHO. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019L0790&from=SL.
[11] FUKUOKA, Shinnosuke; NUMAZAWA, Shu. **The use of copyrighted works in data sets for machine learning - Commentary on the 2018 reform of the Japanese Copyright Act.** Fev. 2019. Disponível em: https://www.nishimura.com/sites/default/files/newsletter_pdf/en/en_newsletter_1902_robotics-artificial-intelligence.pdf.

Não há, portanto, impacto sobre a utilização das obras protegidas por direitos autorais por parte dos autores e titulares. Isto porque a mineração em bancos de dados de obras protegidas não é uma exploração das obras, mas a simples extração de dados e informações sobre a obra, atividade não protegida, pois, afinal, o que se protege pelos direitos autorais é a expressão, a forma expressiva da criação, e não as informações e dados sobre as expressões (obras).

Diante disso, e até para alinhar o Brasil à tendência global, liderada pelos dos principais polos tecnológicos no mundo, reforçamos a necessidade de que seja mantido e detalhado o dispositivo que permite superar as barreiras graves, acima mencionadas, para os processos de treinamento de sistemas de inteligência artificial, pelo menos para fins de pesquisa, desenvolvimento e inovação. **Para evitar ambiguidades sobre a redação do inciso VIII do art. 5º, que se inclua o trecho "e outras obras intelectuais" ao lado da palavra "textos", a fim dar segurança para minerações de dados que envolvam, por exemplo, imagens.**

Os alertas feitos anteriormente não excluem, por óbvio que seja, a necessidade de que o caso concreto determine eventual **aplicação de normas atinentes e transversais como o Código de Defesa do Consumidor, a Lei Geral de Proteção de Dados e as medidas e garantias presentes nestas normas.**

4. Gradação de riscos e hipóteses de riscos inaceitáveis

Atualmente, existe ampla discussão a nível global sobre como diferenciar, de modo preciso, o que seria uma atividade de **IA de baixo risco de uma de alto risco**. Esse debate culminou em duas propostas, sendo uma delas prescritiva e a outra procedimental[12].

A **proposta prescritiva** é aquela ancorada em classificações rígidas que indicam previamente o tipo de utilização e o tipo de setor em que a aplicação poderá ser considerada de alto risco, como, por exemplo, a utilização de

[12] Andrade, Norberto Nuno Gomes de; Kontschieder, Verena. **AI impact assessment: a policy prototyping experimente.** Open Loop, 2021. Disponível em: https://openloop.org/wp-content/uploads/2021/01/AI_Impact_Assessment_A_Policy_Prototyping_Experiment.pdf.

sistemas de IA para identificação de padrões de doenças no setor da saúde[13]. Essa classificação demanda a observação de um requisito duplo e cumulativo para caracterizar um sistema de IA como de alto risco. No caso em questão, tanto o setor quanto a utilização pretendida devem representar riscos significativos relativos à proteção da segurança, aos direitos dos consumidores e aos direitos fundamentais em setores de saúde, transportes e energia, por exemplo[14].

Por outro lado, **a proposta procedimental** defende que a definição de alto risco depende de um conjunto de etapas e indagações destinadas a alcançar uma identificação do risco mediante diálogo, reflexão e uma análise qualitativa de informações associadas ao sistema de IA em si, e não somente ao setor e tipo de utilização a que se propõe[15]. A definição do risco, portanto, não se consagra aprioristicamente, e depende assim de uma análise do caso concreto.

Além dos riscos acima exemplificados, existem ainda usos de sistemas de IA que violam direitos fundamentais, como aqueles que vulnerabilizam de sobremaneira a subsistência, a segurança e a saúde física e mental das pessoas. Nesses casos, os riscos são difíceis de evitar, mitigar ou compensar, razão pela qual se caracterizam como expressivos e desproporcionais. Estes são classificados como riscos inaceitáveis, devendo seu uso ser banido da sociedade.

A **primeira hipótese de risco inaceitável** está ligada à discriminação racial no uso de tecnologias de **reconhecimento biométrico e facial** para promoção de vigilância em massa no setor de segurança pública. A baixa acurácia atrelada aos vieses raciais encontrados nessa tecnologia aumentam a ocorrência da discriminação algorítmica[16]. Além disso, a coleta de dados biométricos e seu uso em ferramentas de estatísticas tendem a criar um ciclo retroalimentativo de marginalização de grupos vulneráveis, já que sistemas de

[13] Comissão Europeia. **Livro Branco sobre a Inteligência Artificial: Uma abordagem europeia virada para a excelência e a confiança** (2020). Disponível em: https://op.europa.eu/pt/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1.
[14] *Ibid*.
[15] Andrade, Norberto Nuno Gomes de; Kontschieder, Verena. Op. cit.
[16] Access Now. **Carta aberta para banimento global de usos de reconhecimento facial e outros reconhecimentos biométricos remotos que permitam vigilância em massa, discriminatória e enviesada** (2021). Disponível em: https://www.accessnow.org/cms/assets/uploads/2021/06/BanBS-Portuguese.pdf.

IA se alimentam de dados que são historicamente enviesados pelo racismo estrutural.

Nessa mesma linha, pode-se ainda citar o **policiamento preditivo**, cujo propósito seria o de usar e analisar dados para monitoramento e identificação de situações suspeitas. Por serem sistemas baseados em conjuntos de dados originariamente opacos, racistas e inconsistentes, seu uso, além de não haver comprovação alguma de benefício para a segurança pública, da mesma forma aumenta a vigilância, práticas discriminatórias e desigualdades socioeconômicas.

Assim, o uso dessas tecnologias deve ser banido, pois, caso contrário, estaremos promovendo ferramentas que fomentam a vigilância, a cultura do encarceramento de populações negras e vulneráveis e do punitivismo do sistema penal.

A **segunda hipótese de risco inaceitável** é o investimento e o desenvolvimento de **armas autônomas** baseadas em inteligência artificial e com potencial de causar morte em um confronto armado. Além de serem sistemas cuja finalidade por si só não é neutra, colocando o direito fundamental mais caro em risco, há mínima interferência de um ser humano no poder decisório e impossibilidade de exigir total responsabilização de quem os opera.

A **terceira hipótese** está ligada ao uso de sistemas de IA que se valem de vulnerabilidades físicas, emocionais e psicológicas para distorcer e manipular o comportamento de indivíduos ou grupo de indivíduos,[17] como o **reconhecimento de emoções**. Além dos riscos inerentes ao uso da IA para este fim, há falta de fundamento científico de que seja possível identificar emoções somente com base em expressões faciais.

Por fim, a **quarta hipótese de risco inaceitável** refere-se ao uso de sistemas de IA que valoram a confiança de um indivíduo ou de um grupo de indivíduos mediante análise de conduta social ou de características pessoais ou de personalidade (conhecidas ou preditivas), causando um tratamento

[17] Comissão Europeia. **Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de Inteligência Artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União** (2021), Artigo 5º. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52021PC0206.

prejudicial ou desfavorável capaz de injustamente limitar ou impossibilitar o regular exercício de direitos, como o **crédito social** (s*ocial scoring*)[18].

Assim, pode-se citar como sistemas de IA que geram **riscos inaceitáveis, devendo ser banidos no ordenamento jurídico brasileiro**: as aplicações para reconhecimento facial em espaços públicos, policiamento preditivo, armas autônomas, reconhecimento de emoções e crédito social (*social scoring*). No entanto, vale ressaltar que outros casos os quais o uso deva ser banido podem surgir com o tempo. Sugere-se, portanto, que a futura legislação preveja a possibilidade de adição de novos casos pela autoridade reguladora competente.

5. Transparência

É hora de impor medidas de transparência juridicamente vinculativas aos agentes que atuam na cadeia de desenvolvimento e operação de sistemas de inteligência artificial. **Precisamos abandonar a autorregulação para uma regulamentação pública de exigências de transparência** aos agentes que atuam na cadeia de inteligência artificial, ao mesmo tempo em que se assegura a proteção dos direitos humanos e não se asfixia a inovação.

Evidentemente, o dever de transparência não é uma bala de prata que vai resolver todos os problemas relacionados aos usos e abusos de sistemas de inteligência artificial, mas é uma condição necessária para estabelecer um equilíbrio de poder entre as entidades privadas e os demais setores, em especial a sociedade civil e o setor governamental.

O dever de transparência é uma consequência natural do poder que os agentes que atuam na cadeia de desenvolvimento e operação de sistemas de inteligência artificial detêm sobre uma série de produtos e serviços essenciais. Nesse sentido, as atuais estruturas legais de propriedade intelectual não devem impedir tal transparência, nem a administração pública ou o setor privado devem procurar explorá-las para este fim. Nesse sentido, vale retomar as recomendações do Conselho da Europa aos seus Estados membros: "Os níveis

[18] *Ibid.*

de transparência devem ser tão altos quanto possível e proporcionais à gravidade dos impactos adversos aos direitos humanos"[19].

É importante relembrar que o dever de transparência e o direito à informação adequada e clara sobre os diferentes produtos e serviços é um dos grandes avanços do ponto de vista da modernização e estruturação da proteção ao cidadão brasileiro. O direito à segurança, à liberdade de escolha e à informação adequada e clara sobre os serviços encontram-se previstos no art. 6º, incisos I, II e III, do Código de Defesa do Consumidor (CDC). Ainda, a Lei Geral de Proteção de Dados determina requisitos para o devido tratamento dos dados pessoais, impondo seus princípios como o da adequação, necessidade, transparência e não discriminação. Para tanto, a Lei impõe que qualquer processo de tratamento de dados pessoais seja proporcional, de acordo com as finalidades pretendidas, e norteado pela transparência e segurança a seus titulares.

Em um momento tão delicado sobre regular e consolidar uma legislação ampla e específica voltada a disciplinar os agentes que atuam na cadeia de desenvolvimento e operação de sistemas de IA, é preciso reforçar que processos como esse já ocorreram em outros momentos da história legislativa brasileira. No início de sua vigência, o Código de Defesa do Consumidor , promulgado em 1990, enfrentou resistência geral dos empresários, em especial dos publicitários e grandes conglomerados. No entanto, atualmente, não há mais questionamentos quanto à mudança ocasionada pela legislação consumerista na relação fornecedor-consumidor, que fez com que a qualidade de produtos e serviços, bem como informações mais adequadas viessem à tona.

O CDC fez, dentre outras coisas, o mercado perceber a importância de amadurecer. Isso motivou, por exemplo, o surgimento de serviços de atendimento ao cliente nas empresas bem como o das ouvidorias e a apresentação de informação dos produtos, como o prazo de validade e a indicação de símbolos como o "T" de transgênico nos alimentos.

[19] **Recommendation CM/Rec(2020)1 of the Committee of Ministers to member states on the human rights impacts of algorithmic systems.** (2020). Disponível em: https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2020-1-of-the-committee-of-ministers-to-member-states-on-the-human-rights-impacts-of-algorithmic-systems?_101_INSTANCE_aDXmrol0vvsU_viewMode=view/.

É fundamental que a **transparência seja ativamente exercida pelos agentes de inteligência artificial,** especialmente em serviços de alta complexidade em sua cadeia e com alta assimetria informacional, como no caso de serviços baseados em dados. Além disso, para fins de transparência, deve-se sempre levar em conta as diversas vulnerabilidades do cidadão.

Ou seja, os cidadãos, especialmente os hipossuficientes e vulneráveis, devem ser capacitados e devidamente protegidos, independentemente da sua idade, gênero, capacidades ou das suas características. Estes 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.

A **explicabilidade e transparência dos algoritmos gera confiança** aos cidadãos, o que auxilia na implementação e utilização destas tecnologias, além de permitir **controle social sobre elas**. É essencial que sejam informados de forma adequada, compreensível e acessível dos eventuais resultados, consequências e da própria existência dos sistemas algorítmicos. Logo, o consumidor saberá como a tecnologia funciona e, caso necessário, como as decisões podem ser verificadas, contestadas e corrigidas.

Dessa maneira, não deve ficar a cargo do cidadão investigar e entender um fluxo de informação extremamente complexo, que envolve cruzamento de dados provenientes de múltiplos contextos, diversas empresas e produtos. Assim, entendemos que o desenvolvimento tecnológico impõe novos desafios, mas o direito brasileiro continua oferecendo respostas adequadas à questão da transparência de agentes que atuam na cadeia de inteligência artificial.

Uma nova legislação para lidar com os agentes que atuam na cadeia de desenvolvimento e operação de sistemas de inteligência artificial deve seguir os mesmos níveis de exigência já estabelecidos no atual ordenamento jurídico brasileiro. Por isso, reforçamos **a necessidade de regras específicas que fortifiquem a necessidade de um consentimento informado e que estabeleçam novos regramentos sobre o direito à explicação e imponham o direito à revisão humana**.

Além disso, é preciso que se ampliem as exigências referentes à publicação de informações sobre a especificação correta das características,

composição, qualidade, bem como sobre os riscos que apresentem os serviços e produtos ofertados por agentes que atuam na cadeia de inteligência artificial, tal como temos estabelecido em diplomas legais como o CDC e a LGPD.

6. Revisão e correção de viés

Além das garantias dos arts. 4º, VIII, e 5º, XLII Constituição Federal e art. 20, §§ 2º, 3º, III, da Lei nº 7.716/1989,[20] o Brasil também está comprometidono plano internacional em enfrentar o racismo, a discriminação racial e formas correlatas de intolerância, nos termos da Convenção Interamericana firmada pela República Federativa do Brasil, na Guatemala, em 5 de junho de 2013 e promulgada em 10 de janeiro de 2022.[21]

Assim, **é necessário afirmar em lei o dever de as tecnologias de inteligência artificial serem antirracistas:** ativamente contrárias à produção de desigualdades raciais mediante a adoção de qualquer vínculo causal entre as características fenotípicas ou genotípicas de pessoas físicas ou grupos e seus traços intelectuais, culturais, comportamentais e de personalidade.

Uma norma legal abstrata não tem efetiva capacidade de pronta aplicação no dia a dia do trabalho tecnológico de quem programa, revisa ou aprimora códigos na área de inteligência artificial. Não obstante, as previsões principiológicas do PL 21/2020 não podem ser aceitas sem um compromisso expressamente assumido com o antirracismo como um critério legal de validade para atividades de fomento, desenvolvimento e uso de inteligência artificial no Brasil.

Nesse sentido, destaca-se também a **importância da existência de instrumentos de ação preventiva**, como o relatório de impacto de inteligência artificial, a fim de que seja possível mensurar os possíveis riscos envolvidos no desenvolvimento e uso de novas tecnologias. Isso poderá ajudar a identificar previamente danos potenciais à sociedade, em especial, no que tange a minorias, como também à população negra.

[20] Referida lei define os crimes resultantes de preconceito de raça ou de cor.
[21] Por meio do Decreto nº 10.932/2022.

Além disso, **relatórios de impacto** têm o condão de trazer maior responsabilidade para os agentes que atuam nesse processo, que deverão participar ativamente para sanar eventuais problemas encontrados. Assim, faz-se importante pensar também em que tipo de sistemas de inteligência artificial podem ser efetivamente relevantes para o desenvolvimento e evolução social e quais, pelos seus riscos e problemas, possuem mais desvantagens do que benefícios.

7. Direito à intervenção humana

A preponderância da obrigatoriedade de revisão humana de decisões automatizadas pressupõe a garantia efetiva dos direitos (i) à **autodeterminação informativa**; (ii) a **não discriminação e transparência**; (iii) o **direito de informação** sobre critérios e parâmetros de decisões, revisão, explicação e oposição às decisões automatizadas[22].

Entre as disposições normativas com a finalidade de proteger os interesses, direitos e garantias dos titulares cujos dados são analisados por distintos modelos de inteligências artificiais, ou seja, regulamentações que defendem direitos relacionados à participação humana em decisões automatizadas, estão: o Regulamento Geral de Proteção de Dados da Europa (GDPR ou General Data Protection Regulation); a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (conhecida como Convenção 108+); a Recomendação do Conselho de Inteligência Artificial da Organização para a Cooperação e Desenvolvimento Econômico (OCDE); a Proposta de Regulamento de IA da União Europeia e Recomendação da UNESCO sobre Ética da Inteligência Artificial.

Convém enfatizar a relevância do respeito à Convenção Interamericana contra o Racismo, a Discriminação Racial e Formas Correlatas de Intolerância, visto que há uma obrigatoriedade da promoção e defesa de direitos relativos à proteção contra formas de racismo. Logo, impõe-se deveres aos agentes de

[22] Santos, Natane da Silva. **Lei Geral de Proteção de Dados e os possíveis impactos da não obrigatoriedade de revisão humana de decisões automatizadas**. (Monografia Jurídica) 2021.2. Faculdade Nacional de Direito da Universidade Federal do Estado do Rio de Janeiro - FND/UFRJ.

sistemas de inteligência artificial, dentre eles, a **identificação e eliminação de vieses racistas.**

Então, percebe-se uma cautela na edição de leis e regulamentos sobre a aplicação de inteligência artificial em diferentes nações. Isso se dá, especialmente, no que tange à elaboração e execução ética de sistemas de IA, oportunizando a centralidade na pessoa humana, o regime de responsabilidade adequado e o crescimento socioeconômico global inclusivo e responsável. Ainda observa-se a aderência aprincípios relevantes para promoção efetiva dos direitos do titular de dados pessoais, dentre eles, não discriminação, transparência, explicabilidade e accountability. Por fim, vale ressaltar que a **intervenção humana é fundamental para proporcionar maior segurança jurídica,** através do estabelecimento de normas, boas práticas, fiscalização e sanções, de fato privilegiando o respeito ao tratamento igualitário e a diversidade nos setores público e privado.

8. Regime de responsabilidade civil

Diversos são os temas afetados pelo conjunto do debate da responsabilidade civil tecnológica. A inteligência artificial, fazendo parte deste grupo, é atravessada por considerações já enfrentadas em outros produtos tecnológicos, como a Internet. O tema da responsabilidade civil é fonte frequente de equívocos conceituais. A discussão relaciona-se às circunstâncias, características e agentes aos quais se determina o dever de comprovar culpa e o ônus de responder pelos danos existentes, o que confere importância ímpar ao tema no âmbito de regulação de novas tecnologias.

Em uma legislação que se pretende específica, direcionada e atenta às demandas decorrentes da presença de inteligência artificial nas mais diferentes atividades humanas, é necessário que o tema receba tratamento adequado. Como a inteligência artificial pode ser avaliada a partir de outras legislações, ao ser classificada como um produto no Código de Defesa do Consumidor, por exemplo, prescrições errôneas e específicas no Marco Normativo de IA podem acabar por enfraquecer diretrizes já existentes.

Por isso, o tema da responsabilidade civil chama nossa atenção na forma como está posta no PL 21/2020. Como ocorre em outras áreas relacionadas à

inovação industrial e tecnológica, o **"princípio da responsabilidade pela culpa"**, base da **responsabilidade subjetiva** atualmente prevista, é incapaz de tutelar corretamente lesões referentes ao terreno das aplicações abarcadas pelo guarda-chuva da inteligência artificial.

Esse regime remete ao consumidor (aquele que imputa o fato) o ônus de comprovar os danos sofridos e estabelece uma visão limitada quanto à responsabilidade tecnológica dos envolvidos no ciclo de vida do produto. **É anacrônico, portanto, em relação à compreensão de responsabilidade civil nesse âmbito e expressa baixo comprometimento com os riscos acarretados pela inteligência artificial.** Ao retirar a imposição objetal, faz com que eventuais ofensores do campo do desenvolvimento em produtos de IA possam causar dano sem serem devidamente responsabilizados.

O regime de responsabilidade civil também não exclui o cenário de diálogo normativo. Afinal, e de forma exemplificativa, quando o **caso concreto** tratar de relação de consumo, a responsabilidade do diploma especial está previamente estabelecida. Não há razão técnica para diferenciar, a priori, uma IA posta no mercado como produto, do conceito geral de produto - assim como nos casos de consumidor e fornecedor, dentro da relação de consumo.

O mesmo aplica-se ao regime geral do Código Civil. **O alerta que deve ser marcado aqui é que, por seus usos específicos, a IA não comporta tratamento geral pela responsabilidade subjetiva.**

9. Fiscalização, regulação responsiva e órgão regulador

Fiscalização pressupõe obrigações e sanções para o seu descumprimento. Sem isso, qualquer atividade fiscalizatória sequer existe, afinal, não há fiscalização possível se a regulação não prevê obrigações a serem cumpridas.

Então, tudo depende da opção legislativa adotada. Se a opção for por um padrão principiológico de regulação, apenas com diretrizes gerais, mas sem qualquer obrigação específica para os entes envolvidos e, também, sem a atribuição de sanções para o descumprimento, qualquer regime fiscalizatório perde a razão de existir. Tendo em vista o texto atual do PL 21/20, cuja opção legislativa foi exatamente essa, principiológica, sem atribuição de obrigações,

não há que se falar em arranjos fiscalizatórios, considerando que a própria lei não atribui o que fiscalizar. Um possível órgão regulador, nesse caso, nascerá esvaziado de atribuições.

Porém, caso a opção legislativa seja pelo modelo oposto, **com definição de competências, obrigações específicas, boas práticas metrificadas e as respectivas sanções para o seu descumprimento, os arranjos fiscalizatórios passam a ser não só desejáveis como uma imposição legal**, merecendo uma boa reflexão por parte do legislador.

Nesse sentido, é mister ressaltar que a discussão sobre autoridades específicas de fiscalização vem sendo posta em todas as tentativas de regulação de novas tecnologias desde a Lei Geral de Proteção de Dados Pessoais e a criação da Autoridade Nacional de Proteção de Dados (ANPD), como por exemplo no PL 2630/2020, que pretende definir regras para a regulação da atividade das plataformas de redes sociais, mecanismos de busca e aplicativos de mensagem privada. No entanto, é preciso questionar se esse movimento de ampliação da máquina pública se mostra eficaz, através da criação de sucessivas autoridades fiscalizatórias para temas diversos que abrangem a adoção de novas tecnologias e seu amplo uso pelos vários setores da sociedade.

Por outro lado, **deve-se questionar se a ausência de um órgão com independência funcional e orçamentária não levaria à criação de uma legislação sem obrigações, apenas no papel.**

10. Avaliações de Impacto

A avaliação de impacto é uma ferramenta para endereçar as possíveis consequências negativas de uma iniciativa sobre um ou mais interesses sociais relevantes, com o objetivo de informar uma decisão sobre a sua formulação, bem como sua continuidade. É o gênero de uma série de ações desdobradas no campo ambiental, das agências reguladoras, da proteção de dados, entre outras arenas[23]. A título de exemplo, no Brasil tais avaliações de impacto encontram

[23] Kloza, D., Van Dijk, N., Gellert, R. M., Borocz, I. M., Tanas, A., Mantovani, E., & Quinn, P. **Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals.** 2017. d.pia.lab Policy Brief, (1/2017), 1-4.

previsão legal, respectivamente, na Constituição Federal (art. 225, IV), na Lei das Agências Reguladoras (art. 6º) e de Liberdade Econômica (art. 5º) e, por fim, na Lei Geral de Proteção de Dados Pessoais (art. 5º, XVII).

O emprego de IA pode gerar uma multiplicidade de efeitos colaterais que não se confinam à proteção de dados pessoais. Por esse motivo, a regulação deve considerar uma espécie de avaliação de impacto que seja capaz de cobrir essa plêiade de direitos fundamentais em jogo e, sobretudo, mais voltada a uma dimensão sistêmica-coletiva e não apenas individual.

Assim, **a regulação deve incluir, como diretriz, a ideia de avaliação de impacto sobre os direitos humanos**, partindo do pressuposto de que as diversas aplicações de inteligência artificial têm, potencialmente, efeitos transversais sobre a proteção e o gozo de direitos e liberdades fundamentais que assumem uma dimensão coletiva-difusa e não apenas individual.

Além de considerar que a elaboração e a adoção de tais relatórios de impacto a direitos humanos deve não apenas estar sujeito a um amplo escrutínio público, mas, também, ser resultado de um processo de deliberação pública pela qual se inclua a revisão por organizações ou consultore(a)s externas afetadas e com expertise em direitos fundamentais. Caso contrário, corre-se o risco de tal documentação procedimentalizar uma tecnocracia que é justamente o que se pretende evitar com essa espécie de avaliação de impacto.

No caso específico da inteligência artificial, a **Avaliação de Impacto de Inteligência Artificial (AIIA)** é vista como um instrumento de governança que possibilita ao desenvolvedor ou aplicador da tecnologia identificar e reduzir possíveis riscos que determinado sistema de IA possa causar aos direitos e liberdades fundamentais.

Como um instrumento de governança, a AIIA ajuda a manter a **transparência e a confiança** dos usuários na tecnologia, permitindo expor as capacidades e a finalidade do sistema de IA a todos aqueles que sejam por ela afetados. Além disso, a AIIA permite a **gestão e o tratamento dos riscos** que uma atividade pode causar, possibilitando a definição de técnicas e processos para mitigá-los ou evitá-los. Assume, portanto, especial relevância em uma sociedade com forte tradição consumerista, onde acesso à informação figura como direito básico.

Existem ao menos **cinco momentos** em que é recomendável realizar uma AIIA:

(i) no início da fase de *design* de um projeto[24];

(ii) após finalizar o desenvolvimento do sistema de IA[25];

(iii) após uma modificação substancial do sistema de IA[26];

(iv) antes da aquisição/utilização do sistema de IA, e;

(v) em avaliações periódicas[27].

Além do envolvimento da equipe interna da organização, a depender da **amplitude**,[28] da **finalidade**[29] ou do **risco**[30] associado ao desenvolvimento ou operação do sistema de IA - em outras palavras, aplicações que afetam significativamente a sociedade, ainda que em grupos específicos ou minorias - é altamente recomendado que terceiros externos à organização possam participar da AIIA.

Ainda, é imprescindível o envolvimento, desde a fase de levantamento de riscos, dos mais diversos grupos, como sociedade civil, academia e os próprios usuários finais afetados pela aplicação, especialmente grupos marginalizados. Além desse envolvimento prévio, e observados os segredos comercial e industrial, é necessário que a AIIA seja acessível ao público, para

[24]CANADÁ. **Algorithmic Impact Assessment Tool**. Disponível em: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html#toc3-1.
[25] *idem*.
[26] EPC | Platform for the Information Society. **Artificial Intelligence Impact Assessment** (2018). Disponível em: https://ecp.nl/wp-content/uploads/2019/01/Artificial-Intelligence-Impact-Assessment-English.pdf. REISMAN, Dillon; SCHULTZ, Jason; CRAWFORD, Kate; WHITTAKER, Meredith. **Algorithmic Impact Assessment in the public sector.** AI Now, 2018. Disponível em: https://ainowinstitute.org/aiareport2018.pdf.
[27] REISMAN, Dillon; SCHULTZ, Jason; CRAWFORD, Kate; WHITTAKER, Meredith**.** Op. cit., p. 10.
[28] Por exemplo, um sistema de IA privado que pretende utilizar reconhecimento facial em locais públicos, como o metrô ou outra zona de grande movimento de pessoas.
[29] Por exemplo, o desenvolvimento de *hardwares* ou *softwares* baseados em inteligência artificial que possibilitem grande automação de processos e procedimentos e que, consequentemente, possam causar impacto no mercado de trabalho.
[30] Por exemplo, o desenvolvimento de um sistema de IA voltado para moderação de conteúdo de redes sociais.

garantir a possibilidade de compreensão sobre o funcionamento e riscos do sistema de IA. Isso, inclusive, demonstrará transparência e responsabilidade social, refletindo também no valor reputacional.[31]

Assim, **o uso de instrumentos de governança deve ser adotado e estimulado**, de modo que os responsáveis por desenvolver ou operar sistemas de inteligência artificial de alto risco possam identificar impactos negativos para os direitos fundamentais, definir salvaguardas e medidas de segurança para eliminá-los ou mitigá-los e permitir que as pessoas afetadas compreendam como o sistema de IA funciona e os impacta.

11. Conclusão

Em virtude do apresentado, a Coalizão Direitos na Rede compreende ser premente uma revisão ampla e geral do desenho legal adotado pelos PLs em discussão, em especial o texto aprovado na Câmara dos Deputados para o PL nº 21/2020, a fim de que seja alcançado o efetivo equilíbrio entre o potencial econômico e inovativo das tecnologias de IA e a proteção de direitos fundamentais. **Em seu estado atual, contudo, o texto corre o risco de constituir-se meramente como um conjunto - insuficiente, cabe ressaltar - de princípios, objetivos e parâmetros éticos sem mecanismos efetivos de concretização.** Assim, cabe a esta Comissão remediar tal cenário para impedir que os interesses econômicos de atores empresariais prevaleçam sobre os de toda a sociedade, uma vez que o uso crescente dessa família de tecnologias torna inevitável que todo e qualquer cidadão eventualmente se ache na categoria de pessoa afetada por decisão tomada por um sistema de IA.

Normas como o Marco Civil da Internet e a Lei Geral de Proteção de Dados foram exitosas em realizar tal harmonia, constituindo-se hoje como referências globais em maturidade técnica e cívica. **É fundamental que o Marco Legal da Inteligência Artificial dê continuidade a esse legado, constituindo-se como um instrumento elaborado com respeito ao multissetorialismo, aos**

[31] EPC | Platform for the Information Society. **Artificial Intelligence Impact Assessment** (2018). Disponível em: https://ecp.nl/wp-content/uploads/2019/01/Artificial-Intelligence-Impact-Assessment-English.pdf.

direitos humanos e aos últimos avanços internacionais no debate sobre o tema. Desse modo, o arcabouço normativo nacional referente aos direitos humanos na área digital poderá continuar a se consolidar como um exemplo internacional de excelência e observância dos princípios e valores democráticos.

Atenciosamente,

Cynthia Picolo

Ponto Focal do Grupo de Trabalho de Inteligêcia Artificial

André Fernandes

Ponto Focal do Grupo de Trabalho de Inteligência Artificial

Fabricio Solagna

Secretário Executivo

Coalizão Direitos na Rede

Contatos
Secretaria Executiva:
Fabricio Solagna
E-mail: secretariaexecutiva@direitosnarede.org.br
Telefone: 51 99281-9425

Grupo de Trabalho de Inteligência Artificial:
Cynthia Picolo
E-mail: cynthia.picolo@lapin.org.br
Telefone: 19 99537-0308

André Fernandes
E-mail: andrefernandes@ip.rec.br
Telefone: 81 9860-4714

Entidades que compõem a Coalizão Direitos na Rede

1. Ação Educativa – Assessoria, Pesquisa e Informação
2. Actantes
3. Amarc Brasil – Associação Mundial de Rádios Comunitárias
4. ANPED – Associação Nacional de Pós-Graduação e Pesquisa em Educação
5. AqualtuneLab – Cruzando o Atlântico
6. Artigo 19
7. ASL – Associação Software Livre
8. Associação Brasileira de Pesquisadores e Profissionais em Educomunicação – ABPEducom
9. Associação Data Privacy Brasil de Pesquisa
10. Casa da Cultura Digital de Porto Alegre
11. Casa Hacker
12. Centro de Estudos da Mídia Alternativa Barão de Itararé
13. Centro de Pesquisa em Comunicação e Trabalho – CPCT-ECA/USP
14. Ciranda da Comunicação Compartilhada
15. Coding Rights
16. Colaboratório de Desenvolvimento e Participação-COLAB-USP
17. Coletivo Digital
18. Coolab – Laboratório Cooperativista de Tecnologias Comunitárias
19. Creative Commons Brasil
20. Fórum Nacional pela Democratização da Comunicação – FNDC
21. Garoa Hacker Clube
22. Grupo de Pesquisa em Políticas Públicas para o Acesso a Informação/GPoPAI da USP
23. Idec-Instituto Brasileiro de Defesa do Consumidor
24. Instituto Bem-Estar Brasil
25. Instituto Beta: Internet & Democracia
26. Instituto de Pesquisa em Direito e Tecnologia do Recife – IP.rec
27. Instituto Educadigital
28. Instituto Igarapé
29. Instituto de Referência em Internet e Sociedade – IRIS
30. Instituto Nupef
31. Instituto Observatório do Direito Autoral – IODA
32. Instituto SIGILO
33. Instituto Telecom
34. Instituto Vero
35. Internet Sem Fronteiras Brasil
36. InternetLab – Centro de pesquisa em direito e tecnologia
37. Intervozes-Coletivo Brasil de Comunicação Social
38. ITS-Rio-Instituto de Tecnologia e Sociedade do Rio de Janeiro
39. LAPCOM – UnB – Laboratório de Políticas de Comunicação da UnB
40. LAPIN – Laboratório de Políticas Públicas e Internet
41. LAVITS-Rede latina-americana de estudos sobre vigilância, tecnologia e Sociedade
42. Me Representa
43. Movimento Mega

44. NUREP – Núcleo de Pesquisas em Direitos Fundamentais, Relações Privadas e Políticas Públicas
45. Observatório da Ética Jornalística – objETHOS
46. Open Knowledge Brasil
47. Instituto Alana
48. Projeto Saúde e Alegria
49. PROTESTE - Associação de Consumidores
50. Transparência Brasil
51. Wiki Movimento Brasil