

AUDIÊNCIA

TEMÁTICA DA CIDH:

2026

*PRESTAÇÃO DE CONTAS DAS PLATAFORMAS
DIGITAIS E SEU IMPACTO NOS
DIREITOS HUMANOS*



RESUMO EXECUTIVO

Pelo Centro de Estudos de Direito, Justiça e Sociedade – DEJUSTICIA, Colômbia; RedPaPaz, Colômbia; Artigo 19 Brasil e América do Sul, Brasil; CELS, Argentina; Conectas Direitos Humanos, Brasil; Instituto Alana, Brasil e Tech Justice Law, Estados Unidos da América, solicitamos à Comissão Interamericana de Direitos Humanos (CIDH) a realização de uma audiência temática sobre “Prestação de contas das plataformas digitais e seu impacto nos direitos humanos”. Nosso pedido foi aprovado e a audiência ocorreu em Washington, DC, em 4 de agosto de 2026, no âmbito da 197ª sessão da CIDH.

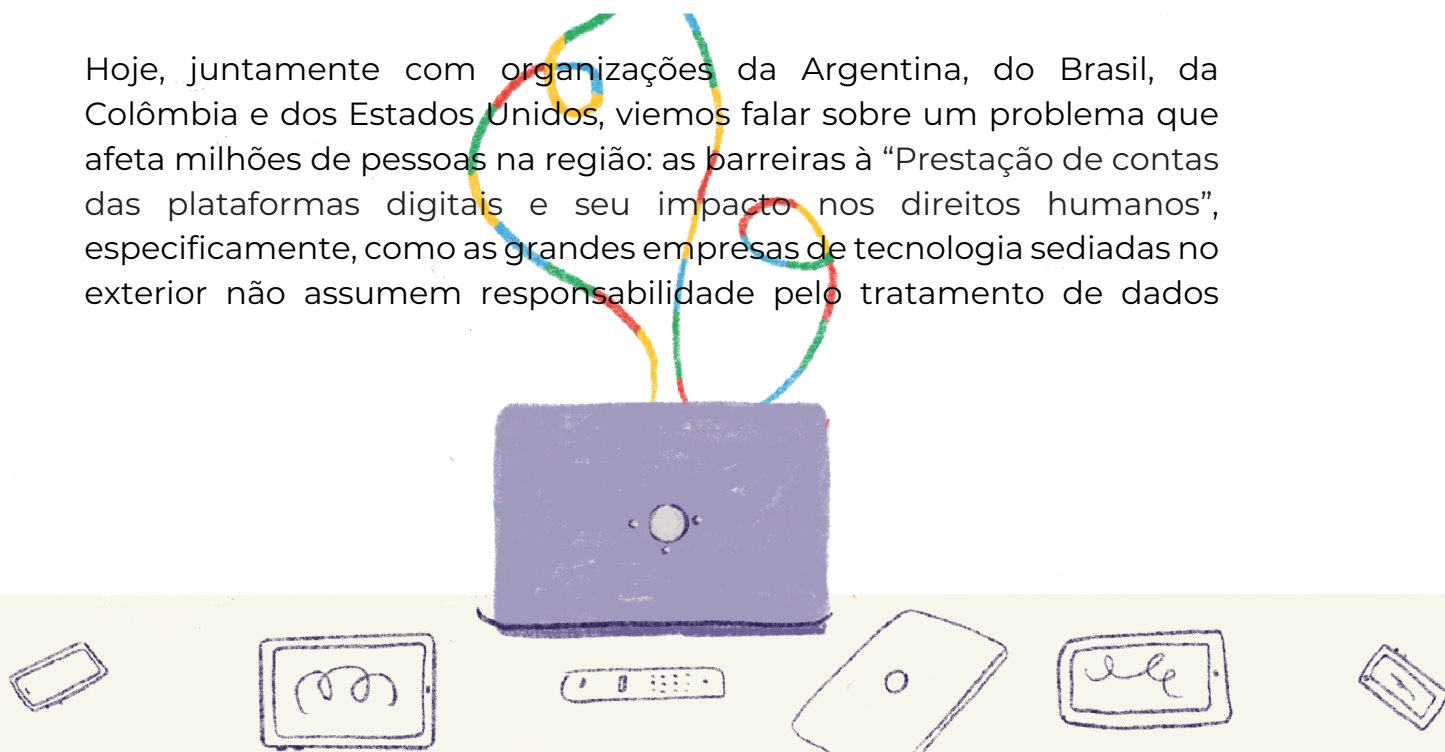
Como parte do processo de preparação para a audiência, nós, as requerentes, apresentamos algumas contribuições prévias à CIDH, que decidimos tornar públicas devido à sua utilidade acadêmica. Além disso, como parte do resumo executivo desta publicação, apresentamos as intervenções orais de cada um dos representantes das organizações requerentes.

ABERTURA: DEJUSTICIA

Ilustres membros da Comissão Interamericana de Direitos Humanos e relatores, agradeço por este valioso espaço, que demonstra a grande relevância do tema para a região.

Meu nome é Maryluz Barragán González e sou subdiretora do Centro de Direito, Justiça e Sociedade – Dejusticia. Uma ONG colombiana com mais de 20 anos de trabalho em defesa dos direitos humanos, da democracia e do Estado de Direito.

Hoje, juntamente com organizações da Argentina, do Brasil, da Colômbia e dos Estados Unidos, viemos falar sobre um problema que afeta milhões de pessoas na região: as barreiras à “Prestação de contas das plataformas digitais e seu impacto nos direitos humanos”, especificamente, como as grandes empresas de tecnologia sediadas no exterior não assumem responsabilidade pelo tratamento de dados



peçoais dos cidadãos e, com isso, violam maciçamente nosso direito ao habeas data e outros direitos fundamentais.

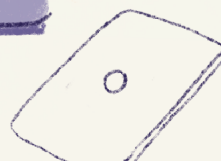
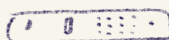
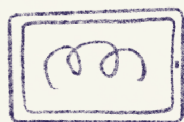
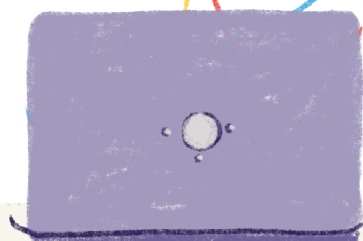
Nesta primeira parte, vou me concentrar na questão da jurisdição e das leis aplicáveis às empresas de tecnologia. Em seguida, meus colegas abordarão os impactos concretos em questões como a integridade democrática, a saúde mental e os efeitos diferenciados na infância.

As empresas de tecnologia baseiam seu modelo de negócios na exploração em massa de dados pessoais. Por meio de tecnologias como cookies, SDKs (kits de desenvolvimento de software) e pixels (que são instalados nos dispositivos dos usuários), elas coletam, armazenam e monetizam informações íntimas: localização, hábitos de consumo e até mesmo dados de saúde. Sobre este último ponto, há pesquisas de 2022 que constataram que rastreadores da Meta em sites de telessaúde enviavam ao Facebook informações íntimas dos pacientes. Tudo dentro da legalidade, o que revela uma lacuna regulatória.

O importante para esta Comissão é o seguinte: esse tratamento de dados ocorre fisicamente em nossos países, nos países da América Latina. O dispositivo onde o cookie é instalado, onde o SDK é executado, onde o pixel é exibido, está na Colômbia ou em qualquer outro país da região. Não se trata de um detalhe técnico: é onde ocorre o dano.

No entanto, empresas como o Google iniciaram ações judiciais na Colômbia para contestar a competência da Superintendência de Indústria e Comércio, argumentando que o tratamento ocorre em servidores no exterior. Essa postura contradiz a tendência jurisprudencial internacional e comparada. O Tribunal de Justiça da União Europeia, nos casos Google Spain, Google v. CNIL e Schrems I e II, foi enfático: as empresas não podem se esquivar da legislação local alegando domicílio no exterior quando sua atividade afeta pessoas dentro do território. Até mesmo um tribunal canadense, no caso Giustra vs. Twitter, rejeitou o mesmo argumento.

Ou seja: o mundo caminha para o reconhecimento da jurisdição local. Mas os países do Sul Global, sem o peso político da União Europeia,



enfrentam maior resistência dessas empresas para fazer valer suas próprias leis. De fato, os Estados Unidos, mais recentemente, assinaram acordos comerciais recíprocos com quatro países da América (Argentina, Equador, Guatemala e El Salvador) que poderiam enfraquecer a proteção dos dados pessoais. Meu colega do CELS explicará isso com mais detalhes.

Este não é um debate abstrato. Quando essas empresas se subtraem à jurisdição, deixam milhões de pessoas indefesas diante do uso manipulador de seus dados. Estamos falando aqui de impactos concretos na saúde mental causados por designs viciantes, riscos para grupos vulneráveis e influência indevida em processos democráticos, como veremos nas próximas intervenções.

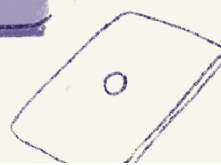
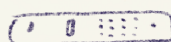
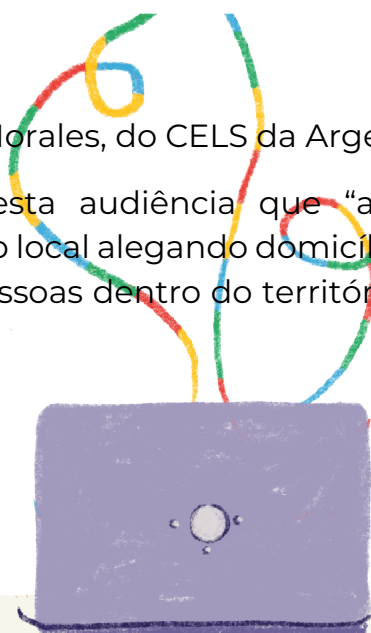
Por isso, solicitamos respeitosamente à Comissão que considere: em primeiro lugar, a elaboração de um relatório temático ou de diretrizes regionais sobre a responsabilidade das empresas de tecnologia em relação aos direitos humanos, incluindo o habeas data, na região. Em segundo lugar, que exorte os Estados-membros a fortalecerem seus marcos normativos de proteção de dados com critérios claros de jurisdição, em consonância com os padrões já existentes no direito comparado.

A questão fundamental é simples: as empresas mais poderosas do mundo podem decidir a quais leis se submetem? Nossa posição é que não. A proteção dos direitos humanos não pode depender da localização de um servidor. Muito obrigado.

CELS

Meu nome é Diego Morales, do CELS da Argentina.

Já foi destacado nesta audiência que “as empresas não podem contornar a legislação local alegando domicílio no exterior quando suas atividades afetam pessoas dentro do território”. Acrescentamos agora



3



mais uma preocupação, que é a questão da transferência transnacional de dados pessoais.

À tendência de enfraquecimento dos marcos de prestação de contas das plataformas soma-se o risco associado aos acordos econômicos bilaterais promovidos pelos Estados Unidos, que alteram os padrões de proteção de dados de outros países para facilitar o tráfego transnacional de dados para aquele país. Em particular, vamos nos referir ao acordo assinado em fevereiro deste ano entre os Estados Unidos e a Argentina.

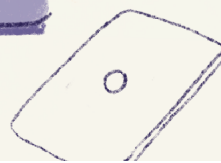
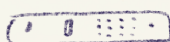
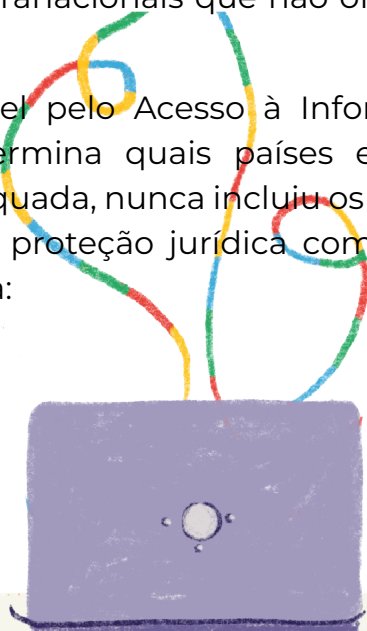
Trata-se de um acordo ainda não ratificado sobre “investimento e comércio recíproco”, que implica que a Argentina reduza ou elimine barreiras tarifárias e não tarifárias e conceda privilégios comerciais aos produtos norte-americanos.

Esse acordo já foi mencionado na audiência de ontem sobre a situação do direito à saúde na Argentina, pois nosso país, por decisão unilateral, decidiu revogar os critérios rigorosos de patenteabilidade de medicamentos.

No que aqui interessa, o artigo 2º do anexo 3 do acordo contém uma alteração ao marco jurídico nacional em matéria de dados pessoais. E estabelece que, para fins de transferência de dados para os Estados Unidos, a Argentina considerará que os Estados Unidos garantem uma proteção jurídica “adequada” para tais dados. A Argentina, além disso, “proporcionará certeza quanto à possibilidade de transferir dados pessoais de seu território para os Estados Unidos”.

No entanto, o artigo 12 da Lei de Dados Pessoais proíbe a transferência desses dados, de qualquer tipo, para “países ou organizações internacionais ou supranacionais que não ofereçam níveis adequados de proteção”.

A agência responsável pelo Acesso à Informação Pública, que é a autoridade que determina quais países e organizações oferecem proteção jurídica adequada, nunca incluiu os Estados Unidos na lista de países que oferecem proteção jurídica com essas características. Na opinião dessa agência:



- Os Estados Unidos carecem de uma regulamentação federal uniforme sobre o tratamento de dados pessoais e de uma autoridade de controle eficaz.
- E que as normas de “autorregulação” não são exigíveis nem uniformes nos cinquenta estados da União.

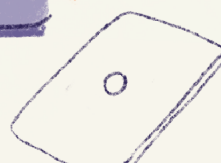
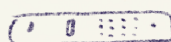
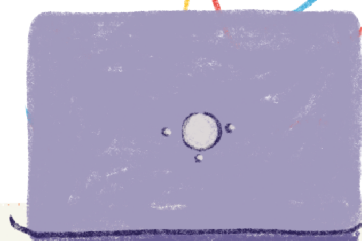
O acordo, portanto, cria uma exceção à proibição de transferências de dados pessoais. Isso pode ocorrer devido à entrada em vigor de um “tratado internacional do qual a Argentina é parte” — questão prevista pela própria lei de dados pessoais — ou porque a Agência de Acesso à Informação Pública emita uma resolução declarando que os Estados Unidos são uma jurisdição adequada. Isso contraria a avaliação que a agência argentina já formulou em diversas ocasiões.

Qualquer uma dessas situações implicaria autorizar transferências internacionais de dados para um país que não é considerado uma “jurisdição adequada” pelo governo argentino, sem que as circunstâncias nesse país tenham mudado. Ou, o que é ainda mais grave, que tenham piorado devido a o uso dos dados como ferramenta de vigilância (por exemplo, contra migrantes) e/ou por sua aliança estratégica com empresas de inteligência artificial e processamento de grandes volumes de dados.

Com esse tipo de acordo, a transferência ou venda de dados pessoais a responsáveis ou encarregados do tratamento norte-americanos (incluindo as grandes empresas de tecnologia) não estará mais sujeita às normas da lei de proteção de dados pessoais da Argentina.

A Suprema Corte, em um caso recente, declarou inconstitucional um artigo da lei de dados pessoais que permitia a cessão de dados pessoais entre órgãos do mesmo Estado, mas sem o consentimento específico dos interessados. O Tribunal sustentou que os artigos 19 (autonomia) e 43, parágrafo 3 (habeas data), da Constituição Nacional consagram o direito à autodeterminação informativa — questão já reconhecida pela Corte Interamericana de Direitos Humanos no caso CAJAR.

No entanto, as transferências de dados para os Estados Unidos (seja para as autoridades ou para empresas) deixarão de estar sujeitas às garantias constitucionais ou aos princípios estabelecidos pela Lei de Proteção de Dados Pessoais, como o consentimento, a finalidade ou a



habilitação de uma instância de proteção legal de habeas data para limitar seu tratamento. Além disso, essas transferências, nos termos do acordo, não estarão sujeitas às competências de supervisão da Agência de Acesso à Informação Pública.

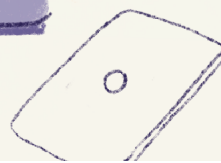
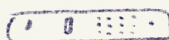
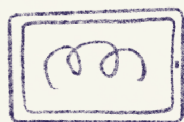
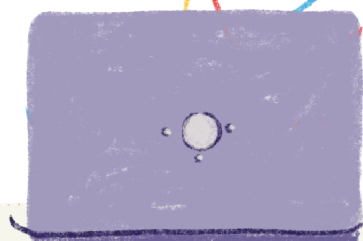
Consequentemente, propomos à Comissão que inclua no referido Relatório uma análise específica sobre os efeitos de acordos transnacionais como o mencionado nos marcos nacionais de proteção de dados e que analise sua compatibilidade com os compromissos assumidos no âmbito da CADH.

ARTIGO 19

Prezados representantes da Comissão Interamericana de Direitos Humanos, bom dia. Meu nome é Raquel da Cruz Lima e represento a ARTÍCULO 19 Brasil e América do Sul.

O objetivo desta intervenção é chamar a atenção da Comissão para um dos aspectos estruturais que permitem que as grandes plataformas digitais manipulem o debate público e afetem a integridade democrática e o exercício dos direitos humanos nas Américas: a profunda concentração do poder econômico.

Como já foi exposto por meus colegas, o modelo de negócios dessas corporações baseia-se na coleta massiva de dados pessoais e na amplificação algorítmica para reter a atenção. Esse modelo não apenas gera lucros extraordinários, mas também é um mecanismo que produz e reproduz a concentração do poder econômico. Ao controlar os dados de bilhões de pessoas e as infraestruturas pelas quais a informação circula, essas empresas acumulam poder suficiente para definir as condições sob as quais as ideias e os pensamentos podem circular. As implicações são diretas para a liberdade de pensamento e de expressão, para os direitos políticos, a igualdade e a não discriminação, conforme definidos nos artigos 13, 23, 24 e 1.1 da CADH. O funcionamento dos sistemas de recomendação baseados no engajamento prioriza a circulação de conteúdos extremos e polarizadores, afetando de maneira desproporcional os grupos historicamente marginalizados e dificultando sua participação política



em condições de igualdade. Outra dinâmica que afeta a participação política de grupos historicamente vulneráveis, especialmente a comunidade LGBTQIAPN+, é o “shadow banning”, ou seja, a redução da visibilidade ou do alcance de seus conteúdos.

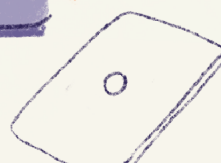
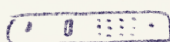
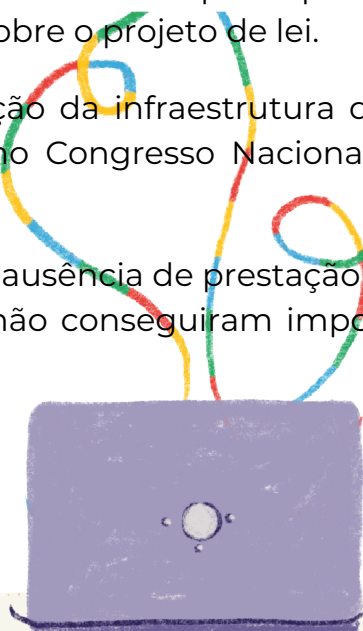
Esse poder das plataformas de definir quais vozes serão ouvidas na esfera pública decorre da concentração de poder nas mãos de poucas empresas. De fato, no relatório “Inclusão Digital e Governança de Conteúdos”, a RELE e a Comissão afirmaram que a Internet é marcada pelo domínio de poucos grandes atores do setor tecnológico, o que afeta negativamente a diversidade na infraestrutura de comunicação. Gostaria também de salientar que o Marco Jurídico Interamericano sobre o Direito à Liberdade de Expressão reconhece que os monopólios ou oligopólios na propriedade e no controle dos meios de comunicação restringem a pluralidade e a diversidade da informação. Quero afirmar, nesta ocasião, que, atualmente, esse poder de restrição indireta sobre a liberdade de expressão está principalmente nas mãos das plataformas digitais.

No Brasil, isso ficou evidente durante as discussões do Projeto de Lei 2.630, que buscava estabelecer mecanismos de prestação de contas para essas empresas. Diante da votação iminente do projeto, o Google abusou de sua posição dominante, com mais de 80% do mercado de buscas.

A empresa alterou o design de sua página inicial, inserindo abaixo da barra de busca um link que afirmava que o projeto “poderia aumentar a confusão sobre o que é verdadeiro ou falso no Brasil”. Simultaneamente, pesquisadores comprovaram que o mecanismo de busca manipulava os resultados para quem utilizava o Google para buscar informações sobre o projeto de lei.

Essa instrumentalização da infraestrutura digital conseguiu alterar o equilíbrio de forças no Congresso Nacional e impedir a votação do projeto de lei.

O mais alarmante é a ausência de prestação de contas que se seguiu a isso. As autoridades não conseguiram impor sanções nem alterar de



forma significativa a capacidade dessas empresas de usar suas próprias ferramentas para influenciar o debate público.

Conforme alerta a Resolução 2/26 da REDESCA sobre Políticas Fiscais e Direitos Humanos, a concentração de poder e a captura das instituições privam as decisões públicas de uma deliberação efetiva e de uma orientação para o interesse geral. O caso brasileiro revela a ausência de instrumentos adequados para enfrentar a concentração do poder econômico em si.

Portanto, entendemos que a proteção do debate público requer o combate estrutural a essa assimetria de poder. Nesse sentido, solicitamos respeitosamente que esta Comissão considere:

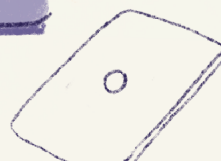
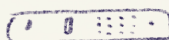
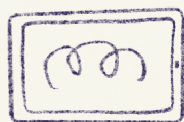
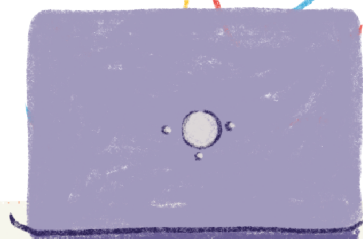
1. Reconhecer que a concentração do poder econômico nas plataformas digitais constitui uma restrição indireta à liberdade de expressão e uma ameaça estrutural ao pluralismo informativo e à integridade dos processos eleitorais.
2. Afirmar a necessidade de que os Estados fortaleçam suas autoridades de concorrência com uma abordagem baseada nos direitos humanos, dotando essas instituições de independência e de um poder sancionatório eficaz para prevenir a captura corporativa e punir os abusos de posição dominante nos mercados digitais.

Muito obrigada.

TECH JUSTICE

Meu nome é Tiffany Brown e sou advogada litigante na Tech Justice Law. A Tech Justice Law é uma organização sem fins lucrativos e apartidária, dedicada a promover a prestação de contas, a transparência e a justiça no setor tecnológico. Em 2024, entramos com a primeira ação judicial contra uma empresa de inteligência artificial por seu produto de chatbot defeituoso e, desde então, movemos cerca de dez ações semelhantes.

Trabalhamos de forma colaborativa com líderes das áreas do direito, da tecnologia e da pesquisa para defender aqueles que foram



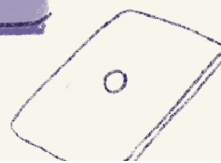
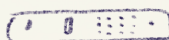
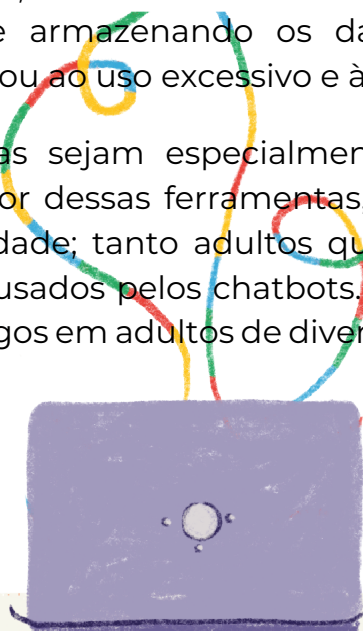
prejudicados por produtos tecnológicos e para responsabilizar as empresas de tecnologia por esses danos. É uma honra estar aqui hoje para compartilhar nossas preocupações e analisar os caminhos rumo a um marco de prestação de contas tecnológica que coloque no centro a dignidade, a privacidade e a liberdade cognitiva.

- Projeto de produtos de IA generativa e implicações para os direitos humanos

Enquanto os consumidores continuam a sofrer o impacto dos danos causados pelas plataformas de redes sociais, enfrentamos agora uma nova ameaça crescente: a implantação irrestrita de produtos de inteligência artificial generativa, especificamente os chatbots. Para muitas pessoas, os chatbots deixaram de ser novidades para se tornarem elementos constantes do nosso cotidiano. Nos Estados Unidos, um em cada quatro adultos conversa diariamente com chatbots de IA. Psicólogos afirmam que seus pacientes recorrem cada vez mais aos chatbots em busca de companhia e como substitutos de terapeutas. As pessoas procuram os chatbots em vez de médicos licenciados para obter orientação médica. Mais da metade dos adolescentes usa chatbots; 16% deles os utilizam várias vezes ao dia ou “quase constantemente”.

A rápida e generalizada disseminação dos chatbots de IA causou graves danos às sociedades em todo o mundo. Embora os chatbots não passem de produtos — máquinas sofisticadas programadas para gerar linguagem, prevendo palavras a partir de dados de treinamento e algoritmos complexos —, não é assim que muitos consumidores os percebem. As empresas de IA projetaram os chatbots para gerar confiança nos usuários, imitando a fala humana, produzindo respostas que os reafirmam e armazenando os dados dos usuários como “memórias”, o que levou ao uso excessivo e à dependência emocional.

E embora as crianças sejam especialmente suscetíveis ao design viciante e manipulador dessas ferramentas, a vulnerabilidade não se define apenas pela idade; tanto adultos quanto crianças podem ser vítimas dos danos causados pelos chatbots. Por exemplo, temos visto chatbots causar estragos em adultos de diversas origens que se sentem



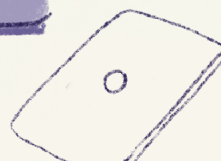
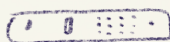
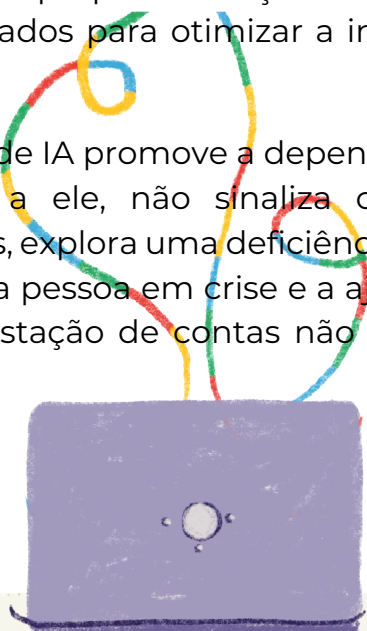
solitários, estão isolados, buscam orientação médica ou enfrentam deficiências de saúde mental.

Os danos causados pelos chatbots incluem suicídio e outras formas de automutilação, indução de delírios relacionados à IA, negligência médica e danos a terceiros, como homicídio e cyberassédio. A total ausência de transparência em torno dos testes de segurança permite que esses danos fiquem fora de controle. Portanto, os produtos de IA devem ser considerados um problema significativo de saúde pública que exige uma atenção regulatória robusta.

No entanto, o governo dos Estados Unidos está tentando impedir qualquer tipo de regulamentação da IA, por considerar que a imposição de regulamentações sufocaria a inovação tecnológica. Por isso, buscar reparação por meio de tribunais nacionais, regionais e estrangeiros é fundamental; o litígio é uma via primordial para a prestação de contas. Foram movidas aproximadamente 50 ações judiciais contra as maiores empresas de IA generativa nos Estados Unidos em relação a esses danos.

Várias disposições do direito internacional, incluindo a Convenção Americana, são afetadas por esses produtos. Uma disposição que gostaríamos de destacar é o Artigo 13, que protege a liberdade de pensamento, não apenas em termos de autodeterminação informativa, mas como um direito que inclui a liberdade contra a doutrinação e a manipulação mal-intencionadas. Quando um sistema de IA é capaz de alterar de forma mensurável o que uma pessoa acredita sobre sua própria realidade, trata-se de uma violação dos direitos humanos. E, em muitos dos casos que observamos, o direito à autodeterminação — de escolher livremente as próprias crenças — está sendo usurpado por sistemas de IA projetados para otimizar a interação e a dependência dos usuários.

Quando um produto de IA promove a dependência emocional de uma criança em relação a ele, não sinaliza conversas relacionadas a pensamentos suicidas, explora uma deficiência que a pessoa revelou ou se interpõe entre uma pessoa em crise e a ajuda humana que poderia salvar sua vida, a prestação de contas não deveria ser opcional. Não



estamos pedindo que a inovação seja interrompida; ao contrário, defendemos que a inovação sem salvaguardas centradas no ser humano não é progresso. É perigosa. Os produtos de IA devem, além disso, ser submetidos a testes de segurança exaustivos e a auditorias independentes. A IA deve ser centrada no ser humano; construída para ampliar a dignidade e a autonomia humanas, não para corroê-las.

Muito obrigada.

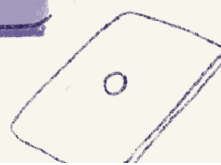
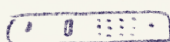
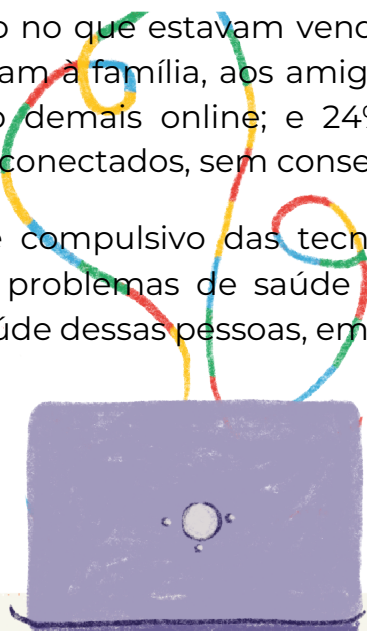
INSTITUTO ALANA

Prezados representantes da Comissão Interamericana de Direitos Humanos e demais participantes da sociedade civil, bom dia.

Na qualidade de representante do Instituto Alana, uma organização dedicada a valorizar a infância e a proteger e promover seus direitos, gostaria de destacar alguns dos impactos que esse segmento particularmente vulnerável da população sofre em decorrência da incorporação de padrões de design viciantes na arquitetura das plataformas digitais.

Os dados da pesquisa TIC Kids Online Brasil de 2024 mostram que a perda de controle sobre o tempo de uso da internet já afeta um grande número de brasileiros entre 9 e 17 anos, o que reflete padrões de dependência tecnológica e efeitos prejudiciais sobre atividades cotidianas essenciais para seu desenvolvimento, sua saúde e seu bem-estar. De acordo com a pesquisa, 15% das crianças e adolescentes entrevistados pularam refeições ou deixaram de dormir por causa da internet; 16% se sentiram angustiados em algum momento por não poderem ficar online; 22% se pegaram navegando na internet sem ter um interesse genuíno no que estavam vendo; 22% dedicaram menos tempo do que deveriam à família, aos amigos ou às tarefas escolares por passarem tempo demais online; e 24% afirmaram ter tentado passar menos tempo conectados, sem conseguir.

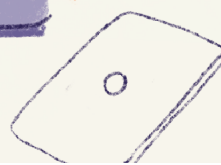
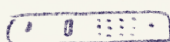
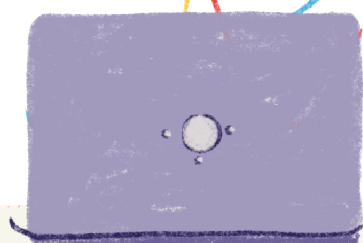
Esse uso excessivo e compulsivo das tecnologias digitais tem sido associado a diversos problemas de saúde mental que colocam em questão o direito à saúde dessas pessoas, em particular a depressão e a



ansiedade, conforme indicado por um conjunto de evidências. Já em maio de 2023, o Cirurgião-Geral dos Estados Unidos emitiu um alerta urgente de saúde pública sobre o impacto do uso das redes sociais na saúde mental e no bem-estar de crianças e adolescentes, ressaltando que os jovens que passam mais de três horas por dia nessas plataformas correm o dobro de risco de desenvolver problemas de saúde mental.

No entanto, os casos clinicamente diagnosticados de depressão, ansiedade e transtornos de saúde mental representam apenas o aspecto mais agudo e grave do conjunto mais amplo de danos potenciais causados pelo uso excessivo de dispositivos digitais durante a infância. Isso se deve ao fato de que tal uso também gera um custo de oportunidade que impede os jovens de viver plenamente sua infância e preenchê-la com experiências que maximizem o potencial dessa etapa única da vida humana. Deve-se garantir às crianças e aos adolescentes tempo para brincadeiras livres — um direito reconhecido explicitamente no artigo 31 da Convenção sobre os Direitos da Criança (CDC) —, bem como tempo para o afeto, o contato com a natureza, o estudo, o descanso e o lazer. Portanto, o design viciante reduz o tempo disponível para outras atividades essenciais ao seu desenvolvimento saudável e integral e para o pleno vivenciamento da infância e da adolescência; pior ainda, os padrões de design viciante privam-nos da autonomia sobre como administram seu tempo e fragmentam sua atenção, o que dificulta que se dediquem a atividades como a leitura e a aprendizagem de longo prazo.

Em termos gerais, o design viciante das redes sociais compromete a integridade física e psicológica das crianças — violando o artigo 5º da Convenção Americana sobre Direitos Humanos — e atenta contra a garantia de um nível de vida adequado para seu desenvolvimento físico, mental, espiritual, moral e social, conforme garantido pelo artigo 27 da Convenção sobre os Direitos da Criança (CDC). No entanto, uma resposta adequada a esse problema requer algo mais do que simplesmente proibir o acesso das crianças às redes sociais; tais medidas são difíceis de implementar na prática e, em última instância, isentam as empresas de tecnologia da necessidade de revisar seus modelos de negócios e transformar seus produtos.

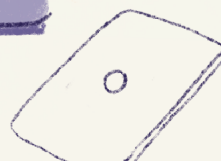
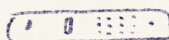
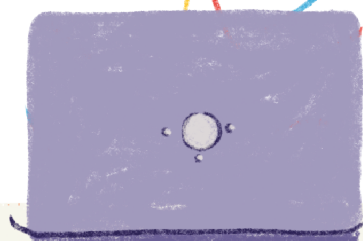


Portanto, são necessários marcos regulatórios que se apliquem a todos os aplicativos utilizados por crianças no ambiente digital, que exijam que os provedores tratem os direitos dessas pessoas como uma prioridade absoluta e incorporem a proteção e a promoção desses direitos na arquitetura de seus serviços digitais. É exatamente isso que dispõe a Observação Geral nº 25 (OG25) do Comitê dos Direitos da Criança da ONU, um documento que detalha como os Estados-membros devem interpretar e implementar a CDN no que se refere ao ambiente digital.

O Estado brasileiro deu um passo importante nessa direção com a aprovação, em 2025, da Lei nº 15.211, mais conhecida como “ECA Digital”. Trata-se de uma lei abrangente que se aplica a todos os produtos e serviços de tecnologia da informação voltados para crianças e adolescentes — ou suscetíveis de serem acessados por eles. Ela exige que esses serviços incorporem medidas de segurança e proteção em suas arquiteturas e que identifiquem e mitiguem os riscos que representam para os jovens, ao mesmo tempo em que designa uma autoridade responsável por supervisionar o cumprimento e, quando for o caso, sancionar os agentes econômicos que descumprirem essas obrigações.

Além de impor amplas obrigações a todos os fornecedores de produtos e serviços digitais que afetam a vida das crianças, a ECA Digital introduz proibições específicas relevantes para o tema desta audiência. A lei exige que a configuração padrão dos serviços digitais não induza ao uso compulsivo e proíbe a incorporação de padrões de design nas interfaces digitais que possam manipular as crianças ou prejudicar seus direitos. Da mesma forma, proíbe a criação de perfis comportamentais das crianças para fins publicitários e a promoção de conteúdos que possam retratar as crianças de forma erotizada.

A experiência brasileira ainda se encontra em seus estágios iniciais, mas acreditamos que possa oferecer contribuições significativas para o debate regional. Os desafios que o Brasil enfrenta não são exclusivos do país, mas são compartilhados por praticamente todas as nações das Américas. Por isso, acreditamos que fortalecer padrões regionais comuns para a proteção da infância e da adolescência no âmbito digital



poderia representar um passo significativo para a promoção de seus direitos em toda a nossa região.

Muito obrigado.

REDE PAPA

Exmos. Comissários, membros da Comissão Interamericana de Direitos Humanos e presentes: uma saudação cordial.

Sou Carolina Piñeros, diretora executiva da Rede PaPaz Colômbia, e estou aqui como representante da sociedade civil para complementar o que já foi dito com nossos argumentos sobre o impacto das plataformas digitais nos direitos de meninas, meninos e adolescentes.

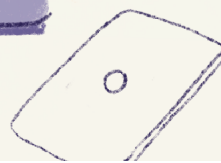
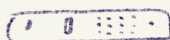
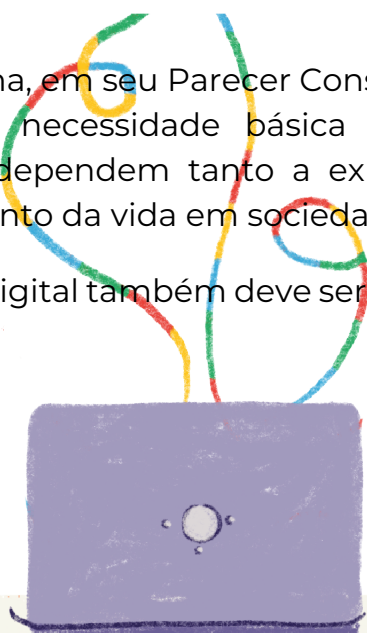
Agradeço a convocação para esta audiência tão necessária, que nos permite dar visibilidade ao imenso desafio que temos pela frente: meninas, meninos e adolescentes crescendo em ambientes digitais projetados por empresas privadas, que não priorizam o cuidado com eles.

Conforme reconhecido pelo Comitê dos Direitos da Criança em sua Observação Geral nº 25, o ambiente digital é o espaço onde, hoje, as crianças passam uma parte significativa de sua vida, constroem laços afetivos, formam sua identidade e exercem seus direitos.

Esse ambiente possui uma característica determinante: é um espaço projetado. Cada botão, notificação e algoritmo é uma decisão das empresas privadas. Quando elas projetam o ambiente onde a vida se desenrola, também projetam as condições para o seu desenvolvimento.

A Corte Interamericana, em seu Parecer Consultivo nº 31, reconheceu o cuidado como uma necessidade básica e ineludível, um direito autônomo, do qual dependem tanto a existência da vida humana quanto o funcionamento da vida em sociedade.

Por isso, o ambiente digital também deve ser um ambiente de cuidado.



A questão fundamental é: o design não neutro das plataformas facilita ou impossibilita o cuidado?

Hoje, as plataformas operam sob uma lógica de maximização da atenção: quanto maior o tempo de permanência, mais dados, mais segmentação comercial e mais valor econômico. Essa lógica faz com que os interesses econômicos se sobreponham ao Interesse Superior da Criança, impossibilitando seu cuidado.

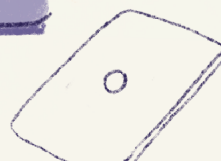
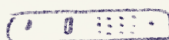
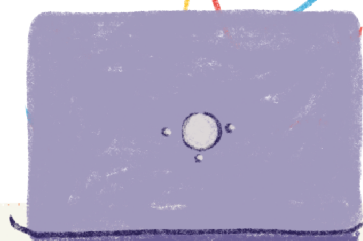
Isso levanta três desafios para o bem-estar e a proteção da infância:

- Primeiro, designs viciantes por padrão que promovem a hipersegmentação para produtos nocivos e riscos digitais crescentes, como violência sexual, exploração, recrutamento e o antropomorfismo da IA.
- Segundo, a transferência desproporcional da responsabilidade pelo cuidado para as famílias e escolas, em detrimento das gigantes da tecnologia.
- Em terceiro lugar, a ausência de visibilidade, exigibilidade e prestação de contas.

Diante de um problema estrutural, uma resposta estrutural. De acordo com o artigo 19 da Convenção Americana, nenhuma métrica comercial nem algoritmo deveria estar acima do bem-estar de meninas, meninos e adolescentes.

Por isso, da Colômbia, a Rede PaPaz e, de forma mais ampla, a sociedade civil, fazemos três apelos à Comissão:

1. Reconhecer expressamente que as obrigações estatais de proteção sejam aplicadas com o mesmo rigor nos ambientes digitais.
2. Desenvolver uma Norma Interamericana relacionada às obrigações internacionais relativas aos direitos ao cuidado e ao artigo 19 da Convenção, que obrigue as plataformas a demonstrar, de forma verificável, que o bem-estar das crianças prevalece sobre os incentivos de monetização.
3. Exigir mecanismos **eficazes** de transparência, supervisão independente e prestação de contas.



Por fim, solicitamos respeitosamente à Ilustre Comissão que avance na elaboração de um Relatório Temático sobre os Direitos da Criança e do Adolescente no Ambiente Digital ou que incorpore, de forma prioritária, esses critérios em seus Relatórios Especiais; contem com nosso interesse em apoiar esse processo.

Muito obrigado.

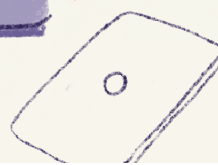
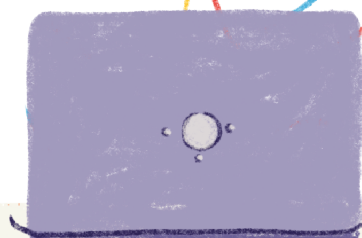
ENCERRAMENTO: DEJUSTICIA

As violações descritas nesta audiência (relacionadas à interferência das plataformas na integridade democrática e à concentração econômica descontrolada, ao design viciante sem prestação de contas, à exploração estatal e comercial de dados) compartilham um facilitador estrutural comum: as grandes plataformas tecnológicas sediadas no exterior negam sistematicamente que sua conduta esteja sujeita à jurisdição dos Estados onde vivem seus usuários e onde ocorre o dano.

Essa preocupação não é alheia à própria Comissão. Em seu Relatório Temático de junho de 2024, “Inclusão digital e governança de conteúdos na internet”, a Relatoria Especial para a Liberdade de Expressão já havia alertado que o controle da experiência digital recai sobre poucos atores dominantes, públicos e privados, e pediu o estabelecimento de marcos jurídicos garantistas que delimitem as responsabilidades desses atores dominantes. Esse mesmo relatório convidou a uma reflexão sobre a governança interna das empresas de tecnologia e pediu que elas reafirmassem seu compromisso democrático por meio de mecanismos internos de controle para a tomada de decisões que afetem os direitos humanos. O que solicitamos hoje é a extensão desse mesmo princípio (responsabilidade dos atores dominantes) ao âmbito específico da proteção de dados pessoais, onde ainda não existe um desenvolvimento equivalente.

Por isso, solicitamos a elaboração de um relatório temático sobre a prestação de contas das plataformas tecnológicas e seus impactos nos direitos humanos, que contribua ou avance na seguinte direção:

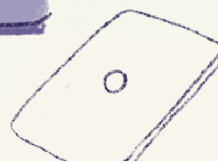
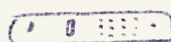
- Desenvolver um padrão interamericano de devida diligência estatal em relação às plataformas digitais: prevenir, investigar,



punir e reparar as violações dos direitos fundamentais. Que a CIDH elabore um padrão convencional (artigos 1.1 e 2) que esclareça a obrigação dos Estados de garantir os direitos humanos diante da evasão jurisdicional das empresas tecnológicas privadas.

- Que a CIDH elabore critérios de transparência e supervisão relacionados à proteção de dados pessoais, privacidade e liberdade de pensamento, especificamente no que diz respeito à atividade comercial das plataformas e ao uso por parte dos Estados.
- Que a CIDH reconheça expressamente que a obrigação de proteger a infância se aplica com o mesmo rigor em ambientes digitais, elabore um padrão interamericano vinculado ao artigo 19 da Convenção sobre exploração infantil e monetização e priorize esses critérios em seus relatórios, em particular diante dos impactos do design viciante.

Agradecemos profundamente que a comissão tenha aceitado esta audiência, dada a necessidade e a urgência com que devemos discutir este tema. Gostaríamos de conhecer as prioridades da comissão nesse sentido e, como sociedade civil, estamos abertos a um diálogo no âmbito desta audiência e em futuros processos de trabalho, neste momento tão relevante para a região.

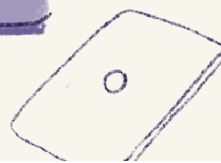
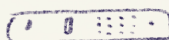
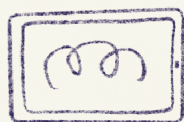
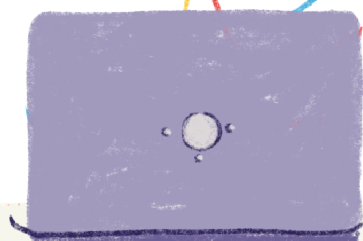


SUBSÍDIOS APRESENTADOS À CIDH PREVIAMENTE¹ À AUDIÊNCIA TEMÁTICA SOBRE A RESPONSABILIDADE DAS PLATAFORMAS DIGITAIS E SEU IMPACTO NOS DIREITOS HUMANOS.

PS 196-1983.

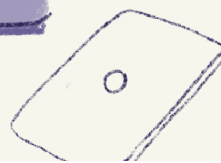
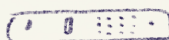
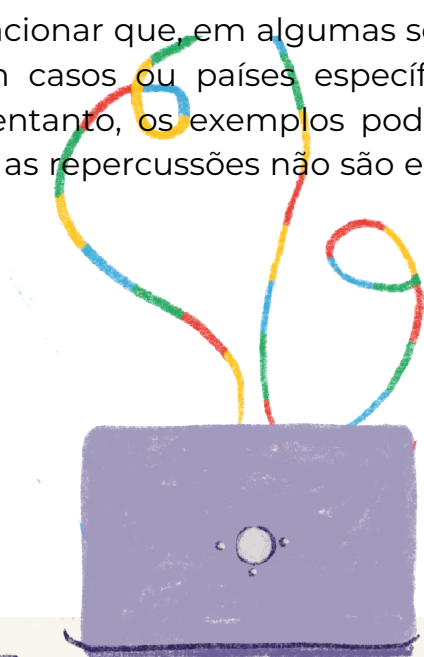
1.	A falta de prestação de contas por parte das empresas de tecnologia digital sediadas no exterior e sua relutância em se submeter às nossas jurisdições	20
1.1.	Contexto geral: modelos de negócios na era digital.....	20
1.2.	Sobre o tratamento de dados pessoais.....	22
1.2.1.	Cookies	23
1.2.2.	SDK.....	25
1.2.3.	Pixels	27
1.3.	O tratamento de dados pessoais por meio dessas tecnologias ocorre na Colômbia e em outros países do Sul Global.....	29
1.4.	As principais plataformas tiveram que prestar contas perante outras jurisdições	32
1.4.1.	O caso Google Spain contra AEPD (2014).....	32
1.4.2.	O caso Google contra CNIL (2019).....	33
1.4.3.	Os processos Schrems I (2015) e Schrems II (2020).....	34
1.4.4.	O caso do Twitter no Canadá: Giustra contra Twitter, Inc. (2021)	35
1.4.5.	O processo contra a Microsoft julgado pelo Superior Tribunal de Justiça do Brasil (2020)	36

¹ Foram feitas algumas alterações mínimas após a audiência. Algumas seções deste relatório foram traduzidas de sua versão original usando o DeepL.



1.4.6. O caso P.A.E. contra Facebook Argentina S.R.L. (medida cautelar de 2019)	37
1.5. O caso da tributação	38
1.6. Conclusão: As empresas de tecnologia estão violando os direitos à proteção de dados pessoais e outros direitos fundamentais de milhões de pessoas que vivem em países como a Colômbia ao se recusarem a cumprir a legislação nacional e a reconhecer a jurisdição de suas autoridades.	40
2. Enfraquecimento das normas de proteção de dados pessoais coletados pelas plataformas e sua transferência para os Estados Unidos em virtude de acordos bilaterais	41
3. Impactos dos modelos de negócios baseados em dados nos direitos fundamentais e humanos	45
3.1. Repercussões no voto, na igualdade e na não discriminação	45
3.2. Manipulação do debate público: o caso do Projeto de Lei 2630 do Brasil	51
3.3. Efeitos sobre a saúde mental relacionados principalmente às plataformas de IA generativa	56
3.4. Repercussões nos direitos das crianças.....	61
3.4.1. Os sistemas algorítmicos de recomendação de conteúdo devem ser reconhecidos como um componente integral do design viciante das redes sociais.	61
3.4.2. Os impactos específicos dos sistemas de recomendação algorítmica na vida e nos direitos de crianças e adolescentes.....	67

É importante mencionar que, em algumas seções do documento, nos concentramos em casos ou países específicos para ilustrar nossos argumentos. No entanto, os exemplos podem se repetir em outros países da região e as repercussões não são exclusivas de nenhum país em particular.



1. A FALTA DE PRESTAÇÃO DE CONTAS POR PARTE DAS EMPRESAS DE TECNOLOGIA DIGITAL SEDIADAS NO EXTERIOR E SUA RELUTÂNCIA EM SE SUBMETER ÀS NOSSAS JURISDIÇÕES

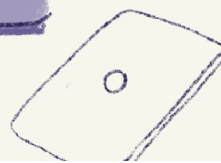
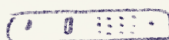
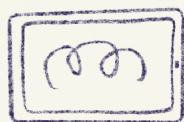
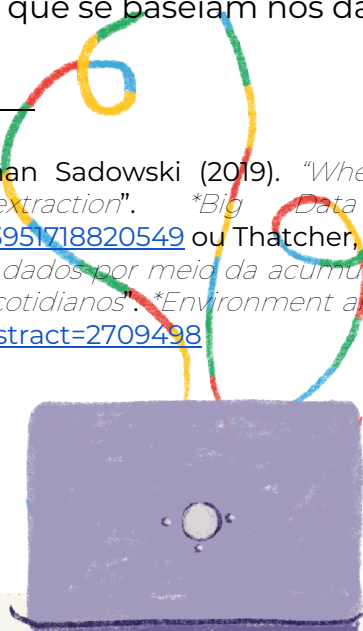
***Nota:** Parte das informações apresentadas nesta seção baseia-se em pesquisas anteriores e documentos elaborados para processos judiciais na Colômbia.

1.1. CONTEXTO GERAL: MODELOS DE NEGÓCIOS NA ERA DIGITAL

A tecnologia digital permeou a vida das pessoas e o funcionamento dos Estados a tal ponto que transformou radicalmente a economia, bem como as relações sociais, trabalhistas e políticas, entre muitos outros âmbitos. No entanto, ela também agravou as desigualdades pré-existentes, permitindo o fortalecimento econômico de poucas entidades poderosas que contribuíram para o que a literatura tem denominado de “extrativismo de dados”, “colonialismo de dados” ou “capitalismo de dados”². Isso se deve principalmente ao fato de que os maiores desenvolvedores de tecnologia digital — tanto de hardware quanto de software — estão localizados no Norte Global. Mesmo assim, os cidadãos e os Estados do Sul Global são usuários assíduos e dependentes desses serviços, o que significa que nossos dados fazem parte dos ativos dessas empresas.

Ora, para analisar esse fenômeno, devemos aprofundar-nos em como funciona o modelo de negócios nesse âmbito digital. Para isso, nos referiremos, entre outras coisas, às empresas com modelos de negócios baseados em dados (DBMC), que são definidas como “empresas com ‘modelos de negócios que se baseiam nos dados como recurso-chave”

² Ver, por exemplo, Jathan Sadowski (2019). “When data is capital: Datafication, accumulation, and extraction”. **Big Data & Society**, 6(1), 1-12. <https://doi.org/10.1177/2053951718820549> ou Thatcher, J., O’Sullivan, D. e Mahmoudi, D. (2015). “O colonialismo de dados por meio da acumulação por desapropriação: novas metáforas para os dados cotidianos”. **Environment and Planning D**, a ser publicado, SSRN: <https://ssrn.com/abstract=2709498>



(Hartmann, Zaki, Feldmann e Hartmann, 2014, p. 6)³. Essas empresas podem oferecer diversos serviços, mas caracterizam-se pelo fato de que seu ativo mais importante — ou pelo menos um deles — são os dados pessoais.

Os dados pessoais têm sido chamados de “novo petróleo”⁴ devido ao valor econômico que representam. De fato, muitas das empresas mais valiosas da atualidade são empresas de tecnologia digital que exploram dados e têm sede nos Estados Unidos. Em 2026, as empresas com maior capitalização de mercado do mundo são: (i) Nvidia, (ii) Alphabet Inc. (proprietária do Google), (iii) Apple Inc., (iv) Microsoft Corp., (v) Amazon Inc. e (vi) TSMC⁵. Dessas seis principais, apenas a TSMC não tem sede nos Estados Unidos — ela está localizada em Taiwan —, mas todas são empresas de tecnologia.

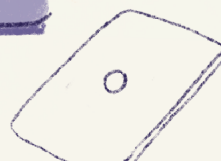
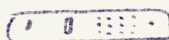
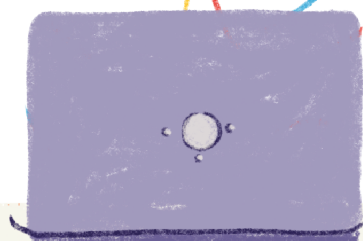
As empresas de tecnologia digital conseguiram acumular grandes quantidades de capital porque seus modelos de negócios não exigem presença física para gerar receita. Pelo contrário, a internet permitiu a interconexão entre países, de modo que, sem a necessidade de presença física, as empresas podem oferecer seus serviços a pessoas em todo o mundo. Algumas dessas empresas fazem isso vendendo serviços diretamente, como as plataformas de streaming ou as empresas de comércio eletrônico. Outras, no entanto, dão a impressão de serem gratuitas, como as plataformas de redes sociais.

De qualquer forma, todas essas plataformas — tanto as que vendem serviços diretamente quanto as que parecem não fazê-lo — conseguem monetizar a coleta em massa de dados pessoais. Isso não apenas ajuda a aprimorar e personalizar seus serviços, mas também lhes proporciona um ativo que podem vender a terceiros.

³ Newman Pont, V., e Ángel Arango, M. P. (2019). *A prestação de contas do Google e de outras empresas na Colômbia: a proteção de dados pessoais na era digital* (Dejusticia Papers n.º 48). Centro de Estudos sobre Direito, Justiça e Sociedade (Dejusticia). <https://publicaciones.dejusticia.org/server/api/core/bitstreams/90265a11-c1a1-4b1a-99c6-6c811076936a/content>

⁴ Mejías, U. A., e Couldry, N. (2019). “Colonialismo de dados: repensando a relação entre o big data e o sujeito contemporâneo”. *Virtualis*, 10(18), 78-97.

⁵ CompaniesMarketCap. (s. f.). *Empresas classificadas por capitalização de mercado*. CompaniesMarketCap. <https://companiesmarketcap.com/>



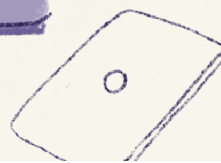
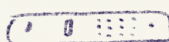
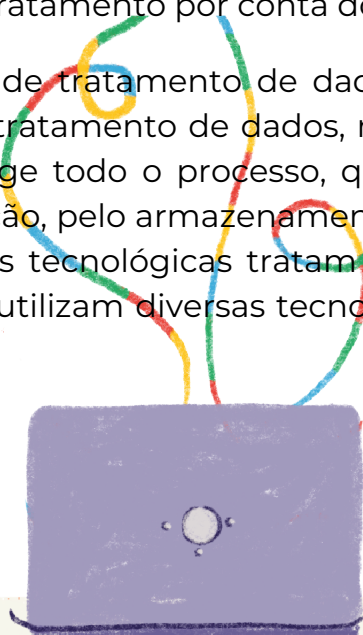
De fato, hoje em dia, a grande maioria dos sites e aplicativos — independentemente do que ofereçam (videogames, redes sociais, sites de comércio eletrônico) — coleta e trata dados pessoais, seja diretamente ou por meio de terceiros, para prever ou influenciar o comportamento das pessoas e oferecer publicidade direcionada, personalizada e eficaz que maximize seus lucros. Consequentemente, quando acessamos um site ou utilizamos um aplicativo, nosso dispositivo se conecta e troca informações não apenas com o servidor web do site ou aplicativo que estamos visitando, mas — na grande maioria dos casos — nossas informações também são compartilhadas com terceiros que foram previamente autorizados a instalar ferramentas de coleta de dados, como cookies ou pixels, no site visitado.

Para ilustrar nosso argumento, nos referiremos especificamente ao caso colombiano ao longo desta seção. No entanto, acreditamos que os argumentos e as questões sejam igualmente importantes e aplicáveis a outros países da região.

1.2. SOBRE O TRATAMENTO DE DADOS PESSOAIS

Na Colômbia, de acordo com o artigo 3º da Lei nº 1.581 de 2012, o tratamento de dados pessoais é definido como “qualquer operação ou conjunto de operações realizadas sobre dados pessoais, tais como a coleta, o armazenamento, o uso, a divulgação ou a supressão”. Essas operações podem ser realizadas pelo “encarregado do tratamento” e pelo “responsável pelo tratamento”, seja diretamente ou em parceria com terceiros. A Lei define o “responsável pelo tratamento” como a pessoa física ou jurídica que toma as decisões relativas ao banco de dados e ao tratamento; e o “encarregado do tratamento” como a pessoa que realiza o tratamento por conta do responsável.

Portanto, o conceito de tratamento de dados pessoais não abrange apenas uma fase do tratamento de dados, nem uma única operação. Pelo contrário, abrange todo o processo, que começa com a coleta, seguida pela divulgação, pelo armazenamento e pelo uso posterior. As principais plataformas tecnológicas tratam dados pessoais de forma quase contínua. Elas utilizam diversas tecnologias que lhes permitem



coletar dados pessoais a partir de ações tão simples quanto visitar um site, clicar em um link ou pesquisar uma notícia.

Conforme explicado anteriormente, essa coleta de dados não se limita ao território em que as empresas estão sediadas, mas se estende a países em todo o mundo. Isso é possível por meio do uso de tecnologias complexas, algumas das quais explicaremos a seguir para ilustrar nosso argumento:

1.2.1. COOKIES

Os cookies são “pequenos arquivos de texto armazenados no computador de um usuário para guardar informações sobre ele e suas preferências”⁶ ; são dispositivos para “armazenar e recuperar dados utilizados no equipamento terminal de um usuário com o objetivo de armazenar informações e recuperar as informações já armazenadas (...) Os cookies permitem armazenar quantidades de dados que variam de alguns kilobytes a vários megabytes no dispositivo do usuário”⁷ .

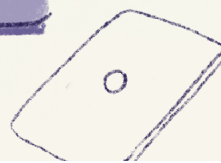
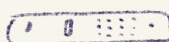
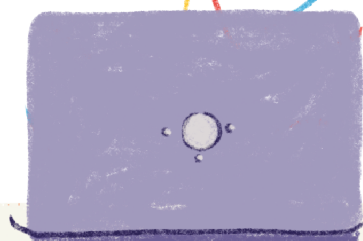
Nesse sentido, os cookies são uma ferramenta tecnológica que permite que um site ou um aplicativo rastreie e identifique os usuários de seus serviços, com a capacidade de extrair informações sobre eles. A esse respeito, é importante ressaltar que “os cookies não coletam dados automaticamente”⁸ ; eles devem ser programados especificamente para esse fim, desviando-se, em muitas ocasiões, de sua finalidade original de beneficiar os usuários. Os cookies envolvem um processo complexo que pode ser simplificado da seguinte maneira.

Começa quando um usuário acessa um site; continua quando esse site cria e envia um cookie — um pequeno arquivo de texto — para o dispositivo do usuário, onde fica armazenado; esse pequeno arquivo de texto armazenará o número de identificação do usuário para o site ou

⁶ Rubinstein, I. S., Lee, R. D. e Schwartz, P. M. (2008). Mineração de dados e criação de perfis na Internet: novas abordagens normativas e tecnológicas. *University of Chicago Law Review*, 75(1), 261-286.

⁷ “Guia sobre o uso de cookies”. Agência Espanhola de Proteção de Dados, <https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf>

⁸ Pantelic, O.; Jovic, K.; Krstovic, S. Análise da implementação de cookies e seu impacto na privacidade dos usuários em relação aos regulamentos do RGPD e da CCPA. *Sustainability* 2022, 14, 5015. <https://doi.org/10.3390/su14095015>



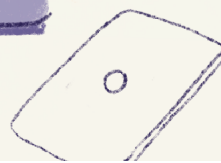
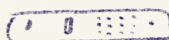
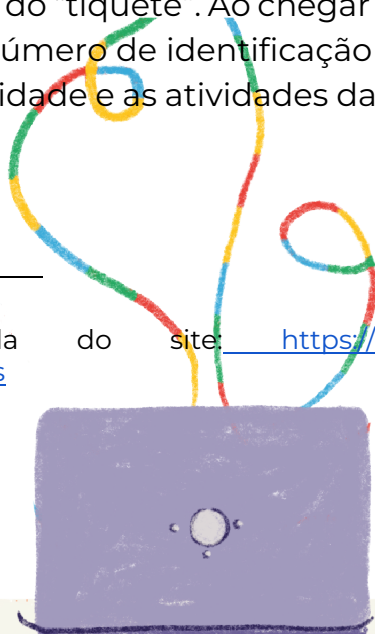
algum outro tipo de informação, dependendo de como estiver programado. Uma vez instalado o cookie no dispositivo eletrônico do usuário, sempre que ele visitar o site, os cookies armazenados anteriormente em seu computador serão reenviados ao seu criador, o que permite ao site identificar quem é o usuário e qual atividade online ele está realizando. Posteriormente, o site pode processar esses dados para criar um perfil da atividade anterior do usuário⁹.

Geralmente, os cookies só podem ser lidos pelo site visitado, que é quem os criou. No entanto, existem os chamados “cookies de terceiros”, que são resultado de acordos comerciais entre gigantes da tecnologia, como o Google ou a Meta, o que permite que essas empresas instalem e criem cookies para sites que não lhes pertencem. Dessa forma, elas podem, por exemplo, instalar seus cookies também em sites de mídia, com o objetivo de coletar uma gama ainda mais ampla de informações sobre os usuários. Assim como os cookies de terceiros, existem outros tipos de cookies que recebem esse nome de acordo com sua finalidade, seu tempo de vida útil e outras características.

Eis uma analogia que ajuda a explicar como os cookies funcionam e o que eles fazem: uma pessoa vai a uma festa e, ao chegar, deixa seu casaco no vestiário; lá, o responsável pelo vestiário lhe entrega um “cachê” que a identifica como a dona do casaco que deixou; em seguida, a pessoa sai para aproveitar a festa. No entanto, pouco tempo depois, ela volta ao vestiário e entrega o “tíquete” que a identifica como a dona do casaco¹⁰. Nesse caso, o vestiário é o site, o “tíquete” é o cookie e a pessoa que está na festa é o usuário do site. Por outro lado, o responsável pelo vestiário é a empresa que cria o cookie para identificar a pessoa e coleta informações sobre o dono do casaco, já que pode identificá-lo por meio do “tíquete”. Ao chegar ao vestiário, o participante da festa recebe um número de identificação que permitirá ao vestiário reconhecer sua identidade e as atividades das quais participou na festa quando ele retornar.

⁹ Ibid.

¹⁰ Analogia extraída do site: <https://latam.kaspersky.com/resource-center/definitions/cookies>



Os cookies, de fato, utilizam uma tecnologia que lhes permite instalar-se no dispositivo de um usuário, coletar informações, armazená-las e transmiti-las, para finalmente devolvê-las ao proprietário do cookie. Nesse sentido, as funções dos cookies se enquadram na definição legal — e na interpretação da SIC — do tratamento de dados pessoais, o qual, como vimos anteriormente, tem início quando são coletados dados pessoais — entendendo-se por dados pessoais qualquer informação que possa ser associada a uma pessoa física identificada ou identificável, de acordo com o artigo 3º da Lei 1581 de 2012 — e tem por objetivo obter informações sobre uma pessoa física.

1.2.2. SDK

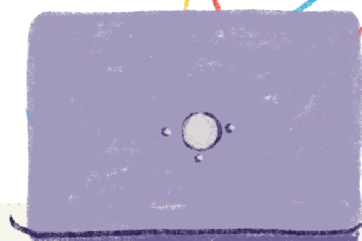
Os kits de desenvolvimento de software (SDK, na sigla em inglês) são “os componentes básicos para criar aplicativos: conectores modulares que vêm pré-carregados com ferramentas prontas para uso, código, bibliotecas e tutoriais de plataformas e/ou de terceiros que fazem parte integrante da cadeia de suprimentos de software”¹¹. Algumas dessas ferramentas são essenciais para o funcionamento das plataformas; por isso, são incorporadas aos aplicativos e acabam sendo instaladas nos dispositivos dos usuários finais.

Se quiséssemos simplificar a definição dos SDKs, poderíamos estabelecer uma analogia com uma caixa de ferramentas que fornece tudo o que é necessário para construir uma casa, desde tijolos até martelos e chaves de fenda¹². No nosso exemplo, a casa representa os aplicativos instalados nos dispositivos eletrônicos, e os SDKs constituem a base do software desses aplicativos.

O que foi documentado é que, embora os SDKs desempenhem, em princípio, um papel indispensável no desenvolvimento de aplicativos, eles também se tornaram ferramentas utilizadas para a coleta de dados pessoais. De fato, o fato de os dispositivos possuírem um ambiente fechado — ou seja, um ambiente controlado, integrado e limitado aos

¹¹ Pybus, J., e Coté, M. (2024). “Super SDKs: Rastreamento de dados pessoais e monopólios das plataformas em dispositivos móveis”. **Big Data & Society**, 11(1). <https://doi.org/10.1177/20539517241231270>
Em: <https://journals.sagepub.com/doi/epub/10.1177/20539517241231270>

¹² Exemplo extraído de: <https://iberbox.es/sdk-kit-de-desarrollo-de-software/>



aplicativos que vêm pré-instalados no celular ou que o usuário baixa — “permite que qualquer aplicativo estabeleça uma relação muito mais íntima com os usuários finais”¹³. Nesse sentido, uma vez instalados no dispositivo — e dependendo de sua funcionalidade —, os SDKs podem coletar dados do usuário do dispositivo, como sua localização, onde ele clica ou por onde navega dentro do aplicativo.

Enquanto os cookies, como mencionado anteriormente, são ferramentas tecnológicas que ajudam a identificar e lembrar os usuários, os SDKs podem se conectar diretamente aos dados dos usuários nos dispositivos móveis. Além disso, os aplicativos também contêm SDKs de terceiros, o que significa que os aplicativos desenvolvidos pela empresa X também podem ter SDKs da empresa W integrados a eles. Os SDKs de terceiros são utilizados para fornecer diversas funcionalidades, como “autenticação de usuários e criptografia de dados, bem como componentes especializados, como análise, veiculação de anúncios e melhorias na interface do usuário”¹⁴ e outros.

Até 2025, por exemplo, constatou-se que “a maioria dos aplicativos Android incorpora múltiplos SDKs de terceiros, com uma média de aproximadamente 8,6 SDKs por aplicativo”¹⁵. Essa média, combinada com as práticas opacas de tratamento de dados de alguns SDKs, pode comprometer os direitos à privacidade ou à proteção de dados pessoais¹⁶.

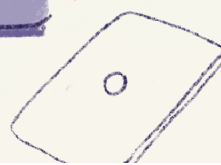
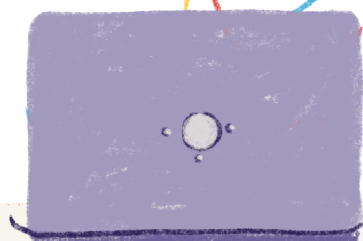
Vale reiterar que essa coleta de dados começa com o download dos aplicativos nos dispositivos móveis. Esses aplicativos contêm SDKs que

¹³ Pybus, J., e Coté, M. (2024). Super SDKs: Rastreamento de dados pessoais e monopólios das plataformas em dispositivos móveis. *Big Data & Society*, 11(1). <https://doi.org/10.1177/20539517241231270>

¹⁴ Meng, M. H., Yan, C., Zhang, Q., Wang, Z., Wang, K., Teo, S. G., Bai, G. e Dong, J. S. (2025). Avaliação da conformidade com as normas de privacidade dos SDKs de terceiros para Android. *arXiv*. <https://doi.org/10.48550/arXiv.2409.10411>

¹⁵ Meng, M. H., Yan, C., Zhang, Q., Wang, Z., Wang, K., Teo, S. G., Bai, G. e Dong, J. S. (2025). Avaliação da conformidade com as normas de privacidade dos SDKs de terceiros para Android. *arXiv*. <https://doi.org/10.48550/arXiv.2409.10411>

¹⁶ Meng, M. H., Yan, C., Zhang, Q., Wang, Z., Wang, K., Teo, S. G., Bai, G. e Dong, J. S. (2025). Avaliação da conformidade com as normas de privacidade dos SDKs de terceiros para Android. *arXiv*. <https://doi.org/10.48550/arXiv.2409.10411>



permitem a coleta de dados pessoais dos usuários, às vezes para o desenvolvedor do aplicativo e outras vezes para terceiros.

1.2.3. PIXELS

Os pixels são pequenas imagens transparentes incorporadas em páginas da web ou e-mails¹⁷. São invisíveis a olho nu, mas têm grande capacidade de coletar e rastrear dados pessoais, como endereços IP, sistemas operacionais, navegadores utilizados, comportamento online etc. Os pixels podem rastrear como os usuários interagem com um site e podem ser usados para monitorar o comportamento dos consumidores e exibir anúncios personalizados¹⁸.

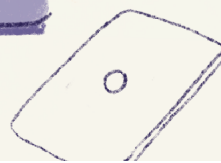
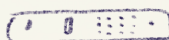
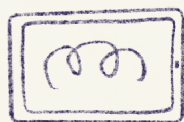
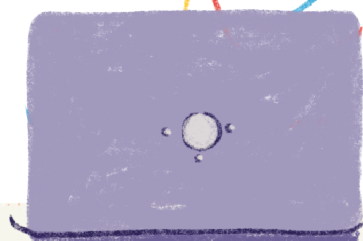
Tecnicamente, esses pixels são pequenos fragmentos de código que permitem o rastreamento das atividades on-line dos usuários assim que eles visitam um site. Ao contrário dos cookies, os usuários não sabem que os pixels estão sendo utilizados. Na verdade, “para mitigar o uso de pixels de rastreamento por conta própria, normalmente é preciso usar extensões do navegador que podem alterar o funcionamento do site, desativar todas as solicitações de imagens em um site ou visualizar e-mails apenas em texto sem formatação”¹⁹. Em outras palavras, desativar essa tecnologia de rastreamento requer conhecimentos técnicos avançados.

De acordo com a Agência de Proteção ao Consumidor dos EUA, os pixels podem ser monetizados de diversas formas: venda de publicidade direcionada, otimização dos próprios sistemas de segmentação das plataformas, entre outras. Em 2022, o The Markup e o STAT — veículos de comunicação alternativos focados em tecnologia e saúde, respectivamente — analisaram 100 sites de hospitais

¹⁷ Newman, L. H. (2022). A imagem viral da internet que você nunca viu. Em T. Bosch (Ed.), *Não se espera que você entenda isso: Como 26 linhas de código mudaram o mundo*. Princeton University Press. <https://www.jstor.org/stable/j.ctv2ks6t89.18>

¹⁸ Comissão Federal de Comércio, Escritório de Tecnologia. (16 de março de 2023). *À espreita sob a superfície: os impactos ocultos do rastreamento de pixels*. <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking>

¹⁹ Newman, L. H. (2022). A imagem viral da internet que você nunca viu. Em T. Bosch (Ed.), *Não se espera que você entenda isso: Como 26 linhas de código mudaram o mundo*. Princeton University Press. <https://www.jstor.org/stable/j.ctv2ks6t89.18>



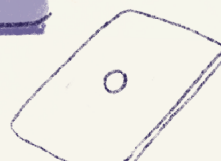
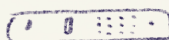
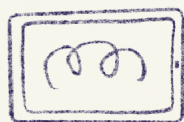
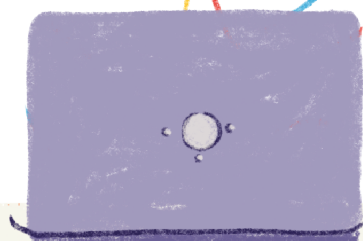
americanos. Em 33 deles, encontraram um rastreador chamado “Meta Pixel que “enviava um pacote de dados ao Facebook toda vez que uma pessoa clicava em um botão para marcar uma consulta médica”. Os dados estão vinculados a um endereço IP — um identificador que funciona como o endereço postal de um computador e que, geralmente, pode ser associado a uma pessoa ou residência específica —, o que fornece ao Facebook um registro detalhado da solicitação de consulta”²⁰.

Como parte de sua pesquisa, eles também examinaram sites utilizados para prestar serviços de telessaúde e descobriram que 13 dos 50 sites continham pelo menos um rastreador do Meta, Google, TikTok, Bing, Snap, Twitter, LinkedIn ou Pinterest²¹. Esses rastreadores — em alguns casos, pixels — coletavam informações sobre respostas relacionadas a “autolesões, uso de drogas e álcool, e [...] dados pessoais — incluindo nome, endereço de e-mail e número de telefone — e as enviavam ao Facebook”²². Como vimos, esses pequenos fragmentos de código incorporados em imagens transparentes em e-mails ou em páginas da web têm o potencial de coletar dados de qualquer pessoa que abra o e-mail ou visite o site, e são utilizados por diversas gigantes da tecnologia.

²⁰ Feathers, T., Fondrie-Teitler, S., Waller, A. e Mattu, S. (16 de junho de 2022). *O Facebook está recebendo informações médicas confidenciais dos sites dos hospitais*. The Markup. <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>

²¹ Feathers, T., Palmer, K. e Fondrie-Teitler, S. (13 de dezembro de 2022). *“Fora de controle”: dezenas de startups de telessaúde enviaram informações confidenciais de saúde para grandes empresas de tecnologia*. The Markup. <https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies>

²² Feathers, T., Palmer, K. e Fondrie-Teitler, S. (13 de dezembro de 2022). *“Fora de controle”: Dezenas de startups de telessaúde enviaram informações confidenciais de saúde para grandes empresas de tecnologia*. The Markup. <https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies>



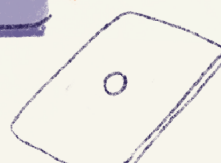
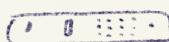
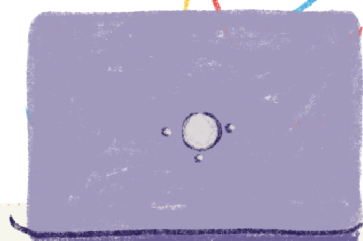
1.3. O TRATAMENTO DE DADOS PESSOAIS POR MEIO DESSAS TECNOLOGIAS OCORRE NA COLÔMBIA E EM OUTROS PAÍSES DO SUL GLOBAL

Depois de explicarmos como funciona a coleta local de dados por meio de cookies, SDKs e pixels — e sabendo que existem muitos outros métodos utilizados pelas gigantes da tecnologia para tratar dados pessoais —, explicaremos agora por que se pode afirmar que esse tratamento de dados pessoais ocorre na Colômbia e, portanto, está sujeito à Lei 1581 de 2012. Também destacamos que esse argumento se aplica a outros países nos quais, sem dúvida, as técnicas de coleta e tratamento são as mesmas e nos quais os dados de seus residentes estão sendo tratados.

Lembremos que os cookies são mecanismos que permitem a coleta de dados pessoais, o armazenamento de informações e a transmissão dessas informações. Conforme explicado anteriormente, isso ocorre porque os cookies são pequenos arquivos de texto criados e enviados pelos sites para os dispositivos dos usuários, a fim de obter e armazenar informações sobre eles. Essas informações são recuperadas pelo site quando o próprio usuário o visita novamente.

Os cookies persistentes — ou seja, aqueles que duram mais tempo e não expiram a cada sessão — são armazenados no dispositivo eletrônico do usuário. Se esse dispositivo estiver na Colômbia, as operações de coleta, transferência e armazenamento dos dados pessoais ocorrem, total ou inicialmente, em território colombiano — e o mesmo se aplica a qualquer outro país. Consequentemente, o tratamento de dados pessoais ocorre na Colômbia.

De fato, nesse cenário, os dados são extraídos de um usuário localizado na Colômbia e, em seguida, armazenados em um cookie instalado em seu dispositivo — que também se encontra na Colômbia. Em seguida, ocorre um processo de transmissão de dados que se inicia na Colômbia, pois, quando o usuário retorna e visita o mesmo site, o cookie é transferido do dispositivo localizado na Colômbia para o servidor do site, que pretende ler as informações. Assim, embora o servidor que recebe os dados esteja em outro país, essa coleta de dados ocorreu inicialmente na Colômbia, uma vez que o dispositivo está dentro do



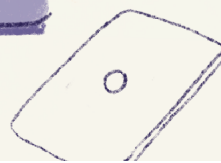
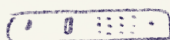
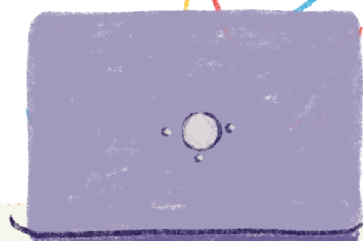
nosso território. Consequentemente, é na Colômbia que o cookie foi instalado e onde foram capturados os dados que permitem identificar o usuário em visitas futuras.

Uma situação semelhante ocorre no caso dos SDKs. Conforme descrito anteriormente, os SDKs são componentes básicos e necessários para o funcionamento dos aplicativos tecnológicos. Esses aplicativos, por sua vez, estão disponíveis para download em plataformas como a Google Play Store ou a Apple App Store. Uma vez que os aplicativos estejam em dispositivos móveis localizados em território colombiano, eles executam seus próprios SDKs e os de terceiros, o que facilita a coleta de dados dos usuários dos aplicativos. Essa coleta ocorre na Colômbia — ou no país em que o usuário se encontra —, na medida em que os aplicativos e seus SDKs operacionais estejam instalados em dispositivos móveis localizados em nosso território. Portanto, a coleta ocorre em território colombiano.

Por fim, gostaríamos de destacar que, embora os pixels não sejam baixados no dispositivo, trata-se de imagens transparentes que — embora invisíveis a olho nu — são exibidas nas telas dos dispositivos dos usuários. Uma vez que a ordem de coleta de dados entre em vigor, ela pode ser enviada a partir de um servidor no exterior, mas a coleta propriamente dita ocorre no dispositivo localizado na Colômbia. Assim, parte do tratamento é realizada em nosso país.

Como se pode observar, a realidade é que, embora as empresas de tecnologia tenham sede no exterior e prestem seus serviços pela Internet, os dados pessoais que tratam são extraídos de pessoas e dispositivos localizados fora de seus territórios. Isso significa que, na prática, tanto parte do tratamento quanto o impacto sobre os direitos das pessoas ocorrem fora da jurisdição à qual estão física e tradicionalmente vinculadas.

Uma interpretação tradicional e anacrônica da territorialidade levou as grandes empresas de tecnologia a resistirem ao cumprimento das leis de proteção de dados dos países nos quais tratam dados e dos quais extraem dados pessoais que monetizam. Isso ocorreu principalmente em países do Sul Global, que carecem de um capital político nem de

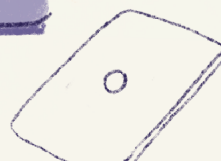
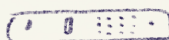
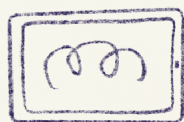
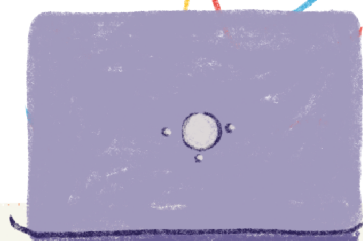


longe comparável ao da União Europeia, a qual conseguiu fazer cumprir com sucesso sua regulamentação em matéria de proteção de dados pessoais.

Na Colômbia, por exemplo, o Escritório de Proteção de Dados Pessoais da Superintendência de Indústria e Comércio (SIC) tem envidado esforços significativos para garantir a proteção dos dados pessoais dos colombianos. A SIC baseou sua competência e a aplicação da legislação colombiana precisamente no fato de que o tratamento de dados pessoais ocorre na Colômbia e emitiu resoluções que obrigam as grandes empresas a cumprir os requisitos legais para tal tratamento.

No entanto, pelo menos três dessas grandes empresas de tecnologia entraram com ações judiciais²³ com o objetivo de contestar a competência da SIC e se recusar a cumprir a legislação colombiana. Entre os argumentos apresentados por essas empresas, destacam-se: que, em sua opinião, o tratamento de dados pessoais não ocorre em território colombiano, mas em servidores localizados no exterior; que, na ausência de um tratado internacional, bilateral ou multilateral que habilite a autoridade colombiana de proteção de dados a julgar seus casos, qualquer medida adotada por ela é irregular; e que elas têm sede social em outros países e não possuem escritórios no território nacional. No entanto, na maioria dos casos, essas empresas são acionistas majoritárias e exercem controle sobre sociedades constituídas de

²³**Processo “Google LTDA”**, nº do processo: 25000234100020220044800, Objeto: Anulação e restabelecimento com suspensão provisória das Resoluções 70315, de 4 de novembro de 2020, e 38869, de 24 de junho de 2021; Apresentado em 21 de abril de 2022; Juiz presidente: LUIS NORBERTO CERMEÑO; Requerente: GOOGLE COLOMBIA LTDA, Requerida: SUPERINTENDÊNCIA DE INDÚSTRIA E COMÉRCIO; **Processo Google LLC**, nº do processo: 25000234100020220044400, Objeto: nulidade e restabelecimento de direitos com suspensão provisória das resoluções nº 53593, de 3 de setembro de 2020, nº 14010, de 16 de março de 2021, e nº 60478, de 21 de setembro de 2021, Apresentada em 20 de abril de 2022, Juíza relatora: ANA MARGOTH CHAMORRO BENAVIDES, Autora: GOOGLE LLC, Ré: SUPERINTENDÊNCIA DE INDÚSTRIA E COMÉRCIO; **Processo WhatsApp**, requerente: WhatsApp LLC, requerida: SIC, nº do processo: 25000-23-41-000-2022-01520-00, Assunto: Anulação e restabelecimento de direitos em relação às Resoluções 4554 de 2022, 29826 de 2021 e 15342 de 2022, Juíza: Ana Margoth Chamorro Benavides, Data da ação: 06/12/2022; **Processo TikTok**, requerente: Bytedance LTD, requerido: SIC, nº do processo: 25000234100020220106400, Objeto: Anulação e restabelecimento de direitos — Decisões 62132, de 5 de outubro de 2020, 14015, de 16 de março de 2021, e 75009, de 22 de novembro de 2021, proferidas pela SIC.



acordo com a legislação colombiana, embora afirmem ser entidades jurídicas independentes.

Em última instância, isso destaca a falta de proteção enfrentada por milhões de pessoas que utilizam diariamente serviços digitais em países diferentes daqueles onde as grandes empresas prestadoras desses serviços têm sua sede. Essas pessoas ficam indefesas diante do imenso poder econômico e político das grandes empresas de tecnologia, que acabam extraindo seus dados e transformando-os em um importante ativo econômico. Em seguida, esses dados são utilizados para personalizar conteúdos e, por vezes, para manipular mentes, influenciando não apenas as decisões dos consumidores, mas também as preferências políticas e outras esferas. Nas seções a seguir, aprofundamos algumas dessas dimensões e como esses riscos se concretizaram em diversos países da região.

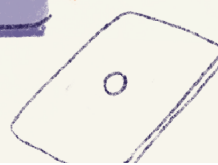
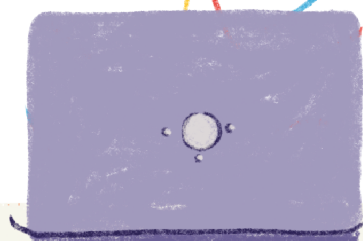
1.4. AS PRINCIPAIS PLATAFORMAS TIVERAM QUE PRESTAR CONTAS PERANTE OUTRAS JURISDIÇÕES

O tratamento de dados pessoais em diferentes territórios representa um desafio na hora de avaliá-lo e garantir a proteção jurídica dos titulares dos dados. Nesse contexto, diversos tribunais em todo o mundo reconheceram que as empresas com sede no exterior não podem se eximir da aplicação das leis locais de proteção de dados alegando formalmente que não possuem sede social em um país específico. A seguir, apresentamos alguns exemplos:

1.4.1. O CASO GOOGLE SPAIN CONTRA AEPD (2014)

Em 2014, o Tribunal de Justiça da União Europeia (TJUE) proferiu decisão sobre o referido caso **Google Spain contra a Agência Espanhola de Proteção de Dados (C-131/12)**²⁴. O caso teve origem em um pedido de um cidadão espanhol para que o Google removesse de seus resultados de busca um link que prejudicava sua reputação. O Google alegou que a legislação europeia em matéria de proteção de

²⁴ TJUE. Google Spain contra AEPD (C-131/12, 2014). Disponível em: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62012CJ0131>



dados não se aplicava a ele, uma vez que sua sede central estava localizada nos Estados Unidos e o tratamento de dados era realizado fora do território europeu.

O Tribunal rejeitou esse argumento e concluiu que o Google estava sujeito à legislação europeia, uma vez que existia um vínculo direto entre as atividades da matriz norte-americana e as de sua filial na Espanha. Na opinião do Tribunal,

“A Google Inc. administra o Google Search do ponto de vista técnico e administrativo, e não foi comprovado que a Google Espanha realize, na Espanha, qualquer atividade diretamente ligada à indexação ou ao armazenamento de informações ou dados contidos em sites de terceiros. No entanto, **a promoção e a venda de espaços publicitários — pelas quais a Google España é responsável na Espanha — constituem a parte essencial da atividade comercial do grupo Google e podem ser consideradas intimamente ligadas ao Google Search**».²⁵ (negrito adicionado).

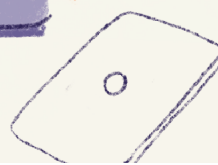
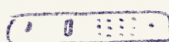
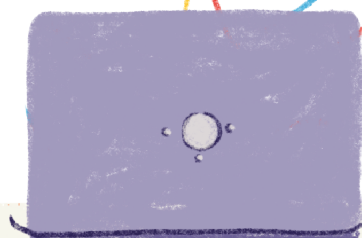
Assim, o TJUE interpretou o conceito de “estabelecimento” de forma ampla e estabeleceu uma norma para a aplicação funcional da lei: quando uma empresa opera em um território por meio de filiais que possibilitam ou tornam rentável sua atividade econômica, ela é obrigada a cumprir a legislação de proteção de dados desse país.

1.4.2. O CASO GOOGLE CONTRA CNIL (2019)

Outro precedente significativo foi o **caso Google LLC contra CNIL**, decidido em 2019 pelo TJUE²⁶ e, posteriormente, pelo Conselho de Estado francês. A autoridade francesa de proteção de dados (CNIL) aplicou uma multa ao Google por se recusar a desindexar, em nível mundial, os resultados de busca solicitados com base no “direito ao esquecimento”. O Google argumentou que sua obrigação deveria se

²⁵ Ibid.

²⁶ TJUE. Google contra CNIL (C-507/17, 2019). Disponível em: https://eur-lex.europa.eu.translate.google/legal-content/EN/TXT/?uri=celex:62017CJ0507&x_tr_sl=en&x_tr_tl=es&x_tr_hl=es&x_tr_pto=tc



limitar aos domínios europeus de seu mecanismo de busca e não se estender ao resto do mundo.

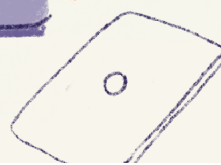
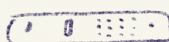
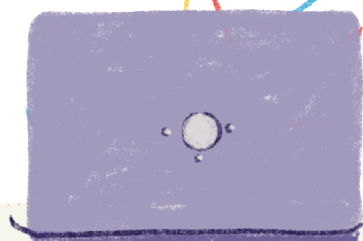
O Tribunal de Justiça da União Europeia reconheceu que a proteção do direito ao esquecimento deve ser ponderada em relação à liberdade de informação, mas deixou claro que as autoridades nacionais podem exigir a aplicação extraterritorial das normas quando necessário para garantir a eficácia dos direitos das pessoas. Esse acórdão ecoa o raciocínio do caso espanhol, no sentido de que

«[O] estabelecimento do Google em território francês **realiza, entre outras coisas, atividades comerciais e publicitárias que estão indissociavelmente ligadas ao tratamento de dados pessoais para o funcionamento do mecanismo de busca** em questão; e, em segundo lugar, que tal mecanismo de busca — dada, entre outras coisas, a existência de portais de conexão entre suas diferentes versões nacionais — deve ser considerado como **realizando um único tratamento de dados pessoais**. O tribunal de origem considera que, nessas circunstâncias, tal tratamento é realizado no âmbito do estabelecimento do Google na França» (ênfase acrescentada)

Em sua decisão definitiva, o Conselho de Estado francês confirmou a sanção imposta pela CNIL e ressaltou que as empresas globais devem garantir o cumprimento coerente das decisões em matéria de proteção de dados em todas as versões territoriais de seus serviços.

1.4.3. OS PROCESSOS SCHREMS I (2015) E SCHREMS II (2020)

Após o caso Google Spain, o TJUE ampliou sua jurisprudência sobre a dimensão transfronteiriça do “habeas data”. Nos casos **Schrems I (C-362/14)** e **Schrems II (C-311/18)**, o Tribunal examinou a legalidade dos mecanismos que permitem a transferência de dados pessoais da União Europeia para os Estados Unidos. No primeiro caso, conhecido como Schrems I, o Tribunal declarou nulo o acordo “Safe Harbor”, ao considerar que o sistema norte-americano não garantia um nível adequado de proteção contra a vigilância em massa por parte dos serviços de inteligência.



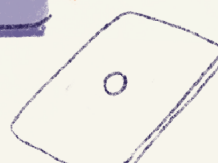
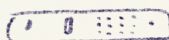
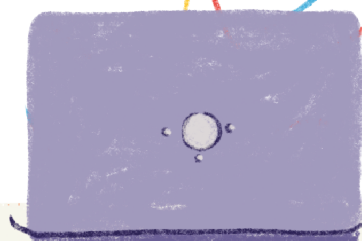
O requerente, Max Schrems, demonstrou que os órgãos de segurança norte-americanos podiam acessar os dados pessoais transferidos da Europa para os Estados Unidos sem uma supervisão judicial efetiva, o que violava os princípios da proporcionalidade e da necessidade no tratamento de dados. O TJUE concluiu que as empresas europeias — ou aquelas que operam na Europa — não podiam transferir suas responsabilidades para as autoridades de outro país e que a proteção deveria ser garantida em todos os momentos, independentemente do local onde os dados fossem armazenados.

No **caso Schrems II**, o Tribunal chegou a uma conclusão ainda mais contundente: invalidou o mecanismo do “Privacy Shield” — sucessor do “Safe Harbor” —, reiterando que a proteção de dados pessoais é um direito fundamental que não pode ser prejudicado por acordos comerciais nem por mecanismos de autorregulação. Nessa decisão, o TJUE sustentou que as empresas que transferem dados para fora da União Europeia devem garantir que as pessoas desfrutem de um nível de proteção substancialmente equivalente ao oferecido pela legislação da UE.

1.4.4. O CASO DO TWITTER NO CANADÁ: GIUSTRA CONTRA TWITTER, INC. (2021)

Este caso foi levado aos tribunais da Colúmbia Britânica (Canadá) depois que o Sr. Giustra entrou com uma ação judicial por causa de alguns tuítes que, em sua opinião, prejudicavam sua reputação. O Twitter, parte ré no processo, solicitou que o caso fosse indeferido por falta de competência ou por “forum non conveniens”. Na opinião do Twitter, a Califórnia era o foro adequado, uma vez que se tratava de uma empresa norte-americana, as mensagens haviam sido publicadas principalmente nos EUA e versavam sobre questões políticas daquele país. No entanto, tanto em primeira instância quanto em recurso, os tribunais canadenses confirmaram sua competência, alegando que os tuítes haviam sido publicados na Colúmbia Britânica e causado prejuízo a um residente da Colúmbia Britânica²⁷.

²⁷ Ver Bookman, P. K. (2024). *“If Not Here, Where?: Transnational Litigation Against U.S. Tech Giants Around the World”*. 56 New York University Journal of International Law

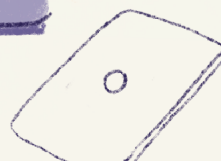
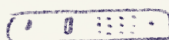
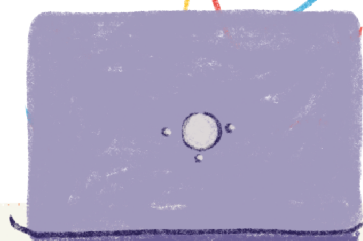


1.4.5. O PROCESSO CONTRA A MICROSOFT JULGADO PELO SUPERIOR TRIBUNAL DE JUSTIÇA DO BRASIL (2020)

Um executivo de uma empresa de transportes do Brasil, que recebeu ameaças por meio de uma conta de e-mail da Microsoft, moveu uma ação contra a Microsoft solicitando que esta lhe fornecesse os registros de acesso (IP, data e hora) que permitissem identificar o autor das ameaças. O tribunal de primeira instância concedeu a medida cautelar e fixou uma multa diária de R\$ 10.000 por descumprimento; diante da recusa da empresa em entregar os dados, a multa foi executada provisoriamente até atingir R\$ 310.000. A Microsoft, em sua defesa, alegou que a justiça brasileira não tinha competência porque as ameaças estavam escritas em inglês, a conta de e-mail havia sido acessada do exterior, o provedor de internet também estava fora do Brasil e que cumprir a ordem implicaria violar a legislação dos Estados Unidos, local onde o acesso teria ocorrido. No entanto, o Superior Tribunal de Justiça do Brasil rejeitou o argumento por unanimidade e destacou que basta que pelo menos um dispositivo (o do usuário ameaçado, neste caso) envolvido no tratamento de dados pessoais esteja em território nacional para que a legislação nacional seja aplicada, independentemente de se tratar de uma empresa estrangeira:

“É um equívoco imaginar que qualquer aplicativo hospedado fora do Brasil não possa ser abrangido pela jurisdição nacional ou que as leis brasileiras não sejam aplicáveis às suas atividades. A lei brasileira se aplica sempre que qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e aplicativos da internet **ocorra em território nacional, mesmo que apenas um dos dispositivos da comunicação esteja no Brasil e mesmo que as atividades sejam realizadas por**

and Politics 29. Disponível em *Faculty Scholarship, Faculdade de Direito de Fordham* (https://ir.lawnet.fordham.edu/faculty_scholarship/1337)



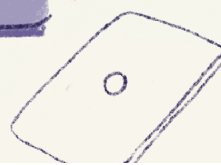
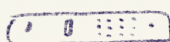
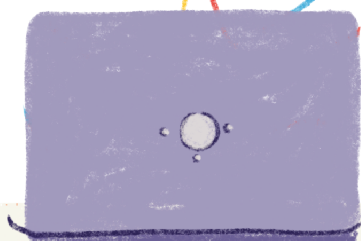
empresa com sede no exterior.” (tradução própria, resumo, pontos 5 e 6)”.

“A recorrente, por si só, é uma empresa subsidiária destinada exclusivamente a operações no Brasil, mas **pertence ao grupo econômico** reconhecido mundialmente.” (tradução própria, parágrafo XXXI da relatora Adigri

1.4.6. O CASO P.A.E. CONTRA FACEBOOK ARGENTINA S.R.L. (MEDIDA CAUTELAR DE 2019)

Nesse caso, uma pessoa propôs uma medida cautelar contra a Facebook Argentina S.R.L. para solicitar a remoção de publicações que continham o nome e a imagem de seus filhos. O juiz de primeira instância concedeu a medida inicialmente. No entanto, essa decisão foi apelada pela Facebook Argentina, alegando falta de legitimidade passiva, uma vez que não é ela quem opera o site “facebook.com”. O Tribunal Superior confirmou a decisão do juiz de primeira instância e observou que a exceção de falta de legitimidade passiva era improcedente, uma vez que a filial está sujeita à legislação argentina. A sentença destaca que, independentemente das formas societárias que a empresa adote, ela está representada no país; e que, além disso, a constituição societária no exterior não significa que as normas do país não se apliquem a ela, quando os atos e contratos são celebrados no próprio país:

“A sociedade constituída no exterior rege-se, no que diz respeito à sua existência e forma, pelas leis do local de constituição, o que **não impede a aplicação das leis argentinas aos atos e contratos celebrados em nosso** país, pois sua presença neste último implica total submissão à jurisdição e às leis argentinas, ainda que sua capacidade seja regida pela lei do domicílio. Também não escapa à análise o fato de que as redes sociais, assim como outras formas de comunicação eletrônica e tratamento de dados pela Internet, constituíram um quadro complexo de competências jurisdicionais e responsabilidades que exigem uma legislação adequada e específica. No entanto,



essa situação não é impedimento para que os juízes possam decidir sobre a apresentação de um caso concreto. (...)

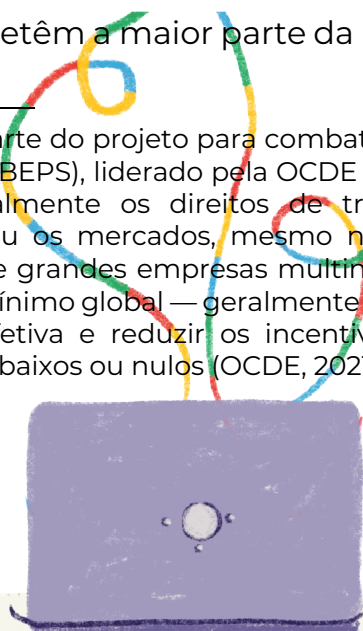
A Facebook Argentina S.R.L. não pode se eximir das ordens judiciais impostas alegando que não possui competência para tal; portanto, a empresa deve tomar conhecimento e cumprir as decisões judiciais notificadas no endereço por ela constituído no país”.

1.5. O CASO DA TRIBUTAÇÃO

Nesta seção, nos concentramos tanto nos riscos quanto na falta de fundamento jurídico que está por trás da relutância das grandes empresas de tecnologia em reconhecer a jurisdição de outros países sobre elas, e especialmente nas implicações que isso tem para garantir o direito à proteção de dados pessoais. No entanto, o fato é que essa relutância também existe em outros âmbitos jurídicos e repercute em outros direitos. A seguir, analisaremos outro exemplo.

A crescente digitalização da economia revelou as limitações do sistema tributário internacional tradicional, que foi concebido para empresas que operavam por meio de uma presença física em um determinado território. Atualmente, as grandes plataformas e os prestadores de serviços digitais podem gerar receitas significativas provenientes de usuários e consumidores localizados em países como a Colômbia, sem a necessidade de estabelecer uma presença física no local, o que reduz a capacidade desses Estados de tributar as receitas geradas em seus mercados. Esse fenômeno foi identificado pelo projeto BEPS da OCDE²⁸ como um dos principais desafios da tributação internacional: enquanto as principais economias — onde estão localizadas as sedes das empresas digitais — detêm a maior parte da receita tributária, os países

²⁸ Os pilares I e II fazem parte do projeto para combater a erosão da base tributária e a transferência de lucros (BEPS), liderado pela OCDE e pelo G-20. O pilar I tem como objetivo reatribuir parcialmente os direitos de tributação aos países onde se encontram os usuários ou os mercados, mesmo na ausência de presença física, especialmente no caso de grandes empresas multinacionais. O pilar II, por sua vez, estabelece um imposto mínimo global — geralmente de 15% — para garantir um nível mínimo de tributação efetiva e reduzir os incentivos para transferir lucros para jurisdições com impostos baixos ou nulos (OCDE, 2021).

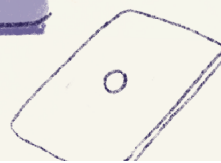
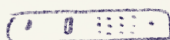
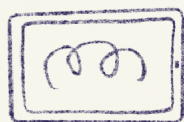


onde se encontram os usuários e consumidores recebem uma parcela muito menor desses recursos.

Isso contribui para agravar as desigualdades globais, pois reduz a capacidade dos países de baixa renda de financiar políticas públicas e garantir os direitos fundamentais à sua população. As receitas que os governos podem arrecadar constituem a principal fonte de financiamento para garantir direitos como assistência à saúde, educação, proteção social e acesso à justiça. Quando as normas internacionais impedem que os países onde se geram o consumo e o valor econômico tributem adequadamente as receitas decorrentes dos serviços digitais, sua capacidade fiscal fica prejudicada, o que limita sua capacidade de investir nos setores sociais.

Nesse sentido, é fundamental buscar reforçar a tributação dos serviços digitais transfronteiriços, de modo que os países onde se geram o consumo e o valor econômico possam participar de forma mais equitativa na arrecadação de receitas fiscais. Para isso, devem ser promovidos mecanismos que permitam tributar essas atividades independentemente da presença física das empresas, e devem ser apoiadas iniciativas internacionais como a Convenção-Quadro das Nações Unidas sobre Cooperação Fiscal Internacional²⁹ — destinada a uma distribuição mais equitativa dos direitos de tributação na economia digital.

²⁹ Ver: <https://financing.desa.un.org/unfcitc>



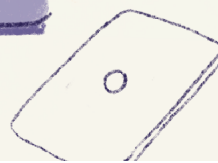
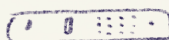
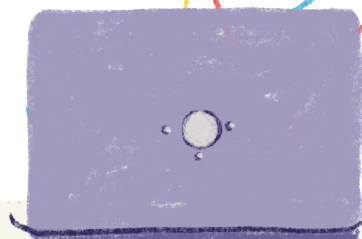
1.6. CONCLUSÃO: AS EMPRESAS DE TECNOLOGIA ESTÃO VIOLANDO OS DIREITOS À PROTEÇÃO DE DADOS PESSOAIS E OUTROS DIREITOS FUNDAMENTAIS DE MILHÕES DE PESSOAS QUE VIVEM EM PAÍSES COMO A COLÔMBIA AO SE RECUSAREM A CUMPRIR A LEGISLAÇÃO NACIONAL E A RECONHECER A JURISDIÇÃO DE SUAS AUTORIDADES.

O fato de não reconhecerem a jurisdição e a autoridade de governos como o da Colômbia, bem como a relutância das grandes empresas de tecnologia digital em cumprir as leis dos países nos quais não têm sede, está provocando graves violações dos direitos humanos. Nesta seção, nos concentramos principalmente no direito de habeas data, pois acreditamos que os dados pessoais são o motor do modelo de negócios das grandes empresas de tecnologia e constituem seu ativo mais importante. Também nos concentramos nesse direito específico porque sua violação ameaça “outros direitos que podem ser afetados devido à disponibilidade massiva de dados pessoais nas mãos de terceiros e ao maior poder computacional que isso confere àqueles que os tratam”³⁰. De fato, como será analisado mais adiante, certos grupos da população são especialmente vulneráveis ao uso de seus dados, e valores essenciais como a democracia correm risco devido ao uso manipulador dos dados pessoais. Da mesma forma, direitos como a saúde física e mental são afetados pelo design viciante, pela criação de perfis e pela influência nos hábitos de consumo.

Na medida em que as interações atuais ocorrem principalmente — embora não exclusivamente — no ciberespaço³¹ e por meio da Internet, é essencial reforçar a autoridade e a jurisdição das autoridades locais para proteger os direitos de seus cidadãos. Essa é a opinião do Tribunal Constitucional da Colômbia, que tem insistido que “o Estado não pode

³⁰ Ángel, M. P. (2025). Mineração de dados: a inteligência artificial e suas implicações para a privacidade e a proteção de dados pessoais na Colômbia. Em H. Rank (Ed.), Cinco perspectivas sobre o presente e o futuro da inteligência artificial na Colômbia (pp. 50-65). Konrad-Adenauer-Stiftung

³¹ Definido pelo MinTic como “o ambiente físico e virtual composto por computadores, sistemas de informação, programas de computador (software), redes de telecomunicações, dados e informações utilizados para a interação entre os usuários”. <https://www.mintic.gov.co/portal/inicio/Glosario/>



renunciar à sua jurisdição sobre a Internet”³² ; portanto, neste caso, o princípio da territorialidade é utilizado “para determinar se a controvérsia tem uma conexão relevante com o país, como a prestação de serviços a usuários na Colômbia ou o tratamento de dados pessoais dentro do território nacional”³³ . O Tribunal também observou que, “quando ocorrer uma ameaça ou uma violação dos direitos fundamentais no ciberespaço, o juiz responsável pelo recurso de tutela terá competência para decidir se tal ameaça ou violação tem efeitos relevantes na Colômbia”³⁴ .

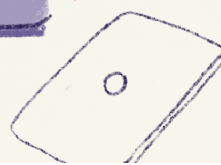
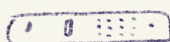
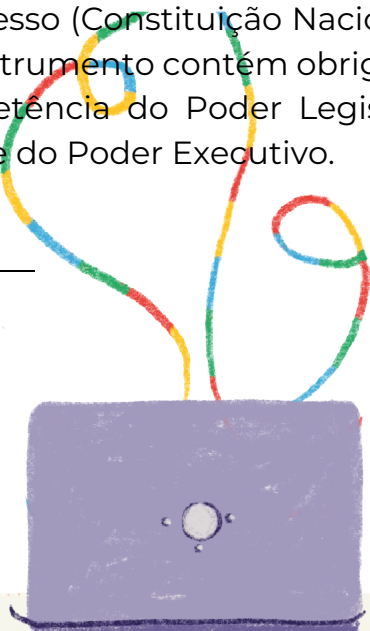
2. ENFRAQUECIMENTO DAS NORMAS DE PROTEÇÃO DE DADOS PESSOAIS COLETADOS PELAS PLATAFORMAS E SUA TRANSFERÊNCIA PARA OS ESTADOS UNIDOS EM VIRTUDE DE ACORDOS BILATERAIS

O Acordo entre os Estados Unidos da América e a República Argentina sobre Investimento e Comércio Recíproco (“AICR”), assinado em fevereiro de 2026, liberaliza o comércio entre os dois países por meio da eliminação, por parte da República Argentina, das barreiras tarifárias e não tarifárias aos produtos norte-americanos, a redução de subsídios e privilégios comerciais para empresas estatais argentinas, a harmonização das normas nacionais de qualidade para permitir a entrada de mercadorias provenientes dos Estados Unidos, a reforma do regime de propriedade intelectual, a abertura do mercado de mineração (AICR; anexo III, art. 4) e a eliminação de determinadas proteções de dados pessoais (AICR; anexo III, art. 2). O AICR entrará em vigor sessenta dias após a data em que ambos os Estados certificarem o cumprimento de seus respectivos requisitos legais internos (AICR; 6.7). Na República Argentina, isso significa que o tratado deve ser aprovado pelo Congresso (Constituição Nacional, CN; art. 75, parágrafo 22), uma vez que o instrumento contém obrigações que se enquadram no âmbito de competência do Poder Legislativo e que excedem o alcance da autoridade do Poder Executivo.

³² Ibid.

³³ Ibid.

³⁴ Ibid.

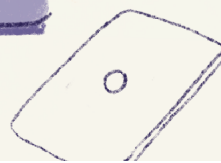
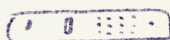
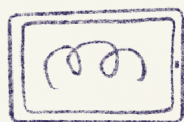
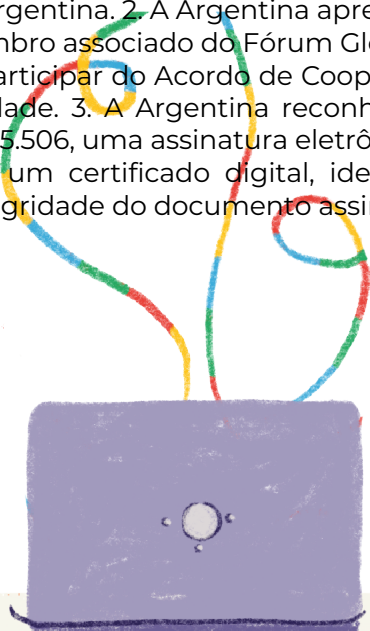


O artigo 2º do anexo III do AICR, que detalha os compromissos assumidos pela Argentina em virtude do tratado, contém uma série de modificações significativas no marco jurídico nacional em matéria de dados pessoais.

O AICR tem por objetivo “proporcionar segurança jurídica” para a exportação para os Estados Unidos de dados pessoais coletados na República Argentina. Nesse sentido, o AICR estabelece que, para fins de transferência de dados pessoais para os Estados Unidos, a Argentina considerará que os Estados Unidos garantem uma proteção jurídica “adequada” para tais dados³⁵. Além disso, o AICR prevê a participação da República Argentina em fóruns multilaterais por meio dos quais se promova o fluxo transfronteiriço de dados e a cooperação internacional entre as autoridades de controle em matéria de tratamento de dados. Por fim, a AICR estabelece que os documentos assinados eletronicamente nos Estados Unidos devem ser considerados equivalentes aos documentos assinados digitalmente, produzindo os mesmos efeitos jurídicos que uma assinatura digital e cumprindo os requisitos de integridade e autenticidade estabelecidos na legislação nacional (Lei 25.506; artigos 5, 7, 8, 9 e 11).

O artigo 12 da Lei 25.326 proíbe a transferência de dados pessoais de qualquer tipo para “países ou organizações internacionais ou supranacionais que não ofereçam níveis adequados de proteção”. A Agência de Acesso à Informação Pública (AAIP) determina, por

³⁵ AICR, Anexo III, art. 2 (“Comércio digital e tecnologia. 1. A Argentina garantirá a segurança jurídica no que diz respeito à possibilidade de transferir dados pessoais de seu território para os Estados Unidos, entre outras coisas, reconhecendo os Estados Unidos como um país ou jurisdição que oferece proteção de dados adequada de acordo com a legislação argentina. 2. A Argentina apresentará sua carta de intenções para participar como membro associado do Fórum Global de Normas de Privacidade Transfronteiriças e para participar do Acordo de Cooperação Global para a Aplicação da Normativa de Privacidade. 3. A Argentina reconhecerá como assinatura digital válida, nos termos da Lei 25.506, uma assinatura eletrônica criada nos Estados Unidos que seja respaldada por um certificado digital, identifique de forma confiável o signatário e garanta a integridade do documento assinado.



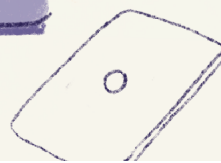
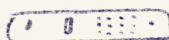
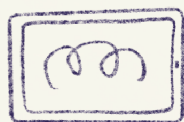
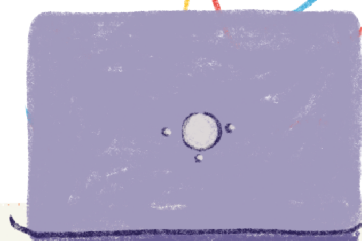
iniciativa própria ou a pedido de uma parte, quais países ou organizações oferecem proteção jurídica adequada (Decreto 1.558/2001; anexo I, 12).

Os Estados Unidos nunca constaram nem constam atualmente na lista de países que, segundo a AAIP, oferecem proteção jurídica adequada aos dados pessoais. Os fatores que, na opinião da autoridade reguladora argentina, suscitam preocupação são:

- Ao contrário da República Argentina, os Estados Unidos carecem de uma legislação federal uniforme sobre o tratamento de dados pessoais e de uma autoridade de controle eficaz.
- Consequentemente, as normas de “autorregulação” não são exigíveis nem uniformes nos cinquenta estados da União.

O AICR constituiria uma exceção à proibição de transferências de dados pessoais, seja como “tratado internacional do qual a Argentina é parte” (conforme estabelecido no artigo 12 da Lei 25.326) ou porque a AAIP emita — seja por instrução do presidente ou por meio do cumprimento voluntário do acordo — uma resolução na qual se declare que os Estados Unidos são uma jurisdição adequada. Isso implica autorizar transferências internacionais de dados para um país que, até agora, não era considerado uma “jurisdição adequada” pelo governo argentino, sem que as circunstâncias nesse país tenham mudado nem um pouco; ou, o que é ainda pior, apesar de essas circunstâncias terem se agravado no contexto do uso estratégico dos dados por parte do governo dos EUA como ferramenta de vigilância³⁶.

³⁶ Isso está relacionado ao debate atual no Congresso dos Estados Unidos sobre a renovação da seção 702 da Lei de Vigilância de Inteligência Estrangeira (FISA). A seção 702 permite que as agências de inteligência americanas coletem dados sobre qualquer pessoa não americana em relação à qual haja suspeita razoável de que se encontre fora do país, com o objetivo de obter “informações de inteligência estrangeira”. Essa autorização expira em junho. O programa serviu de base para a decisão europeia citada a seguir (Schrems II), que bloqueou as transferências de dados entre a UE e os EUA. Desde então, o governo Biden promoveu certas mudanças por meio de um decreto executivo, e a União Europeia voltou a permitir essas transferências; no entanto, essas reformas não foram incorporadas à legislação e, sob o governo de Trump, persistem riscos significativos de que a coleta massiva de dados continue sem as garantias adequadas.



Em virtude do AICR, a venda de dados pessoais a controladores ou processadores norte-americanos — incluindo as grandes empresas de tecnologia sediadas naquele país — não estará mais sujeita à regulamentação da lei de proteção de dados nem à AAIP, nem será exigido o cumprimento das cláusulas-modelo de proteção nem do requisito de autorização administrativa prévia, caso estas contenham disposições diferentes. Pelo simples fato de seus dados terem sido vendidos aos Estados Unidos, os titulares dos dados não gozarão mais das proteções oferecidas pela legislação argentina e poderão ser privados da proteção de seus tribunais.

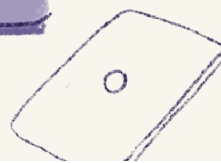
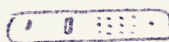
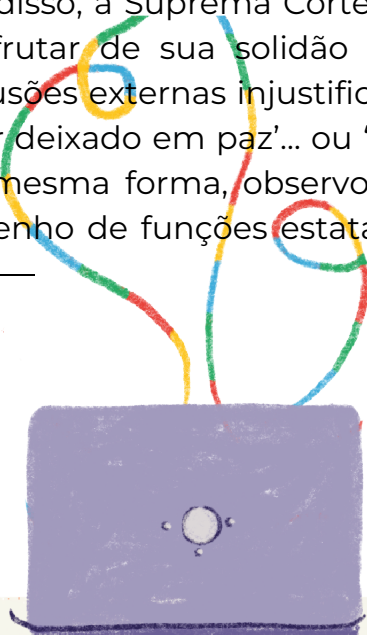
Em uma decisão recente sobre o caso “Torres Abad”, a Suprema Corte de Justiça da Nação interpretou o alcance dos artigos 19 e 43 da Constituição Nacional de uma forma que entra em conflito com as disposições da AICR. Nesse caso, o Tribunal declarou inconstitucional a cessão de dados pessoais sem o consentimento específico dos interessados nos casos em que a lei de proteção de dados pessoais autorizava tais cessões “no cumprimento de funções estatais” ou em virtude de um mandato legal relativo a tais autoridades, ou por meio de acordos celebrados entre elas no âmbito de suas respectivas competências.

O Tribunal sustentou que os artigos 19 e 43, parágrafo 3, da Constituição Nacional consagram o direito à autodeterminação informativa³⁷ — já reconhecido pela Corte Interamericana de Direitos Humanos no caso CAJAR — e o direito a “ser deixado em paz”. Quanto ao primeiro, o Tribunal afirmou que “toda pessoa tem o direito de dispor dos dados que lhe dizem respeito, de decidir com quem e em que medida deseja compartilhá-los e, quando for o caso, de controlar o uso que terceiros fazem deles”.³⁸ Além disso, a Suprema Corte reconheceu “o direito de toda pessoa de desfrutar de sua solidão e tranquilidade, sem ser incomodada por intrusões externas injustificadas, também conhecido como o ‘direito de ser deixado em paz’... ou ‘direito de ser deixado em tranquilidade’”.³⁹ Da mesma forma, observou que as exceções legais relativas ao “desempenho de funções estatais” ou equivalentes eram

³⁷ Torres Abad, consid. 8.

³⁸ Torres Abad, consid. 8.

³⁹ Torres Abad, consid. 8.



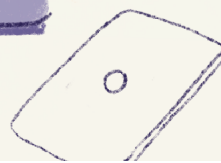
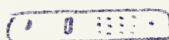
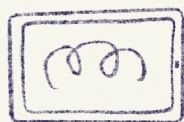
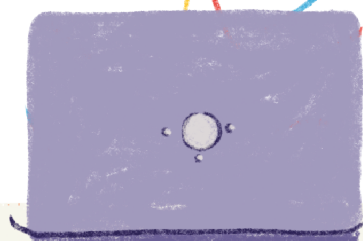
tão amplas que, por si sós, não atendiam aos requisitos de finalidade legítima ou proporcionalidade.

A AICR não garantirá a autonomia informativa tal como reconhecida pela Corte Interamericana e pela Suprema Corte, pelo menos no que diz respeito às operações posteriores realizadas nos Estados Unidos com dados pessoais exportados da Argentina. Ao contrário da posição defendida na Europa — e até mesmo durante décadas pelas próprias autoridades argentinas — de que os Estados Unidos apresentam riscos gerais decorrentes da falta de proteção jurídica e da extensão da jurisdição, bem como riscos específicos decorrentes da aplicação da Lei FISA, que autoriza o governo dos Estados Unidos a coletar dados pessoais vendidos por empresas privadas para fins de vigilância estatal, a AICR classifica os Estados Unidos como uma “jurisdição adequada”. Como consequência dessa classificação, as transferências de dados para os Estados Unidos deixarão de estar sujeitas às garantias estabelecidas pela Lei de Proteção de Dados Pessoais, às cláusulas-modelo ou aos poderes de supervisão da AAIP após a conclusão da transferência. Consequentemente, os titulares dos dados verão reduzida, se não eliminada, sua capacidade de invocar o princípio do consentimento — ou de contestar a ilegalidade, a ilegitimidade ou o caráter desproporcional dos usos que possam ser feitos de seus dados — uma vez que seus dados sejam transferidos para empresas americanas e/ou, a partir delas, para o governo federal dos Estados Unidos.

3. IMPACTOS DOS MODELOS DE NEGÓCIOS BASEADOS EM DADOS NOS DIREITOS FUNDAMENTAIS E HUMANOS

3.1. REPERCUSSÕES NO VOTO, NA IGUALDADE E NA NÃO DISCRIMINAÇÃO

Os modelos de negócios das plataformas digitais, baseados na coleta em grande escala de dados pessoais e na amplificação algorítmica, têm implicações diretas para o exercício da cidadania e para alguns direitos fundamentais. Em particular, essas dinâmicas afetam os direitos ao voto livre, à igualdade e à não discriminação, consagrados nos artigos 23 e 24 da Convenção Americana sobre Direitos Humanos (CADH). Essa

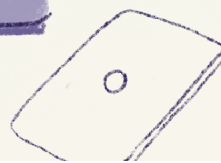
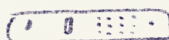
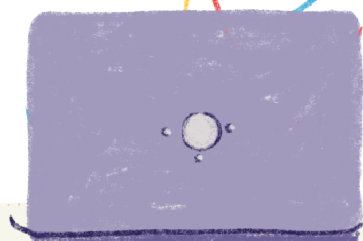


conexão reside no fato de que o gozo efetivo do direito ao voto depende não apenas da capacidade formal de votar, mas também da existência de condições que garantam uma participação livre, informada e igualitária na vida política e pública.

E, ao longo da última década, os processos eleitorais em todo o mundo, mas também em nossa região, têm se desenrolado em ambientes públicos cada vez mais polarizados e conflituosos, caracterizados pela circulação generalizada de desinformação, informações errôneas, discurso de ódio e violência política online. Esse contexto é ainda mais intensificado pelos modelos de negócios e pelos sistemas de recomendação das plataformas digitais. O avanço das ferramentas de inteligência artificial capazes de produzir conteúdos sintéticos muito realistas também aumentou os desafios que a proteção do debate público democrático apresenta.

A microsegmentação política é uma prática que utiliza dados pessoais, comportamento online e inferências algorítmicas para segmentar eleitores e enviar mensagens políticas altamente personalizadas a grupos ou indivíduos específicos. Essa prática é possível graças aos modelos de negócios das plataformas digitais e se baseia na coleta de dados em grande escala por parte dessas plataformas. Esse novo fenômeno tornou a comunicação eleitoral cada vez mais opaca e dependente de infraestruturas algorítmicas controladas por empresas — uma dinâmica que chamou a atenção mundial após o caso da Cambridge Analytica e suas implicações para a democracia.

Como exemplo adicional, o problema da segmentação do público — e, em formas mais avançadas, da microsegmentação — na comunicação eleitoral também pôde ser observado nas eleições brasileiras de 2018. A autorização da promoção paga de conteúdos políticos em plataformas digitais como o Facebook contribuiu para mudanças nas estratégias de comunicação eleitoral, permitindo formas de segmentação do público com base em critérios demográficos, territoriais e de idade. As campanhas políticas passaram a adaptar suas mensagens a diferentes grupos de eleitores, transferindo parte da mediação eleitoral e da distribuição de anúncios para as infraestruturas de plataformas digitais privadas. Esse processo ampliou o papel da segmentação mediada



pelas plataformas na comunicação eleitoral e suscitou preocupações, especialmente no que diz respeito à transparência.⁴⁰

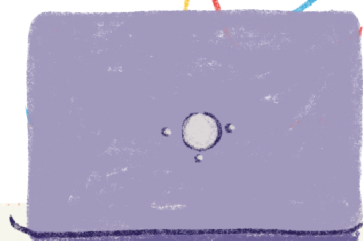
Além disso, conforme destacado anteriormente no documento que fundamentou o pedido desta audiência, a interseção entre a criação de perfis algorítmicos e a publicidade eleitoral digital tornou-se uma das ameaças mais significativas à integridade dos processos democráticos na América Latina. Os dados da Colômbia e do Brasil⁴¹, por exemplo, demonstram que, em média, 70% das pessoas se baseiam em informações online para formar suas opiniões políticas. Esse contexto complexo implica que as garantias formais do direito ao voto, tal como costumávamos considerá-las, são insuficientes se não forem acompanhadas de condições materiais que protejam a autonomia informativa dos eleitores. A criação de cenários que manipulam intencionalmente as informações que chegam aos eleitores, com o objetivo de desinformá-los, pode minar os princípios básicos da liberdade de expressão e do pluralismo informativo.⁴²

É igualmente importante destacar que, com as plataformas digitais e as tecnologias emergentes, a difusão personalizada e individualizada de narrativas eleitorais direcionadas a um público específico torna-se possível com notável facilidade, baixo custo e transparência limitada. Além da previsão, esses sistemas operam cada vez mais por meio da configuração contínua de percepções e comportamentos por meio de ambientes informativos personalizados, especialmente em contextos marcados por níveis desiguais de alfabetização digital: segundo dados

⁴⁰ Alves, Marcelo; Tavares, Camila. "Propaganda eleitoral digital no Brasil: estratégias de segmentação das candidaturas à presidência em 2018 no Facebook". Revista Ecopós, 2023. Disponível em: <https://revistaecopos.eco.ufrj.br/ecopos/article/view/27914/15405>

⁴¹ Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC). As plataformas da internet são o principal meio de acesso à informação entre os brasileiros e superam o rádio e a televisão, segundo aponta uma nova pesquisa. 2026. Disponível em: <https://cetic.br/pt/noticia/plataformas-da-internet-sao-o-principal-meio-de-acesso-a-informacao-entre-brasileiros-e-superam-radio-e-tv-aponta-nova-pesquisa/>.

⁴² López, Vanessa. "Nem tudo vale, nem na campanha nem na internet". Dejusticia, 5 de março de 2026. Disponível em: <https://www.dejusticia.org/no-todo-vale-ni-en-campana-ni-en-internet/>



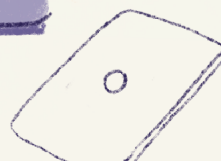
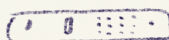
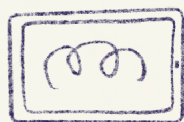
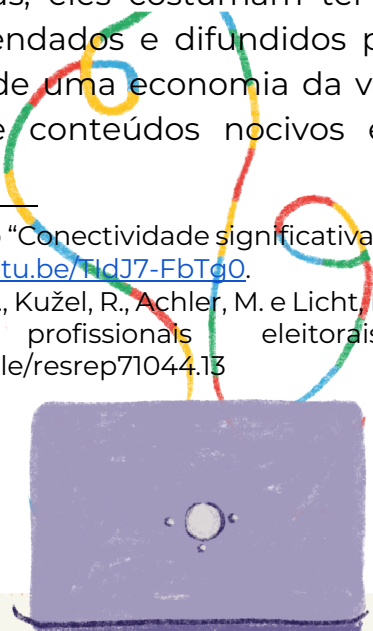
de 2023, apenas 28% da população da América Latina possui competências digitais básicas.⁴³

Além disso, a preocupação que a microsegmentação suscita reside no fato de que ela permite que diferentes grupos recebam mensagens radicalmente distintas sobre os mesmos candidatos ou propostas, sem que nenhum ator externo possa verificar o conteúdo ou o alcance dessas comunicações. Da mesma forma, “os candidatos e os partidos podem fazer promessas diferentes ou até mesmo declarações contraditórias a distintos grupos de eleitores, com pouca supervisão ou prestação de contas”.⁴⁴ Quem possui as bases de dados mais completas são as redes sociais, uma vez que permitem a elaboração de perfis com base no histórico de navegação, nas interações sociais, nos interesses e nas vulnerabilidades inferidas, o que pode levar a uma distorção da informação. Isso, por sua vez, gera importantes assimetrias na competição eleitoral, ao conferir capacidades desiguais para moldar as percepções de dos eleitores e adaptar a comunicação política. Em resumo, quando combinadas com práticas de segmentação opacas e acesso desigual às infraestruturas publicitárias baseadas em dados, essas disparidades podem contribuir para o reforço dos desequilíbrios estruturais entre candidatos e partidos, o que suscita preocupações em relação ao abuso de poder econômico e político nos ambientes de campanha digital.

Os sistemas de recomendação das plataformas digitais e outros mecanismos algorítmicos, ao ampliarem a velocidade e o alcance dos fluxos de informação, também tendem a priorizar os conteúdos que geram maiores níveis de atenção e participação. Como conteúdos violentos, polarizadores ou carregados de emoção podem provocar reações mais intensas, eles costumam ter mais chances de serem amplificados, recomendados e difundidos por sistemas algorítmicos que operam dentro de uma economia da visibilidade. Essa dinâmica facilita a difusão de conteúdos nocivos e configura o ambiente

⁴³ Maribel Dalio. Seminário “Conectividade significativa: um novo desafio para o Brasil”. Disponível em: <https://youtu.be/FldJ7-FbTg0>.

⁴⁴ Krimmer, R., Rabitsch, A., Kužel, R., Achler, M. e Licht, N. (2022). Eleições na era digital: um guia para profissionais eleitorais (Relatório). UNESCO. <https://www.jstor.org/stable/resrep71044.13>



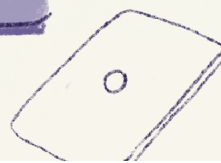
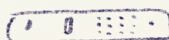
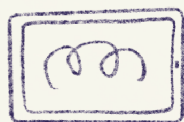
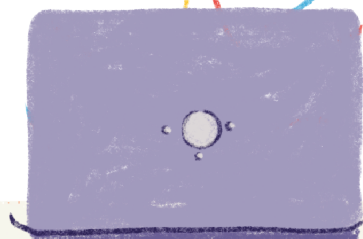
informativo no qual os cidadãos formam suas percepções sobre as questões públicas. Nesse contexto, isso pode afetar as condições para uma participação significativa na vida política e pública, especialmente ao limitar a capacidade de grupos historicamente marginalizados de participar em condições de igualdade nos processos democráticos.

Nesse sentido, volta a ser importante destacar o caso do Brasil. Um estudo de 2025 realizado pelo Instituto Marielle Franco mostra que a internet tem sido instrumentalizada como um espaço de violência política destinado a obstruir a participação política de mulheres, ativistas e representantes eleitos, em particular de mulheres negras e pessoas LGBTQIA+. Entre os casos registrados de violência online, 71% consistem em ameaças de morte e de estupro, frequentemente associadas a conteúdos discriminatórios e ao discurso de ódio.⁴⁵ O relatório “MonitorA” de 2024 também mostra que essa violência é sistemática, e não apenas episódica, e afeta de forma desproporcional as candidatas, especialmente mulheres negras e pessoas LGBTQIA+. O relatório também aponta casos de conteúdos manipulados e alterados, incluindo referências a deepfakes e a conteúdos sexuais⁴⁶ sintéticos sem consentimento (“deepnudes”), como parte das tendências emergentes na violência política digital. Essas dinâmicas se inscrevem no contexto dos debates eleitorais, nos quais se observa uma intensificação das interações violentas durante os ciclos eleitorais.⁴⁷ Conforme se depreende do relatório elaborado pela Terra de Direitos e pela Justiça Global, o crescente impacto das plataformas digitais na disputa política deu origem a uma dinâmica dual: embora essas plataformas ofereçam novas oportunidades para a participação democrática, elas também apresentam importantes desafios para a democracia ao permitirem a proliferação do discurso de ódio, da

⁴⁵ Instituto Marielle Franco. Regime de ameaça: violência política de gênero e raça no âmbito digital. 2025. Disponível em: <https://www.violenciapolitica.org/>.

⁴⁶ Sobre esse ponto, o UNICEF realizou um estudo na Colômbia, intitulado “Disrupting Harm: Exploração e abuso sexual de meninas, meninos e adolescentes facilitados pela tecnologia na Colômbia”. Disponível em: <https://www.unicef.org/colombia/informes/disrupting-harm>

⁴⁷ Internetlab; Revista Azmina; Núcleo de Jornalismo; LABHD UFBA. MonitorA: relatório sobre a violência política contra candidatas e candidatos na internet. Edição 2024. São Paulo, 2025. Disponível em: https://internetlab.org.br/wp-content/uploads/2025/05/MonitorA-Relatorio_2024-3.pdf



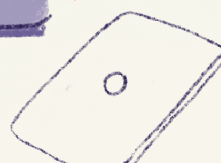
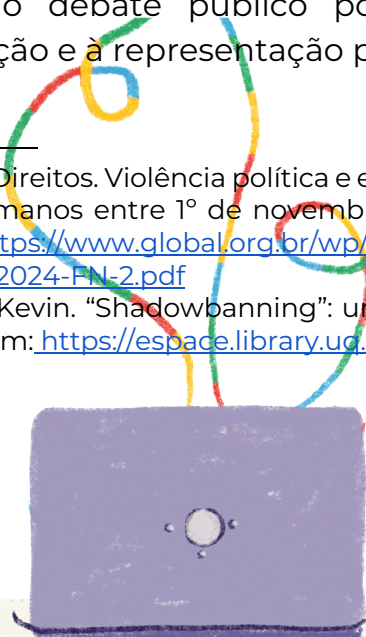
desinformação e dos ataques seletivos, o que prejudica a participação de determinados grupos nos processos democráticos.⁴⁸

É nesse contexto que a violência política online atua como um mecanismo estrutural que prejudica a participação política, ao gerar ambientes excludentes que limitam a plena participação de grupos historicamente marginalizados na vida democrática. Mais do que se tratar de conteúdos isolados, essa violência online está integrada às lógicas de interação das plataformas digitais. Sua dinâmica pode contribuir para a amplificação de conteúdos nocivos direcionados a candidaturas de pessoas específicas, uma vez que os sistemas algorítmicos podem distribuir ainda mais esse material quando ele gera altos níveis de interação, especialmente quando combinado com uma segmentação prévia do público com base em dados comportamentais.

Outra preocupação é o fenômeno, cada vez mais documentado, do “shadow banning”. Estudos recentes sugerem que pessoas pertencentes a grupos historicamente marginalizados (como minorias raciais e étnicas, pessoas LGBTQ+, pessoas trans e/ou não binárias) relatam ter sofrido o “shadow banning”.⁴⁹ Na prática, isso significa que as arquiteturas das plataformas digitais e os sistemas algorítmicos podem reduzir a visibilidade e o alcance de certos tipos de conteúdo, limitando a divulgação de algumas mensagens por meio da supressão algorítmica ou da redução da visibilidade. No âmbito político, essas dinâmicas podem afetar de forma desproporcional os candidatos de grupos sub-representados, prejudicando sua capacidade de alcançar os eleitores, se dar a conhecer e competir em igualdade de condições em ambientes de campanha digital. Como resultado, as vozes que já são sub-representadas no debate público podem enfrentar barreiras adicionais à participação e à representação políticas.

⁴⁸ Justiça Global; Terra de Direitos. Violência política e eleitoral no Brasil. Panorama das violações dos direitos humanos entre 1º de novembro de 2022 e 27 de outubro de 2024. Disponível em: https://www.global.org.br/wp/wp-content/uploads/2024/12/11-25_VIOLENCIA-POLITICA-2024-FNL-2.pdf

⁴⁹ Risius, Marten; Blasiak, Kevin. “Shadowbanning”: uma forma opaca de moderação de conteúdo. Disponível em: <https://espace.library.uq.edu.au/view/UQ:15cd999>.



Diante desse cenário, os Estados da região têm a obrigação de garantir não apenas o direito ao voto como ato formal, mas também as condições materiais que tornam esse voto verdadeiramente livre e informado. Um processo eleitoral em que os dados pessoais dos cidadãos são utilizados de forma não transparente para criar perfis políticos, direcionar mensagens diferenciadas e amplificar narrativas que contêm desinformação e discurso de ódio não é um processo em que a liberdade de voto esteja plenamente garantida.

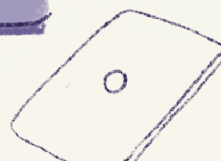
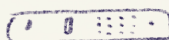
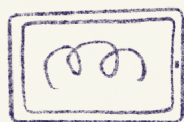
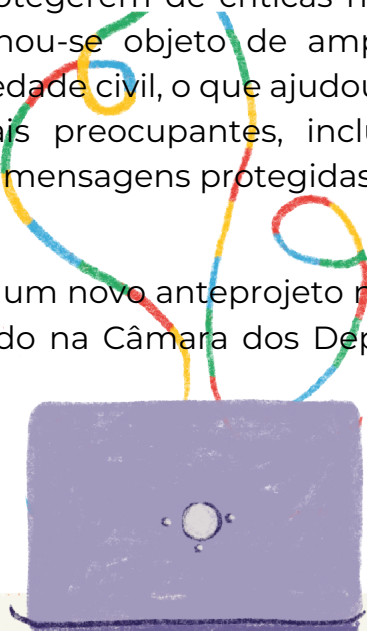
A falta de prestação de contas por parte das principais plataformas em relação a essas práticas compromete, conseqüentemente, não apenas os direitos individuais ao habeas data e à informação, mas também o direito coletivo de viver em uma democracia cujos processos sejam genuinamente soberanos e livres de interferências algorítmicas.

3.2. MANIPULAÇÃO DO DEBATE PÚBLICO: O CASO DO PROJETO DE LEI 2630 DO BRASIL

Os riscos descritos acima não se limitam à publicidade eleitoral ou à circulação de conteúdo nocivo durante as campanhas. Eles também surgem quando plataformas digitais dominantes utilizam suas próprias infraestruturas, sua posição de mercado e seu controle sobre os fluxos de informação para moldar o debate público sobre as regras que deveriam regê-las. Um exemplo particularmente ilustrativo pode ser encontrado no debate brasileiro em torno do Projeto de Lei 2630, comumente conhecido como o “PL das Fake News”.

O Projeto de Lei 2630 foi apresentado no Senado brasileiro em 2020. Em sua forma inicial, a proposta refletia, em parte, o desejo de alguns legisladores de se protegerem de críticas nos ambientes digitais. No entanto, o texto tornou-se objeto de amplo debate público e de engajamento da sociedade civil, o que ajudou a neutralizar algumas de suas disposições mais preocupantes, incluindo uma proposta de obrigação de rastrear mensagens protegidas por criptografia de ponta a ponta.

Após a divulgação de um novo anteprojeto no início de 2022, o projeto permaneceu paralisado na Câmara dos Deputados até o começo de



2023. Na esteira da tentativa fracassada de grupos de extrema direita de derrubar o recém-empossado governo do presidente Lula da Silva, e em meio a um pico de ataques violentos em escolas brasileiras, o Projeto de Lei 2630 tornou-se o principal veículo legislativo para tratar de preocupações mais amplas sobre o uso de tecnologias digitais em contextos de convulsão social. Para tanto, o Poder Executivo propôs um texto revisado ao relator do projeto, introduzindo diversas mudanças inspiradas em marcos regulatórios como a NetzDG da Alemanha, a Lei de Serviços Digitais da União Europeia e o Projeto de Lei de Segurança Online do Reino Unido.

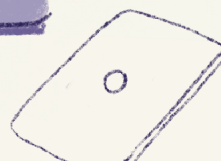
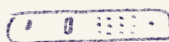
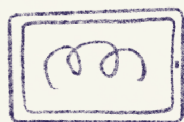
Em uma tentativa de fazer a proposta avançar, o presidente da Câmara dos Deputados marcou um requerimento de urgência para 25 de abril de 2023, que teria acelerado o processo legislativo ao permitir que o projeto fosse apreciado diretamente pelo plenário.

Diante da perspectiva de uma rápida aprovação do projeto, as grandes empresas de tecnologia mobilizaram uma série de estratégias para influenciar o debate.

A primeira estratégia consistiu em um lobby intensificado direcionado a legisladores e atores políticos, enfatizando os supostos impactos negativos do PL das Fake News. Um elemento decisivo na campanha de oposição foi o apoio obtido da Bancada Evangélica, supostamente por meio de um lobby coordenado liderado pela Meta, que argumentou que as obrigações de prevenir conteúdos potencialmente ilegais poderiam resultar na remoção de publicações que citassem passagens bíblicas.⁵⁰

O poder econômico dessas empresas foi central para a escala do esforço de lobby realizado no Congresso. Conforme noticiado pela Agência Pública, os lobistas da Meta estiveram entre os visitantes mais frequentes da Câmara dos Deputados: os gerentes de políticas públicas

⁵⁰ Metrôpoles. Associação de lobby que reúne Facebook, Google e TikTok espalhou que PL das Fake News censura religião. <https://www.metropoles.com/colunas/guilherme-amado/associacao-de-lobby-que-reune-facebook-google-e-tiktok-espalhou-que-pl-das-fake-news-censura-religiao> (27 abr. 2023).



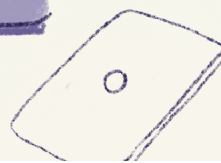
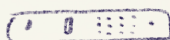
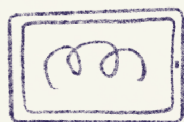
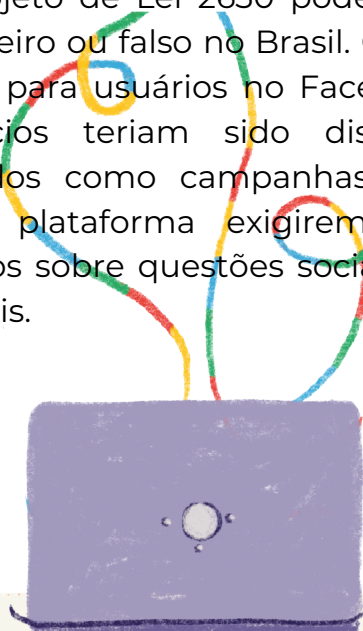
da Meta, Marconi Machado e André Atadeu, registraram cada um mais de cem visitas entre julho de 2022 e maio de 2025². No entanto, outras estratégias deixaram ainda mais claro como a concentração de poder econômico nos mercados de plataformas digitais pode ser usada para direcionar o debate público.

Na manhã de 25 de abril de 2023, dia em que a votação do requerimento de urgência estava marcada, o YouTube lançou uma campanha contra o Projeto de Lei 2630 voltada aos criadores de conteúdo. A empresa argumentou que a proposta poderia dar ao governo o poder de “controlar aspectos centrais da plataforma” e forçá-la a “remover grandes quantidades de conteúdo legítimo”.

A campanha foi disseminada por meio dos canais internos de criadores da plataforma, por e-mail e no blog da empresa, incentivando o uso da hashtag #MaisDebate2630. O YouTube também incentivou influenciadores a “se fazerem ouvir”, resultando em vídeos que reproduziam os argumentos da empresa. Essa estratégia, que mobilizou um grupo de pessoas economicamente dependentes da plataforma para defender seus interesses corporativos, sugeria fortemente que a participação das empresas no debate público seria moldada pelo uso de seu poder econômico.

Com outra etapa da votação prevista para 2 de maio, as empresas aumentaram a pressão.

Entre 27 de abril e 2 de maio, o Google teria investido mais de R\$ 2 milhões em anúncios em jornais impressos, televisão e redes sociais. Em um único anúncio, exibido entre 1º e 3 de maio, o Google pagou à Meta entre R\$ 200 mil e R\$ 250 mil por um vídeo de 15 segundos afirmando que o Projeto de Lei 2630 poderia aumentar a confusão sobre o que é verdadeiro ou falso no Brasil. O vídeo apareceu mais de um milhão de vezes para usuários no Facebook e no Instagram no Brasil. Esses anúncios teriam sido disseminados sem serem devidamente rotulados como campanhas políticas, apesar de as próprias regras da plataforma exigirem que anunciantes que patrocinam conteúdos sobre questões sociais, eleições ou política os identifiquem como tais.



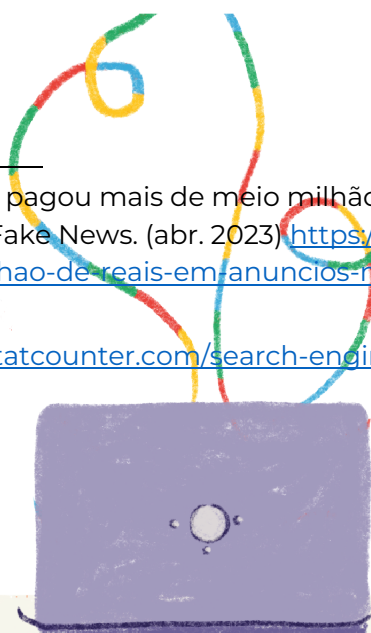
A escala desse investimento é particularmente reveladora. Antes da campanha contra o Projeto de Lei 2630, a última campanha registrada do Google no Facebook e no Instagram havia ocorrido em novembro de 2022, durante o Mês da Consciência Negra, quando a empresa teria pago menos de R\$ 100 e alcançado aproximadamente 35.000 telas.⁵¹

Em 1º de maio, o Google modificou o design de sua página inicial para incluir um link contrário ao projeto. Os usuários que acessavam o mecanismo de busca viam, abaixo da caixa de pesquisa, a afirmação de que “o PL das Fake News poderia aumentar a confusão sobre o que é verdadeiro ou falso no Brasil”. Ao clicar na frase, os usuários eram direcionados a publicações do Google que defendiam a posição da empresa contra o projeto. Essas mensagens foram vistas por milhões de brasileiros, justamente por causa do controle do Google sobre o mercado de buscas: o Google é o mecanismo de busca usado por aproximadamente 86% dos 160 milhões de brasileiros que usam a internet.⁵²

Outra ação mapeada pelos pesquisadores do NetLab dizia respeito à suposta manipulação dos resultados de busca. Um exemplo envolveu as perguntas relacionadas sugeridas pelo Google quando os usuários pesquisavam “PL 2630”. Aos usuários que digitavam “PL 2630” na caixa de busca eram exibidas perguntas como “O PL da censura foi aprovado?” e “O que é o PL da Censura?” — um termo pejorativo usado pelos opositores da regulação das plataformas, em vez do nome oficial do projeto ou do rótulo midiático mais comum, “PL das Fake News”. Os pesquisadores consideraram esse resultado significativo porque, segundo dados da Semrush, as consultas mais comuns no Google

⁵¹Agência Pública. Google pagou mais de meio milhão de reais em anúncios no Facebook contra PL das Fake News. (abr. 2023) <https://apublica.org/2023/05/google-pagou-mais-de-meio-milhao-de-reais-em-anuncios-no-facebook-contr-pl-das-fake-news> (abr. 2023).

⁵²Statcounter: <https://gs.statcounter.com/search-engine-market-share/all/brazil/2023>



relacionadas ao Projeto de Lei 2630 não usavam o termo “PL da Censura”.⁵³

A equipe de pesquisa também identificou que o primeiro resultado exibido para os usuários que buscavam informações sobre o projeto era uma publicação patrocinada do próprio blog do Google intitulada “conheça o PL da Censura”.

Em conjunto, essas ações ilustram como o Google utilizou sua posição dominante no mercado de buscas para moldar a percepção dos usuários sobre o projeto de uma forma alinhada aos seus interesses comerciais.

A pressão teve efeitos políticos mensuráveis. Em 26 de abril de 2023, 193 deputados se opunham ao projeto e 236 o apoiavam. Três dias depois, o equilíbrio havia mudado: 228 deputados se opunham ao projeto, 223 o apoiavam e 62 permaneciam indecisos. Pouco depois, o relator do projeto decidiu retirá-lo da pauta, e a proposta acabou perdendo qualquer perspectiva realista de aprovação⁵⁴.

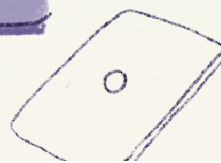
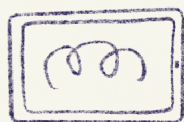
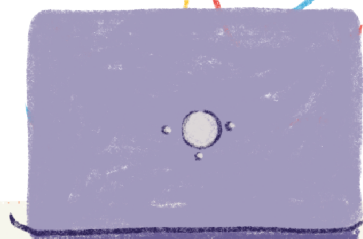
Algumas autoridades públicas, incluindo o Ministério Público Federal e a Secretaria Nacional do Consumidor, buscaram investigar a conduta das grandes empresas de tecnologia na campanha contra o projeto, particularmente o possível abuso de poder econômico.⁵⁵ O Conselho Administrativo de Defesa Econômica do Brasil também abriu um processo administrativo para examinar o suposto abuso de posição dominante por parte do Google e da Meta em conexão com os debates em torno do Projeto de Lei 2630.⁵⁶ No entanto, nenhuma dessas

⁵³NetLab. A guerra das plataformas. (abr. 2023) <https://netlab.eco.ufrj.br/post/google-e-telegram-abusaram-do-poder-econ%C3%B4mico-nas-campanhas-contr-o-pl-2630>

⁵⁴Agência Pública. Como as big techs mataram o PL das Fake News. (9 set. 2025) <https://apublica.org/2025/09/como-as-big-techs-mataram-o-pl-das-fake-news/>.

⁵⁵Agência Brasil. MPF questiona Google sobre campanha contra PL das Fake News. (2 maio 2023) <https://agenciabrasil.ebc.com.br/politica/noticia/2023-05/mpf-questiona-google-sobre-campanha-contr-pl-das-fake-news>

⁵⁶Cade. Cade abre investigação contra Google e Meta para apurar abuso de posição dominante nas discussões sobre o PL das Fake News. (2 maio 2023) <https://www.gov.br/cade/pt-br/assuntos/noticias/cade-abre-investigacao-contr>



iniciativas resultou em responsabilização significativa das plataformas nem alterou materialmente sua capacidade de usar suas próprias ferramentas para influenciar o debate público.

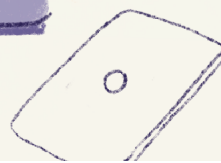
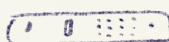
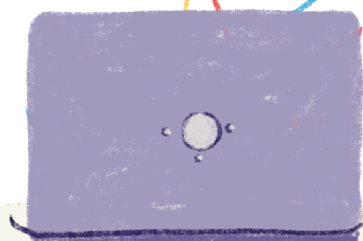
A relação entre a posição monopolista das grandes plataformas e sua capacidade de capturar e manipular o debate público tornou-se particularmente visível na discussão em torno do Projeto de Lei 2630, mas permaneceu praticamente inalterada nos últimos anos. Embora o Brasil tenha avançado em novos mecanismos de responsabilização das plataformas, pouco foi feito para reduzir o poder econômico desfrutado por essas empresas. O que a experiência brasileira revela, portanto, é a ausência de instrumentos adequados para lidar com a própria concentração de poder econômico. Por essa razão, no ano passado o Brasil começou a discutir o Projeto de Lei 4675, que busca ampliar os poderes da autoridade de concorrência para que ela possa responder aos novos desafios impostos pelos mercados digitais e pela conduta das grandes empresas de tecnologia.

3.3. EFEITOS SOBRE A SAÚDE MENTAL RELACIONADOS PRINCIPALMENTE ÀS PLATAFORMAS DE IA GENERATIVA

O surgimento dos produtos de IA generativa agravou a ameaça que o design viciante representa para os direitos humanos nas Américas. Os chatbots de IA generativa, que funcionam com grandes modelos de linguagem (LLM), são agentes conversacionais sofisticados, programados para sintetizar respostas totalmente novas e sensíveis ao contexto, prevendo palavras a partir de enormes conjuntos de dados de treinamento. Como resultado, as respostas dos chatbots baseados em LLM imitam a fala humana e geram respostas que reafirmam seus usuários.⁵⁷ Essas características de design, como o antropomorfismo e a bajulação, levaram muitos consumidores a perceber tanto os

[google-e-meta-para-apurar-abuso-de-posicao-dominante-nas-discussoes-sobre-o-pl-das-fake-news.](#)

⁵⁷ Alicia DeVrio et al., “A Taxonomy of Linguistic Expressions That Contribute To Anthropomorphism of Language Technologies”, arXiv (14 de fevereiro de 2025), <https://arxiv.org/pdf/2502.09870>; Mrinank Sharma et al., “Rumo à compreensão da adulação em modelos linguísticos”, arXiv (10 de maio de 2025), <https://arxiv.org/pdf/2310.13548>.



chatbots de uso geral, como o ChatGPT, quanto os chatbots de companhia, como o Character.AI, como confidentes com disponibilidade ilimitada que sempre concordam com eles, o que incentiva o uso excessivo e a dependência.⁵⁸

Além disso, assim como as plataformas de redes sociais, muitos chatbots coletam uma grande quantidade de dados sobre usuários individuais e utilizam esses dados para personalizar as respostas do chatbot por meio de recursos como a “Memória” do ChatGPT, com o objetivo de captar a atenção dos usuários de forma mais eficaz e mantê-los conectados por mais tempo.⁵⁹ Os dados dos usuários também são utilizados para treinar modelos de IA, de modo que os chatbots simulem a linguagem humana de forma ainda mais eficaz.⁶⁰ Devido às respostas calorosas e de caráter humano dos chatbots, os consumidores tendem a incluir informações mais íntimas sobre si mesmos em suas mensagens, o que aumenta a capacidade das empresas de IA de explorar seus dados pessoais com o objetivo de aumentar o engajamento.⁶¹

A combinação de um design lisonjeiro e de aparência humana com funcionalidades que exploram dados pessoais para personalizar a experiência do usuário tem se mostrado muito eficaz. Em fevereiro de 2026, um em cada quatro adultos norte-americanos utilizava diariamente chatbots de IA generativa.⁶² Crianças e pessoas com deficiência parecem especialmente vulneráveis às características

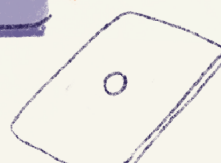
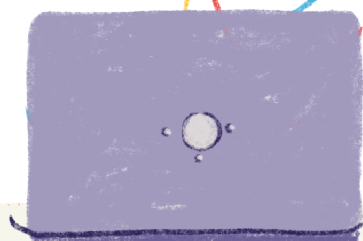
⁵⁸ Zilan Qian et al., “Mapeamento do mercado de IA parasocial: tendências dos usuários, participação e riscos”, arXiv (22 de julho de 2025), <https://arxiv.org/pdf/2507.14226>.

⁵⁹ Por exemplo, “Dreaming: Melhor Memória para um ChatGPT Mais Útil”, OpenAI (4 de junho de 2026), <https://openai.com/index/chatgpt-memory-dreaming/>.

⁶⁰ Nikki Goth Itoi, “Cuidado com o que você conta ao seu chatbot de IA”, Centro de Inteligência Artificial Centrada no Ser Humano da Universidade de Stanford (15 de outubro de 2025), <https://hai.stanford.edu/news/be-careful-what-you-tell-your-ai-chatbot>.

⁶¹ Muhammad Jazlan, “Rastreamento de conversas: medição da exposição de conteúdo e identidade em chatbots de IA”, arXiv, 1 (13 de maio de 2026), <https://arxiv.org/pdf/2604.27438>.

⁶² Gottfried et al., “Os americanos e a IA em 2026: chatbots, dispositivos inteligentes e opiniões sobre seu impacto”, Pew Research Center (17 de junho de 2026), <https://www.pewresearch.org/internet/2026/06/17/americans-and-ai-2026-chatbots-smart-devices-and-views-on-impact>



viciantes dos chatbots de IA. Mais da metade dos adolescentes usa chatbots; três em cada dez o fazem diariamente e 16% os utilizam várias vezes ao dia ou “quase constantemente”.⁶³ Mais de um terço dos psicólogos norte-americanos relatam ter pacientes que recorrem aos chatbots de IA como um profissional de saúde mental adicional.⁶⁴

O design viciante dos chatbots com IA tem efeitos devastadores sobre a saúde mental e os direitos humanos dos usuários, especialmente no caso de crianças e pessoas com deficiência. Nos Estados Unidos, foram apresentadas várias ações judiciais relacionadas a pessoas que cometeram suicídio após períodos intensos de uso de chatbots, durante os quais o produto de IA reafirmava ou incentivava suas tendências suicidas.⁶⁵ Outras pessoas desenvolveram delírios incapacitantes após serem persuadidas por um chatbot de IA de que delírios cada vez mais graves eram verdadeiros.⁶⁶ Pessoas que antes tinham um alto nível de funcionamento e que desenvolveram delírios provocados pela IA tentaram cometer e cometeram homicídios,⁶⁷ perderam seus empregos e acumularam dívidas financeiras,⁶⁸ e sofreram crises psíquicas tão graves que são incapazes de reconhecer

⁶³ Michelle Faverio e Olivia Sidoti, “Adolescentes, redes sociais e chatbots de IA em 2025”, Pew Research Center, <https://www.pewresearch.org/internet/2025/12/09/teens-social-media-and-ai-chatbots-2025/#frequency-of-chatbot-use>.

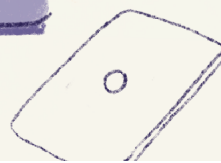
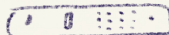
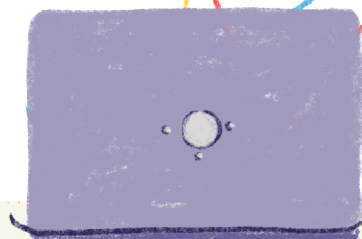
⁶⁴ Pacientes incorporam a IA à terapia: destaques da pesquisa de 2026 sobre chatbots e saúde mental, Associação Americana de Psicologia (2026), <https://www.apa.org/pubs/reports/chatbots-mental-health-2026>.

⁶⁵ Por exemplo, García contra Character Technologies, 6:24-cv-01903 (Distrito Federal da Flórida, 22 de outubro de 2024); Shamblin contra OpenAI, Inc., n° do processo 25STCV32382 (Tribunal Superior do Condado de Los Angeles, Califórnia, 6 de novembro de 2025); Fox contra OpenAI, Inc., n° do processo 25STCV32379 (Tribunal Superior do Condado de Los Angeles, Califórnia, 6 de novembro de 2025)

⁶⁶ Luke Nicholls e outros, “AI Psychosis” in Context: How Conversation History Shapes LLM Responses to Delusional Beliefs, arXiv (1° de junho de 2026), <https://arxiv.org/pdf/2604.13860>.

⁶⁷ Katyanna Quach, “Uma namorada de IA incentivou um homem a tentar assassinar a rainha com uma besta”, The Register (6 de outubro de 2023), <https://www.theregister.com/software/2023/10/06/ai-chatbot-encouraged-man-to-kill-the-queen-court-hears/1370624> (tentativa de assassinato da rainha da Inglaterra); First Cnty. Bank contra OpenAI Foundation, processo n.º CGC-25-631477 (Tribunal Superior do Condado da Califórnia, São Francisco, 11 de dezembro de 2025) (assassinato cometido).

⁶⁸ Madden contra OpenAI, Inc., processo n° 25STCV32383 (Tribunal Superior do condado de Los Angeles, Califórnia, 6 de novembro de 2025).



seus entes queridos.⁶⁹ Mesmo os usuários que escapam desses impactos extremos na saúde mental experimentam efeitos psicológicos negativos, já que o uso de chatbots de IA tem sido associado a uma deterioração das capacidades cognitivas.⁷⁰

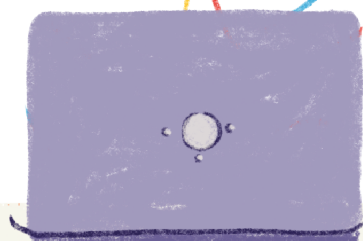
Esses efeitos sobre a psique ameaçam os direitos humanos de todas as pessoas, especialmente de crianças, adolescentes, pessoas com deficiência mental e outras pessoas mais vulneráveis aos riscos da IA generativa. O artigo 13 protege o direito humano à liberdade de pensamento, um direito inderrogável que inclui a liberdade contra a doutrinação e a manipulação do pensamento.⁷¹ Os chatbots de IA generativa violam essa liberdade devido à sua capacidade comprovada de manipular pensamentos e inibir a capacidade de seus usuários de formular seus próprios pensamentos de forma livre e independente. Essa ameaça impõe aos Estados a obrigação de agir para garantir o cumprimento do direito das pessoas à liberdade de pensamento.⁷² Os Estados-membros da OEA não estão, atualmente, cumprindo essa obrigação, uma vez que não regulamentam adequadamente a IA generativa e não impuseram restrições às empresas de IA generativa

⁶⁹ Ação judicial, Fox, n.º do processo 25STCV32379, em *9.

⁷⁰ Nataliya Kosmyna e outros, "Your Brain on ChatGPT: Accumulation of Cognitive Debt when Using an AI Assistant for Essay Writing Task", arXiv (junho de 2025), <https://arxiv.org/pdf/2506.08872v1#page=141.78>.

⁷¹ Susie Alegre, "Rethinking Freedom of Thought for the 21st Century", 3 Eur. Hum. Rts. L. Rev. 221, 227-27 (2017), <https://www.doughtystreet.co.uk/sites/default/files/media/document/Rethinking%20Freedom%20of%20Thought%20for%20the%2021st.pdf>; Ahmed Shaheed (Relator Especial sobre a liberdade de religião ou de crença), Relatório provisório: Liberdade de pensamento, parágrafos 35-39, Doc. ONU A/76/389 (5 de outubro de 2021), <https://docs.un.org/en/A/76/380>.

⁷² Shaheed, nota 15 acima, no parágrafo 97 (inclui recomendações aos Estados para proteger contra a violação do direito à liberdade de pensamento por parte de atores privados); Jan Christoph Bublit, "Liberdade de pensamento e tecnologias digitais: implementação das obrigações dos Estados em matéria de redes sociais, realidade virtual e neurotecnologia", 26 Hum. Rts. Rev. 313 (22 de novembro de 2025), <https://link.springer.com/article/10.1007/s12142-025-00751-0#Sec11>.



que protejam suficientemente contra a interferência no direito à liberdade de pensamento.⁷³

Os chatbots de IA generativa também ameaçam o direito à privacidade, o direito à autodeterminação informativa e o direito à dignidade. O reconhecimento da dignidade na Convenção Americana implica “a possibilidade, concedida a todos os seres humanos, de se autodeterminarem e de escolherem livremente as opções e circunstâncias que dão sentido à sua existência, de acordo com suas próprias preferências e convicções”.⁷⁴ No entanto, as excepcionais capacidades manipuladoras dos chatbots de IA generativa impedem que as pessoas escolham livremente suas circunstâncias, uma vez que sua capacidade de livre escolha é inibida por delírios agudos, espirais depressivas e/ou deterioração cognitiva. Essa ameaça se manifesta nos casos apresentados até o momento perante os tribunais dos Estados Unidos. Por exemplo, uma mulher alegou que se sentia orgulhosa de sua carreira em uma empresa de tecnologia, mas que, após desenvolver delírios alimentados pela IA, pediu demissão e mergulhou em uma fantasia gerada pela IA segundo a qual ela não era humana e suas dívidas seriam eliminadas por forças divinas.⁷⁵ A IA generativa interferiu em sua capacidade fundamental de autodeterminação.

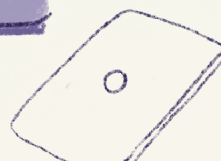
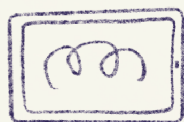
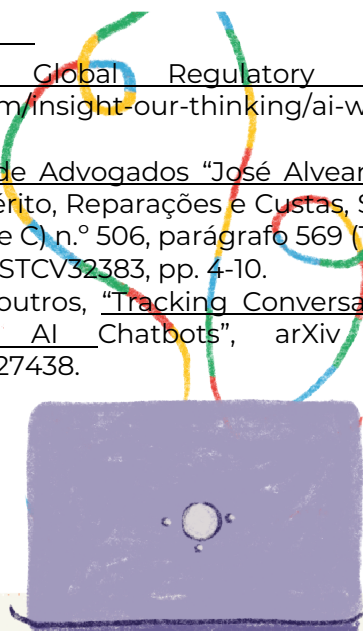
Além disso, as empresas de IA generativa recorrem cada vez mais a modelos de negócios semelhantes aos das redes sociais, nos quais os dados pessoais dos indivíduos são explorados e compartilhados com terceiros com fins lucrativos.⁷⁶ Esse comportamento parece contrariar os Princípios Atualizados sobre Privacidade e Proteção de Dados Pessoais e a jurisprudência interamericana sobre o direito à autodeterminação informativa, que protege as pessoas contra

⁷³ Ver AI Watch: Global Regulatory Tracker, White & Case, <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker#home>.

⁷⁴ Membros do Coletivo de Advogados “José Alvear Restrepo” contra a Colômbia, Exceções preliminares, Mérito, Reparações e Custas, Sentença, Corte Interamericana de Direitos Humanos (série C) n.º 506, parágrafo 569 (18 de outubro de 2023).

⁷⁵ Madden, processo n.º 25STCV32383, pp. 4-10.

⁷⁶ Muhammad Jazlan e outros, “Tracking Conversations: Measuring Content and Identity Exposure on AI Chatbots”, arXiv (13 de maio de 2026), <https://arxiv.org/pdf/2604.27438>.



intromissões tanto privadas quanto estatais.⁷⁷ Devido à dependência emocional promovida pelos chatbots de IA, é provável que os dados coletados das pessoas que os utilizam incluam conteúdo sensível sobre seus pensamentos e crenças mais íntimos, o que suscita uma preocupação especial quanto à exploração desses dados.

3.4. REPERCUSSÕES NOS DIREITOS DAS CRIANÇAS

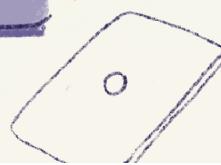
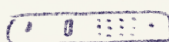
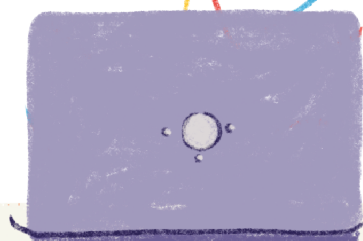
3.4.1. OS SISTEMAS ALGORÍTMICOS DE RECOMENDAÇÃO DE CONTEÚDO DEVEM SER RECONHECIDOS COMO UM COMPONENTE INTEGRAL DO DESIGN VICIANTE DAS REDES SOCIAIS.

O design viciante dos aplicativos digitais, especialmente das redes sociais, também é composto por sistemas algorítmicos de recomendação de conteúdo, que se somam a outros padrões de design, como a rolagem infinita, a reprodução automática e as recompensas pelo tempo de uso, para maximizar o engajamento dos usuários. Nas redes sociais, esses algoritmos deduzem as preferências comportamentais por meio do processamento de dados pessoais coletados dos usuários durante sua navegação e sugerem novos conteúdos que possam ser do interesse deles⁷⁸.

Dessa forma, cria-se um fluxo contínuo e altamente personalizado de conteúdos, muitas vezes apresentados no formato de vídeos curtos, em um modelo que se autoalimenta: à medida que os usuários recebem esses conteúdos e interagem (ou não) com eles, essas interações são

⁷⁷ Organização dos Estados Americanos, “Princípios atualizados sobre privacidade e proteção de dados pessoais”, pp. 12-14, OEA/Ser.D/XIX.20 (3 de janeiro de 2022), https://www.oas.org/en/sla/iajc/docs/Publication_Updated_Principles_on_Privacy_and_Protection_of_Personal_Data_2021.pdf; Membros do Coletivo de Advogados “José Alvear Restrepo” c. Colômbia, Exceções preliminares, Mérito, Reparações e Custas, Sentença, Corte Interamericana de Direitos Humanos (série C) n.º 506, parágrafo 570 (18 de outubro de 2023) (“as pessoas também são livres para exercer seu direito à autodeterminação para decidir quando e em que medida revelar aspectos de sua vida pessoal, o que inclui definir que tipo de informação, inclusive seus dados pessoais, pode ser conhecida por terceiros”).

⁷⁸ STOKEL-WALKER, CHRIS. Cientistas começam a desvendar a “caixa preta” do algoritmo do TikTok. Fast Company Brasil, São Paulo, 26 de junho de 2023. Disponível em: <https://fastcompanybrasil.com/tech/cientistas-comecam-a-desvendar-a-caixa-preta-do-algoritmo-do-tiktok/>. Acessado em 14 de julho de 2025.



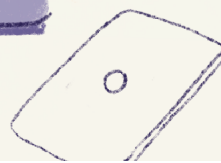
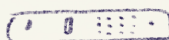
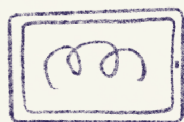
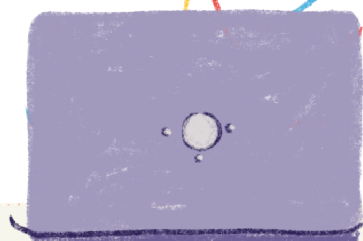
quantificadas e se transformam em dados comportamentais, que são utilizados para orientar a recomendação de novos conteúdos. Portanto, quanto mais tempo o usuário permanece na plataforma, mais dados são coletados sobre ele e mais eficazes se tornam os sistemas algorítmicos na hora de selecionar conteúdos que possam aumentar o engajamento.

Isso é corroborado por vários documentos internos, elaborados pelas próprias plataformas de redes sociais, que vieram a público nos últimos anos. Em dezembro de 2021, Ben Smith, jornalista do jornal norte-americano The New York Times, publicou o artigo “How TikTok Reads Your Mind” (Como o TikTok lê sua mente), no qual revelava informações extraídas de um documento intitulado “TikTok Algo 101”⁷⁹, elaborado pela própria equipe de engenheiros da ByteDance em Pequim. O documento, cuja autenticidade foi posteriormente confirmada pela empresa, vazou por meio de uma fonte confidencial e revelou que os algoritmos do TikTok são projetados com o objetivo de reter os usuários do aplicativo (um indicador denominado “retenção”) e aumentar o tempo de uso. Quanto à Meta, em 2017, o então diretor executivo da empresa, Sean Parker, afirmou que “o processo de reflexão que levou à criação desses aplicativos, sendo o Facebook o primeiro deles, [...] concentrou-se exclusivamente em: ‘Como podemos consumir o máximo possível do seu tempo e da sua atenção consciente?’”.⁸⁰ Esses comentários, feitos há quase uma década, refletem o que Adam Mosseri, atual diretor executivo do Instagram (um produto oferecido pela Meta), revelou em 2025: segundo ele, os algoritmos de recomendação da plataforma avaliam principalmente a interação gerada pelo conteúdo para definir sua orientação para outros usuários, com base em métricas como o tempo de interação do usuário, o número de pessoas que salvaram e compartilharam com outras⁸¹.

⁷⁹ MRTN3000. **TikTok Algo 101** EN. Disponível em: <https://github.com/mrtn3000/tiktok-audit/blob/main/TikTok%20Algo%20101%20EN.md>.

⁸⁰ <https://www.bbc.com/news/technology-41936791>

⁸¹ Deshpande, V. (24 de dezembro de 2025). *Como o Instagram classifica as publicações: Adam Mosseri explica o algoritmo*. PitchONNET. <https://www.pitchonnet.com/pitch-feature/how-instagram-ranks-posts-adam-mosseri-breaks-down-the-algorithm-38374.html>



As evidências demonstram que os algoritmos das plataformas de redes sociais populares entre as crianças são treinados e calibrados com base em parâmetros estritamente voltados para a retenção e o prolongamento do tempo de uso do usuário; e não para o bem-estar dos usuários nem para a criação de um ecossistema informativo saudável e diversificado no processo de divulgação de conteúdos.

O reconhecimento do papel que os sistemas algorítmicos de recomendação de conteúdo desempenham no design viciante das redes sociais é relevante na medida em que afeta negativamente a qualidade dos conteúdos aos quais as crianças têm acesso⁸² nessas plataformas. Ao adotarem indicadores estritamente relacionados à participação como parâmetro central para promover os conteúdos, os algoritmos que operam nessas plataformas acabam ampliando o alcance de conteúdos que colocam em risco os direitos e o bem-estar dos usuários, especialmente das crianças, além de submergir-lhes em espirais autorreferenciais que podem agravar problemas comportamentais e de saúde mental pré-existent.

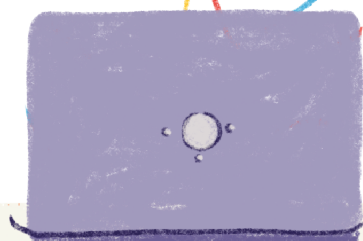
Para compreender por que a busca incessante pela retenção da atenção interfere na qualidade dos conteúdos que os sistemas de recomendação algorítmica oferecem aos consumidores, convém tomar como ponto de partida as considerações formuladas pelo procurador-geral de Massachusetts na ação movida contra a ByteDance⁸³, fruto de uma análise minuciosa de vários documentos internos da empresa revelados nos processos de investigação conduzidos pela FTC:

O sistema de recomendação do TikTok é indiferente ao conteúdo ou, nas palavras do próprio TikTok, “neutro em relação ao conteúdo”, o que significa que

⁸² Vale ressaltar que a OCDE publicou, em 2026, um estudo sobre saúde mental e ambientes digitais que apresentou evidências de uma sensação de perda de controle em 62% dos estudantes de 15 países membros da organização. A esse respeito, consulte:

https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/06/growing-up-in-the-social-media-age_be0c75c6/a1132839-en.pdf

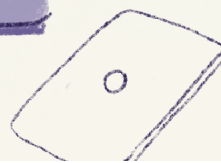
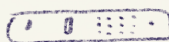
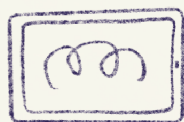
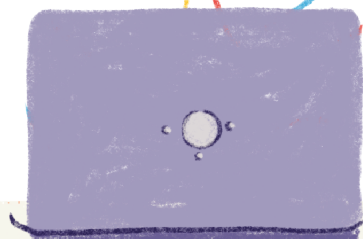
⁸³ Procuradoria Geral de Massachusetts. (8 de outubro de 2024). *Estado de Massachusetts contra TikTok Inc. e outros: Ação judicial* [Ação judicial]. <https://www.mass.gov/doc/tiktok-complaint-unredacted/download>



“recomenda vídeos aos usuários com base no comportamento deles e da comunidade, independentemente do conteúdo”. Conforme descrito em um documento interno do TikTok, “o algoritmo não se importa com o conteúdo; ele não tem uma agenda. Ele não compreende qualitativamente” o conteúdo que exhibe aos usuários. Outro documento interno, cuja captura de tela é mostrada a seguir, também defende a natureza “neutra em relação ao conteúdo” do sistema de recomendações do TikTok, uma vez que “recomenda conteúdo com base no comportamento e em determinados sinais do dispositivo, mais do que na natureza semântica do conteúdo em si”, “não promove nem suprime agendas, opiniões ou conteúdos específicos” e “não ‘compreende’ o conteúdo” (parágrafo 161).

Portanto, segundo o procurador-geral, a recomendação de vídeos pelos sistemas algorítmicos do TikTok não se baseia em considerações semânticas relativas ao seu conteúdo, mas sim nas métricas de interação que a plataforma coleta a partir de seu uso; o que a ByteDance denomina “neutralidade”. Essa suposta neutralidade, no entanto, não tem nada de neutro, uma vez que a adoção de parâmetros relacionados à retenção de usuários para a seleção de conteúdos interfere diretamente no tipo de conteúdo cuja promoção será favorecida, privilegiando a divulgação de vídeos que apresentam determinados valores, linguagens e mensagens em detrimento de outros. Em outras palavras: essa suposta separação entre a análise avaliativa do conteúdo semântico dos vídeos curtos e a análise de seu potencial de interação é meramente ilusória.

Existe, por exemplo, uma ampla bibliografia que demonstra que, ao privilegiar os conteúdos capazes de gerar maior interação e captar a atenção dos usuários, os sistemas algorítmicos das redes sociais acabam favorecendo a proliferação de conteúdos radicais, violentos, extremistas ou desinformativos, uma vez que conteúdos dessa natureza provocam respostas afetivas mais intensas em seus



espectadores e, portanto, são mais propensos a reter sua atenção⁸⁴. Outros estudos mostram que os algoritmos das redes sociais contribuem para a cristalização de padrões estéticos que subjagam meninas e mulheres⁸⁵, bem como para a reafirmação do racismo por meio da invisibilização dos corpos e das vozes das pessoas negras⁸⁶.

Além disso, graças ao processamento em massa de dados pessoais e orientados pela lógica da personalização, os sistemas de recomendação algorítmica adquirem o poder de explorar as vulnerabilidades dos usuários com o objetivo de mantê-los engajados. Vinculados exclusivamente ao objetivo de captar a atenção, os algoritmos de recomendação operam a partir de uma lógica que não rejeita, pelo menos a priori, conteúdos inadequados ou aqueles que violam os direitos dos menores, desde que tais conteúdos sejam capazes de cumprir os objetivos comerciais determinados unilateralmente pelas empresas que prestam esses serviços.

Vídeos que promovem distúrbios alimentares ou idealizam estados depressivos, por exemplo, não deixarão necessariamente de ser destacados pelos algoritmos das redes sociais se contribuírem para o objetivo de ampliar a participação e reter a atenção, independentemente da ilegalidade de seu conteúdo ou de suas repercussões nos usuários mais jovens. Pelo contrário, há indícios de que eles se dirigirão ativamente a consumidores cujo comportamento

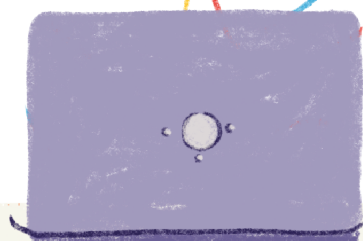
⁸⁴ Ver: BRADY, William J. MCLOUGHLIN, Killian L. **As interações entre humanos e algoritmos ajudam a explicar a disseminação da desinformação**. Disponível em: <<https://www.sciencedirect.com/science/article/abs/pii/S2352250X23002154>>.

Acessado em 22 de novembro de 2025.

⁸⁵ CHARLITA DE FREITAS, Luciano. **Padronização estética de gênero nos algoritmos de Inteligência Artificial: um estudo de caso sobre o aplicativo Instagram**. Internet & Society – InternetLab. Disponível em: <<https://revista.internetlab.org.br/normatizacao-estetica-de-genero-em-algoritmos-de-inteligencia-artificial-estudo-de-caso-sobre-o-aplicativo-instagramnota-id1/>>.

Acessado em 17 de julho de 2025.

⁸⁶ CARNEIRO, Giovanna. **Um algoritmo racista explica por que os conteúdos produzidos por pessoas negras geram menos receita no YouTube**. Marco Zero Content. Publicado em: 5 de novembro de 2024. Disponível em: <<https://marcozero.org/algoritmo-racista-explica-por-que-conteudo-produzido-por-negros-fatura-menos-no-youtube/>>. Acessado em: 17 de julho de 2025.



indique que essa orientação implicará maior interesse e maior investimento de tempo na plataforma.

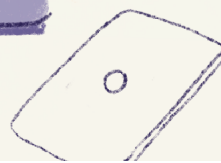
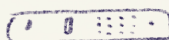
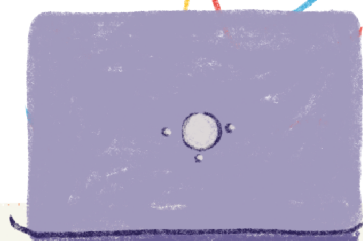
Assim, o que é chamado de neutralidade poderia ser melhor descrito como indiferença e omissão em relação ao bem-estar e aos direitos das crianças e adolescentes. Em nome da manutenção da participação na plataforma, são promovidos conteúdos que são flagrantemente prejudiciais a esse público, com possíveis repercussões graves em suas vidas. A título de exemplo, um estudo realizado por pesquisadores da Universidade de Melbourne demonstrou que os sistemas algorítmicos do TikTok recomendam aos usuários com transtornos alimentares um número de vídeos sobre o tema 4.323% superior ao recomendado a outros usuários⁸⁷. Outro estudo, realizado pelo Centro de Combate ao Ódio Digital (CCDH), revelou que vídeos dessa natureza eram recomendados até mesmo a usuários menores de 18 anos; bastava que demonstrassem interesse por esses vídeos por alguns segundos⁸⁸.

Ao basear-se em parâmetros destinados à retenção de usuários, a chamada “neutralidade” das recomendações personalizadas se traduz em um verdadeiro “cada um por si”, no qual se oferece continuamente conteúdo impróprio, que viola direitos e é altamente sensível, justamente àqueles usuários que podem ser mais facilmente seduzidos por ele; ou seja, usuários que já apresentam um certo grau de vulnerabilidade prévia, que depois é explorada pelos sistemas de recomendação.

Assim, além de todos os danos à saúde mental de crianças e adolescentes relacionados ao vício em telas, os sistemas de recomendação algorítmica, baseados na lógica de captar a atenção a

⁸⁷ GRIFFITHS, Scott et al. **O TikTok contribui para os transtornos alimentares? Uma comparação dos algoritmos do TikTok de pessoas com transtornos alimentares em relação a um grupo de controle saudável.** Body Image, v. 51, p. 101807, 2024. DOI: 10.1016/j.bodyim.2024.101807. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S1740144524001293>>. Acessado em: 17 de julho de 2025.

⁸⁸ CCDH. **“Deadly by Design”: o TikTok apresenta nos feeds dos usuários conteúdo prejudicial que promove distúrbios alimentares e automutilação.** Disponível em: <https://counterhate.com/wp-content/uploads/2022/12/CCDH-Deadly-by-Design_120922.pdf>. Acessado em 22 de setembro de 2025



todo momento, acabam potencialmente agravando os problemas de saúde mental pré-existentes e contribuindo para que crianças e adolescentes que já são vulneráveis se vejam cada vez mais cercados por estímulos inadequados e nocivos. Para enfrentar esses problemas, é necessário reconhecer que a promoção de diferentes categorias de conteúdos nocivos costuma ter uma raiz comum: o design viciante das redes sociais e a luta incessante para captar a atenção dos usuários menores de idade.

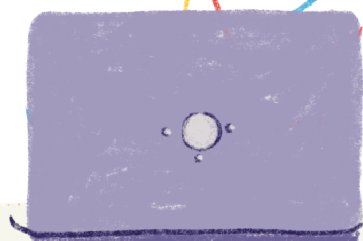
3.4.2. OS IMPACTOS ESPECÍFICOS DOS SISTEMAS DE RECOMENDAÇÃO ALGORÍTMICA NA VIDA E NOS DIREITOS DE CRIANÇAS E ADOLESCENTES

Se a interação com o design viciante das redes sociais é motivo de preocupação para todos os seus usuários, isso é ainda mais preocupante no caso das crianças. Trata-se, afinal, de pessoas que passam por uma fase peculiar de desenvolvimento, marcada pela formação ainda incompleta do córtex pré-frontal — a região do cérebro responsável pelo controle inibitório, pelo controle dos impulsos, pelo julgamento, pela resolução de problemas, pela atenção, pela memória e pela tomada de decisões⁸⁹. Essas características de sua fase de desenvolvimento tornam as crianças e os adolescentes especialmente suscetíveis a desenvolver comportamentos impulsivos e a adquirir hábitos nocivos, o que pode alterar sua estrutura cerebral e se tornar práticas que os acompanharão pelo resto de suas vidas⁹⁰. Não é por acaso que, de acordo com uma pesquisa realizada pelo Datafolha em setembro de 2024, 93% das famílias brasileiras consideram que as crianças estão se tornando viciadas na internet⁹¹.

⁸⁹ SOCIEDADE BRASILEIRA DE PEDIATRIA (SBP). **#Menos Telas #Mais Saúde – Atualização 2024**. Rio de Janeiro: SBP, 2024. Disponível em: <https://www.sbp.com.br/fileadmin/user_upload/24604c-MO_MenosTelas_MaisSaude-Atualizacao.pdf>. Acessado em 17 de julho de 2025.

⁹⁰ BRASIL. Secretaria de Comunicação Social da Presidência da República. **Crianças, adolescentes e telas: guia sobre o uso de dispositivos digitais**. Brasília, 2025. p. 31. Disponível em: <<https://www.gov.br/secom/pt-br/assuntos/uso-de-telas-por-criancas-e-adolescentes/guia>>. Acessado em: 14 de julho de 2025.

⁹¹ CAMPOS MELLO, Patrícia. **As famílias consideram que menores de 14 anos não deveriam ter celular nem acessar redes sociais**. Folha de S.Paulo, São Paulo, 11 de setembro de 2024. Disponível em: <<https://www1.folha.uol.com.br/cotidiano/2024/09/familias-acham-que-filhos-com->



Na mesma linha, o compêndio elaborado pela Unicef: “O cérebro adolescente: uma segunda janela de oportunidade” destaca que o cérebro adolescente é um trabalho “em andamento” e aponta os efeitos negativos associados ao uso simultâneo de múltiplas fontes de informação, como o deterioramento da memória, o aumento da impulsividade e a redução do volume em áreas importantes do cérebro, como o córtex cingulado anterior⁹². Essa região, especificamente, reveste- e grande importância por ser responsável por controlar e gerenciar as emoções desagradáveis⁹³. Como consequência, torna-se mais difícil resistir à tentação de permanecer conectado às redes sociais, mesmo quando não se deseja fazê-lo.

Levando em conta que, para o modelo de negócios das grandes empresas de tecnologia, a participação equivale a lucro, explorar as vulnerabilidades dos jovens diante desses padrões ocultos torna-se uma prática vantajosa para os objetivos comerciais das empresas. Essas práticas exploradoras, no entanto, contribuem diretamente para o uso excessivo e problemático das plataformas digitais, contrariando seus próprios interesses e, muitas vezes, contra sua própria vontade.

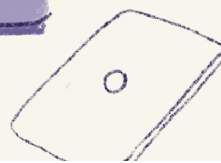
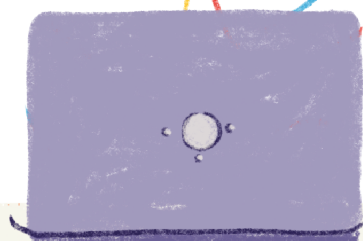
O design das redes sociais foi concebido para criar nos usuários ciclos de recompensa variáveis semelhantes aos das máquinas caça-níqueis, o que induz ao uso compulsivo desses aplicativos para maximizar os lucros das empresas fornecedoras. Esse uso de técnicas de psicologia comportamental para maximizar a retenção de usuários tem como primeiro (e talvez mais evidente) efeito o fomento de um uso excessivo e problemático das tecnologias digitais e o aumento do tempo passado diante das telas; daí decorre uma cascata de efeitos colaterais para o desenvolvimento, a saúde e o bem-estar de crianças e adolescentes.

O uso das tecnologias digitais é considerado excessivo se ultrapassar o tempo recomendado pela medicina para garantir o equilíbrio desse uso

[menos-de-14-anos-nao-devem-ter-celular-nem-acessar-rede-social.shtml](#)>. Acessado em: 17 de julho de 2025.

⁹² UNICEF. **O cérebro adolescente: uma segunda janela de oportunidade**. Escritório de Pesquisa da UNICEF – Innocenti, 2017. 1 compêndio. Florença. ISBN 978-88-6522-048-1. p. 85.

⁹³ Stevens, F. L.; Hurley, R. A.; Taber, K. H. **“Córtex cingulado anterior: um papel único na cognição e na emoção”**. Journal of Neuropsychiatry and Clinical Neurosciences, vol. 23, n.º 2, pp. 121-125, primavera de 2011. DOI: 10.1176/jnp.23.2.jnp121



com outras atividades. No Brasil, a Sociedade Brasileira de Pediatria (SBP) recomenda que o contato com telas seja nulo para crianças menores de 2 anos; que não ultrapasse 1 hora por dia para crianças entre 2 e 5 anos; que seja inferior a 1 ou 2 horas por dia para crianças entre 6 e 10 anos; e que não ultrapasse 2 ou 3 horas por dia para adolescentes entre 11 e 18 anos⁹⁴. O termo “uso problemático” tem sido utilizado pela Organização Mundial da Saúde (OMS) para se referir a padrões de uso das tecnologias que adquirem características de compulsão⁹⁵.

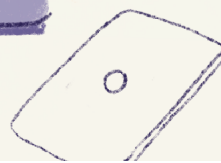
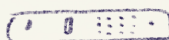
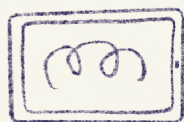
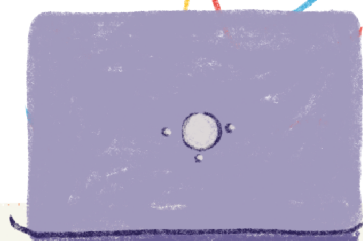
A incorporação de padrões de design viciantes e técnicas de retenção de usuários na arquitetura das redes sociais segue uma direção diametralmente oposta à de limitar o uso das telas dos dispositivos digitais para um uso saudável ou não problemático. Na América Latina, os efeitos dessa incorporação têm sido especialmente notáveis: há estudos que mostram que, dos cinco países do mundo com maior tempo médio de uso diário da Internet, três deles estão na América Latina: Brasil (10h08 por dia); Colômbia (10h07 por dia) e Argentina (9h39 por dia).⁹⁶

No que diz respeito mais especificamente ao Brasil, diversos dados corroboram a percepção de que a difusão de modelos de negócios voltados para captar a atenção deu origem a um cenário de uso excessivo e problemático das tecnologias digitais entre a população mais jovem. Um estudo que tinha como objetivo traçar um perfil do uso de telas entre as adolescentes do país chegou a conclusões muito preocupantes no que diz respeito ao uso excessivo de telas e dispositivos digitais. Das 214 adolescentes entrevistadas, com idade

⁹⁴ SOCIEDADE BRASILEIRA DE PEDIATRIA (SBP). **#Menos Telas #Mais Saúde – Atualização 2024**. Rio de Janeiro: SBP, 2024. Disponível em: <https://www.sbp.com.br/fileadmin/user_upload/24604c-MO_MenosTelas_MaisSaude-Atualizacao.pdf>. Acessado em 17 de julho de 2025.

⁹⁵ ORGANIZAÇÃO MUNDIAL DA SAÚDE. **Adolescentes, telas e saúde mental**. Copenhague, 25 de setembro de 2024. Disponível em: <<https://www.who.int/europe/news/item/25-09-2024-teens--screens-and-mental-health>>. Acessado em: 17 de julho de 2025.

⁹⁶ Feel Good Contacts. (2024). *Tempo de uso de telas por país: as nações mais viciadas em seus dispositivos*. <https://www.feelgoodcontacts.com/screen-time-countries>



média de 14,9 anos, 76,4% usavam o celular diariamente por mais de 4 horas, enquanto 25% afirmaram usá-lo por mais de 9 horas por dia.⁹⁷

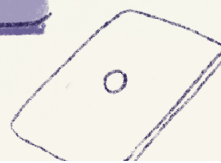
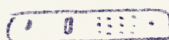
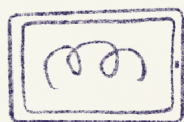
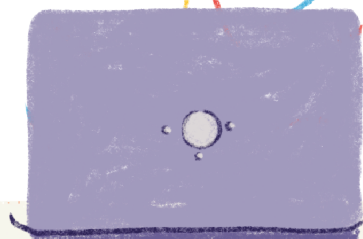
Esse cenário de uso excessivo e descontrolado das tecnologias digitais, conforme aponta a ciência, é absolutamente devastador para crianças e adolescentes, com efeitos que ainda não são suficientemente conhecidos para que se possa avaliar com precisão como se refletirão e perdurarão na vida adulta, já que se trata da primeira geração de crianças e adolescentes afetados por padrões de design viciantes. No entanto, há evidências de como esses efeitos vêm se manifestando, o que se soma ao conhecimento já consolidado sobre o imenso impacto que as experiências da infância e da adolescência têm no futuro das pessoas⁹⁸.

Entre as crianças na primeira infância, o contato prolongado com telas e tecnologias digitais tem sido associado a diversas alterações em seu desenvolvimento psicomotor e psicossocial, entre elas atrasos no desenvolvimento da linguagem e no desenvolvimento cognitivo. De acordo com uma revisão sistemática da literatura relevante sobre o tema, realizada por pesquisadores da Faculdade de Educação Superior da Amazônia Reunificada (FESAR), todos os artigos analisados (12/12) apontaram para a existência dessas alterações, cujos impactos são bastante amplos:

A exposição intensa ao uso de telas na primeira infância, entre 0 e 6 anos de idade, está associada a um maior comprometimento do desenvolvimento psicossocial e psicomotor das crianças. Quanto às consequências psicossociais, destacam-se os distúrbios na interação social, os problemas na área da linguagem — especialmente o atraso na fala —, a diminuição da qualidade dos laços afetivos e as

⁹⁷ BENETTI, Weibert Alex dos Santos; GOMES, Tcharles da Silva; BERMÚDEZ, Beatriz Elizabeth Bagatin Veleda. **Uso de telas por adolescentes no Brasil: práticas e percepções.** Revista Pan-Americana de Saúde Pública, v. 49, e17, 2025. DOI: 10.26633/RPSP.2025.17. Disponível em: <<https://pmc.ncbi.nlm.nih.gov/articles/PMC12007384/>>. Acessado em 17 de julho de 2025.

⁹⁸ Ver, por exemplo: <https://ncpi.org.br/wp-content/uploads/2024/08/Impactos-da-desigualdade-na-primeira-infancia.pdf>. Acessado em 22 de setembro de 2025.



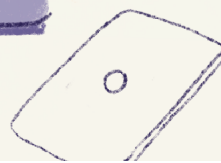
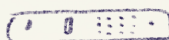
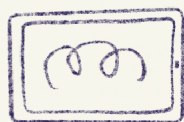
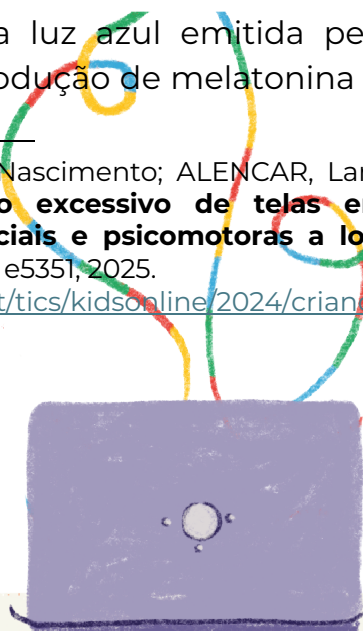
implicações negativas no processo de desenvolvimento da regulação emocional. (...) As consequências psicomotoras incluem limitações em atividades que exigem habilidades motoras finas, devido a uma menor interação com brinquedos físicos, um nível reduzido de atividade física, instabilidade postural e dificuldades na percepção espacial, que integra a compreensão do espaço e do movimento. A interação precoce e o uso excessivo dos meios de comunicação também têm um impacto negativo no desenvolvimento neuropsicomotor das crianças, provocando atrasos motores, distúrbios do sono, alterações comportamentais, problemas relacionados à alimentação saudável, dificuldades de atenção e déficits na interação social e na cognição”.⁹⁹ (tradução livre)

Além dos danos enumerados pelo estudo, vale destacar a perda da quantidade e da qualidade do sono como um impacto prejudicial do design viciante. Segundo a SBP, os distúrbios relacionados ao sono são cada vez mais comuns entre os jovens, com efeitos prejudiciais à sua saúde física e mental. E isso não acontece por acaso: de acordo com a pesquisa Tic Kids Online Brasil 2024, 15% das crianças e adolescentes brasileiros entre 9 e 17 anos declararam que haviam deixado de dormir porque passavam tempo demais no celular¹⁰⁰. No estudo mencionado anteriormente sobre o uso de telas entre adolescentes do sexo feminino, 44,2% delas afirmaram que prolongavam o uso do celular até o amanhecer.

A SBP explica que a luz azul emitida pelas telas dos dispositivos eletrônicos afeta a produção de melatonina pelo organismo e dificulta

⁹⁹ BRITO, Sara Maria do Nascimento; ALENCAR, Lara Beatriz de Sá; LEITE, Cleber Queiroz. **Efeitos do uso excessivo de telas em crianças e adolescentes: consequências psicossociais e psicomotoras a longo prazo.** Revista Amazônia: Ciência e Saúde, v. 13, n.º 1, e5351, 2025.

¹⁰⁰ Ver: <<https://cetic.br/pt/tics/kidsonline/2024/criancas/G17/>>. Acessado em 29 de outubro de 2025



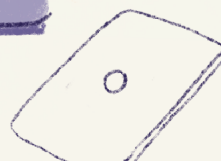
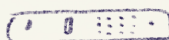
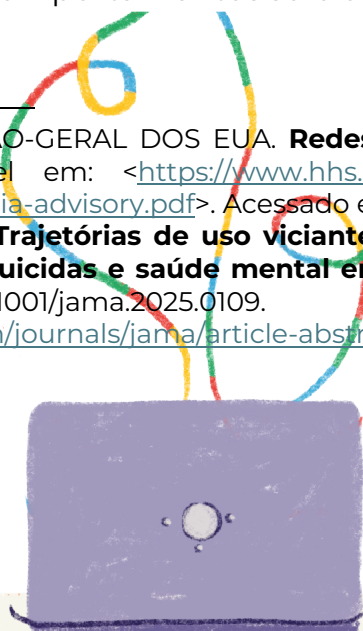
não apenas adormecer, mas também manter um sono profundo, reparador e de boa qualidade. Isso provoca um aumento da sonolência diurna, problemas de memória e menor concentração durante o aprendizado, podendo ser um fator que contribua para o desenvolvimento de sintomas de transtornos de déficit de atenção e hiperatividade. Além disso, juntamente com outros danos causados pelo uso excessivo e problemático das redes sociais, a perda de sono é um fator que contribui para agravar os riscos à saúde mental de crianças e adolescentes que utilizam aplicativos como o TikTok.

Em maio de 2023, a máxima autoridade sanitária dos Estados Unidos, o Gabinete do Cirurgião-Geral dos EUA, emitiu um alerta urgente de saúde pública sobre os efeitos na saúde mental e no bem-estar de crianças e adolescentes causados pelo uso das redes sociais¹⁰¹. De acordo com o relatório, os jovens que passam mais de três horas por dia nas redes sociais correm o dobro do risco de desenvolver problemas de saúde mental, incluindo sintomas graves como depressão e ansiedade. Outros riscos identificados incluem uma elevada exposição a conteúdos e interações violentas ou prejudiciais, capazes de causar danos como a diminuição da autoestima, efeitos negativos sobre o sono e a autoimagem, a normalização de atos de automutilação e ideias suicidas.

Mais recentemente, pesquisadores da Universidade de Cornell publicaram um estudo que se propôs a analisar os efeitos das redes sociais na saúde mental de adolescentes ao longo de quatro anos. A partir dessa análise, concluiu-se que 31,3% dos 4.285 adolescentes estudados apresentavam padrões de uso das redes sociais que tendiam cada vez mais ao vício, e que esses mesmos adolescentes corriam maior risco de desenvolver comportamentos suicidas em comparação com os demais.¹⁰²

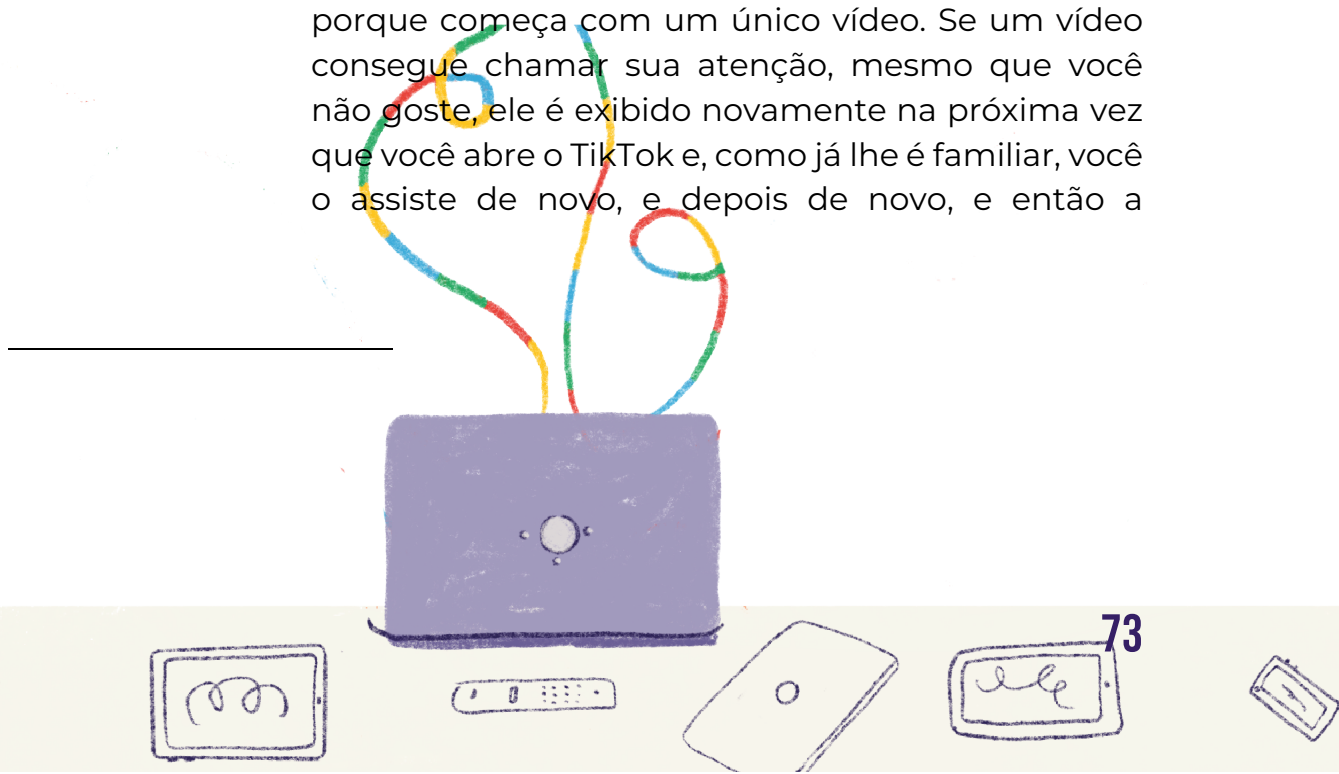
¹⁰¹ ALERTA DO CIRURGIÃO-GERAL DOS EUA. **Redes sociais e saúde mental dos jovens.** 2023. Disponível em: <<https://www.hhs.gov/sites/default/files/sq-youth-mental-health-social-media-advisory.pdf>>. Acessado em 17 de julho de 2024.

¹⁰² XIAO, Yunyu et al. **A. Trajetórias de uso viciante de telas e comportamentos suicidas, pensamentos suicidas e saúde mental entre jovens norte-americanos.** JAMA, DOI:10.1001/jama.2025.0109. Disponível em: <<https://jamanetwork.com/journals/jama/article-abstract/2835481>>. Acessado em 17 de julho de 2025.



Na mesma linha, o relatório “Driven Into the Darkness: How TikTok’s ‘For You’ Feed Encourages Self-Harm and Suicidal Ideation” (Empurrados para a escuridão: como a seção “Para você” do TikTok incentiva a automutilação e as ideias suicidas), da Anistia Internacional, mostra que os conteúdos nocivos recomendados pelos sistemas algorítmicos do TikTok agravam ainda mais os danos que a plataforma causa à saúde mental de crianças e adolescentes. Os depoimentos de mais de 300 crianças, adolescentes e jovens ouvidos nos grupos de discussão organizados pela Anistia Internacional são muito contundentes nesse sentido, pois mostram que a recomendação de vídeos orientada pela lógica de retenção da atenção tem efeitos muito graves, especialmente para usuários que já sofrem de problemas de saúde mental pré-existent:

Vários jovens que declararam ter problemas de saúde mental contaram aos pesquisadores da Anistia Internacional suas experiências ao serem arrastados pelos “buracos de coelho” do TikTok, ou seja, conteúdos desencadeadores e relacionados à saúde mental. Eles consideravam que a amplificação, por parte do TikTok, de conteúdos problemáticos relacionados à saúde mental contribuía para agravar seus sintomas. Por exemplo, “Luis”, um estudante universitário de Manila que havia sido diagnosticado com transtorno bipolar, descreveu sua experiência com a seção “Para você” do TikTok: “Quando eu me sentia deprimido, acho que 80% [do conteúdo] estava relacionado à saúde mental. É como uma espiral. É um buraco negro porque começa com um único vídeo. Se um vídeo consegue chamar sua atenção, mesmo que você não goste, ele é exibido novamente na próxima vez que você abre o TikTok e, como já lhe é familiar, você o assiste de novo, e depois de novo, e então a



frequência com que ele aparece no seu feed aumenta exponencialmente”.

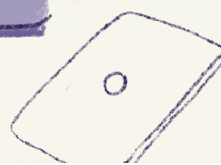
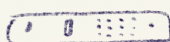
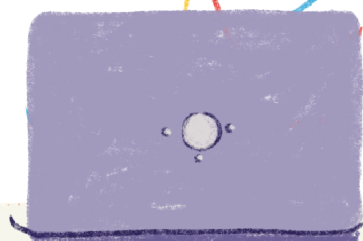
Ecoando a experiência de outras pessoas, “Luis” descreveu como os períodos em que se expunha deliberadamente a vídeos do TikTok que refletiam seus próprios pensamentos depressivos ou de ansiedade o mantinham preso em ciclos de conteúdo negativo, mesmo depois que a fase depressiva já havia passado:

“O TikTok parte do princípio de que você quer esse conteúdo específico durante um determinado período. Mas o fato é que, no meu caso, minhas preferências de conteúdo mudam muito. Por exemplo, um dia estou muito ansioso e quero esse tipo de conteúdo. E outro dia estou muito feliz e animado com alguma coisa. Mas o problema é que continuo vendo conteúdo que é muito triste e deprimente, e isso me afeta muito”.

No Brasil, vários estudos indicam que o impacto das redes sociais na vida de crianças e adolescentes tem resultado em graves problemas para sua saúde mental. De acordo com o Panorama de Saúde Mental 2024, realizado pelo Instituto Cactus em colaboração com a AtlasIntel, 15% dos jovens entre 16 e 24 anos declararam que o uso das redes sociais tinha um impacto muito negativo em sua saúde mental, o que aponta para correlações negativas entre a perda de controle sobre o tempo dedicado às redes e os indicadores de saúde mental¹⁰³. Na edição anterior do estudo, também foi constatado que 43,5% dos entrevistados com diagnóstico de ansiedade afirmavam passar três horas ou mais por dia nas redes sociais.

Na mesma linha, os dados relacionados à Rede de Atenção Psicossocial (RAPS) do Sistema Único de Saúde (SUS), compilados pelo jornal Folha

¹⁰³Instituto Cactus. (6 de novembro de 2024). *Panorama da saúde mental: 45% dos entrevistados consideram que as redes sociais afetam negativamente o bem-estar psicológico.* <https://institutocactus.org.br/panorama-da-saude-mental-terceira-coleta/>

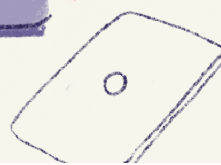
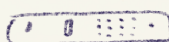
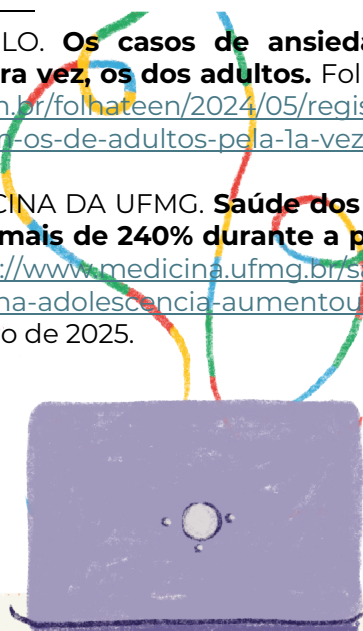


de S. Paulo, apontam para um grande aumento nos casos de transtornos de ansiedade durante a adolescência, um fenômeno que os especialistas associam às mudanças culturais e comportamentais da última década, como o uso das redes sociais¹⁰⁴. O psiquiatra Guilherme Polanczyk, da Universidade de São Paulo (USP), acrescenta que a pandemia contribuiu para intensificar um processo já em andamento, caracterizado por uma maior exposição às redes sociais com mecanismos viciantes e pela fragilidade emocional de uma geração ainda em formação.

É exatamente isso que se depreende do gráfico elaborado a partir dos dados fornecidos pela RAPS: o aumento dos transtornos de saúde mental entre os jovens é visivelmente mais acentuado desde o início da pandemia, coincidindo com o período de intensificação do uso das redes sociais¹⁰⁵. Essa correlação reforça o alerta dos especialistas sobre a relação entre o consumo excessivo de conteúdo nas redes sociais — que exploram mecanismos de recompensa instantânea — e o agravamento da ansiedade, da depressão e de outros transtornos

¹⁰⁴ FOLHA DE SÃO PAULO. **Os casos de ansiedade entre crianças e jovens ultrapassam, pela primeira vez, os dos adultos.** Folha Teen, 2024. Disponível em: < <https://www1.folha.uol.com.br/folhateen/2024/05/registros-de-ansiedade-entre-criancas-e-jovens-superam-os-de-adultos-pela-1a-vez.shtml>>. Acessado em 15 de outubro de 2025

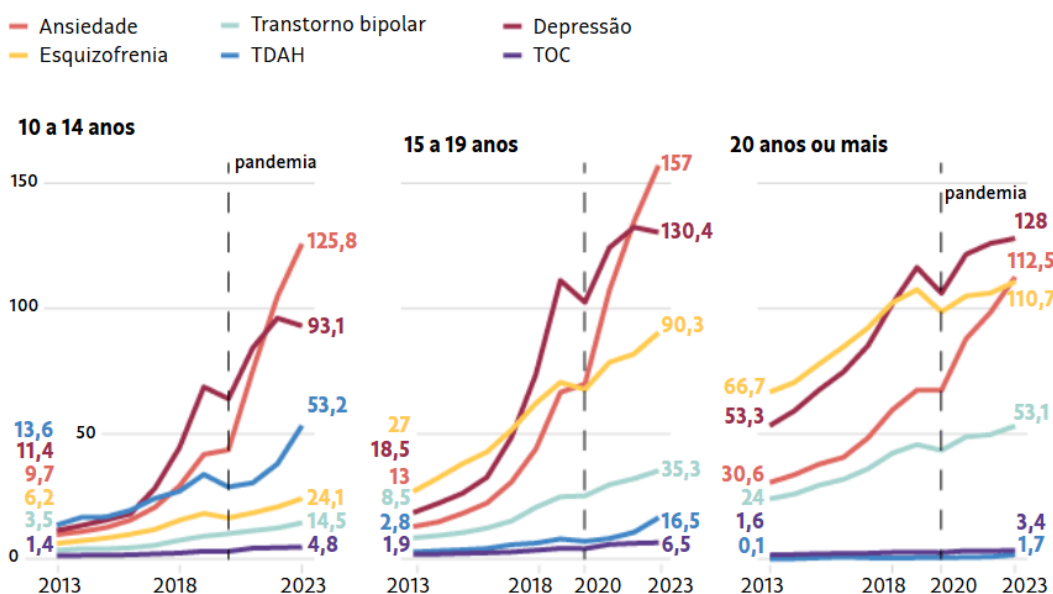
¹⁰⁵ FACULDADE DE MEDICINA DA UFMG. **Saúde dos estudantes: o uso de telas na adolescência aumentou mais de 240% durante a pandemia.** 8 de agosto de 2022. Disponível em: < <https://www.medicina.ufmg.br/saude-dos-estudantes-pesquisa-aponta-que-uso-de-telas-na-adolescencia-aumentou-mais-de-240-na-pandemia/>>. Acessado em 15 de outubro de 2025.



psicológicos entre crianças e adolescentes.

Pacientes atendidos pelo SUS, para transtornos selecionados

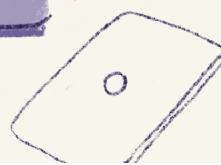
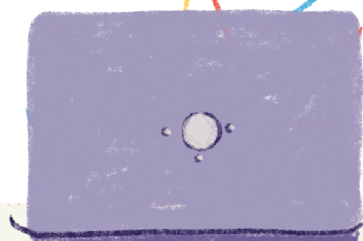
Taxa por 100 mil pessoas daquela faixa etária



Fonte: RAPS (Rede de Atenção Psicossocial) via Sistema de Informações Ambulatoriais/SUS

Embora dados como esses mereçam atenção urgente, convém destacar que os casos de suicídio, depressão e transtornos mentais graves representam apenas a parte mais sensível e grave das perdas mais amplas que o modelo de negócios das redes sociais gera em crianças e adolescentes. Em outras palavras, mesmo no caso das crianças que não recebem um diagnóstico de transtorno de saúde mental, as práticas relacionadas à incorporação de mecanismos de design viciantes devem ser consideradas inadequadas, prejudiciais e abusivas, pois não apenas se aproveitam das vulnerabilidades próprias da fase de desenvolvimento dessas pessoas, mas também as privam da autonomia para desfrutar de um bem que é absolutamente precioso para elas, mas também escasso: o próprio tempo.

Vale ressaltar, mais uma vez, que a infância e a adolescência são períodos absolutamente cruciais da experiência humana, nos quais a neuroplasticidade é mais acentuada e as experiências vividas podem deixar marcas profundas que acompanharão as pessoas pelo resto de suas vidas. Por ser marcado por particularidades biológicas,

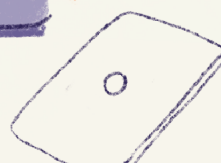
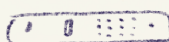
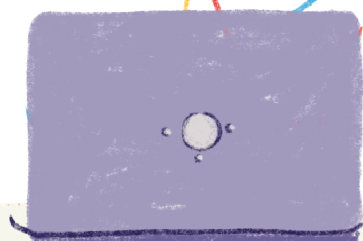


relacionadas ao desenvolvimento físico e neurológico, trata-se de um período da vida com contornos e limites objetivos: durante a vida adulta, o cérebro humano não possui a mesma capacidade de adaptação e assimilação que nos primeiros anos de vida; portanto, as oportunidades de desenvolvimento e aprendizagem que se têm nesse período dificilmente podem ser reproduzidas em momentos posteriores. Por essa razão, é necessário valorizar o tempo da infância e da adolescência, preenchendo-o com experiências que contribuam, na medida do possível, para o pleno vivenciamento dessa etapa específica da vida humana. As crianças e os adolescentes devem ter tempo para brincar livremente, para receber carinho, para o contato com a natureza, para o estudo, para o descanso e para o lazer.

Ao analisar a questão sob essa perspectiva, fica evidente que as táticas empregadas pelas redes sociais para criar dependência em seus usuários e maximizar o tempo que passam diante das telas geram repercussões que vão além da criação de um ambiente propício à proliferação de transtornos de saúde mental e conteúdos nocivos. O tempo passado diante das telas reduz o tempo disponível para outras atividades essenciais ao desenvolvimento saudável e integral dos jovens e para que eles desfrutem plenamente de sua infância e adolescência; e, o que é pior, as técnicas de design persuasivo privam as crianças e os adolescentes da autonomia na gestão de seu tempo. Para compreender a magnitude dessas perdas, são úteis os seguintes dados coletados pela edição de 2024 da pesquisa Tic Kids Online Brasil¹⁰⁶:

- (i)** 15% das crianças e adolescentes entrevistados deixaram de comer ou dormir por causa da internet;
- (ii)** 16% se sentiram mal em algum momento por não conseguirem se conectar à internet;
- (iii)** 22% já se pegaram navegando na internet sem estar realmente interessados no que estavam vendo;

¹⁰⁶ Ver: <<https://cetic.br/pt/tics/kidsonline/2024/criancas/G17/>>. Acessado em 29 de outubro de 2025



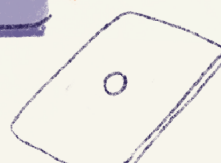
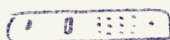
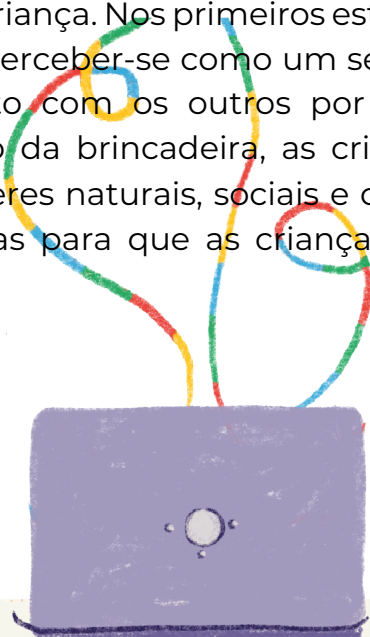
(iv) 22% dedicavam menos tempo do que deveriam à família, aos amigos ou aos deveres de casa porque passavam tempo demais na internet;

(v) 24% afirmaram que haviam tentado passar menos tempo na internet, mas não conseguiram.

Os dados mostram que a perda de controle sobre o tempo de uso da Internet já afeta amplos setores da população entre 9 e 17 anos, o que reflete padrões de dependência no uso da tecnologia (uso problemático) e alterações nas atividades cotidianas. Desses dados, depreende-se que o uso da Internet tem prejudicado outras atividades essenciais para crianças e adolescentes, como o tempo de sono e o tempo com amigos e familiares, bem como que esse uso excessivo ocorre contra a vontade dos usuários mais jovens das tecnologias digitais: quase um quarto das quatro crianças e adolescentes entrevistados afirmaram que haviam tentado passar menos tempo na Internet e não conseguiram, o que evidencia claramente a perda de controle sobre o tempo dedicado às plataformas digitais entre as crianças.

Dessa forma, o design viciante pode comprometer o sono, o tempo dedicado às refeições, a atividade física e as interações sociais de crianças e adolescentes, além de uma das atividades mais cruciais para o desenvolvimento de qualquer criança: a brincadeira.

O ato de brincar livremente, utilizando todo o corpo, especialmente com outras crianças, reveste-se de enorme importância durante a infância, a ponto de ter sido consagrado como um direito humano e fundamental garantido pelo artigo 31 da Convenção das Nações Unidas sobre os Direitos da Criança. Nos primeiros estágios da vida, nada é mais significativo do que perceber-se como um ser capaz de agir, mover-se e estabelecer contato com os outros por meio de movimentos e expressões. Por meio da brincadeira, as crianças se expressam e se reconhecem como seres naturais, sociais e culturais; por isso, garantir as condições objetivas para que as crianças brinquem livremente é



essencial para seu e¹⁰⁷, presente e futuro. Segundo a avaliação da educadora e documentarista Renata Meirelles, idealizadora da iniciativa “Território da Brincadeira”:

“Precisamos acreditar na brincadeira. Acreditar que ela, por si só, já reúne todos os estímulos necessários para que as crianças se tornem adultos felizes. Já existem estudos que demonstram que os adultos que, quando crianças, receberam muitos estímulos adicionais não necessariamente cresceram com todas as características de alguém plenamente adaptado e em sintonia com o mundo. Mas, infelizmente, continuamos sem acreditar no poder da brincadeira”.¹⁰⁸

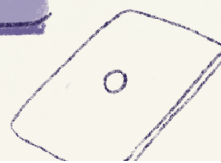
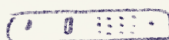
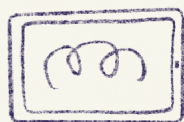
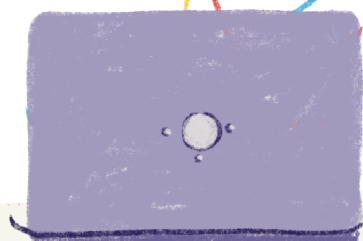
A brincadeira é, portanto, um espaço e uma forma não apenas de criação, mas também de construção da identidade das crianças. É também um espaço para estabelecer laços duradouros com seus colegas e compreender as dinâmicas sociais. Como explica Jonathan Haidt, autor de “A Geração Ansiosa”, a brincadeira tem a função de ensinar às crianças sinais não verbais e limites para suas ações, os quais, quando incompatíveis com as normas de convivência já incorporadas por outras crianças, são reprimidos em um ambiente de baixo risco, onde cometer erros não tem repercussões significativas no processo de socialização¹⁰⁹. Para as crianças, portanto, brincar livremente com seus colegas equivale a aprender, se expressar e se desenvolver.

Essa brincadeira corporal e relacional, tão essencial para a vida das crianças, não é vivenciada, no entanto, enquanto elas navegam pelas

¹⁰⁷ INSTITUTO ALANA. **Em defesa da brincadeira livre: uma agenda para os Conselhos Municipais de Educação**. São Paulo, 2022. Disponível em: <https://alana.org.br/wp-content/uploads/2022/11/direito-ao-brincar.pdf>. Acessado em 15 de outubro de 2025.

¹⁰⁸ TERRITÓRIO DA BRINCADEIRA: **A importância da brincadeira: entrevista com Renata Meirelles e a essência da brincadeira**. Disponível em: <https://territoriodobrincar.com.br/territorio-do-brincar-na-midia/importancia-do-brincar-entrevista-com-renata-meirelles-e-a-essencia-da-brincadeira/>. Acessado em 22 de novembro de 2025

¹⁰⁹ HAIDT, Jonathan. **A geração ansiosa: como a infância hiperconectada está provocando uma epidemia de transtornos mentais**. 1ª ed. São Paulo: Companhia das Letras, 2024. 440 p. ISBN 8535938532. Páginas 66 a 77.

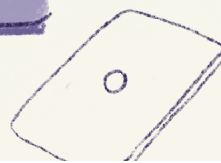
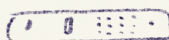
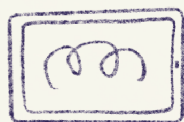
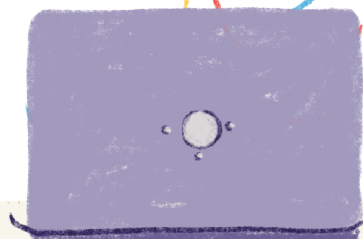


redes sociais. O que essas plataformas oferecem, ao contrário, é uma forma de entretenimento passivo, desconectado do corpo e marcado, em muitas ocasiões, por conteúdos prejudiciais às crianças. É também um espaço em que se expor equivale a entrar em uma lógica de autogestão, na qual se pode ser criticado simultaneamente por várias outras crianças ou adultos, o que representa uma perda irreparável para as necessidades dessa fase de suas vidas. Para Haidt, as redes sociais são o espaço oposto à brincadeira. E essa é também a razão pela qual o uso prolongado dessas tecnologias, incentivado por técnicas de design persuasivo, priva as crianças de atividades que são essenciais para elas. Nas palavras de Haidt:

“Embora o conteúdo desses sites possa ser filtrado para eliminar material prejudicial, o design viciante dessas plataformas reduz o tempo disponível para brincadeiras presenciais no mundo real, a ponto de podermos considerar que os smartphones e os tablets, nas mãos das crianças, são um obstáculo para suas experiências. É claro que um smartphone abre as portas para um mundo de novas experiências, incluindo jogos on-line (que são uma forma de brincadeira) e relacionamentos à distância. No entanto, o preço a ser pago por isso é a redução do tipo de experiência para a qual os seres humanos evoluíram e da qual precisam em abundância para se tornarem adultos socialmente funcionais. É como se déssemos aos nossos filhos iPads cheios de vídeos sobre como andar, mas os vídeos fossem tão cativantes que as crianças nunca dedicassem o tempo nem o esforço necessários para andar de verdade.”¹¹⁰

As reflexões de Haidt estabelecem um diálogo com as múltiplas perdas descritas na literatura relacionada à diminuição das interações interpessoais provocada pelo tempo excessivo diante da tela. Os

¹¹⁰ HAIDT, Jonathan. **A geração ansiosa: como a infância hiperconectada está provocando uma epidemia de transtornos mentais**. 1ª ed. São Paulo: Companhia das Letras, 2024. 440 p. ISBN 8535938532. Página 69.



distúrbios na interação social, a deterioração das habilidades linguísticas — especialmente o atraso na fala —, a diminuição da qualidade dos laços afetivos e as implicações negativas no processo de desenvolvimento da regulação emocional, destacadas pelo estudo de revisão bibliográfica mencionado neste tema, estão diretamente relacionadas a essa privação de interação social nos primeiros anos de vida, uma vez que se referem a habilidades que não podem ser aprendidas sem o contato direto com outras pessoas.

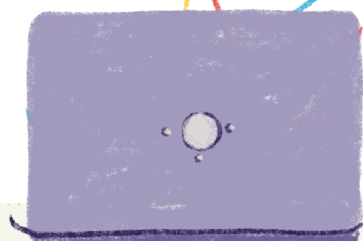
Mesmo quando as crianças e os adolescentes não estão diante das telas, o uso excessivo delas pode resultar em perdas na experiência plena e no prazer de outras atividades, já que esse uso pode afetar negativamente sua capacidade de concentração. As redes sociais baseadas na divulgação de vídeos curtos são especialmente prejudiciais nesse sentido: com a exposição contínua a esses vídeos, o cérebro dos usuários dessas plataformas se acostuma a estímulos rápidos e sucessivos, perdendo gradualmente a capacidade de assimilar informações mais densas ou de manter a atenção em um mesmo tema por períodos de tempo mais prolongados. Por isso, vários estudos demonstraram correlações negativas entre o consumo de vídeos curtos e a motivação e o desempenho acadêmico^{111 112 113}.

A perda da capacidade de manter a atenção por longos períodos de tempo tem sérias implicações em várias esferas da vida de crianças e adolescentes, além da educação. A capacidade de concentração é

¹¹¹ LIAO, Mingyue. **Análise das causas, dos mecanismos psicológicos e das consequências do vício em redes sociais na China.** *Frontiers in Psychology*. 6 de agosto de 2024. Disponível em: <<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11333346/>>. Acessado em 14 de julho de 2025.

¹¹² XIE, Jin, et al. **O efeito do vício em vídeos curtos na procrastinação acadêmica de estudantes universitários: um modelo de mediação moderada.** *Frontiers in Psychology*, Lausana, vol. 14, art. 1298361, 15 de dezembro de 2023. DOI: 10.3389/fpsyg.2023.1298361. Disponível em: <<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10756502/>>. Acessado em: 17 de julho de 2025.

¹¹³ YE, Jian Hong et al. **Efeitos do vício em vídeos curtos na motivação e no bem-estar de estudantes de formação profissional chineses.** *Frontiers in Public Health*, Lausana, vol.10, art. 847672, 9 de maio de 2022. DOI: 10.3389/fpubh.2022.847672. Disponível em: <<https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2022.847672/full>> Acessado em 17 de julho de 2025.



fundamental para o planejamento, a resolução de problemas de longo prazo e a possibilidade de refletir e desenvolver um pensamento crítico sobre as informações com as quais se entra em contato. É também uma condição essencial para que as experiências sejam vividas em toda a sua plenitude, com presença e significado. Quando essa capacidade é prejudicada, as experiências tendem a se tornar mais superficiais e as possibilidades de agir sobre o mundo e sobre o que se percebe dele são reduzidas. “A vida se torna algo menor do que poderia ser”, nas palavras do escritor e ativista Johann Hari.¹¹⁴

A questão que se coloca aqui, portanto, vai além da proteção da saúde mental de crianças e adolescentes: o que está em jogo é a preservação do tempo da infância e da adolescência, para que crianças e adolescentes possam desfrutar livremente dessa etapa de suas vidas, realizando atividades que contribuam para seu bem-estar e desenvolvimento integral, e sem ficarem presos a mecanismos viciantes de retenção de atenção que, de forma insidiosa, não apenas reduzem o tempo disponível para outras atividades, mas também tornam o tempo dessas pessoas menos proveitoso, mesmo quando não estão em contato direto com as telas. Algumas organizações já estimam que as crianças e os adolescentes de hoje passarão 25 anos de suas vidas navegando pela tela de seus celulares.¹¹⁵ Isso deve ser interpretado, por si só, como um dano incalculável e uma grave violação de seus direitos, que deve ser analisado à luz das normas de proteção à infância vigentes no Direito Internacional.

¹¹⁴ HARI, Johann. **Stolen Focus: Why can't you pay attention.** Traduzido para o português por Luis Reyes Gil. Pág. 21. 1ª ed. Porto Alegre: Vestígio, 2023. 320 p. ISBN 978-6560020047.

¹¹⁵ SCRIPPS NEWS. **Um estudo alerta que os estudantes estão a caminho de passar 25 anos de suas vidas grudados no celular.** Disponível em: <<https://www.scrippsnews.com/science-and-tech/social-media/students-on-track-to-spend-25-years-of-their-lifetime-on-phones-study-warns>>. Acessado em 18 de julho de 2025.

