Contribuição de partes interessadas
41ª Sessão período - Brasil

Contribuição de partes interessadas

Organizações que submetem esta contribuição:

Association for Progressive Communications - APC (principal)
Artigo 19 Brasil e América do Sul
Derechos Digitales
Intervozes - Coletivo Brasil de Comunicação Social

APC[1] A Associação para o Progresso das Comunicações (APC) é uma organização internacional que trabalha para empoderar e apoiar organizações da sociedade civil, movimentos sociais e indivíduos através do uso das tecnologias da informação e comunicação. Trabalhamos na intersecção entre tecnologia e justiça social, de gênero e ambiental. A APC foi formada em 1990 e conta hoje com 62 membros institucionais e 29 individuais, ativos em 74 países, principalmente no Sul Global.

Artigo 19 Brasil e América do Sul[2] é uma organização não-governamental de direitos humanos nascida em 1987, em Londres, com a missão de defender e promover o direito à liberdade de expressão e de acesso à informação em todo o mundo. Seu nome tem origem no 19º artigo da Declaração Universal dos Direitos Humanos da ONU. Com escritórios em nove países, a ARTIGO 19 está no Brasil desde 2007, onde adota estratégias, ações e parcerias diversas e nos mais variados aspectos desta agenda. O escritório sediado em São Paulo defende e promove a liberdade de expressão e informação e sua importância para a conquista e concretização de outros direitos fundamentais no Brasil e na América do Sul.

Derechos Digitales[3] é uma organização não governamental e sem fins de lucro, fundada em 2005, conta com status consultivo no ECOSOC, com sede principal em Santiago do Chile, com alcance latino-americano em seu trabalho, dedicando-se a defesa e promoção de direitos humanos no entorno digital, em particular aqueles relacionados à liberdade de expressão, privacidade e acesso ao conhecimento e informação.

Intervozes[4] - Coletivo Brasil de Comunicação Social é uma organização da sociedade civil, fundada em 2003, que trabalha pela efetivação do direito humano à comunicação. Para o Intervozes, o direito à comunicação é indissociável do pleno exercício da cidadania, da democracia e dos demais direitos. O coletivo atua nas áreas de telecomunicação, dos direitos digitais e da radiodifusão, buscando um sistema de mídia democrático, que respeite os direitos humanos e a liberdade de expressão. É integrante da APC e, no Brasil, da Coalizão Direitos na Rede, composta por cerca de 50 entidades de direitos digitais.

1. Association for Progressive Communications: https://www.apc.org
2. Artigo 19: https://artigo19.org
3. Derechos Digitales: https://www.derechosdigitales.org
4. Intervozes: https://intervozes.org.br

I. INTRODUÇÃO

1. O Estado brasileiro foi considerado referência internacional na proteção de direitos no ambiente digital com a adoção de um Marco Civil da Internet em 2014 e assumiu um papel central na promoção de padrões internacionais em favor da privacidade na era digital. No entanto, a garantia desses direitos encontra importantes limites a nível nacional que comprometeram, nos últimos 5 anos, o exercício de outros direitos fundamentais – situação que se agravou durante a pandemia da COVID-19 em 2020 e 2021.
2. Esta submissão centra-se no cumprimento de obrigações de direitos humanos no contexto digital pelo Brasil e busca fortalecer recomendações focadas na garantia do acesso universal à internet de modo a viabilizar a livre expressão e associação, o acesso à informação, conhecimento, cultura e o exercício de direitos econômicos e sociais de maneira segura, respeitosa à privacidade, à autonomia e livre de qualquer forma de discriminação. Ela se divide da seguinte maneira: introdução; direitos econômicos, sociais e culturais; direitos civis e políticos e recomendações ao Estado brasileiro.

II. DIREITOS ECONÔMICOS E SOCIAIS

Acesso à Internet

3. Cada vez mais o acesso à internet é crucial para o exercício de direitos. Isso se tornou evidente durante a pandemia da COVID-19 nos anos de 2020 e 2021, quando boa parte das atividades escolares, laborais e os serviços do Estado passaram a ocorrer de maneira online. Dados de 2020 apontam que 83% dos domicílios brasileiros contavam com alguma forma de acesso à internet e 81% da população com mais de 10 anos havia acessado a rede. A proporção de domicílios com acesso a um computador nesse ano foi de 45%.[1]
4. No Brasil, as desigualdades no acesso à internet reproduzem desigualdades estruturais e quando se trata de populações em condição de vulnerabilidade, a situação é preocupante: apenas 30% dos brasileiros das classes D/E já usaram um computador uma vez na vida, enquanto os números são bem maiores nas classes C (66%), B (91%) e A (88%). A desigualdade se observa também quando analisado o componente racial: somente 52% dos indígenas e 57% das pessoas pretas já utilizaram computador pelo menos uma vez na vida. Entre as pessoas brancas, o índice é de 64%.[2] O tipo de dispositivo para acessar a internet é outro indicador da desigualdade: 62% de indígenas e 60% dos pretos e pretas utilizam a rede exclusivamente pelo celular, numa proporção superior à das pessoas brancas (48%). Quando acrescida a perspectiva de classe social, essa desigualdade se agrava ainda mais: 90% das pessoas das classes D/E têm apenas o celular como meio de uso da internet, uma diferença abissal para as demais: 58% na classe C, 25% na classe B e 11% na classe A.[3] As desigualdades de acesso são também territoriais e estão relacionadas à distribuição desigual da infraestrutura: no meio urbano, 86% dos domicílios têm acesso à internet e no meio rural este índice é de apenas 65%.[4]
5. Quando se trata de povos e comunidades tradicionais e populações rurais, o direito de acesso à internet, reconhecido pelo Marco Civil da Internet[5], está longe de ser respeitado.[6] A maioria dessas populações se conecta através de planos com limite

de dados via celular que oferecem um limitado número de aplicações, em especial plataformas de redes sociais, por meio de acordos de zero rating. Os custos de conexão chegam a comprometer mais de 30% da renda mensal das famílias pesquisadas, segundo dados do Coletivo Intervozes.

Direito à educação

6. Diante do avanço da COVID-19, o governo brasileiro implementou medidas de caráter urgente para que estudantes pudessem continuar seu processo de aprendizagem diante das limitações impostas pela restrição à circulação e isolamento da população. A falta de planejamento e estruturação das políticas adotadas, somada à precariedade de acesso à internet das famílias, afetou o êxito dessas medidas e resultou em índices de evasão escolar que representaram um aumento de quase 200% na faixa de 5 a 9 anos entre 2019 e 2020.[7]
7. Um levantamento do INEP evidenciou os impactos do abismo digital para o acesso à educação no âmbito rural: dois milhões de estudantes de escolas rurais passaram todo o ano de 2020 sem acesso a conteúdos digitais,[8] sendo a distribuição de materiais impressos a única alternativa encontrada em diversos lugares. Em oito dos nove estados do Nordeste brasileiro, mais de 20% das escolas rurais funcionaram exclusivamente desta forma durante todo o período de distanciamento físico.[9]
8. Quando adotadas, as políticas de acesso à internet para estudantes do sistema público foram insuficientes e pouco focadas na conectividade domiciliar, o que resultou na desconexão de várias famílias, prejudicando seriamente o acesso à educação durante a pandemia. Novamente, desigualdades estruturais se reproduzem: dados oficiais indicam que crianças e jovens negras e indígenas de escolas públicas representam mais de 70% dos estudantes sem acesso domiciliar à internet em banda larga ou 3G/4G.[10] A situação agravou o quadro de desigualdade entre uma elite estudantil com acesso à internet em condições adequadas para prosseguir com os estudos e a maioria dos estudantes de rede pública, com conexões mínimas à internet, por meio de planos de internet móvel e equipamentos inadequados para uma participação significativa na rotina escolar.[11]

Direito à saúde

9. O direito à saúde se viu impactado pelas limitações de acesso à internet, mas também pelos riscos à privacidade e proteção de dados representados pela digitalização de serviços e, em particular, por políticas de monitoramento e controle implementadas no contexto da pandemia da COVID-19.
10. Nos âmbitos federal, estadual e municipal foram desenvolvidas parcerias entre governos e empresas privadas para promover o monitoramento do avanço de casos ou do cumprimento das medidas de isolamento social aplicadas. Elas envolviam a localização de indivíduos por meio de diferentes tecnologias, como geolocalização ou conexão a redes celulares, mas apresentavam escassas salvaguardas e não foram precedidas de debates públicos e estudos de impacto em direitos humanos que permitissem prevenir usos abusivos. Além da exposição a sistemas de vigilância públicos e privados, algumas soluções apresentavam riscos de reidentificação de indivíduos com importante potencial de discriminação.[12]
11. Aplicações criadas para oferecer acesso à informação oficial sobre medidas de prevenção e tratamento da COVID-19, assim como para auxiliar no monitoramento do seu avanço, como a Coronavírus SUS, lançada em 2020 pelo governo federal, tampouco ofereceram

garantias suficientes com relação aos dados pessoais sensíveis coletados e as condições do seu processamento, como o prazo de armazenamento, limitações ao acesso por terceiros, etc.[13,14]

12. Ainda durante a pandemia, vários episódios de vazamento, exposição indevida de dados pessoais, vulnerabilidades em sistemas, falhas graves e ausência de segurança de informações sensíveis foram verificadas no Brasil, explicitando políticas públicas insuficientes para lidar com dados sensíveis coletados pelo poder público no âmbito da saúde.[15]

Digitalização do Estado e segurança social

13. A análise de políticas públicas relacionadas a direitos sociais prestacionais revelam que não há transparência, treinamento adequado de pessoal e relatórios de impacto sobre a utilização dos dados pessoais envolvidos. A digitalização de políticas sociais e a falta de uma política pública adequada de acesso à internet e proteção de dados impede a fruição de direitos sociais ou ainda impõe novos obstáculos ao exercício de outros direitos. Um exemplo foi o auxílio emergencial - programa de transferência de renda em razão do impacto da pandemia de COVID-19 sobre os mais vulneráveis.[16] Outro se refere à implementação de sistemas automatizados no âmbito de políticas públicas sem garantias de transparência e participação ou a realização de estudos de impacto que analisem potenciais riscos ao exercício de direitos, como no caso do Sistema Nacional de Emprego (SINE).[17]
14. 14. Segundo dados da TIC Domicílios, na pandemia de COVID-19, somente 39% das famílias rurais buscaram informações sobre saúde na internet e apenas 16% realizaram serviços públicos online (nas zonas urbanas, os índices foram de 55% e 39%, respectivamente).[18] Mulheres negras, acessando a internet primordialmente apenas pelo celular (67%), realizaram menos transações financeiras (37%), acessaram menos serviços públicos (31%) e cursos (18%) online do que homens brancos (51%, 49% e 30%, respectivamente).[19]
15. 15. A falta de acesso à internet 3G/4G no celular foi um motivo para que 39% dos usuários da classe C, D e E deixassem de acessar políticas públicas, de modo que 33% deixaram de acessar serviços públicos e 28% deixaram de receber algum benefício social, como auxílio emergencial.[20]

III. DIREITOS CIVIS E POLÍTICOS

Privacidade e proteção de dados

a. Tecnologias de vigilância, reconhecimento facial e bases de dados de biometria

16. A utilização de tecnologias de vigilância com sistemas de reconhecimento facial tem se ampliado nos âmbitos público e privado no Brasil,[21] colocando em risco o exercício de direitos fundamentais principalmente de pessoas em situação de vulnerabilidade, mulheres, pessoas negras, pobres e transexuais.[22] O reconhecimento facial tem sido utilizado pelo setor público para diversos fins, tais como segurança pública, transporte urbano, escolas, gestão de benefícios sociais, controle alfandegário e validação de identidade.[23]

17. No que diz respeito à segurança pública, o Ministério da Justiça e Segurança Pública emitiu duas portarias - em 2019 e 2020 - visando o estímulo à implementação de câmeras de vigilância com tecnologias de reconhecimento facial pelos órgãos de segurança pública.[24] Ainda que essas disposições não estejam mais em vigor, já demonstravam o interesse do governo federal em utilizar dados biométricos para tais fins.
18. Em julho de 2021, a Polícia Federal anunciou a implementação da Solução Automatizada de Identificação Biométrica com objetivo de unificar bases de dados de secretarias de segurança pública estaduais.[25] Nesse contexto, é relevante destacar que desde 2018 encontra-se em vigência a Lei n. 13.675/2018, que institui o Sistema Único de Segurança Pública (Susp) e prevê a integração, dentre outros, de bancos de perfis genéticos e digitais.[26] Em paralelo, identifica-se uma crescente implementação de ferramentas de reconhecimento facial aplicadas em imagens coletadas em espaços públicos ou acessíveis ao público em diferentes estados do Brasil.[27]
19. O uso de reconhecimento facial para fins de segurança pública gera grande preocupação por diversos fatores: em primeiro lugar, a Lei Geral de Proteção de Dados (LGPD) brasileira, Lei n.13.709/2018, não regulamenta o tratamento de dados para fins de segurança pública e persecução criminal, determinando que lei específica deve regulamentar a matéria. Além disso, identifica-se uma geral falta de transparência que permita à sociedade civil analisar adequadamente se o uso dessas tecnologias biométricas observam parâmetros mínimos de legalidade, necessidade e proporcionalidade.[28] Há também reiteradas denúncias públicas a respeito da reprodução de expedientes racistas na implementação dessas ferramentas.[29]
20. Apesar da falta de dados oficiais sobre a utilização desse tipo de tecnologia e seus resultados, estudos independentes indicam que a grande maioria da população que é presa com base no reconhecimento facial é negra.[30] Em levantamento de março a outubro de 2019, 151 pessoas foram detidas em cinco estados, das quais 90% são negras.[31]
21. Para além da segurança pública, os sistemas de reconhecimento facial têm sido implementados em diferentes espaços: está em testes a identificação de passageiros para o embarque em aeroportos[32], assim como já foi identificado o uso em escolas públicas[33], no transporte público, entre outros.
22. Como declarado por diversas autoridades internacionais, inclusive a Alta Comissária de Direitos Humanos, o reconhecimento facial em espaços públicos apresenta riscos gravíssimos aos direitos humanos. Por conta disso, Michelle Bachelet pediu uma moratória do uso desse tipo de tecnologias nos espaços públicos.[34]

b. Cibercrimes e criminalização da defesa de direitos humanos no âmbito digital

23. Em dezembro de 2021, o Brasil aprovou a adesão à Convenção de Budapeste sobre Crimes Cibernéticos. O texto foi aprovado sem ressalvas pelo Estado brasileiro e gera preocupações relativas à criminalização de pesquisadores e ativistas da segurança da informação. Isso porque o texto e as penas previstas se aplicam sem considerações relacionadas à existência de uma intenção maliciosa no caso de intrusão em sistemas informáticos. O risco se agrava diante da ausência de um arcabouço robusto para a proteção de dados pessoais na esfera criminal[35] e a uma inclinação legislativa que aponta à violação da segurança de defensores e defensoras de direitos digitais.
24. Esta tendência pode ser vista no âmbito da Lei do Estado Democrático, a qual substituiu recentemente a Lei de Segurança Nacional no país. Na elaboração da nova lei foram debatidas questões como tipificar o crime de espionagem, sem trazer qualquer ressalva ou segurança ao trabalho de fiscalização realizado por jornalistas e a sociedade civil que

muitas vezes se vale de trabalhos da imprensa internacional ou de denunciantes (whistleblowers) para defender direitos fundamentais.[36] O debate dessas medidas denuncia o risco de criminalização de atividades relacionadas à segurança da informação e ativismo digital no país, reproduzindo tendência identificada internacionalmente.[37]

25. O acesso a sistemas informáticos pode levar à descoberta e alerta sobre relevantes falhas de segurança e à obtenção de informações sobre a violação de direitos humanos. A possibilidade de criminalização de condutas relacionadas ao último caso pode desencorajar a divulgação dessas informações de crucial interesse público, principalmente considerando que o Brasil não possui uma legislação abrangente para proteger as atividades de denunciantes, também chamados "whistleblowers".
26. Já em 2015, o então relator especial da ONU para Liberdade de Expressão, David Kaye, destacou que a criptografia e o anonimato online são condições fundamentais para o exercício da liberdade de expressão.[38] Nesse sentido, medidas de vedação do anonimato, como a presente na Constituição Brasileira, não devem ser interpretadas de modo a criar um cenário em que pesquisadores da segurança da informação e outros ativistas online estejam desprotegidos ou submetidos a constante vigilância, como poderiam indicar alguns trechos da Convenção de Budapeste, aprovada integralmente no país. A inclusão de barreiras à identificação de pessoas online é uma postura legítima conforme os parâmetros internacionais de direitos humanos e não viola a vedação do anonimato, dentre outros motivos, porque não impede completamente uma identificação e atribuição de responsabilidades posteriores, quando necessário.

Liberdade de expressão, violência e acesso à informação

e. Vigilância de jornalistas e pessoas defensoras de direitos humanos

27. Nos últimos anos houve uma adoção crescente de medidas de cibervigilância da população realizadas por órgãos vinculados ao Governo Federal envolvendo tentativas de adquirir sistemas de espionagem questionados por autoridades internacionais de direitos humanos. A Secretaria de Operações Integradas (SEOPI), órgão vinculado ao Ministério da Justiça e Segurança Pública do governo federal, por exemplo, contratou por meio de licitação pública um sistema de espionagem da empresa Harpia Tecnologia Eireli; a licitação foi suspensa pelo Tribunal de Contas da União em novembro de 2021.[39] Denúncias também apontam para uma suposta tentativa de articulação para contratação do sistema Pegasus por parte de Carlos Bolsonaro, filho do Presidente da República[40], apesar da ausência de competência legal para interferir em procedimento administrativo relativo a operações de inteligência em âmbito federal, de incumbencia exclusiva da Agência Brasileira de Inteligência (ABIN). A imprensa também noticiou tentativas de compra de outros sistemas de vigilância em 2022, entre eles a ferramenta chamada DarkMatter.[41]
28. Além das denúncias de compra de sistemas de vigilância com enorme potencial para violação de direitos fundamentais, o governo também tem utilizado OSINTs - sigla usada em inglês para descrever Inteligência de Código Aberto em investigações conduzidas por Ministérios Públicos Estaduais e Federal sem que haja regulamentação correspondente.[42] A prática abre espaço para potenciais violações de direitos humanos: em 2021 relatos indicam o fichamento e categorização de pessoas pelo governo a partir de suas posições políticas para fins de monitoramento com base em posições políticas.[43] Esse tipo de monitoramento já teria tido como resultado a detenção de um homem por conta de informações postadas em seu perfil de rede social, conteúdo que foi considerado pela Polícia Militar como "incitamento à violência" contra o presidente.[44] O indivíduo não representava nenhum grupo organizado ou entidade e a vigilância teria sido baseada em sua visão crítica em relação à atual administração.

29. Outro exemplo das praticas de vigilancia crescentes foi a elaboração de um "dossiê antifascista" pelo Ministério da Justiça do governo federal em 2020.[45] O relatório buscava mapear os trabalhadores do funcionalismo público contrários a Bolsonaro a partir da coleta de informações disponíveis nas redes sociais sobre esses indivíduos.[46] O Supremo Tribunal Federal decidiu em 2021 pela proibição da elaboração do Dossiê.[47]

b. Violência de gênero online

30. Em um país marcado por altos índices de violência intrafamiliar e violência de gênero, os meios digitais têm sido crescentemente utilizados para atacar mulheres e pessoas LGBTQIA+. As formas de ataque envolvem fotomontagens racistas, invasão de contas em redes sociais com motivações racistas e misóginas, ameaças, difamação, acusações falsas, entre outras.[48]
31. Durante a pandemia, com a migração de boa parte das atividades de grupos ativistas para o contexto online, multiplicaram-se denúncias de ataques, assim como as invasões de reuniões com a exposição de imagens e sons chocantes, fenômeno que ficou conhecido como "zoombombing", porque inicialmente ocorriam com mais frequência na plataforma Zoom.[49]
32. Em 2021, a Central Nacional de Denúncias de Crimes Cibernéticos da Safernet no Brasil recebeu 5.347 denúncias de LGBTfobia, 6.888 denúncias de racismo e 8.174 denúncias de violência e discriminação contra mulheres.[50]

c. Desinformação e discurso político violento

33. A violência de gênero online se mescla com violência política em diversas ocasiões no Brasil, por exemplo, quando autoridades públicas utilizam suas redes sociais pessoais para atacar ou repercutir ataques contra jornalistas e ativistas mulheres. Da mesma forma, o próprio presidente Jair Bolsonaro em distintas ocasiões expôs jornalistas mulheres questionando suas motivações, disseminando desinformação, fazendo insinuações de caráter sexual e/ou compartilhando dados pessoais das profissionais que investigam denúncias de corrupção envolvendo o governo federal ou os familiares do presidente em evidente ataque a sua liberdade de expressão. Um exemplo foram as declarações relativas à Constança Resende em 2019; na ocasião, o presidente compartilhou um áudio que se mostrou falso para insinuar parcialidade no trabalho da jornalista.[51] Em 2018, os administradores das contas da jornalista Patrícia Campos Mello também foram alvos de ataques após a publicação de uma reportagem da jornalista sobre possíveis ilegalidades na campanha de Bolsonaro.[52] Esses e outros casos foram denunciados pela sociedade civil em audiências diante da Comissão Interamericana de Direitos Humanos em março de 2020, no Haiti, e em outubro do mesmo ano.[53]
34. Em 2018, durante a campanha eleitoral presidencial, foram verificados vários ataques online contra grupos políticos e jornalistas. Em setembro daquele ano, um grupo no Facebook chamado "Mulheres contra Bolsonaro" foi derrubado e seus moderadores receberam ataques diretos.[54]
35. A violência política online e a desinformação também afeta candidatos e candidatas e pessoas eleitas e - em uma sociedade marcada pelo racismo, homofobia e transfobia - é ainda mais intensa no caso de integrantes de grupos historicamente vulnerabilizados. Um levantamento da TretAqui.org mostrou que machismo, ódio ideológico, racismo e LGBTfobia foram os principais temas de ataques contra candidaturas no primeiro turno das eleições de 2020.[55]

36. A difusão de conteúdos desinformativos têm se direcionado ao ataque às instituições democráticas, buscando comprometer a confiança da população no pleito eleitoral. São notáveis os prejuízos da desinformação para os direitos humanos e para a democracia também fora dos períodos eleitorais. A disseminação de desinformação também ocorre por meio de agentes públicos que contribuem ativamente com a criação de um ambiente polarizado e anti democrático.[56]
37. Jair Bolsonaro, sua família e outros atores políticos que o apoiam têm usado as plataformas de mídia social para mobilizar e inflamar sua base ultraconservadora. O presidente já foi acusado da prática de "discurso de ódio" e xenofobia em razão de ataques a minorias e grupos marginalizados, como pessoas negras, mulheres e população LGBTQIA+.[57] A postura do chefe do executivo nas redes sociais chegou a levar a exclusão e bloqueio de determinados conteúdos postados por Bolsonaro pelas próprias plataformas.[58]
38. A discussão sobre desinformação e discurso político violento passa também pelo debate sobre o papel das grandes plataformas digitais na priorização e moderação de conteúdo, feita de forma pouco transparente, como mostrou pesquisa realizada pelo Intervozes[59] e declaração conjunta de entidades latino-americanas sobre o tema[60].

d. Medidas legislativas e judiciais para a regulação do discurso online

39. Nos últimos anos, várias iniciativas legislativas têm sido propostas com o objetivo de responder aos desafios da digitalização, como a concentração das grandes plataformas digitais, políticas abusivas relacionadas à exploração de dados pessoais, e baixa responsividade dessas mesmas plataformas quanto à proliferação de discurso de ódio em suas redes. Muitos destes projetos, apesar de buscarem fins supostamente legítimos, acabam adotando dispositivos inefetivos e desproporcionais e que podem apresentar real risco à liberdade de expressão. Dois importantes exemplos nos últimos 5 anos foram a tentativa de legislar sobre sobre a responsabilidade de intermediários e desinformação.[61]
40. A rejeição de medidas de filtragem e bloqueio ou a promoção de um sistema de notificação judicial para responsabilizar intermediários pelo conteúdo de terceiros foi estabelecida como baluarte central na garantia da liberdade de expressão online. É o que prevê o Marco Civil da Internet no Brasil. O objetivo é proteger as plataformas e os mecanismos de pesquisa da responsabilização indevida por comportamentos de usuários e com isso desincentivar a remoção de conteúdos sem ordem judicial. No entanto, os desafios recentes com a disseminação de conteúdos danosos por meio de redes sociais, assim como a compreensão do papel das grandes plataformas na priorização ou não desses conteúdos, têm gerado novas tentativas de responsabilização. No Congresso Nacional, tramitam em 2022 mais de 30 projetos que têm o objetivo de combater a desinformação. Parte deles visa modificar o Marco Civil da Internet em temas como privacidade, liberdade de expressão e responsabilização dos intermediários.
41. Em 2021, Bolsonaro tentou, por meio de uma Medida Provisória (MP n. 1.068), incorporar novas regras para moderação de conteúdos por plataformas digitais e mudar o regime jurídico estabelecido pelo Marco Civil. A mudança exigiria mais burocracia para suspender ou cancelar contas, além de determinar a restituição de conteúdos banidos, e foi apresentada em um contexto de pressão judicial para a remoção de conteúdos abusivos compartilhados por apoiadores do presidente. A Medida Provisória - ato do poder Executivo - não consiste no mecanismo legal adequado para inovar na regulamentação desse tema e foi devolvida ao Poder Executivo, perdendo efetividade. Ela se transformou em mais um projeto de lei sobre o tema atualmente em discussão no Congresso Nacional.[62]

42. Tramita também no Legislativo o Projeto de Lei (PL) n.º 2630/2020, conhecido como "PL das Fake News". Inicialmente alvo de preocupações pelas medidas de controle previstas, o PL foi revisado e traz uma série de determinações relativas à regulamentação das plataformas digitais e a previsão de que os princípios da administração pública devem ser aplicados também aos perfis de redes sociais de agentes políticos.
43. Os bloqueios de aplicações também têm sido alvo de preocupação e discutidos desde 2016 pelo Supremo Tribunal Federal, após uma série de decisões judiciais que determinavam o bloqueio integral do WhatsApp por descumprimento de decisões que determinavam o acesso ao conteúdo de mensagens, inclusive com a quebra da criptografia ponta-a-ponta. O julgamento está suspenso desde 2021.[63] Em março de 2022, o Ministro Alexandre de Moraes determinou o bloqueio do aplicativo Telegram em todo o território nacional, determinando multas diárias no valor de R$ 100 mil para qualquer pessoa que tentasse utilizá-lo.[64] A ordem só foi revogada três dias depois.[65] O bloqueio do Telegram também tem sido aventado pelo Tribunal Superior Eleitoral devido à falta de resposta em relação à contribuição com as autoridades brasileiras.[66]
44. Finalmente, a expansão de medidas criminalizando expressões legítimas online continua a ser uma área de extrema preocupação. Medidas contidas na previamente mencionada Lei do Estado Democrática, por exemplo, criminaliza amplamente as chamadas "desinformação em massa" ou "insurreição" e propagação de fatos sabidamente falso" e pode aprofundar um ambiente de autocensura que impacta não apenas a liberdade de expressão, mas também o acesso à informação.[67]

e. Acesso à informação e proteção de dados pessoais

45. O Estado brasileiro conta com uma Lei de Acesso à Informação (LAI) desde 2011, que possibilitou mais de um milhão de solicitações de informações dirigidas a órgãos e entidades do poder executivo federal. Dez anos após sua aprovação, no entanto, repetidas tentativas de alteração da LAI têm sido observadas - especialmente por meio de decretos e portarias - e que resultam em ameaças à transparência no país. Entre elas destacamos a MP 928/2020, que tentou impor, sem sucesso, a suspensão dos prazos de resposta aos pedidos de acesso à informação durante a pandemia; o Decreto 9.690/2019, que tentou aumentar drasticamente o número de autoridades com poder de veto no acesso à informação; e a Portaria 880/2019, que banaliza o sigilo de documentos produzidos pelo Ministério da Justiça e Segurança Pública.
46. Por outro lado, aumentou nos últimos anos uma interpretação expansiva e abusiva do artigo 31 da LAI, que se refere ao tratamento e compartilhamento de informações pessoais, para justificar a ocultação de informações de interesse público em patente ataque ao direito de acesso. A análise desses casos indica que a classificação adotada contraria a finalidade pela qual a LAI foi promulgada: estabelecer a transparência como regra e o sigilo como exceção. Dados considerados confidenciais segundo essa regra dizem respeito a nomes dos servidores que postam no perfil do Twitter da Secretaria de Comunicação; os dados dos crachás de acesso ao Palácio do Planalto dos filhos do presidente; o processo disciplinar que absolveu um general e ex-ministro da Saúde por ter participado de uma manifestação política ao lado do presidente, entre outros. A antes mencionada LGPD, aprovada em 2018, também tem sido utilizada inapropriadamente como pretexto para negar o acesso a informações públicas.[68]
47. Em contradição à suposta tentativa de proteção de dados pessoais, o governo vetou da LGPD, em 2019, um importante dispositivo que visava a proibição do compartilhamento de dados pessoais de requerentes de informação com instituições públicas ou pessoas jurídicas de direito privado.[69] Seu objetivo era proteger a identidade de solicitantes de informações para evitar negativas infundadas de acesso, possíveis constrangimentos ou retaliações/perseguição.

48. Os ataques à transparência pública identificados podem dificultar o monitoramento das ações governamentais por parte da cidadania e impedir a apuração de eventuais crimes de responsabilidade, por exemplo, na condução das medidas de enfrentamento à pandemia; ou do envolvimento de agentes do governo na preparação e divulgação de informações falsas e discursos de ódio na Internet. As ações listadas subvertem, por princípio, a premissa que guiou o estabelecimento e promulgação de leis como a LAI e a LGPD: a proteção da população comum frente ao Estado, e não a blindagem de ações de agentes políticos poderosos diante do escrutínio público.

IV. SÍNTESE DAS RECOMENDAÇÕES AO ESTADO BRASILEIRO

49. Frente às violações identificadas ao exercício de direitos humanos no ambiente digital no Brasil, seus impactos para o gozo de direitos no contexto offline e, consequentemente, o não cumprimento com os compromissos internacionais assumidos pelo país, inclusive com o alcance dos Objetivos de Desenvolvimento Sustentável, recomendamos ao Estado brasileiro:

A. A criação urgente de políticas públicas de inclusão digital que incluam um plano de metas priorizando populações em condição de vulnerabilidade e que considerem:

a. a universalização do acesso à internet de qualidade;
b. a ampla participação da população nos processos de formulação, revisão e avaliação de políticas de conectividade, inclusive de populações rurais e Povos e Comunidades Tradicionais;
c. a educação para os meios digitais enfocada na recepção crítica de conteúdos, em práticas de comunicação baseada em princípios de direitos humanos e na segurança digital; e
d. a promoção de alternativas para a conectividade, inclusive por meio de redes comunitárias, com garantia de assessoria técnica gratuita aos territórios de Povos e Comunidades Tradicionais;

B. A produção e divulgação periódica de dados e estatísticas atualizadas e desagregadas por raça, gênero, idade, localidade e renda sobre o acesso à internet no país para orientar a formulação de políticas públicas, inclusive eventuais medidas emergenciais em contextos de isolamento social no âmbito da educação, saúde e/ou assistência social de modo a evitar o acirramento de desigualdades estruturais pré-existentes;

C. A adoção urgente de medidas transversais para a adequação dos serviços públicos às exigências da Lei Geral de Proteção de Dados no que diz respeito aos direitos das pessoas titulares de dados processados pelo Poder Público, incluindo:

a. a garantia de que terceiros envolvidos no processamento desses dados obedeçam às normativas vigentes;
b. a garantia da integridade e correção das vulnerabilidades encontradas nos sistemas eletrônicos estatais, inclusive do Ministério da Saúde, assim como garantir políticas de segurança, contenção de dados existentes e remédios adequados em caso de vazamentos e exposição indevida de dados pessoais, em particular, sensíveis;
c. a oferta de informação transparente sobre os critérios de coleta, processamento e compartilhamento de informações e a criação de canais para a solução de dúvidas e resposta a requerimentos relacionados à gestão de dados pessoais.

D. A adoção urgente de medidas para fortalecer a independência da autoridade nacional de proteção de dados para que possa supervisionar a observação das regras previstas na LGPD por instituições públicas e privadas e apresentar orientações com relação à interpretação de dispositivos previstos na lei;

E. A abstenção de implementar políticas de digitalização, automação ou inteligência artificial no setor público sem antes contar com os seguintes requisitos, que também deveriam ser considerados em contextos de eventual urgência:

a. estudos de impacto que garantam que elas não gerarão um aprofundamento em desigualdades históricas, discriminação ou riscos ao exercícios de direitos humanos, inclusive direitos econômicos e sociais e privacidade;
b. processos de consulta prévia que envolvam os grupos potencialmente afetados e/ou seus representantes;
c. planos de monitoramento e avaliação periódicos independentes e transparentes;
d. garantias explícitas em relação ao exercício dos direitos de revisão, reparação e não repetição do ilícito à cidadania.

F. A adoção de uma moratória limitando o uso de tecnologias de reconhecimento facial em espaços públicos até que haja um consenso internacional sobre a segurança dessas tecnologias em relação ao cumprimento dos direitos humanos e a proibição do seu uso para fins de segurança pública ou controle de acesso a espaços ou serviços estatais;

G. A garantia do respeito e adoção de normas que limitem o uso de tecnologias de vigilância para além do reconhecimento facial aos princípios da legalidade, necessidade e proporcionalidade estabelecidos pelos padrões de direitos humanos; estabeleçam mecanismos legais de reparação consistentes com a obrigação de fornecer às vítimas de abusos um remédio eficaz; e criem mecanismos que assegurem a aprovação, supervisão e controle público ou comunitário da compra de tecnologias de vigilância.

H. A revogação, não adoção ou revisão de normas que facilitem a vigilância online e a criminalização de ativistas de direitos humanos e segurança da informação; e atenção a critérios de legalidade, necessidade e proporcionalidade na implementação de qualquer ação de intervenção em comunicações privadas, como estabelecido pelos marcos internacionais de direitos humanos ratificados pelo Brasil;

I. A adoção de normas e práticas estatais de respeito à criptografia e ao anonimato online como fatores importantes para o exercício de direitos humanos, assim como a garantia de proteção a denunciantes de violações de direitos humanos, chamados “whistleblowers”, por meio da edição de uma normativa específica sobre o tema;

J. A criação de políticas públicas e medidas adequadas para combater todas as formas de violência baseadas em gênero, online e offline;

K. A adoção de medidas para combater o financiamento de campanhas desinformativas com recursos públicos, tomando em consideração as obrigações e princípios internacionais de direitos humanos;

L. A rejeição de legislações abusivas de regulação de conteúdos em redes sociais e plataformas de mensagens que promovam a responsabilização dos intermediários, ferindo os princípios estabelecidos em documentos internacionais de direitos humanos e o Marco Civil da Internet. Recomenda-se também que a necessária regulação das grandes

plataformas digitais seja fruto de um debate amplo e multisetorial, com todas as partes envolvidas, e que respeitem os padrões internacionais de direitos humanos.

M. A adoção de medidas para garantir o respeito à legislação existente que regula o acesso à informação pública, sem a instrumentalização da proteção de dados para impedir esse acesso. A análise da observância dos princípios da legalidade, necessidade e proporcionalidade na restrição do direito à privacidade é necessária também para avaliar o interesse público frente a informações que estão sob tutela do Estado.

V. REFERÊNCIAS

1. Cetic.br, 2020. Executive Summary: ICT Household Survey 2020. Disponível em: https://www.cetic.br/media/docs/publicacoes/2/20211124201635/executive_summary_ict_households_2020.pdf
2. Cetic.br, 2020. ICT Household Survey 2020. Disponível em: https://cetic.br/pt/tics/domicilios/2020/individuos/B1/.
3. Cetic.br, 2020. ICT Household Survey 2020. Disponível em: https://cetic.br/pt/tics/domicilios/2020/individuos/C16A/
4. Cetic.br, 2020. ICT Household Survey 2020. Disponível em: https://cetic.br/pt/tics/domicilios/2020/domicilios/A4/.
5. Marco Civil da Internet no Brasil, Lei n. 12.965/2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.
6. Intervozes, 2022. Territórios Livres, Tecnologias Livres. Disponível em: http://territorios-livres.online/.
7. Neri, M. & Osorio, M., 2022. Retorno para Escola, Jornada e Pandemia. Disponível em: https://www.cps.fgv.br/cps/RetornoParaEscola/.
8. Intervozes, 2022. Territórios Livres, Tecnologias Livres. Disponível em: http://territorios-livres.online/.
9. Intervozes, 2022. Territórios Livres, Tecnologias Livres. Disponível em: http://territorios-livres.online/.
10. IPEA, 2020. Nota técnica n. 88. Acesso domiciliar à internet e ensino remoto durante a pandemia. Disponível em: http://repositorio.ipea.gov.br/bitstream/11058/10228/1/NT_88_Disoc_AcesDomInternEnsinoRemoPandemia.pdf.
11. Nogueira, J., 2021. Acesso à internet residencial de estudantes. Disponível em: https://idec.org.br/arquivos/pesquisas-acesso-internet/idec_pesquisa-acesso-internet_acesso-a-internet-residencial-dos-estudantes.pdf.
12. Venturini, J. & Souza, J. Tecnologias e Covid-19 no Brasil: vigilância e desigualdade na periferia do capitalismo. Disponível em: https://br.boell.org/sites/default/files/2020-06/Tecnologias%20e%20Covid-19%20no%20Brasil%20vigil%C3%A2ncia%20e%20desigualdade%20social%20na%20periferia%20do%20capitalismo.pdf.
13. Venturini, J. et al., 2021. Informe Observatorio Covid-19 del Consorcio Al Sur: Un análisis crítico de las tecnologías desplegadas en América Latina contra la pandemia. Disponível em: https://www.alsur.lat/sites/default/files/2021-06/Informe%20Observatorio%20Covid-19%20del%20Consorcio%20Al%20Sur(2).pdf.
14. Hernández, L. (2021). Uso de Tecnologías para el combate de la pandemia. Datos personales en América Latina. Disponível em: https://globalnetworkinitiative.org/wp-content/uploads/2021/11/COVID19-LAC-SPA.pdf.
15. OKBR, 2020. Ministério da Saúde já havia deixado dados pessoais expostos no próprio sistema da Covid-19 em junho; aqui está a prova. Disponível em: https://ok.org.br/noticia/ministerio-da-saude-ja-havia-deixado-dados-pessoais-expostos-no-proprio-sistema-da-covid-19-em-junho-aqui-esta-a-prova/.
16. InternetLab. O Auxílio Emergencial no Brasil: desafios na implementação de uma política de proteção social datificada. (Report not yet published.)

17. Fernanda Bruno, Paula Cardoso e Paulo Fatay. Sistema Nacional de Emprego e a gestão automatizada do desemprego. Disponível em: https://ia.derechosdigitales.org/wp-content/uploads/2021/04/CPC_informe_BRASIL.pdf.
18. Cetic.br, 2020. Executive Summary: ICT Household Survey 2020. Disponível em: https://www.cetic.br/media/docs/publicacoes/2/20211124201635/executive_summary_ict_households_2020.pdf
19. Cetic.br, 2020. Executive Summary: ICT Household Survey 2020. Disponível em: https://www.cetic.br/media/docs/publicacoes/2/20211124201635/executive_summary_ict_households_2020.pdf
20. Idec & Locomotiva, 2021. Barreiras e limitações no acesso à internet e hábitos de uso e navegação na rede nas classes C, D e E. Disponível em: https://idec.org.br/sites/default/files/versao_revisada_pesquisa_locomotiva.pdf.
21. Souza, M. R. & Zanatta, R. A. F., 2021 The Problem of Automated Facial Recognition Technologies in Brazil: Social Countermovements and the New Frontiers of Fundamental Rights. Disponível em: https://revistas.ufg.br/lahrs/article/view/69423.
22. Silva, Mariah Rafaela, 2022. Orbitando telas: Tecnopolíticas de segurança, o paradigma smart e o vigilantismo de gênero em tempos de acumulação de dados. Disponível em: https://sur.conectas.org/orbitando-telas/; Coding Rights, 2021. Reconhecimento Facial no Setor Público e Identidades Trans. Disponível em: https://codingrights.org/docs/rec-facial-id-trans.pdf.
23. Reis, C. et al, 2021. Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil: versão resumida. Disponível em: https://lapin.org.br//download/4141/.
24. Biblioteca Digital do Ministério da Justiça e Segurança Pública. Portaria nº 793, of October 24, 2019. Disponível em: <https://dspace.mj.gov.br/handle/1/1380>; Portaria nº 630, of November 27, 2020. Disponível em: <https://dspace.mj.gov.br/handle/1/2367>.
25. Coalizão Direitos na Rede, 2021. OFÍCIO PARA ANPD | Entidades solicitam medidas contra solução automatizada de identificação biométrica da Polícia Federal. Disponível em: https://direitosnarede.org.br/2021/07/19/oficio-para-anpd-entidades-solicitam-medidas-contra-solucao-automatizada-de-identificacao-biometrica-da-policia-federal/.
26. Lei 13675/2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13675.htm.
27. Folha de S. Paulo. Sob críticas por viés racial, reconhecimento facial chega a 20 estados. Disponível em: https://www1.folha.uol.com.br/cotidiano/2021/07/sob-criticas-por-vies-racial-reconhecimento-facial-chega-a-20-estados.shtml.
28. Consórcio Al Sur. Reconocimiento facial en América Latina Tendencias en la implementación de una tecnología perversa. Disponível em: https://estudio.reconocimientofacial.info/reports/ALSUR-Reconocimiento_facial_en_Latam-ES.pdf.
29. Revista Piauí, 2021. Nos erros do reconhecimento facial, um “caso isolado” atrás do outro. Disponível em: https://piaui.folha.uol.com.br/nos-erros-de-reconhecimento-facial-um-caso-isolado-atras-do-outro/.
30. Monitor do reconhecimento facial no Brasil. Disponível em: https://opanoptico.com.br/.
31. Folha de S. Paulo, 2019. 151 pessoas são presas por reconhecimento facial no país; 90% são negras. Disponível em: https://www1.folha.uol.com.br/cotidiano/2019/11/151-pessoas-sao-presas-por-reconhecimento-facial-no-pais-90-sao-negras.shtml.
32. INFRAERO. Aeroporto de Congonhas testa embarque por reconhecimento facial com tripulantes. Disponível em: https://www4.infraero.gov.br/imprensa/noticias/aeropor-

to-de-congonhas-testa-embarque-por-reconhecimento-facial-com-tripulantes/; SERPRO. Embarque nos aeroportos brasileiros poderá ser realizado sem apresentação de documentos. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2020/embarque-biometria-serpro-1.

33. G1, 2017. Escolas municipais de Jaboatão adotam reconhecimento facial para controlar frequência de alunos. Disponível em: https://g1.globo.com/pernambuco/noticia/escolas-municipais-de-jaboatao-adotam-reconhecimento-facial-para-controlar-frequencia-de-alunos.ghtml.
34. Ver: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session48/Documents/A_HRC_48_31_AdvanceEditedVersion.docx
35. Lapin, 2021. Histórico da LGPD Penal: o que foi feito até aqui e quais são os próximos passos? Disponível em: https://lapin.org.br/2021/04/16/lgpd-penal-o-que-foi-feito-ate-aqui-e-quais-sao-os-proximos-passos/.
36. Coalizão Direitos na Rede. A Internet e as propostas de Lei de Defesa do Estado Democrático de Direito. Disponível em: https://direitosnarede.org.br/2021/04/16/a-internet-e-as-propostas-de-lei-de-defesa-do-estado-democratico-de-direito/.
37. Access Now, 2021. La persecución de la comunidad infosec en América Latina. Disponível em: https://www.accessnow.org/cms/assets/uploads/2021/08/persecusion-latam-seguridad-digital.pdf.
38. Artigo 19, 2015. Criptografia e anonimato são essenciais para liberdade de expressão. Disponível em: https://artigo19.org/2015/06/01/criptografia-e-anonimato-sao-essenciais-para-liberdade-de-expressao/.
39. UOL. "TCU suspende pregão para a compra de sistema espião pelo governo Bolsonaro." Disponível em: https://noticias.uol.com.br/politica/ultimas-noticias/2021/11/11/tcu-suspensao-compra-governo.htm. Accessed March 2022.
40. IstoÉ, 2021. Além do Pegasus, Carlos Bolsonaro queria outra ferramenta para espionagem dentro do governo. Disponível em: https://istoe.com.br/alem-do-pegasus-carlos-bolsonaro-queria-outra-ferramenta-para-espionagem-dentro-do-governo.
41. UOL, 2022. Gabinete do ódio busca comprar nova ferramenta espiã intitulada DarkMatter. Disponível em: https://noticias.uol.com.br/politica/ultimas-noticias/2022/01/17/gabinete-do-odio-usou-viagem-de-bolsonaro-para-negociar-sistema-espiao.htmOSINT/
42. MPPE. Curso de Inteligência e Investigação em Fontes Abertas - OSINT. Disponível em: https://www.mppe.mp.br/mppe/institucional/escola-superior/ultimas-noticias-escola-superior/15370-curso-de-inteligencia-e-investigacao-em-fontes-abertas-osint; Twitter.MPF. Disponível em: https://twitter.com/oea_cyber/status/1174752582583181313.
43. The Intercept, 2021. Governo Bolsonaro deturpou edital de Dilma para fichar 'detratores' na internet. Disponível em: https://theintercept.com/2021/07/07/governo-bolsonaro-deturpou-edital-de-dilma-para-fichar-detratores-na-internet/.
44. G1, 2021. Jovem é preso em flagrante após publicação sobre visita de Bolsonaro a Uberlândia. Disponível em: https://g1.globo.com/mg/triangulo-mineiro/noticia/2021/03/04/jovem-e-preso-apos-publicacao-sobre-vinda-de-bolsonaro-a-uberlandia.ghtml.
45. G1, 2020. Ministério entrega a comissão do Congresso material com suposto dossiê de opositores do governo. Disponível em: https://g1.globo.com/politica/noticia/2020/08/11/ministerio-entrega-a-comissao-do-congresso-material-com-suposto-dossie-de-opositores-do-governo.ghtml.
46. Conjur, 2020. Dossiê de antifascistas entregue aos EUA cita jornalistas e professores. Disponível em: https://www.conjur.com.br/2020-ago-17/dossie-antifascistas-entregue-aos-eua-cita-jornalistas-professores.

47. G1, 2020. STF decide suspender produção de dossiê sobre antifascistas pelo Ministério da Justiça. Disponível em: https://g1.globo.com/politica/noticia/2020/08/20/stf-forma-maioria-para-proibir-ministerio-da-justica-de-produzir-dossie-contra-antifascistas.ghtml.
48. Coding Rights; InternetLab, 2017. Violências contra mulher na internet: diagnóstico, soluções e desafios. Contribuição conjunta do Brasil para a relatora especial da ONU sobre violência contra a mulher. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2017/11/Relatorio_ViolenciaGenero_ONU.pdf.
49. Perifericas; Gig@ UFBA, 2021. Diálogos feministas sobre a violência digital de gênero no Brasil durante a pandemia de COVID-19 no ano de 2020. Disponível em: https://perifericas.netlify.app/posts/lancamento-de-publicacao-sobre-violencia-digital-de-genero-e-covid-19-no-brasil-em-2020/.
50. Ver: https://indicadores.safernet.org.br/
51. The Media Today. Brazil's Bolsonaro smears reports investigating his son. March 12, 2019. Disponível em: https://www.cjr.org/the_media_today/bolsonaro_twitter_press_threats.php.
52. Folha de S. Paulo, 2018. Folha pede que Polícia Federal investigue ameaças a profissionais. Disponível em: : https://www1.folha.uol.com.br/poder/2018/10/folha-pede-que-policia-federal-investigue-ameacas-a-profissionais.shtml.
53. Intervozes, 2020. Governo Bolsonaro promove desinformação e acusa organizações da sociedade civil de censura na CIDH. Disponível em: : https://intervozes.org.br/violencia-e-divergencia-de-opiniao-e-desinformacao-e-liberdade-de-expressao-afirma-governo-na-cidh/.
54. El País, 2018. Grupo "Mulheres contra Bolsonaro" no Facebook sofre ataque cibernético. Disponível em: : https://brasil.elpais.com/brasil/2018/09/14/politica/1536941007_569454.html.
55. Ver: https://www.tretaqui.org.
56. Intervozes, 2020. Governo Bolsonaro promove desinformação e acusa organizações da sociedade civil de censura na CIDH. Disponível em: : https://intervozes.org.br/violencia-e-divergencia-de-opiniao-e-desinformacao-e-liberdade-de-expressao-afirma-governo-na-cidh/; Carta Capital, 2021. PF sugere que Bolsonaro seja investigado por desinformação sobre urna eletrônica. Disponível em: : https://www.cartacapital.com.br/politica/pf-sugere-que-bolsonaro-seja-investigado-por-desinformacao-sobre-urna-eletronica/.
57. Carta Capital, 2019. Jair Bolsonaro traz discurso de ódio como fala oficial da Presidência. Disponível em: : https://www.cartacapital.com.br/opiniao/jair-bolsonaro-traz-discurso-de-odio-como-fala-oficial-da-presidencia/; Brasil de Fato, 2020. Bolsonaro pratica xenofobia ideológica com o veto à Sinovac. Disponível em: : https://www.brasildefato.com.br/2020/10/25/bolsonaro-pratica-xenofobia-ideologica-com-o-veto-a-sinovac; Folha de S. Paulo, 2019. Termo 'paraíba' usado por Bolsonaro reflete preconceito ao Nordeste, e cabe punição. Disponível em: : https://www1.folha.uol.com.br/poder/2019/07/termo-paraiba-usado-por-bolsonaro-reflete-preconceito-ao-nordeste-e-cabe-punicao.shtml.
58. UOL, 2021. Facebook e Instagram publican un aviso de información falsa en la publicación de Bolsonaro. Disponível em: : https://www.uol.com.br/tilt/noticias/redacao/2021/04/29/facebook-instagram-informacao-falsa-bolsonaro.htm; UOL, 2020. Instagram oculta publicación de Bolsonaro sobre covid-19: 'Información falsa'. Disponível em: : https://noticias.uol.com.br/saude/ultimas-noticias/redacao/2020/05/11/instagram-tira-do-ar-post-de-bolsonaro-sobre-covid-19-informacao-falsa.htm; EXAME, 2020. Após Twitter, Facebook e Instagram eliminan publicaciones de Bolsonaro. Disponível em: : https://exame.com/brasil/apos-twitter-facebook-e-instagram-removem-posts-de-bolson-

aro/; G1, 2021. YouTube remove live de Bolsonaro com mentira sobre vacina da Covid e Aids e suspende canal por uma semana. Disponível em: https://g1.globo.com/tecnologia/noticia/2021/10/25/youtube-live-bolsonaro.ghtml.

59. Intervozes, 2021. Fake news: how platforms face disinformation. Disponível em: https://intervozes.org.br/publicacoes/fake-news-how-platforms-combat/.
60. Several, 2021. Declaración Latinoamericana sobre Transparencia de Plataformas de Internet. Disponível em: https://intervozes.org.br/wp-content/uploads/2021/11/Declaracio%CC%81n-Latinoamericana-sobre-Transparencia-de-Plataformas-de-Internet.pdf.
61. Intervozes, 2021. Fake News: como as plataformas enfrentam a desinformação. Disponível em: https://intervozes.org.br/publicacoes/fake-news-como-as-plataformas-enfrentam-a-desinformacao/.
62. Conjur, 2021. MP 1.068, regulação de conteúdo em redes sociais e livre iniciativa. Disponível em: https://www.conjur.com.br/2021-set-21/opiniao-mp-1068-regulacao-conteudo-redes-sociais.
63. Conjur, 2020. Segundo Rosa, marco civil da internet não permite que WhatsApp seja suspenso. Disponível em: : https://www.conjur.com.br/2020-mai-27/rosa-marco-civil-internet-nao-permite-whatsapp-seja-suspenso.
64. STF, 2022. Ministro Alexandre de Moraes suspende funcionamento do Telegram no Brasil. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=483659&ori=1.
65. STF, 2022. Ministro Alexandre de Moraes revoga bloqueio após Telegram cumprir determinações do STF. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=483712&ori=1.
66. Tecmundo, 2022. TSE quer banir Telegram durante eleições para combater fake news. Disponível em: https://www.tecmundo.com.br/mercado/232304-tse-quer-banir-telegram-durante-eleicoes-combater-fake-news.htm.
67. Coalizão Direitos na Rede. A Internet e as propostas de Lei de Defesa do Estado Democrático de Direito. Disponível em: https://direitosnarede.org.br/2021/04/16/a-internet-e-as-propostas-de-lei-de-defesa-do-estado-democratico-de-direito/.
68. Ver: https://www.transparencia.org.br/downloads/publicacoes/lgpd_reforco_respostas_negativas_dez_2021.pdf.
69. Artigo 19, 2019. Entre vetos preocupantes, Presidência tenta derrubar proteção de dados pessoais de requerentes de informação pública. Disponível em: https://artigo19.org/2019/07/10/entre-vetos-preocupantes-presidencia-tenta-derrubar-protecao-de-dados-pessoais-de-requerentes-de-informacao-publica/.