Examen Periódico Universal

41° Periodo de sesiones - Brasil

Contribución conjunta de las partes interesadas

Organizaciones que realizan la presentación

Asociación para el Progreso de las Comunicaciones - APC (principal)
Artigo 19 Brasil e América do Sul
Derechos Digitales
Intervozes - Colectivo Brasil de Comunicación Social

APC[1] es una organización internacional y una red de organizaciones sin fines de lucro que trabaja para empoderar y apoyar a organizaciones, movimientos sociales e individuos a través del uso de las tecnologías de información y comunicación. Trabajan en la intersección entre tecnología y justicia social, de género y ambiental. Formada en 1990, APC tiene estatus consultivo ante el Consejo Económico y Social de la ONU (ECOSOC) desde 1995. APC cuenta hoy con 62 miembros organizacionales y 29 individuales, activos en 74 países, principalmente en el Sur Global.

Artigo 19 Brasil e América do Sul[2] es una organización no gubernamental de derechos humanos nacida en 1987 en Londres, con la misión de defender y promover el derecho a la libertad de expresión y de acceso a la información en todo el mundo. Su nombre proviene del Artículo 19 de la Declaración Universal de los Derechos Humanos de la ONU. Con oficinas en nueve países, ARTÍCULO 19 está en Brasil desde 2007, donde adopta diversas estrategias, acciones y alianzas en los más variados aspectos de esta agenda. La oficina con sede en Sao Paulo defiende y promueve la libertad de expresión e información y su importancia para la conquista y concreción de otros derechos fundamentales en Brasil y América del Sur.

Derechos Digitales[3] es una organización no gubernamental y sin fines de lucro, fundada en 2005, cuenta con estatus consultivo en el ECOSOC, con sede principal en Santiago de Chile, con alcance latinoamericano en su trabajo, dedicándose a la defensa y promoción de derechos humanos en el entorno digital, en particular aquéllos relacionados a la libertad de expresión, privacidad y acceso al conocimiento e información.

Intervozes[4] - Colectivo Brasil de Comunicación Social es una organización de la sociedad civil, fundada en 2003, que trabaja por la realización del derecho humano a la comunicación. Para Intervozes, el derecho a la comunicación es indisociable del pleno ejercicio de la ciudadanía, de la democracia y de los demás derechos. El colectivo actúa en las áreas de telecomunicación, de los derechos digitales y de la radiodifusión, buscando un sistema de medios democrático, que respete los derechos humanos y la libertad de expresión. Es miembro de APC y de la “Coalizão Direitos na Rede” en Brasil, la cual está compuesta por alrededor de 50 entidades de derechos digitales.

1. Asociación para el Progreso de las Comunicaciones: https://www.apc.org
2. Artigo 19 Brasil e América do Sul: https://artigo19.org
3. Derechos Digitales: https://www.derechosdigitales.org
4. Intervozes: https://intervozes.org.br

I. INTRODUCCIÓN

1. El Estado brasileño fue considerado un referente internacional respecto a la protección de derechos en el ambiente digital con la adopción del Marco Civil de Internet en 2014 y asumió un papel central en la promoción de estándares internacionales a favor de la privacidad en la era digital. Sin embargo, a nivel nacional, la garantía de estos derechos encuentra importantes limitaciones que han comprometido el ejercicio de otros derechos fundamentales en los últimos cinco años, esta situación se agravó durante la pandemia de COVID-19 en 2020 y 2021.
2. Esta contribución se centra en el cumplimiento de las obligaciones de derechos humanos en el contexto digital por parte de Brasil y busca fortalecer recomendaciones enfocadas en la garantía del acceso universal a internet en orden de ejercer la libre expresión y asociación; el acceso a la información, al conocimiento y a la cultura; y el ejercicio de derechos económicos y sociales de manera segura, respetuosa de la privacidad y de la autonomía y libre de cualquier forma de discriminación. Se divide de la siguiente manera: introducción; derechos económicos, sociales y culturales; derechos civiles y políticos; y recomendaciones al Estado brasileño.

II. DERECHOS ECONÓMICOS Y SOCIALES

Acceso a internet

3. Cada vez más el acceso a internet es crucial para el ejercicio de los derechos. Esto se hizo evidente durante la pandemia de COVID-19 en los años 2020 y 2021, cuando gran parte de las actividades escolares, laborales y los servicios estatales comenzaron a realizarse en línea. Datos de 2020 apuntan que el 83% de los domicilios brasileños contaban con alguna forma de acceso a internet y el 81% de la población con más de diez años había accedido a la red. La proporción de hogares con acceso a una computadora ese año fue del 45%.[1]
4. En Brasil, las desigualdades en el acceso a internet reproducen desigualdades estructurales. Cuando se trata de poblaciones en condición de vulnerabilidad, la situación es preocupante: apenas 30% de los brasileños de las clases D/E han usado una computadora una vez en la vida, mientras que los números son mucho mayores en las clases C (66%), B (91%) y A (88%). La desigualdad se observa también cuando se analiza el componente racial: solamente el 52% de personas indígenas y el 57% de las personas negras han utilizado un ordenador al menos una vez en la vida, mientras que, en las personas blancas, el índice es del 64%.[2] El tipo de dispositivo para acceder a internet es otro indicador de la desigualdad: el 62% de las personas indígenas y el 60% de la población negra utiliza la red exclusivamente por el móvil, en un porcentaje superior al de las personas blancas (48%). Cuando se combina con la perspectiva de clase social, esta desigualdad se agrava aún más: el 90% de las personas de las Clases D/E solamente tienen el celular como medio de acceso a internet, una diferencia considerable para las demás: el 58% en la clase C, el 25% en la clase B y el 11% en la clase A.[3] Las desigualdades de acceso son también territoriales y están relacionadas con una distribución desigual de la infraestructura: en el ámbito urbano, el 86% de los domicilios tienen acceso a internet y en el medio rural este índice es de apenas el 65%.[4]

5. Cuando se trata de pueblos, comunidades tradicionales y poblaciones rurales, el derecho de acceso a internet, que está reconocido en el Marco Civil de Internet5, está lejos de ser respetado.[6] La mayoría de estas poblaciones se conectan a través de planes con límite de datos vía celular, los cuales ofrecen un limitado número de aplicaciones, en especial plataformas de redes sociales, a través de acuerdos de zero rating. Los costos de conexión llegan a comprometer más del 30% de los ingresos mensuales de las familias encuestadas, según datos del colectivo Intervozes.

Derecho a la educación

6. Ante el avance de COVID-19, el gobierno brasileño implementó medidas de carácter urgente para que los estudiantes pudieran continuar su proceso de aprendizaje frente a las limitaciones impuestas por la restricción de la circulación y el aislamiento de la población. La falta de planificación y de estructura en las políticas adoptadas, aunada a la precariedad en el acceso a internet de las familias, afectó el éxito de esas medidas y resultó en índices de deserción escolar que representaron un aumento de casi 200% en el rango de 5 a 9 años entre 2019 y 2020.[7]
7. Una encuesta del Instituto Nacional de Investigaciones y Estudios Educativos (INEP) evidenció los impactos del abismo digital para el acceso a la educación en el ámbito rural: dos millones de estudiantes de escuelas rurales pasaron todo el año 2020 sin acceso a contenidos digitales,[8] por lo que la distribución de materiales impresos fue la única alternativa encontrada en diversos lugares. En ocho de los nueve estados del Nordeste brasileño, más del 20% de las escuelas rurales funcionaron exclusivamente de esta forma durante todo el período de distanciamiento físico.[9]
8. Cuando se adoptaron, las políticas de acceso a internet para los estudiantes del sistema público fueron inadecuadas y se centraron poco en la conectividad en el hogar, lo que resultó en la desconexión de varias familias y perjudicó gravemente el acceso a la educación durante la pandemia. Nuevamente, las desigualdades estructurales se reproducen: los datos oficiales indican que las infancias y las juventudes negras e indígenas de escuelas públicas representan más del 70% de estudiantes sin acceso a internet de banda ancha o 3G/4G en el hogar.[10] La situación exacerbó el cuadro de desigualdad entre una élite estudiantil con acceso a internet en condiciones adecuadas para continuar con los estudios y la mayoría de los y las estudiantes de redes públicas con conexiones mínimas a internet, a través de planes de internet móvil y equipos inadecuados para una participación significativa en la rutina escolar.[11]

Derecho a la salud

9. El derecho a la salud se vio afectado por las limitaciones de acceso a internet, pero también por los riesgos para la privacidad y la protección de datos que representa la digitalización de los servicios y, en particular, por las políticas de monitoreo y control implementadas en el contexto de la pandemia de COVID-19.
10. En los ámbitos federal, estatal y municipal se desarrollaron alianzas entre gobiernos y empresas privadas para promover el monitoreo de la propagación de casos o del cumplimiento de las medidas de aislamiento social aplicadas. Éstas involucraban la localización de individuos a través de diferentes tecnologías, como la geolocalización o la conexión a redes celulares, pero presentaban escasas salvaguardas y no fueron precedidas por debates públicos o estudios de impacto en derechos humanos que permitieran prevenir usos abusivos. Además de la exposición a sistemas de vigilancia públicos y privados, algunas soluciones presentaban riesgos de reidentificación de individuos con un importante potencial de discriminación.[12]

11. Las aplicaciones creadas para ofrecer acceso a la información oficial sobre medidas de prevención y tratamiento de COVID-19, así como para ayudar en el monitoreo de su avance (como el Coronavirus SUS, lanzado en 2020 por el gobierno federal) tampoco ofrecieron garantías suficientes con respecto a los datos personales sensibles recopilados y las condiciones de su procesamiento, así como el plazo de almacenamiento, las limitaciones al acceso por parte de terceros, etc.[13, 14]
12. Incluso durante la pandemia, varios episodios de fuga, exposición indebida de datos personales, vulnerabilidades en sistemas, fallas graves y ausencia de seguridad de informaciones sensibles fueron confirmadas en Brasil, explicitando políticas públicas insuficientes para lidiar con datos sensibles recolectados por las autoridades públicas en el ámbito de la salud.[15]

Digitalización del Estado y seguridad social

13. El análisis de las políticas públicas relacionadas con los derechos sociales de prestación, revela que no hay transparencia, capacitación adecuada del personal ni informes de impacto sobre el uso de los datos personales involucrados. La digitalización de las políticas sociales y la falta de una política pública adecuada de acceso a internet y protección de datos impide el disfrute de los derechos sociales e, incluso, puede imponer nuevos obstáculos al ejercicio de otros derechos. Un ejemplo fue el programa de Ayuda de Emergencia, encargado de la transferencia de ingresos a los sectores más vulnerables en el marco del impacto de la pandemia de COVID-19.[16] Otro ejemplo es la implementación de sistemas automatizados en el marco de políticas públicas sin garantías de transparencia y participación o sin la realización de estudios de impacto que analicen potenciales riesgos al ejercicio de derechos, como en el caso del Sistema Nacional de Empleo (SINE).[17]
14. Según datos de TIC Domicílios, en la pandemia de COVID-19 solo el 39% de los hogares rurales buscaron información de salud en internet y solo el 16% realizó servicios públicos en línea (en las zonas urbanas, los índices fueron del 55% y 39%, respectivamente).[18] Mujeres negras, quienes principalmente acceden a internet solo por teléfono móvil (67%), realizaron menos transacciones financieras (37%), accedieron a menos servicios públicos (31%) y cursos en línea (18%) que los hombres blancos (51%, 49% y 30%, respectivamente).[19]
15. La falta de acceso a internet 3G/4G en el móvil fue una razón para que el 39% de los usuarios de la Clase C, D y E dejaran de acceder a políticas públicas, de modo que el 33% dejó de acceder a servicios públicos y el 28% dejó de recibir algún beneficio social, como el programa Ayuda de Emergencia.[20]

III. DERECHOS CIVILES Y POLÍTICOS

Privacidad y protección de datos

a. Tecnologías de vigilancia, reconocimiento facial y bases de datos biométricas

16. La utilización de tecnologías de vigilancia con sistemas de reconocimiento facial se ha ampliado en los ámbitos público y privado en Brasil,[21] lo que pone en riesgo el ejercicio de derechos fundamentales principalmente de personas en situación de vulnerabilidad,

mujeres, personas negras, pobres y transexuales.[22] El sector público ha utilizado el reconocimiento facial para diversos fines como la seguridad pública, el transporte urbano, las escuelas, la gestión de beneficios sociales, el control aduanero y la validación de identidad.[23]

17. Con respecto a la seguridad pública, el Ministerio de Justicia y Seguridad Pública emitió dos ordenanzas, en 2019 y 2020, destinadas a promover la implementación de cámaras de vigilancia con tecnologías de reconocimiento facial por parte de los organismos de seguridad pública.[24] Aunque estas disposiciones ya no están en vigor, demostraban el interés del gobierno federal en utilizar datos biométricos para tales fines.
18. En julio de 2021, la Policía Federal anunció la implementación de la Solución Automatizada de Identificación Biométrica con el objetivo de unificar bases de datos de secretarías de seguridad pública estatales.[25] En este contexto, es relevante destacar que desde 2018 se encuentra en vigencia la Ley 13.675/2018, que instituye el Sistema Único de Seguridad Pública (SUSP) y prevé la integración, entre otros, de bases de datos de perfiles genéticos y digitales.[26] En paralelo, se identifica una creciente implementación de herramientas de reconocimiento facial aplicadas en imágenes recolectadas en espacios públicos o accesibles al público en diferentes estados de Brasil.[27]]
19. El uso de reconocimiento facial para fines de seguridad pública genera gran preocupación por diversos factores: en primer lugar, la Ley General de Protección de Datos (LGPD) brasileña, Ley 13.709/2018, no regula el tratamiento de datos para fines de seguridad pública y persecución criminal, determinando qué ley específica debe regular la materia. Además, se identifica una falta general de transparencia que permita a la sociedad civil analizar adecuadamente si el uso de esas tecnologías biométricas contiene parámetros mínimos de legalidad, necesidad y proporcionalidad.[28] También hay múltiples denuncias públicas sobre la reproducción de expedientes racistas en la implementación de estas herramientas.[29]
20. A pesar de la falta de datos oficiales sobre el uso de este tipo de tecnología y sus resultados, estudios independientes indican que la gran mayoría de la población que es arrestada sobre la base del reconocimiento facial es negra.[30] En una encuesta de marzo a octubre de 2019, 151 personas fueron detenidas en cinco estados, de las cuales el 90% eran negras.[31]
21. Además de la seguridad pública, los sistemas de reconocimiento facial se han implementado en diferentes espacios: se está probando su uso la identificación de pasajeros para el embarque en aeropuertos[32], así como en escuelas públicas[33], en el transporte público, entre otros.
22. Según lo declarado por diversas autoridades internacionales, incluida la Alta Comisionada de Derechos Humanos, el reconocimiento facial en espacios públicos representa graves riesgos para los derechos humanos. Por ello, Michelle Bachelet pidió una moratoria del uso de este tipo de tecnologías en los espacios públicos.[34]

b. Ciberdelincuencia y criminalización de la defensa de los derechos humanos en el ámbito digital

23. En diciembre de 2021, Brasil aprobó la adhesión a la Convención de Budapest sobre Delitos Cibernéticos. El texto fue aprobado sin reservas por el Estado brasileño y genera preocupaciones relativas a la criminalización de investigadores y activistas de la seguridad de la información. Esto se debe a que el texto y las penas previstas se aplican sin consideraciones relacionadas con la existencia de una intención maliciosa en caso de intrusión en sistemas informáticos. El riesgo se agrava ante la ausencia de un marco robusto para la protección de datos personales en la esfera criminal[35] y una inclinación

legislativa que apunta a la violación de la seguridad de defensores y defensoras de derechos digitales.

24. Esta tendencia se puede ver en el marco de la Ley del Estado Democrático, que recientemente reemplazó a la Ley de Seguridad Nacional en el país. En la elaboración de la nueva ley se debatieron cuestiones como la tipificación del crimen de espionaje, sin aportar ninguna salvedad o seguridad al trabajo de fiscalización realizado por periodistas y la sociedad civil que muchas veces se vale de trabajos de la prensa internacional o de denunciantes (whistleblowers) para defender derechos fundamentales.[36] El debate de estas medidas denuncia el riesgo de criminalización de actividades relacionadas a la seguridad de la información y activismo digital en el país, reproduciendo tendencia identificada internacionalmente.[37]
25. El acceso a los sistemas informáticos puede conducir a la detección y alerta de fallos de seguridad relevantes y a la obtención de información sobre la violación de los derechos humanos. La posibilidad de criminalización de conductas relacionadas con el último caso, puede desalentar la divulgación de esas informaciones de crucial interés público, principalmente considerando que Brasil no posee una legislación integral para proteger las actividades de denunciantes, también llamados "whistleblowers".
26. En 2015, el entonces relator especial de la ONU para la Libertad de Expresión, David Kaye, destacó que la criptografía y el anonimato en línea son condiciones fundamentales para el ejercicio de la libertad de expresión.[38] En ese sentido, las medidas que excluyen el anonimato, como la presente en la Constitución brasileña, no deben interpretarse de manera que creen un escenario en el que los investigadores de seguridad de la información y otros activistas online estén desprotegidos o sometidos a constante vigilancia, como podrían indicar algunos extractos de la Convención de Budapest, aprobada íntegramente en el país. La inclusión de barreras a la identificación de personas online es una postura legítima conforme a los parámetros internacionales de derechos humanos y no viola el sellado del anonimato, entre otros motivos, porque no impide completamente una identificación y atribución de responsabilidades posteriores, cuando sea necesario.

Libertad de expresión, violencia y acceso a la información

e. Vigilancia de periodistas y personas defensoras de derechos humanos

27. En los últimos años ha habido una creciente adopción de medidas de cibervigilancia a la población llevadas a cabo por agencias vinculadas al gobierno federal que involucran intentos de adquirir sistemas de espionaje, mismos que han sido cuestionados por autoridades internacionales de derechos humanos. La Secretaría de Operaciones Integradas (Seopi), un organismo vinculado al Ministerio de Justicia y Seguridad Pública del gobierno federal, por ejemplo, contrató mediante licitación pública un sistema de espionaje de la empresa Harpia tecnologia Eireli; la licitación fue suspendida por el Tribunal de cuentas de la Unión en noviembre de 2021.[39] Denuncias también apuntan a un supuesto intento de coordinación para la contratación del sistema Pegasus por parte de Carlos Bolsonaro, hijo del presidente de la República[40], a pesar de la ausencia de competencia legal para interferir en procedimiento administrativo relativo a operaciones de inteligencia en ámbito federal, de incumbencia exclusiva de la Agencia Brasileña de Inteligencia (ABIN). La prensa también informó sobre intentos de comprar otros sistemas de vigilancia en 2022, entre ellos la herramienta llamada DarkMatter.[41]
28. Además de las denuncias de compra de sistemas de vigilancia con enorme potencial para la violación de derechos fundamentales, el gobierno también ha utilizado OSINTs - sigla usada en inglés para describir Inteligencia de Código Abierto- en investigaciones

realizadas por ministerios públicos estatales y federales sin que exista regulación correspondiente.[42] La práctica deja espacio para posibles violaciones de derechos humanos: en Los informes de 2021 indican la clasificación y categorización de personas por parte del gobierno desde sus posiciones políticas con el propósito de monitorear las posiciones políticas.[43] Este tipo de monitoreo ya ha tenido como resultado la detención de un hombre a causa de informaciones publicadas en su perfil de red social, contenido que fue considerado por la policía militar como "incitación a la violencia" contra el presidente.[44] El individuo no representaba a ningún grupo u entidad organizada y la vigilancia estuvo basada en su visión crítica de la administración actual.

29. Otro ejemplo de las prácticas de vigilancia crecientes fue la elaboración de un" dossier antifascista " por el Ministerio de Justicia del gobierno federal en 2020.[45] El informe buscaba mapear a los trabajadores de la administración pública contrarios a Bolsonaro a partir de la recopilación de información disponible en las redes sociales sobre estos individuos.[46] La Corte Suprema Federal falló en 2021 para prohibir la redacción del expediente.[47]

b. Violencia de género en línea

30. En un país marcado por altos índices de violencia intrafamiliar y violencia de género, los medios digitales se han utilizado cada vez más para atacar a mujeres y personas LGBTQIA+. Las formas de ataque involucran fotomontajes racistas, invasión de cuentas en redes sociales con motivaciones racistas y misóginas, amenazas, difamación, acusaciones falsas, entre otras.[48]
31. Durante la pandemia, con la migración de buena parte de las actividades de grupos activistas al contexto virtual, se multiplicaron denuncias de ataques, así como las intrusiones en reuniones con la exposición de imágenes y sonidos impactantes, fenómeno que se conoció como "zoombombing", ya que inicialmente ocurrían con más frecuencia en la plataforma Zoom.[49]
32. En 2021, la Central Nacional de Denuncias de Delitos Cibernéticos de Safernet en Brasil, recibió 5.347 denuncias de LGBTfobia, 6.888 denuncias de racismo y 8.174 denuncias de violencia y discriminación contra mujeres.[50]

c. Desinformación y discurso político violento

33. En Brasil, la violencia de género en línea se mezcla, en diversas ocasiones, con violencia política. Por ejemplo, cuando autoridades públicas utilizan sus redes sociales personales para atacar o repercutir en ataques contra periodistas y activistas mujeres. Asimismo, el propio presidente Jair Bolsonaro, en distintas ocasiones, exponiendo a periodistas mujeres, cuestionando sus motivaciones, desinformando, haciendo insinuaciones de carácter sexual y/o compartiendo datos personales de las profesionales que investigan denuncias de corrupción que involucran al gobierno federal o a los familiares del presidente, en un evidente ataque a su libertad de expresión. Un ejemplo fueron las declaraciones relativas a Constanza Resende en 2019; en esa ocasión, el presidente compartió un audio falso para insinuar parcialidad en el trabajo de la periodista.[51] En 2018, los administradores de las cuentas de la periodista Patricia Campos Mello también fueron blanco de ataques tras la publicación de un reportaje de la periodista sobre posibles ilegalidades en la campaña de Bolsonaro.[52] Estos y otros casos han sido llevados a la Comisión Interamericana de Derechos Humanos a través de audiencias realizadas en 2020.[53]

34. En 2018, durante la campaña electoral presidencial, se verificaron varios ataques en línea contra grupos políticos y periodistas. En septiembre de ese año, un grupo de Facebook llamado "Mujeres contra Bolsonaro" fue clausurado y sus moderadoras recibieron ataques directos.[54]

35. La violencia política en línea y la desinformación también afectan a candidatos, candidatas y personas elegidas. En una sociedad marcada por el racismo, la homofobia y la transfobia, es aún más intensa la violencia para integrantes de grupos históricamente vulnerados. Un levantamiento de TretAqui.org mostró que el machismo, el odio ideológico, el racismo y la LGBTfobia fueron los principales temas de ataques contra las candidaturas en la primera vuelta de las elecciones de 2020.[55]

36. La difusión de contenidos desinformativos ha estado dirigida al ataque a las instituciones democráticas, buscando comprometer la confianza de la población en los comicios electorales. Son notables los perjuicios de la desinformación para los derechos humanos y para la democracia, también fuera de los períodos electorales. La difusión de la desinformación también ocurre por medio de agentes públicos que contribuyen activamente a la creación de un ambiente polarizado y anti democrático.[56]

37. Jair Bolsonaro, su familia y otros actores políticos que lo apoyan han estado utilizando las plataformas de redes sociales para movilizar e inflamar su base ultraconservadora. El presidente ya ha sido acusado de prácticas de discursos de odio y xenofobia debido a ataques a minorías y grupos marginados, como a personas negras, mujeres y población LGBTQIA+.[57] La postura del presidente en las redes sociales llegó a la exclusión y bloqueo de determinados contenidos publicados por las propias plataformas.[58]

38. Los debates sobre la desinformación y la violencia en el discurso político también se relacionan con el papel de las plataformas de redes sociales y la falta de transparencia en la curación y priorización del contenido, como lo demuestra la investigación realizada por Intervozes[59] y como lo destacan con preocupación las organizaciones de la región.[60]

d. Medidas legislativas y judiciales para la regulación del discurso online

39. En los últimos años, se han propuesto varias iniciativas legislativas con el objetivo de responder a los desafíos de la digitalización, como la concentración de las grandes plataformas digitales, políticas abusivas relacionadas con la explotación de datos personales, y la baja capacidad de respuesta de esas mismas plataformas a la proliferación de discursos de odio en sus redes. Muchos de estos proyectos, a pesar de buscar fines supuestamente legítimos, acaban adoptando mecanismos inefectivos y desproporcionados, que pueden presentar un riesgo real a la libertad de expresión. Dos ejemplos importantes en los últimos cinco años han sido el intento de legislar sobre la responsabilidad de los intermediarios y sobre la desinformación.[61]

40. El rechazo de las medidas de filtrado y bloqueo o la promoción de un sistema de notificación judicial para responsabilizar a los intermediarios por el contenido de terceros, fue establecido como un baluarte central para garantizar la libertad de expresión online. Es lo que prevé el Marco Civil de Internet en Brasil. El objetivo es proteger las plataformas y los motores de búsqueda de responsabilidades indebidas por el comportamiento de los usuarios y, por lo tanto, desalentar la eliminación de contenido sin una orden judicial. Sin embargo, los desafíos recientes con la diseminación de contenidos dañinos a través de redes sociales, así como la comprensión del papel de las grandes plataformas en la priorización o no de esos contenidos, han generado nuevos intentos de responsabilización. En el Congreso Nacional tramitaron en 2022, más de 30 proyectos que tienen el objetivo de combatir la desinformación. Parte de ellos tiene como objetivo modificar el Marco Civil de Internet en temas como la privacidad, la libertad de expresión y la responsabilidad de los intermediarios.

41. En 2021, Bolsonaro intentó, por medio de una Medida Provisional (MP 1.068), incorporar nuevas reglas para la moderación de contenidos en plataformas digitales y cambiar el régimen jurídico establecido por el Marco Civil. La medida requeriría más burocracia para suspender o cancelar cuentas, así como para determinar la restitución de contenido prohibido, y se presentó en un contexto de presión judicial para la eliminación de contenido abusivo compartido por los partidarios del presidente. La Medida Provisional - acto del Poder Ejecutivo - no consistió en un mecanismo legal adecuado para innovar en la reglamentación de ese tema y fue devuelta al Poder Ejecutivo, perdiendo efectividad. Esta medida se convirtió en otro proyecto de ley sobre el tema, actualmente está en discusión en el Congreso Nacional.[62]
42. También se está tramitando en el Poder Legislativo el Proyecto de Ley (PL) n. 2630/2020, conocido como "PL de las Fake News". Inicialmente, fue objeto de preocupaciones por las medidas de control previstas, el PL es revisado y propone una serie de determinaciones relativas a la regulación de las plataformas digitales y la previsión de los principios de la administración pública, que deben ser aplicados también a los perfiles de las redes sociales de los agentes políticos.
43. Los bloqueos de aplicaciones también han sido objeto de preocupación y ha sido debatidos desde 2016 por la Corte Suprema, luego de una serie de decisiones judiciales que determinaban el bloqueo integral de la aplicación, por incumplimiento de medidas que involucraban el acceso al contenido de mensajes, incluso con la ruptura del cifrado de extremo a extremo. El juicio está suspendido desde 2021.[63] En marzo de 2022, el ministro Alexandre de Moraes ordenó el bloqueo de la aplicación Telegram en todo el territorio nacional, determinando multas diarias por un valor de 100 mil reales para cualquier persona que intentara utilizarlo.[65] La orden fue revocada tres días después.[65] El bloqueo de Telegram también ha sido propuesto por el Tribunal Superior Electoral, debido a la falta de respuesta con respecto a la contribución con las autoridades brasileñas.[66]
44. Finalmente, la expansión de medidas que criminalizan la expresión legítima en línea continúa siendo un área de extrema preocupación. Las medidas contenidas en la Ley del Estado Democrático antes mencionada, por ejemplo, criminalizan ampliamente la llamada "desinformación masiva" o "insurrección" y la "propagación de hechos que se sabe que no son ciertos", esto puede profundizar un ambiente de autocensura que impacta no solo la libertad de expresión, sino también acceso a la información.[67]

e. Acceso a la información y protección de datos personales

45. Desde el 2011, el Estado brasileño cuenta con una Ley de Acceso a la Información (LAI), la cual ha posibilitado más de un millón de solicitudes de información dirigidas a órganos y entidades del Poder Ejecutivo Federal. Sin embargo, diez años después de su aprobación, se han observado repetidos intentos de enmendar la LAI, especialmente a través de decretos y ordenanzas, que resultan en amenazas a la transparencia en el país. Entre ellas destacamos la MP 928/2020, que intentó imponer, sin éxito, la suspensión de los plazos de respuesta a las solicitudes de acceso a la información durante la pandemia; el Decreto 9.690/2019, que intentó aumentar drásticamente el número de autoridades con poder de veto en el acceso a la información; y la Ordenanza 880/2019, que trivializa el secreto de documentos producidos por el Ministerio de Justicia y Seguridad Pública.
46. Por otro lado, ha aumentado en los últimos años una interpretación expansiva y abusiva del artículo 31 de la LAI, que se refiere al tratamiento e intercambio de información personal, para justificar que se oculte información de interés público, lo que es un ataque al derecho de acceso. El análisis de estos casos indica que la clasificación adoptada va en contra del propósito por el cual se promulgó la LAI: establecer la transparencia como regla y el secreto como excepción. Los datos considerados confidenciales bajo esta regla

se refieren a los nombres de los servidores que publican en el perfil de Twitter de la Secretaría de Comunicación; los datos de las tarjetas de acceso de los hijos del presidente al Palacio del Planalto; el proceso disciplinario que absolvió a un general y ex ministro de salud por haber participado en una manifestación política junto al presidente, entre otros. La antes mencionada LGPD, aprobada en 2018, también ha sido utilizada inapropiadamente como pretexto para negar el acceso a informaciones públicas.[68]

47. En contradicción con el supuesto intento de protección de datos personales, el Gobierno vetó en el marco de la LGPD, en 2019, un importante mecanismo que apuntaba a la prohibición del intercambio de datos personales de solicitantes de información con instituciones públicas o personas jurídicas del derecho privado.[69] Su objetivo era proteger la identidad de los solicitantes de información, para evitar negativas infundadas de acceso, posibles restricciones o represalias o persecución.

48. Los ataques a la transparencia pública identificados pueden dificultar el monitoreo de las acciones gubernamentales por parte de la ciudadanía e impedir la investigación de eventuales delitos de responsabilidad; por ejemplo, en la gestión de las medidas para enfrentar a la pandemia, o de la implicación de agentes del gobierno en la preparación y divulgación de informaciones falsas y discursos de odio en Internet. Las acciones enumeradas subvierten, por principio, la premisa que orientó el establecimiento y promulgación de leyes como la LAI y la LGPD: la protección de la población común frente al Estado, y no el blindaje de acciones de agentes políticos poderosos ante el escrutinio público.

IV. RESUMEN DE LAS RECOMENDACIONES AL ESTADO BRASILEÑO

49. Frente a las violaciones identificadas al ejercicio de derechos humanos en el ambiente digital en Brasil, sus impactos para el goce de derechos en el contexto offline y, consecuentemente, el incumplimiento con los compromisos internacionales asumidos por el país, incluso con el alcance de los Objetivos de Desarrollo Sostenible, recomendamos al Estado brasileño:

A. La creación urgente de políticas públicas de inclusión digital que incluyan un plan de metas priorizando poblaciones en condición de vulnerabilidad y que consideren:

a. La universalización del acceso a internet de calidad;
b. La amplia participación de la población en los procesos de formulación, revisión y evaluación de políticas de conectividad, incluso de poblaciones rurales, pueblos y comunidades tradicionales;
c. La educación para los medios digitales enfocada en la recepción crítica de contenidos, en prácticas de comunicación basadas en principios de derechos humanos y en la seguridad digital;
d. La promoción de alternativas para la conectividad, incluso a través de redes comunitarias, con garantía de asesoramiento técnico gratuito a los territorios de pueblos y comunidades tradicionales;

B. La producción y divulgación periódica de datos y estadísticas actualizadas y desagregadas por etnia, género, edad, localidad y renta, sobre el acceso a internet en el país, con el fin de orientar la formulación de políticas públicas e inclusive eventuales medidas de emergencia, en contextos de aislamiento social en el ámbito de la educación, salud y /o asistencia social para evitar el agravamiento de desigualdades estructurales preexistentes;

C. La adopción urgente de medidas transversales para la adecuación de los servicios públicos a las exigencias de la Ley General de Protección de Datos con respecto a los derechos de las personas titulares de los datos procesados por el Poder Público, incluyendo:

a. Garantía de que terceros involucrados en el tratamiento de estos datos obedezcan a las normativas vigentes;
b. Garantía de la integridad y corrección de las vulnerabilidades encontradas en los sistemas electrónicos estatales, incluso del Ministerio de Salud, así como garantizar políticas de seguridad, contención de datos existentes y remedios apropiados en caso de fugas y exposición indebida de datos personales, en particular, datos sensibles;
c. Oferta de información transparente sobre los criterios de recolección, procesamiento e intercambio de información y la creación de canales para la solución de dudas y respuesta a requerimientos relacionados a la gestión de datos personales.

D. La adopción urgente de medidas para fortalecer la independencia de la autoridad nacional de protección de datos a fin de que pueda supervisar el cumplimiento de las normas previstas en la LGPD por parte de las instituciones públicas y privadas, así como presentar lineamientos sobre la interpretación de las disposiciones previstas en la ley;

E. La abstención de implementar políticas de digitalización, automatización o inteligencia artificial en el sector público sin antes contar con los siguientes requisitos, los cuales también deberían considerarse en contextos de eventual emergencia:

a. Estudios de impacto que garanticen que las políticas no generarán una profundización en desigualdades históricas, discriminación o riesgos al ejercicio de derechos humanos, incluidos los derechos económicos y sociales y la privacidad;
b. Procesos de consulta previa que involucren a los grupos potencialmente afectados y/o sus representantes;
c. Planes de seguimiento y evaluación periódicos independientes y transparentes;
d. Garantías explícitas en relación al ejercicio de los derechos de revisión, reparación y no repetición de prácticas ilícitas hacia la ciudadanía.

F. La adopción de una moratoria que limite el uso de tecnologías de reconocimiento facial en espacios públicos, hasta que exista un consenso internacional sobre la seguridad de estas tecnologías con respecto al cumplimiento de los derechos humanos y la prohibición de su uso con fines de seguridad pública o control de acceso a espacios o servicios estatales;

G. Garantía de respeto y de la adopción de reglas que limiten el uso de tecnologías de vigilancia más allá del reconocimiento facial a los principios de legalidad, necesidad y proporcionalidad establecidos por los estándares de derechos humanos; definir mecanismos de reparación legal consistentes con la obligación de proporcionar a las víctimas de abuso un recurso efectivo; y crear mecanismos que aseguren la aprobación, supervisión y control público o comunitario sobre la compra de tecnologías de vigilancia.

H. La revocación, no adopción o revisión de normas que faciliten la vigilancia online y la criminalización de activistas de derechos humanos y de seguridad de la información; y atención a criterios de legalidad, necesidad y proporcionalidad en la implementación de cualquier acción de intervención en comunicaciones privadas, según lo establecido por los marcos internacionales de derechos humanos ratificados por Brasil;

I. La adopción de normas y prácticas estatales de respeto a la criptografía y al anonimato online como factores importantes para el ejercicio de derechos humanos, así como la garantía de protección a denunciantes de violaciones de derechos humanos, por medio de la edición de una normativa específica sobre el tema;

J. La creación de políticas públicas y medidas adecuadas para combatir todas las formas de violencia de género, en línea y fuera de línea;

K. La adopción de medidas para combatir la financiación de campañas desinformativas con recursos públicos, teniendo en cuenta las obligaciones y principios internacionales de derechos humanos;

L. El rechazo de legislaciones abusivas de regulación de contenidos en redes sociales y plataformas de mensajería que promuevan la responsabilidad de los intermediarios, violando los principios establecidos en documentos internacionales de derechos humanos y el Marco Civil de Internet. Se recomienda también que la necesaria regulación de las grandes plataformas digitales sea fruto de un debate amplio y multisectorial, con todas las partes interesadas, las cuales respeten los estándares internacionales de derechos humanos.

M. La adopción de medidas para garantizar el respeto a la legislación existente que regula el acceso a la información pública, sin la instrumentalización de la protección de datos para impedir ese acceso. El análisis del cumplimiento de los principios de legalidad, necesidad y proporcionalidad en la restricción del derecho a la privacidad es necesario también para evaluar el interés público frente a informaciones que están bajo tutela del Estado.

V. REFERENCIAS

1. Cetic.br, 2020. Executive Summary: ICT Household Survey 2020. Disponible en: https://www.cetic.br/media/docs/publicacoes/2/20211124201635/executive_summary_ict_households_2020.pdf
2. Cetic.br, 2020. ICT Household Survey 2020. Disponible en: https://cetic.br/pt/tics/domicilios/2020/individuos/B1/.
3. Cetic.br, 2020. ICT Household Survey 2020. Disponible en: https://cetic.br/pt/tics/domicilios/2020/individuos/C16A/
4. Cetic.br, 2020. ICT Household Survey 2020. Disponible en: https://cetic.br/pt/tics/domicilios/2020/domicilios/A4/.
5. Marco Civil da Internet no Brasil, Lei n. 12.965/2014. Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.
6. Intervozes, 2022. Territórios Livres, Tecnologias Livres. Disponible en: http://territorios-livres.online/.
7. Neri, M. & Osorio, M., 2022. Retorno para Escola, Jornada e Pandemia. Disponible en: https://www.cps.fgv.br/cps/RetornoParaEscola/.
8. Intervozes, 2022. Territórios Livres, Tecnologias Livres. Disponible en: http://territorios-livres.online/.
9. Intervozes, 2022. Territórios Livres, Tecnologias Livres. Disponible en: http://territorios-livres.online/.
10. IPEA, 2020. Nota técnica n. 88. Acesso domiciliar à internet e ensino remoto durante a pandemia. Disponible en: http://repositorio.ipea.gov.br/bitstream/11058/10228/1/NT_88_Disoc_AcesDomInternEnsinoRemoPandemia.pdf.
11. Nogueira, J., 2021. Acesso à internet residencial de estudantes. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: https://sur.conectas.org/orbitando-telas/; Coding Rights, 2021. Reconhecimento Facial no Setor Público e Identidades Trans. Disponible en: 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. Disponible en: https://lapin.org.br//download/4141/.
24. Biblioteca Digital do Ministério da Justiça e Segurança Pública. Portaria nº 793, of October 24, 2019. Disponible en: <https://dspace.mj.gov.br/handle/1/1380>; Portaria nº 630, of November 27, 2020. Disponible en: <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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: https://piaui.folha.uol.com.br/nos-erros-de-reconhecimento-facial-um-caso-isolado-atras-do-outro/.
30. Monitor do reconhecimento facial no Brasil. Disponible en: https://opanoptico.com.br/.
31. Folha de S. Paulo, 2019. 151 pessoas são presas por reconhecimento facial no país; 90% são negras. Disponible en: 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. Disponible en: https://www4.infraero.gov.br/imprensa/noticias/aeroporto-de-con-

gonhas-testa-embarque-por-reconhecimento-facial-com-tripulantes/; SERPRO. Embarque nos aeroportos brasileiros poderá ser realizado sem apresentação de documentos. Disponible en: 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. Disponible en: 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? Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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." Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: https://twitter.com/oea_cyber/status/1174752582583181313.
43. The Intercept, 2021. Governo Bolsonaro deturpou edital de Dilma para fichar 'detratores' na internet. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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'. Disponible en: 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. Disponible en: https://exame.com/brasil/apos-twitter-facebook-e-instagram-removem-posts-de-bolsonaro/; G1, 2021. YouTube remove live de Bolsonaro com mentira sobre vacina da Covid e

Aids e suspende canal por uma semana. Disponible en: https://g1.globo.com/tecnologia/noticia/2021/10/25/youtube-live-bolsonaro.ghtml.

59. Intervozes, 2021. Fake news: how platforms face disinformation. Disponible en: https://intervozes.org.br/publicacoes/fake-news-how-platforms-combat/.
60. Several, 2021. Declaración Latinoamericana sobre Transparencia de Plataformas de Internet. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: 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. Disponible en: https://artigo19.org/2019/07/10/entre-vetos-preocupantes-presidencia-tenta-derrubar-protecao-de-dados-pessoais-de-requerentes-de-informacao-publica/.