WhatsApp y transparencia: un análisis sobre los efectos de la opacidad de las plataformas digitales en las agendas de investigación en comunicación política en Brasil

WhatsApp and transparency: an analysis on the effects of digital platforms' opacity in political communication research agendas in Brazil

Viktor Chagas; Gabriella Da-Costa

Note: This article can be read in its English original version on:
https://revista.profesionaldelainformacion.com/index.php/EPI/article/view/87120

Cómo citar este artículo.
Este artículo es una traducción. Por favor cite el original inglés:

Chagas, Viktor; **Da-Costa, Gabriella** (2023). "*WhatsApp* and transparency: an analysis on the effects of digital platforms' opacity in political communication research agendas in Brazil". *Profesional de la información*, v. 32, n. 2, e320223.

https://doi.org/10.3145/epi.2023.mar.23

Artículo recibido el 20-09-2022
Aceptación definitiva: 01-02-2023

Viktor Chagas ✉
https://orcid.org/0000-0002-1806-6062

Fluminense Federal University
Department of Media and Cultural Studies
Rua Professor Marcos Waldemar de Freitas Reis, s/n
Niterói, RJ CEP: 24210-201 Brasil
viktor@midia.uff.br

Gabriella Da-Costa
https://orcid.org/0000-0002-4234-4544

Fluminense Federal University
Communication Graduate Program
Rua Professor Marcos Waldemar de Freitas Reis, s/n
Niterói, RJ CEP: 24210-201 Brasil
gabrielladacosta@gmail.com

Resumen

Este artículo tiene como objetivo discutir lo que llamamos opacidad ambiental, una condición típica de los servicios de mensajería instantánea móvil que operan en base a sistemas de encriptación de extremo a extremo. Partiendo del caso particular de *WhatsApp*, el artículo presenta dos dilemas fundamentales en torno a los cuales se moviliza el tema de la transparencia cuando se trata de comunicación privada digital. El primero se refiere a cómo el cifrado de extremo a extremo es a la vez un activo y un problema para las democracias, ya que protege la privacidad de los usuarios, pero termina permitiendo la circulación de información errónea y contenido dañino. El segundo se refiere a cómo esta opacidad impacta en la ética y la transparencia de la propia investigación académica. El texto también busca presentar una extensa revisión de estudios que han buscado abordar los usos políticos de *WhatsApp* en diferentes dimensiones, y argumenta que países emergentes con grandes bases de usuarios, como Brasil e India, han experimentado una serie de efectos negativos en función de la adopción de *WhatsApp* por parte de grupos políticamente orientados. Entre las principales proposiciones, el artículo sugiere la adopción de medidas que den mayor transparencia a la plataforma y faciliten, en lugar de entorpecer, la investigación científica.

Palabras clave

Transparencia algorítmica; *WhatsApp*; Opacidad ambiental; Comunicación política; Privacidad; Transparencia; Servicios de mensajería instantánea móvil; Ética de la investigación; Políticas.

Abstract

This article aims to discuss what we call environmental opacity, a condition of mobile instant messaging services (MIMS) that operates on the basis of end-to-end encryption systems. Utilizing *WhatsApp* as a specific example, the article presents two fundamental dilemmas around which some issues concerning transparency are mobilized when it comes to digital private communication. The first of them relates to how end-to-end encryption has simultaneously become an asset and a problem for democratic environments; on the one hand, protecting users' privacy, and on the other, allowing for the circulation of misinformation and harmful content. The second dilemma deals with how this environment of opacity impacts the ethics and transparency of scholarly research focused on *WhatsApp* and other MIMSs. The paper also reviews an extensive body of studies that discuss the political uses of *WhatsApp* in different dimensions, and argues that emerging countries with large user bases, such as Brazil and India, have experienced a series of negative effects after the adoption of *WhatsApp* by politically oriented groups. Among the main proposals, the article suggests some measures to foster platform transparency and facilitate scientific research instead of hindering it.

Keywords

Algorithmic transparency; *WhatsApp*; Environmental opacity; Political communication; Privacy; Mobile instant messaging services; Research ethics; Policies.

Financiación

Este artículo cuenta con el apoyo del *Conselho Nacional de Desenvolvimento Científico e Tecnológico-CNPq* (Beca de Productividad PQ-2 No. 306791/2021-8) y de la *Fundação Carlos Chagas Filho de Amparo à Pesquisa* del Estado de Río de Janeiro (Becas No. 259788 y No. 249104). Este estudio fue aprobado por el *Comité de Ética* de la *Universidade Federal Fluminense*, permiso No. 29720620.8.0000.5243.

1. Introducción

En la última media década, los servicios de mensajería instantánea móvil (MIM) se han convertido en motivo de preocupación para los gobiernos, la sociedad civil y los investigadores académicos, debido a su opacidad y a la dificultad de controlar la circulación de contenidos perjudiciales para la democracia, como la desinformación y el discurso de odio, que suelen inundar los grupos de discusión que albergan (**Rossini**; **Stromer-Galley**; **De-Oliveira**, 2020; **Banaji**; **Bhat**, 2019). Hay una reciente pero vasta bibliografía que ha buscado discutir estas plataformas, con énfasis en servicios específicos, como *WhatsApp* (**Bursztyn**; **Birnbaum**, 2019), *Telegram* (**Willaert** *et al.*, 2022; **Santos**; **Saldaña**; **Tsyganova**, 2021) y *WeChat* (**Wu**; **Wall**, 2019), entre otros. Y aunque, entre estos tres ejemplos, los servicios de mensajería privada rusos y chinos plantean igualmente desafíos para sus respectivos contextos, es *WhatsApp*, debido a su enorme popularidad, especialmente en países no occidentales como Brasil y la India, el que ha impulsado el debate público en torno a cuestiones como:

- difusión de noticias falsas (**Resende** *et al*., 2019; **Sacramento**; **Paiva**, 2020);
- aumento de la desconfianza en las instituciones democráticas (**Piaia**; **Alves**, 2020);
- radicalización política (**Evangelista**; **Bruno**, 2019);
- discurso peligroso (**Saha** *et al*., 2021; **Matamoros-Fernández**, 2020).

En todos estos casos se discute mucho sobre estrategias para limitar la difusión masiva de ciertos contenidos y soluciones técnicas para contener el daño a la democracia (**Resende** *et al*., 2019), pero poco o nada se ha discutido sobre los efectos de la opacidad ambiental en las culturas de las plataformas y los valores compartidos por los usuarios de estos servicios, ni sobre los desafíos prácticos para implementar controles democráticos y monitorear estos medios.

Este artículo explora la relación intrínseca entre opacidad y transparencia y entre privacidad y publicidad, derivada del uso político y la investigación académica de los servicios de mensajería instantánea móvil. Nuestro principal objetivo es debatir los retos que plantean los servicios de mensajería privada, en particular *WhatsApp*, al contexto de la transparencia democrática, y cómo afrontarlos. Por lo tanto, el artículo tiene tres secciones:

En la primera presentamos una breve contextualización sobre cómo *WhatsApp* se ha convertido en uno de los principales protagonistas del escenario político brasileño (**Moura**; **Michelson**, 2017), y cómo otros países también han enfrentado situaciones derivadas de la forma en que grupos disidentes han hecho uso del servicio (**Al-Zidjaly**, 2017). Brasil, junto con la India, constituye un caso ejemplar para el análisis. El país cuenta con la segunda mayor base de usuarios del servicio en todo el planeta, y fue quizá el primero en sufrir un duro revés debido a la propagación de noticias falsas y ataques a la democracia en los grupos de debate público de *WhatsApp*. En las elecciones parlamentarias de la India en 2019 (**Garimella**; **Eckles**, 2020), y, en el mismo año, en las elecciones generales de Indonesia (**Baulch**; **Matamoros-Fernández**; **Suwana**, 2022), se temió un efecto similar, y Brasil fue evocado como ejemplo

> Este artículo explora la relación intrínseca entre opacidad y transparencia y entre privacidad y publicidad, derivada del uso político y la investigación académica de los servicios de mensajería instantánea móvil

negativo en varias circunstancias (**Murgia**; **Findlay**; **Schipani**, 2019). Así pues, en esta primera sección del artículo, analizamos cómo y por qué *WhatsApp* ha suscitado preocupación en diferentes democracias.

En la segunda sección, ponemos a *WhatsApp* y a otras plataformas digitales en contexto, con el fin de profundizar en un debate en torno a lo que la bibliografía ha tratado de denominar "transparencia algorítmica" (**Diakopoulos**, 2014). Más específicamente, discutimos las políticas de regulación y moderación de contenidos asumidas por la propia plataforma y los efectos de sus acciones sobre los usuarios. Desde 2018, en Brasil, *WhatsApp* incorporó una serie de restricciones al reenvío de mensajes (**Porter**, 2020), promovió el baneo escalonado de varios usuarios (**Mari**, 2019) y buscó desarrollar alianzas institucionales con agentes estatales, como el *Tribunal Superior Eleitoral* brasileño (*TSE*, 2022). Como contrapunto, uno de sus principales rivales, la rusa *Telegram*, se ha mostrado mucho más reticente a participar en este circuito de negociación. La pregunta que queda en el aire es: ¿han contribuido realmente los esfuerzos llevados a cabo por *WhatsApp* a reducir la opacidad ambiental legada por el servicio?

Por último, en la tercera sección, revisamos algunos de los estudios realizados sobre los usos de *WhatsApp* en contextos políticos. Sin embargo, se trata en esta oportunidad de que, en lugar de centrarnos en debatir cómo *WhatsApp* ha tratado los aspectos relativos a la privacidad de sus usuarios, nos centramos en comprender qué desafíos plantea este modelo de opacidad a los investigadores que tratan directamente con datos privados, y a menudo en entornos hostiles a la investigación académica. Así, si en la sección anterior hablábamos de la transparencia de la plataforma, en ésta abordamos lo que podemos denominar transparencia metodológica en torno a los servicios de mensajería instantánea móvil. Por último, presentamos algunas contribuciones al debate teórico y metodológico en los campos de la ciencia política y la comunicación política respecto a la agenda de investigación relacionada con los MIMs.

2. La mensajería privada como amenaza o redención para las democracias liberales

Los servicios de mensajería privada no son nada nuevo. Aplicaciones como *ICQ*, *AIM* o *MSN Messenger* fueron muy populares en la segunda mitad de los años 1990. Los mensajeros instantáneos, sin embargo, fueron gradualmente sustituidos e incorporados como una funcionalidad de los sitios de redes sociales (SNS), hasta el punto de que los usos de este tipo de plataformas se han reducido profundamente en algunos países en las primeras décadas de los años 2000 (**Barot**; **Oren**, 2015). Los dispositivos móviles, en cambio, han actualizado la oferta de servicios similares y, fortuitamente, se han creado nuevas aplicaciones en períodos de agitación política generalizada en distintas partes del globo.

Entre 2005 y 2010, el declive de las aplicaciones de mensajería instantánea estuvo acompañado, en parte, por el descenso de popularidad de algunos servicios ofrecidos por grandes portales de noticias, como *AOL*, propietaria de *AIM*, que poseía más del 50% del mercado de la comunicación privada en aquel momento (**Barot**; **Oren**, 2015), y *Yahoo!*, propietaria de *Yahoo! Messenger*. Al mismo tiempo, las SNS ofrecían funciones complementarias de mensajería privada a través de los llamados mensajes directos (DM), aún presentes hoy en *Facebook* (que alberga *Messenger*) y *Twitter*. Pero la creciente popularidad de los móviles introdujo un nuevo tipo de aplicaciones cuyo énfasis inmediato era el intercambio rápido de mensajes entre usuarios a través de sus respectivos teléfonos. Paralelamente, el aumento del número de smartphones, la extensión de internet de banda ancha y de las redes móviles de alta velocidad, y el posterior desarrollo de nuevos Voz sobre Protocolo de Internet (VoIP), convirtieron las aplicaciones de mensajería instantánea en potentes canales de comunicación.

El volumen de datos intercambiados a través de chats superó por primera vez a los servicios nativos de mensajes cortos (SMS) en 2013 (**Barot**; **Oren**, 2015; **Church**; **Oliveira**, 2013) y, en Brasil, este mismo hito representa un importante cambio de hábitos en la población. Datos del *Comitê Gestor da Internet no Brasil* (*https://cgi.br*) sobre las actividades de los usuarios online, muestran que de 2011 a 2018 el uso de sitios de redes sociales se mantiene entre el 70 y el 75% entre la población brasileña, mientras que el uso de mensajería instantánea creció del 70 al 92% en el mismo período (**Chagas**, 2022). El número de personas que envían mensajes instantáneos desde internet, según la encuesta, es el más alto entre todos los demás hábitos, como el envío de correos electrónicos, uso de blogs y foros online.

Entre 2011 y 2014 varios países protagonizaron protestas masivas. Levantamientos simbólicos como la *Primavera Árabe*, *Occupy Wall Street*, *Los Indignados* y manifestaciones antigubernamentales en Brasil, Chile y Rusia, entre otros ejemplos, han llamado la atención sobre la conexión entre el uso de plataformas digitales y la participación política (**Bennett**; **Segerberg**, 2012; **Klein-Bosquet**, 2012; **Mendonça** *et al*., 2019). La bibliografía ha concluido que el uso de las redes sociales como fuentes de noticias, la expresión de opiniones políticas y el propio activismo, incluyendo la movilización mediante este tipo de plataformas, son algunos de los factores que aumentan la participación a través de los medios digitales (**Valenzuela**, 2014).

En Brasil, el uso de servicios de mensajería privada ha crecido exponencialmente en los últimos años, a raíz de lo que se ha conocido en el país como las *Jornadas de Junho de 2013* (**Chagas**, 2022). Los sitios de redes sociales y, en particular, los de mensajería instantánea han sido ampliamente adoptados por los manifestantes para organizar protestas, intercambiar información sobre eventos e incluso compartir memes, como se ha visto en otros países (**Mendonça** *et al*., 2019).

> *Según datos de Panorama Mobile Time/ Opinion Box Report* (2020), *WhatsApp* está instalado en más del 99% de los teléfonos móviles de Brasil

Aunque no hay informes de represión estatal y acciones de regulación de los medios sociales que justifiquen algún grado de desconfianza, como ocurre en el contexto chino (**Mina**, 2019), la adopción de sistemas de cifrado de extremo a extremo por parte de los MIMs fue un componente crucial para aumentar la adopción de este tipo de aplicaciones. A esto se suma un factor económico no menos importante: la expansión de la red móvil en Brasil, tras la privatización de las compañías telefónicas a finales de la década de 1990. La competencia entre las compañías telefónicas brasileñas llevó a la popularización de los planes de suscripción prepago entre los usuarios, que pasaron a ofrecer descuentos o incluso la exención de gastos por el uso de determinados servicios, entre ellos *WhatsApp*. Conviene recordar que este tipo de prácticas son contrarias a lo dispuesto en el *Marco Civil de Internet* en Brasil (*Ley 12.965/2014*), que establece la igualdad de trato para todos los servicios incorporados por las compañías telefónicas. Los llamados planes "tasa cero" fueron, tal vez, los principales responsables de la amplia penetración de *WhatsApp* como una de las apps más instaladas en los teléfonos móviles de todo el país (**Evangelista**; **Bruno**, 2019). El resultado de esto es que, hoy en día, una gran capa de las clases populares no sólo utiliza los servicios de mensajería privada como una forma de comunicarse, sino que, en gran medida, depende de ellos para trabajar. Se trata de pequeños comerciantes, mercados locales, repartidores, profesionales autónomos y cooperativas que utilizan *WhatsApp* a diario como herramienta de trabajo y acaban expuestos a otros usos.

Según datos de *WhatsApp*, Brasil contaba con más de 120 millones de usuarios en 2017, y representaba una cuota del 8% de los usuarios a nivel mundial (**Chagas**, 2022). El dato es razonablemente incierto, pero el porcentaje de celulares con *WhatsApp* instalado en Brasil es muy alto. Según *Yahoo! Finance* (2021), el 91% de los smartphones del país tienen *WhatsApp*, lo que sitúa a Brasil en el séptimo lugar entre los mayores usuarios. En América Latina, Argentina (93%) y Colombia (92%) aparecen por delante. Y entre los cinco países con mayor base instalada, tres son africanos, con Kenia en primer lugar (97%). En Europa, Turquía y España (ambos con un 88%) aparecen en las primeras posiciones.

Según datos de *Panorama Mobile Time/Opinion Box Report* (2020), *WhatsApp* está instalado en más del 99% de los teléfonos móviles de Brasil. Si se cruzan estos datos con la encuesta anual divulgada por la *Fundação Getulio Vargas* (**Meirelles**, 2022), según la cual Brasil tiene actualmente más de un smartphone por habitante, y un total de 234 millones de dispositivos en uso, la base de usuarios resultante es realmente impresionante. En número de usuarios activos, Brasil sólo es superado por la India, que cuenta con 390 millones de cuentas (**Iqbal**, 2022).

El consumo de noticias en *WhatsApp* también es reportado por los usuarios como una actividad cada vez más relevante. En Brasil, más del 50% de la población afirmó utilizar la app como fuente de noticias, en 2019 (**Newman** *et al.*, 2019). Un año antes, en 2018, otra encuesta afirmaba que el 62% de la población brasileña creía en las noticias que recibía por *WhatsApp*, mientras que sólo el 8% no lo hacía (**Passos**, 2018). Y una última encuesta, también de 2018, encontró que, entre los votantes de Bolsonaro, seis de cada diez individuos obtienen información principalmente a través de *WhatsApp* y comparten noticias políticas a través de grupos en la app (*Datafolha*, 2018).

Los hábitos de consumo de información de la población brasileña han cambiado significativamente en los últimos tiempos y las plataformas digitales en general, y los servicios de mensajería privada como *WhatsApp* en particular, juegan un papel importante en este proceso. **Rossini** *et al*. (2021), por ejemplo, llaman la atención sobre cómo *WhatsApp* se ha convertido en un elemento central en la forma en que los brasileños acceden a la información política y cómo se comprometen políticamente. Y aunque los autores han sugerido en otro lugar que los usuarios de *WhatsApp* que comparten información disfuncional están más sujetos a la corrección social (**Rossini**; **Stromer-Galley**; **De-Oliveira**, 2020), la preocupación sobre cómo *WhatsApp* se ha convertido en un medio omnipresente capaz de desequilibrar no solo la dieta informativa, sino el propio entorno democrático, se ha evidenciado en muchos estudios. Y no sólo en Brasil.

En la India, uno de los efectos más notables discutidos en la bibliografía es la creación de redes de vigilancia que facilitan y fomentan linchamientos basados en supuestas denuncias recibidas a través de mensajes virales (**Mukherjee**, 2020; **Banaji**; **Bhat**, 2019). El vigilantismo digital, por supuesto, no es exclusivo de los servicios de mensajería instantánea móvil, pero el hecho de que estos usuarios formen parte de una red con alta capilaridad social ha llevado a las autoridades indias a determinar que la plataforma debe compartir los metadatos de los usuarios para la comunicación legal y los protocolos de vigilancia (**Arun**, 2019). El panorama refleja lo que **Phillips** y **Milner** (2020) sostienen sobre los marcos meméticos profundos que utilizan los grupos extremistas con la esperanza de fomentar el pánico moral en la población. Los autores afirman que dichos marcos siempre han sido un instrumento moralizador y a menudo han sido utilizados por grupos conservadores para movilizar a la población a reaccionar. La diferencia que plantea el régimen mediático digital reside en el hecho de que, a diferencia de lo que ocurría antes, en que estas oleadas de moral quedaban confinadas a regiones y barrios concretos, ahora, dicen los autores, la información se descentraliza y circula ampliamente.

En este sentido, estudios como los de **Santos** *et al*. (2019) muestran importantes patrones de circulación en los mensajes de desinformación en *WhatsApp*. Los autores analizan cómo los mensajes que evocaban un supuesto fraude electoral se difundieron viralmente y ganaron escala en progresión geométrica con el uso combinado de *WhatsApp* como servicio de mensajes privados y como canal de difusión, a partir de grupos de discusión públicos que incluyen, cada uno, hasta 256 usuarios.

> Desde una perspectiva empresarial, *WhatsApp* oscila entre la transparencia y la privacidad de forma incoherente

Vermeer *et al*. (2020) también recuerdan que *WhatsApp* parece favorecer la movilización de los usuarios. Y **Gil de Zúñiga**, **Ardèvol-Abreu** y **Casero-Ripollés** (2019) sugieren que *WhatsApp* influye positivamente en el activismo y la participación política de sus usuarios. **Chagas** *et al*. (2022) coinciden con esta conclusión al llamar la atención sobre los efectos de distorsión participativa que la plataforma ejerce a través de llamadas a la acción para votar en consultas públicas, una vez más, difundidas a través de grupos de discusión política.

> Para los usuarios de cuentas empresariales de *WhatsApp*, la privacidad no está contemplada, pero para los usuarios individuales que difunden mensajes a gran escala a través de grupos o listas de difusión, el servicio se reserva el derecho de no actuar, alegando el derecho a la privacidad de su base de usuarios

Aunque la bibliografía no es consensuada y de alguna manera no es concluyente en torno al impacto electoral de *WhatsApp* (**Schaefer** *et al*., 2019), parece claro que los grupos de discusión pública proporcionan un efecto de radicalización en los usuarios, ya que pasan a formar parte de una especie de cámara de eco (**Evangelista**; **Bruno**, 2019). La radicalización es un claro resultado de la mezcla entre audiencias homófilas y dietas informativas hiperpartidistas, según señalan estudios como los de **Mont'Alverne**, **Mitozo** y **Barbosa** (2019) y **Santos**, **Chagas** y **Marinho** (2022). Pero nada de esto sería posible sin un entorno de opacidad extrema.

Arun (2019) sostiene que la misma estructura tecnológica que protege a los usuarios de eventuales invasiones de la privacidad también da lugar a un entorno que fomenta la difusión de discursos dañinos y rumores online. El cifrado de extremo a extremo sería, pues, a la vez la solución y el origen mismo del problema. La cuestión es que la falta de transparencia respecto a los metadatos de los mensajes que circulan por *WhatsApp* se refleja en un entorno de vigilancia extrema y prácticamente sin posibilidad de moderación y regulación democráticas. El síntoma más evidente de ello ha sido el creciente uso de *WhatsApp* para la realización de operaciones de influencia y prácticas de *astroturfing* (**Chagas**, 2022), en las que agentes profesionales de la política actúan de forma encubierta como audiencias movilizadas espontáneamente. Así, la falta de transparencia de la plataforma resulta en acciones y comportamientos no sólo inauténticos, sino engañosos. En la siguiente sección, analizamos un poco más estos efectos.

3. Dilema de la privacidad y la transparencia pública en *WhatsApp*

WhatsApp fue creado en 2009, meses antes que algunos de sus principales competidores actuales como *Viber* (2010-), *Line* (2011-), *WeChat* (2011-), *Telegram* (2013-) y *Signal* (2014-). En febrero de 2014, el servicio fue adquirido por 19.000 millones de dólares por *Facebook, Inc.* (actualmente *Meta Platforms*), en lo que entonces fue la mayor adquisición de una empresa respaldada por capital riesgo de la historia. En noviembre de ese mismo año, mediante de una asociación con la empresa *Open Whisper Systems* (*OWS*), *WhatsApp* anunció la implantación de un sistema de cifrado de extremo a extremo para todos sus clientes, basado en el protocolo creado por otro mensajero instantáneo, *Signal*.

Según el sistema de cifrado de extremo a extremo, sólo el remitente y el destinatario tienen acceso a los mensajes y contenidos compartidos. La empresa afirma que ni siquiera ella tiene acceso a los mensajes, lo que impediría a la propia *Meta* moderar o censurar los contenidos difundidos, y/o rastrear hábitos y mensajes para dirigir anuncios, por ejemplo. Aunque esta es una discusión aún no del todo resuelta, ya que algunos estudios e informes afirman que la empresa tiene acceso a los contenidos cifrados compartidos por los usuarios (**Freitas**, 2019), este modelo tecnológico sumado al discurso adoptado ha permitido a la empresa evitar posibles acusaciones por una actuación más proactiva en casos de circulación de desinformación y discurso de odio.

Existen varios tipos de sistemas de encriptación. Los modelos más sencillos se denominan cifrados simétricos, cuando el emisor y el receptor comparten una clave secreta para interpretar el mensaje cifrado. Un modelo más completo se denomina cifrado asimétrico, en el que receptor y emisor tienen una clave pública y otra privada. De este modo, el texto se cifra con la clave pública entre los dos usuarios, pero sólo se puede descifrar con la clave privada de cada uno. Este último modelo impide que terceros accedan a toda la base de mensajes, en caso de interceptación. Es decir, si un tercero descubre la clave privada, sólo tendrá acceso a un único mensaje, no a todo el sistema (**Teixeira**; **Sabo**; **Sabo**, 2017). El modelo de cifrado adoptado por *WhatsApp*, sin embargo, es un poco misterioso.

WhatsApp comparte información pública sobre su sistema de cifrado de forma general, dando transparencia sólo al modelo de protocolo. Sin embargo, no deja claro cómo funciona el sistema en la práctica dentro de la aplicación. Por ejemplo, la información sobre si la aplicación almacena o no los datos de los usuarios se hace opaca. Aunque *Meta* afirma que no tiene acceso a los mensajes reenviados, no existe una credibilidad fiable de que esto no ocurra realmente, teniendo en cuenta el historial de la compañía, en casos como *Cambridge Analytica*, donde se compartieron datos de usuarios de *Facebook* con terceros para la segmentación de anuncios políticos. Además, una característica adoptada recientemente por *WhatsApp* como una forma de prevenir y destacar el contenido difundido viralmente, una etiqueta que permite identificar los mensajes reenviados con frecuencia, sugiere que incluso los mensajes cifrados pueden ser accedidos e identificados por la empresa.

Otro punto preocupante es la adopción por parte de *WhatsApp*, en 2021, de políticas de privacidad subordinadas a los contextos y normas locales (*Abraji*, 2022). El efecto colateral de este cambio es que, en los países de la Unión Europea, regidos por el *Reglamento General de Protección de Datos* (*GDPR*), las normas de privacidad se han vuelto excesiva-

mente estrictas, pero en países como Brasil, por ejemplo, la nueva política ha facilitado el intercambio de datos de los usuarios con la aplicación de *Facebook*. Así, ahora se interopera con la información de registro, número de teléfono, dirección IP, información del dispositivo móvil como modelo, nivel de batería, intensidad de la señal, versión de la app de mensajería, información del navegador predeterminado, red móvil, e incluso transacciones y pagos de datos y hábitos de navegación (tiempo, frecuencia y duración de las actividades, informes de desempeño, etc.). Además, el contenido de los mensajes intercambiados a través de las cuentas de *WhatsApp Business* ya no está cifrado y los metadatos generados pueden ser utilizados por *Facebook* para proponer anuncios (**Cosseti**, 2021).

En resumen, desde una perspectiva empresarial, *WhatsApp* oscila entre la transparencia y la privacidad de forma incoherente. Para los usuarios de sus cuentas empresariales, la privacidad no está contemplada, pero para los usuarios individuales que difunden mensajes a gran escala a través de grupos o listas de difusión, el servicio se reserva el derecho de no actuar, alegando el derecho a la privacidad de su base de usuarios.

Esta incoherencia ha sido sostenida en diferentes ocasiones por la retórica adoptada por la *Oficina de WhatsApp* en Brasil en discursos públicos en los que se destaca que aproximadamente el 90% de los mensajes intercambiados a través de la aplicación se limitan a comunicaciones interpersonales entre dos usuarios, y que el número medio de usuarios en los grupos alojados por el servicio ronda los siete individuos (D. Durigan, comunicación personal, 27 de octubre de 2020). Y, aunque estos datos se replican en estudios que, habiendo recibido financiación de las propias convocatorias públicas de *WhatsApp*, argumentan que la investigación sobre los efectos políticos del intercambio disfuncional de información no debería hacer hincapié en los grandes grupos dedicados a la discusión política, ya que serían la excepción y no una regla, y no reflejarían la experiencia de la mayoría de los usuarios (**Rossini** *et al*., 2021), es notable que el problema no está relacionado con los intercambios interpersonales, sino con la viralidad de los mensajes compartidos por y dentro de estos grupos (**Santos** *et al*., 2019). Así, ignorar la amenaza que supone el cifrado extremo a extremo aplicado a grupos públicos con la participación de agentes profesionales de la política (**Chagas**, 2022; **Chagas**; **Modesto**; **Magalhães**, 2019) equivale a cegarse ante los matices que adquiere el servicio al incorporar múltiples funcionalidades. Además, tal y como estudios como los de **Santos**, **Chagas** y **Marinho** (2022) y otros han tratado de demostrar, *WhatsApp* funciona principalmente como una especie de *hub* de información, integrando diferentes plataformas y grupos sociales. De esta forma, aunque los grandes grupos de discusión política son absolutamente minoritarios, actúan en el sentido de dinamizar y difundir contenidos a grupos más pequeños y usuarios individuales, de forma muy significativa.

WhatsApp ya no puede ser visto sólo como un mensajero instantáneo uno a uno, en un contexto privado, sino como un canal de difusión muy completo. **Vieira** *et al*. (2019) afirman que con la expansión de la aplicación, y especialmente con el uso masivo de recursos como el reenvío de mensajes a múltiples usuarios y grupos, el mensajero dejó de ser una plataforma meramente tecnológica para convertirse en una plataforma mediática.

> "Como plataforma mediática, al igual que un canal de radio o televisión, difunde contenidos a través de sus funciones de emisión de información y permite que los mensajes se conviertan en virales" (**Vieira** *et al*., 2019, p. 4).

Uno de los efectos perniciosos de esta política adoptada por *WhatsApp* para sus grupos de discusión es la opacidad respecto a operaciones como el envío masivo de mensajes, el spam y la difusión de *fake news* y discursos de odio (**Resende** *et al*., 2019). Como se argumenta más adelante, esta opacidad es aún mayor debido a que la plataforma no cuenta con una API y no ha buscado facilitar iniciativas de monitoreo e investigaciones.

En respuesta a las graves críticas recibidas después de las elecciones presidenciales de 2018 en Brasil, *WhatsApp* afirma que ha prohibido o bloqueado de forma regular y automática una serie de cuentas que violan las reglas de la plataforma o la legislación electoral vigente. Paralelamente, la app ha tratado de crear asociaciones con organizaciones de verificación de hechos como *AFP Checamos*, *Agência Lupa*, *Aos Fatos* y *Estadão Verifica*. En India, iniciativas semejantes incluyen asociaciones con *Digit Eye*, *Fact Crescend*, *Factly*, *India Today*, *Newschecker*, *Newsmobile*, *The Healthy Indian Project*, *The Quint-WebQoof* y *Vishvas News*. También hay comprobadores de hechos que ofrecen el mismo tipo de servicio en Albania, Alemania, Argentina, Colombia, Croacia, Ecuador, España, Estados Unidos, Francia, Georgia, Ghana, Grecia, Guinea, Indonesia, Irlanda, Italia, Costa de Marfil, Kenia, México, Nigeria, Perú, Portugal, Reino Unido, Senegal, Sri Lanka, Sudáfrica y Turquía (*WhatsApp*, 2022).

También se han llevado a cabo asociaciones con instituciones públicas. En Brasil, la *Oficina de WhatsApp* firmó un memorando de acuerdo con el *Tribunal Superior Eleitoral* (*TSE*) en el que se compromete a implementar o ayudar en la implementación de iniciativas para combatir la desinformación sobre el proceso electoral. Entre las acciones previstas, *WhatsApp* propuso:

- realizar seminarios para el *TSE* y los *Tribunais Regionais Eleitorais* (*TREs*) sobre la aplicación;
- producir cartillas sobre el servicio;
- ayudar en la implementación de acciones para la rápida identificación y contención de la desinformación, como la creación de un canal extrajudicial para la denuncia de contenidos que violen la legislación y el desarrollo, en colaboración con el *TSE*, de un *chatbot* con información de fuentes confiables sobre las elecciones (*TSE*, 2022).

Sin embargo, desde el punto de vista técnico, las medidas adoptadas por *WhatsApp* hasta ahora para contener estos efectos se han centrado en limitar el reenvío de mensajes y bloquear/banear a los usuarios que difunden contenidos

infractores. Poco o nada se ha hecho para que el entorno sea más transparente, más bien todo lo contrario. Entre las funciones incorporadas más recientemente, *WhatsApp* permitía:

- bloquear mensajes de números desconocidos y denunciarlos como spam;
- configurar qué usuarios pueden añadir una determinada cuenta a nuevos grupos.

Además, desde 2018, *WhatsApp* limitó el reenvío de un mismo mensaje a solo 20 contactos (incluidos grupos) a la vez en Brasil y, en 2019, volvió a reducir este límite a cinco contactos. En 2020, el servicio comenzó a identificar los mensajes de alta frecuencia (HFM en inglés) con una etiqueta específica, y luego limitó el reenvío de HFM de cinco a un solo contacto a la vez. Según se informa, estos límites redujeron el intercambio de mensajes en Brasil en un 30%, y redujeron el tráfico de mensajes de alta frecuencia en todo el mundo en un 70% (*WhatsApp*, 2021). Pero todavía hay poca transparencia en cuanto a las medidas adoptadas después de que un mensaje haya sido denunciado como spam, y no hay, hasta ahora, mucha claridad también sobre las cuentas expulsadas de la plataforma por mal comportamiento. Según los informes internacionales de la propia empresa, cada mes se expulsan de la plataforma una media de 8 millones de cuentas y alrededor del 95% de las eliminaciones se realizan por detección automática (**Bento**, 2022).

Estas medidas se mostraron ineficaces principalmente en un contexto en el que la difusión de desinformación se ha producido a gran escala y ha tenido una orientación ideológica, como en Brasil. Los grupos públicos de discusión política son administrados en su mayoría por partidarios de la extrema derecha brasileña (**Chagas**, 2022), y, aunque sostenidos por usuarios que muestran un alto grado de compromiso, también están marcados por una expectativa de horizontalidad, en la que la moderación permite compartir libremente los mensajes, siempre y cuando cumplan con la prerrogativa ideológica del propio grupo, es decir, sólo se eliminan sumariamente los contenidos que están políticamente en desacuerdo con las directrices del grupo.

WhatsApp no tiene las mismas características estructurales que otras redes sociales. Por ejemplo, no tiene perfiles públicos, no muestra públicamente las conexiones entre los usuarios, y no tiene funciones recientemente incorporadas por diferentes plataformas digitales, como la línea de tiempo que organiza las publicaciones mostradas a través de un algoritmo social, de acuerdo con las preferencias personales y de navegación de cada usuario.

Según **Sahafizadeh** y **Ladani** (2020) el uso de mensajería instantánea móvil, como *WhatsApp*, ha constituido un nuevo modelo de comunicación online. A diferencia de las redes sociales tradicionales, basadas en relaciones de amistad, los usuarios de MIMS tienen dos modos de comunicación:

- peer-to-peer, suelen necesitar tener registrado en sus dispositivos el contacto de su interlocutor;
- en los grupos de discusión, la plataforma funciona como un modo de difusión, en el que no es necesario conocer a las personas con las que se interactúa.

Gran parte del debate centrado en el peligro que los medios sociales suponen para las democracias contemporáneas hace hincapié en la opacidad que rodea a estos algoritmos sociales y sistemas de recomendación de contenidos. Por ejemplo, hay estudios que hablan de cómo *YouTube* recomienda vídeos a sus usuarios basándose en criterios poco transparentes, lo que se traduce en recomendaciones de contenidos hiperpartidistas o dañinos (**Bryant**, 2020). *Twitter* ya ha admitido que el contenido de extrema derecha se ha visto favorecido y ha obtenido una amplia exposición a través de su plataforma (**Huszár** *et al*., 2021). Y *Meta* y *Facebook* también se han visto sometidas al escrutinio público en varias ocasiones, incluidas las repercusiones del escándalo de *Cambridge Analytica*. **Benkler**, **Faris** y **Roberts** (2018) también trataron de demostrar que las funciones de las plataformas digitales se han utilizado para privilegiar la exposición de contenidos por parte de grupos políticamente interesados, y **Woolley** y **Howard** (2018) llaman la atención sobre cómo los recursos computacionales, incluidos los *bots* y las redes de *sock-puppet*, se han utilizado para difundir propaganda política en los medios digitales.

La bibliografía, sin embargo, rara vez se centra en *WhatsApp*. No sólo por la dificultad de monitorizar la plataforma que plantea a los investigadores, como comentamos a continuación, sino también porque su arquitectura es fundamentalmente diferente a la de las redes sociales y, por ello, los mismos criterios que se aplican a la demanda de una mayor transparencia algorítmica defendida por diversos estudiosos, no se aplican al entorno de opacidad de *WhatsApp*.

> A diferencia de las redes sociales tradicionales, basadas en relaciones de amistad, los usuarios de servicios de mensajería instantánea móvil tienen dos modos de comunicación. En lo primero, peer-to-peer, suelen necesitar tener registrado en sus dispositivos el contacto de su interlocutor. Pero, en los grupos de discusión, la plataforma funciona como un modo de difusión, en el que no es necesario conocer a las personas con las que se interactúa

En el caso de *WhatsApp*, el principal problema no es la opacidad de sus algoritmos, sino la opacidad en los metadatos de sus contenidos y usuarios. En pocas palabras, es imposible determinar cuántos grupos de debate político hay en la plataforma, o cómo circuló un mensaje concreto, si está superando en engagement, o incluso si fue visto por encima de la media. No es posible identificar qué enlaces han circulado más y desde qué fuentes de información (**Santos**; **Chagas**; **Marinho**, 2022; **Mont'Alverne**; **Mitozo**; **Barbosa**, 2019), ni qué memes

o contenidos anticientíficos se han transmitido entre los usuarios y qué usuarios son los que comparten dichos contenidos (**Massuchin** *et al*., 2021). En consecuencia, a diferencia de lo que ocurre en otros medios sociales, en *WhatsApp* el principal problema no es la influencia de sistemas opacos de recomendación de contenidos a los usuarios, sino la ausencia total de parámetros capaces de orientar a los usuarios sobre los contenidos que les llegan por recomendación directa de otros usuarios, lo que aquí denominamos opacidad ambiental.

> La prevención de la desinformación y los contenidos peligrosos en *WhatsApp* no debe limitarse a restricciones técnicas o al bloqueo y prohibición de cuentas basadas en la identificación automatizada de comportamientos no auténticos, sino sobre todo en la necesidad de dotar de mayor transparencia a los metadatos de contenidos y usuarios

No sabemos con absoluta transparencia cómo funciona el cifrado de extremo a extremo adoptado por el servicio, ni si *WhatsApp* almacena o no los mensajes en su propio servidor. No sabemos qué cuentas están vetadas y por qué motivos. Y ni siquiera tenemos mecanismos para rastrear mensajes dañinos o informes sobre las decisiones tomadas por la plataforma.

Por tanto, no se trata solo de exigir responsabilidades algorítmicas a *WhatsApp*, como se hace con otras plataformas (**Diakopoulos**, 2014). La prevención de la desinformación y los contenidos peligrosos en *WhatsApp* no debe limitarse a restricciones técnicas o al bloqueo y prohibición de cuentas basadas en la identificación automatizada de comportamientos no auténticos, sino sobre todo en la necesidad de dotar de mayor transparencia a los metadatos de contenidos y usuarios en la plataforma. Este tipo de solución no viola los principios de privacidad de los usuarios, ya que no es necesario identificarlos a priori. Pero es perfectamente posible desde un punto de vista técnico presentar, por ejemplo, cuántas veces se reenvió un mensaje dado, cuántos usuarios lo vieron, en qué fecha y hora se creó, e incluso cuáles fueron las reacciones globales al mensaje. Estos elementos por sí solos pueden ser insuficientes para discernir si se trata de un contenido nocivo o no, pero sin duda pueden ayudar a decidir quién accede a una determinada pieza. Son precisamente las mismas métricas que tenemos cuando accedemos a un vídeo de *YouTube* o leemos un post de *Facebook*. Pero no están disponibles en *WhatsApp* ni en otros servicios de comunicación privada, a pesar de que, como hemos visto, estas plataformas fusionan la mensajería privada con el modo de difusión.

El tratamiento de estos dos modos de comunicación sobre la base de los mismos principios, con la prevalencia de la privacidad sobre la transparencia pública en el caso de los grupos de discusión y las listas de difusión, ha dado lugar a un primer dilema relativo a la transparencia en *WhatsApp*, según el cual las mismas características que confieren a la plataforma un alto grado de protección de la privacidad de los usuarios contribuyen a socavar el entorno democrático debido a una absoluta falta de transparencia pública. Si a esto añadimos la enorme dificultad de los investigadores para penetrar en estos entornos, como analizamos más adelante, tenemos la fórmula de una bomba de relojería para el descrédito de las instituciones democráticas.

Desde el punto de vista legal, una de las leyes pioneras en equiparar *WhatsApp* y las redes sociales tradicionales, y castigar a quienes crean o distribuyen noticias falsas, exigiendo un informe trimestral sobre las políticas y decisiones de moderación de cada plataforma, es la *Cyber-crime Law* de los Emiratos Árabes Unidos (**Kabha** *et al.*, 2019). Según los autores, aunque recibe críticas por ser demasiado rigurosa, ha impedido usos nocivos de *WhatsApp* y otras redes sociales.

En Brasil, dos casos se encuentran actualmente en discusión en la *Suprema Corte*: la *Ação Direta de Inconstitucionalidade No. 5.527*, y la *Arguição de Descumprimento de Preceito Fundamental No. 403*. En ambos casos se cuestionan las decisiones judiciales de los tribunales inferiores para determinar la suspensión nacional de los servicios de intercambio de mensajes. Los informes de ambas acciones, sin embargo, presentan perspectivas distintas. En el primer caso, el juez Edson Fachin se opone a la suspensión de aplicaciones por órdenes judiciales. En el segundo, la ministra Rosa Weber entendió que el cifrado de extremo a extremo no puede impedir el acceso a los medios judiciales. Recientemente también, el *Senado Federal do Brasil* aprobó el *Projeto de lei 2.630*, denominado *Projeto de lei das fake news*, que dispuso normas para las redes sociales y aplicaciones como *WhatsApp*, para combatir la desinformación. El proyecto aún debe ser aprobado por la *Câmera* para ser sancionado.

En el Ejecutivo brasileño, el nuevo gobierno de Luiz Inácio Lula da Silva aparentemente se ha estado moviendo rápidamente para contener la circulación de mensajes de odio e incitación al crimen en el entorno online. El ahora ministro de Justicia y Seguridad Pública de Brasil, Flávio Dino, entregó un "Paquete Democracia" al *Parlamento*. Las medidas implican tipificar como delito de terrorismo la organización e incitación a manifestaciones antidemocráticas, como las ocurridas en Brasil el 8 de enero de 2023, cuando simpatizantes del expresidente Jair Messias Bolsonaro invadieron y vandalizaron la sede de los tres poderes del Estado, en un claro intento de golpe. La noticia llamó la atención sobre el papel de MIMS como *WhatsApp* y *Telegram* en la movilización de los actos (*Poder360*, 2023).

Sobre la discusión de la regulación, **Medeiros** y **Singh** (2020) argumentan que los legisladores no pueden ignorar las consecuencias negativas de alentar prácticas de moderación demasiado entusiastas. Forzar cambios en la arquitectura de la plataforma, específicamente la eliminación del cifrado de extremo a extremo, y hacer cumplir de manera proactiva las responsabilidades de eliminación de contenido puede ser problemático y comprometer el discurso disidente. Por otro

lado, las propias plataformas se han apoyado en esta defensa para negar la existencia del problema. El punto, sin embargo, es que las conversaciones entre usuarios no se pueden confundir con la permisividad para el caos antidemocrático. Y esta distinción está en la raíz de la diferencia entre la comunicación *peer-to-peer* y la de difusión en estas aplicaciones, algo a lo que la legislación rara vez presta atención.

4. Dilema de la transparencia metodológica en *WhatsApp*

Existen fundamentalmente dos tipos de dificultades a las que se enfrentan los investigadores que centran sus investigaciones en *WhatsApp*, que también pueden describirse como problemas de transparencia metodológica:

- la primera es el reto que supone lidiar con la casi absoluta falta de transparencia por parte de la plataforma respecto a sus datos;
- la segunda y no menos importante es el reto que plantea la necesidad de respetar el carácter privado de los datos relativos a los individuos observados.

En cuanto a la primera dificultad, según **Benevenuto** y **Ortellado** (2020), los investigadores se beneficiarían si *WhatsApp* publicara regularmente dos tipos de información:

- encuestas agregadas sobre los usuarios de la plataforma, como el número de ellos, grupos y número de mensajes distribuidos en los grupos, o información sobre mensajes virales, como el número de veces que se compartió un determinado contenido;
- información y protocolos para la recopilación de datos por parte de investigadores académicos, es decir, una documentación de la API.

En los últimos años, *Twitter* (**Tornes**, 2021), *YouTube* (*YouTube*, 2022) y *TikTok* (**Roth**, 2022) han llevado a cabo programas dirigidos a los investigadores, incluidas APIs específicas para el público académico. Otras plataformas *Meta*, como *Facebook* e *Instagram*, tienen API para desarrolladores y acuerdos con algunas instituciones académicas para la cesión de datos para investigaciones académicas (**Li** *et al*., 2022).

WhatsApp Business dispone de una API para desarrolladores, pero la versión ordinaria de la app, destinada al uso individual, carece de mayor transparencia en cuanto a los procedimientos de *scraping* de datos. Así, la mayor parte de las investigaciones en torno a *WhatsApp* se han anclado o bien en estrategias de análisis cualitativo, como la etnografía (**Cesarino**, 2020), o bien en métodos de *scraping* de datos no autorizados (**Piaia**; **Alves**, 2020), que pueden toparse en los propios filtros automatizados de la plataforma destinados a identificar y desterrar comportamientos no auténticos. Lo que suele ocurrir es que, como el proceso involucra mecanismos de automatización para que los datos sean recolectados, la propia aplicación interpreta que la acción realizada es sospechosa e inactiva la cuenta que estaba siendo utilizada para la investigación, por considerar que el comportamiento viola las normas.

Una alternativa para la recogida de datos a gran escala de *WhatsApp* es la herramienta nativa de exportación de chats de la aplicación o el *scraping* de sesiones de navegación a través de la aplicación web de *WhatsApp*. En ambos casos, los investigadores se enfrentan a retos a la hora de tratar y manejar los datos, ya que los metadatos disponibles son escasos: a menudo sólo se dispone del autor y el contenido del mensaje y de la fecha de su publicación (**Gruber**, 2022).

Al mismo tiempo, como los investigadores no disponen de datos sobre la base de usuarios y grupos del servicio, las muestras que manejan en sus respectivas investigaciones son invariablemente muestras no probabilísticas, lo que dificulta la extracción de conclusiones inferenciales. Para sortear esta situación, algunos investigadores han optado por realizar encuestas a individuos que se autoidentifican como usuarios de *WhatsApp*, en lugar de tratar con los datos publicados a través de la plataforma y los usuarios asociados a ella (**Gil de Zúñiga**; **Ardèvol-Abreu**; **Casero-Ripollés**, 2019; **Rossini**; **Stromer-Galley**; **De-Oliveira**, 2020). Algo similar ocurre con los contenidos virales. Dado que los datos obtenidos no son representativos en escala de lo que circula por *WhatsApp* en general, no es posible certificar si un contenido replicado N veces en un determinado conjunto de grupos observados tuvo realmente un alcance significativo entre toda la base de usuarios del servicio.

Por tanto, el primer problema relacionado con la investigación sobre *WhatsApp* y la transparencia radica en que la opacidad ambiental de la plataforma compromete la extracción y recopilación de datos. Por otro lado, el segundo problema está relacionado, como hemos dicho antes, con los individuos observados.

Este segundo reto se refiere a la naturaleza privada de los datos que circulan en *WhatsApp*. A diferencia de lo que ocurre en otras plataformas de medios sociales, los usuarios de *WhatsApp* no firman un formulario de consentimiento para la publicidad de sus contenidos. Al contrario, *WhatsApp* basa su experiencia en un servicio de mensajería privada. Por lo tanto, los investigadores

> A diferencia de lo que ocurre en otras plataformas de medios sociales, los usuarios de *WhatsApp* no firman un formulario de consentimiento para la publicidad de sus contenidos. Al contrario, *WhatsApp* basa su experiencia en un servicio de mensajería privada. Por lo tanto, los investigadores tienen que hacer frente a una posible violación de la privacidad de los usuarios cuando investigan estos entornos

tienen que hacer frente a una posible violación de la privacidad de los usuarios cuando investigan estos entornos. La investigación de los datos de *WhatsApp*, por regla general, cuenta con dos expedientes diferentes para evitar comprometer las normas de privacidad:

- la anonimización de los datos, que incluye la desidentificación completa de los usuarios;
- la presentación de los resultados únicamente a escala de datos agregados, evitando así los análisis individualizados.

En la Unión Europea, el *Reglamento General de Protección de Datos* (*RGPD*) establece normas estrictas sobre la privacidad y la protección de datos de los ciudadanos residentes en los países miembros. Para 2020, Brasil ha adoptado una legislación similar en este sentido, denominada *Lei Geral de Proteção de Dados Pessoais* (*LGPD, Lei 13.709/2018*), un conjunto de normas para la *Administração Pública Federal*, las empresas y las instituciones relativas al tratamiento de la información personal. La *LGPD* brasileña establece como datos personales

> "[toda] la información relativa a una persona física identificada o identificable",

por lo que considera sensibles, entre otros, los datos relativos a la identidad racial o étnica, género, convicción religiosa, opinión política, afiliación sindical u organización civil, y los relativos a la salud o vida sexual, rasgos genéticos o biométricos de cualquier individuo (**Wimmer**, 2019).

Debido a este tratamiento legal, y también por razones éticas, la investigación en apps de chat privado encriptado ha tratado de garantizar el anonimato total de los sujetos de investigación. No obstante, las dificultades no acaban ahí. La mayoría de los consejos éticos de investigación suelen considerar una buena práctica la aplicación de un formulario de consentimiento informado a los sujetos. El ambiente de los grupos de discusión de *WhatsApp*, por otro lado, es absolutamente volátil, con usuarios que entran y salen todo el tiempo, y grupos de discusión que se crean y de repente se disuelven. Así, Barbosa y Milan llaman la atención sobre lo mucho que este tipo de plataforma requiere un enfoque ético y metodológico innovador, en el que

> "evitar la reducción de la ética de la investigación a una lista de verificación de una sola parada [...]; ir más allá del formulario de consentimiento como el momento único y meramente regulador de la relación investigador-sujeto de investigación" (**Barbosa**; **Milan**, 2019, p. 59).

Los autores, sin embargo, abogan por una agenda de investigación que

> "abrace la transparencia y, cuando la pregunta de investigación permita métodos encubiertos, evite las derivaciones deshonestas" (**Barbosa**; **Milan**, 2019).

Esta mención está en línea con lo que **Chagas**, **Modesto** y **Magalhães** (2019) discuten sobre los protocolos de investigación encubierta. En Brasil, la investigación encubierta está autorizada por la *Resolução 510*, de 7 de abril de 2016, del *Conselho Nacional de Saúde* (*CNS*), órgano colegiado del *Ministério da Saúde* que cuenta con una comisión intersectorial responsable de la aplicación de normas y directrices para la investigación con seres humanos, la *Comissão Nacional de Ética em Pesquisa* (*Conep*). Toda investigación con seres humanos, de cualquier área, debe ser apreciada y evaluada por este órgano antes de su desarrollo. La *Resolução 510* establece que la investigación encubierta es la

> "realizada sin que los participantes sean informados sobre los objetivos y procedimientos del estudio, y sin que se obtenga su consentimiento antes o durante la investigación",

y sólo se justifica

> "en circunstancias en que la información sobre objetivos y procedimientos modifique el comportamiento objetivo del estudio o cuando el uso de este método se presente como la única forma de realizar el estudio".

Se trata de un enfoque metodológico reservado a situaciones liminares, en las que los individuos ni siquiera pueden reconocerse como sujetos observados, ya que ello alteraría su comportamiento habitual. Es un procedimiento diferente, por tanto, al de los estudios clínicos en los que se administran sustancias como placebo a los pacientes ya que, en estos casos, se requiere el consentimiento para la administración del fármaco o vacuna, aunque se aplique solo en una parte de los sujetos de la investigación.

Barbosa y **Milan** (2019) recomiendan evitar al máximo este tipo de estrategia, al igual que **Padilha** *et al*. (2005), que argumentan que este enfoque de investigación suprime el derecho de los sujetos a no ser investigados, pero asienten que hay escenarios en los que la recolección de datos de otras maneras es simplemente inviable. **Chagas**, **Modesto** y **Magalhães** (2019) afirman que, es-

> "El primer dilema se refiere a la relación que dichos servicios han intentado establecer entre la privacidad de sus usuarios y la transparencia pública, apoyándose en la retórica de la protección de la privacidad para negar un entorno de transparencia en relación con los metadatos de contenido potencialmente perjudicial y el comportamiento no auténtico. El segundo dilema se refiere a un efecto del primero, el debilitamiento de los académicos debido a la naturaleza privada de los datos disponibles para la investigación"

pecialmente, las agendas de investigación elaboradas en grupos de comunicación privados de extrema derecha requieren un poco más de flexibilidad con los preceptos de la investigación con seres humanos. Destacan que, en casos como esos, la investigación encubierta suele ser necesaria. Esto se debe a que, en los grupos extremistas, es habitual que la simple presentación del investigador conlleve su expulsión inmediata. Se trata de un campo hostil para la investigación académica, y la transparencia metodológica absoluta no siempre es capaz de resolver los efectos de la radicalización política. Este hallazgo conduce a un segundo dilema importante en relación con la transparencia en *WhatsApp*, según el cual una mayor transparencia metodológica no siempre es capaz de generar el consentimiento de los sujetos de investigación, y los entornos resistentes a la ciencia pueden llegar a exigir un trato excepcional en este sentido.

> Los medios para resolver estos dilemas están en manos de los legisladores y las plataformas digitales. Estos agentes pueden garantizar que la investigación científica tenga unas condiciones mínimas para funcionar, y así proporcionar a la sociedad más datos y aportaciones sobre entornos polarizados, como es el caso de los grupos de discusión política extremista en *WhatsApp*

5. Últimas consideraciones

El objetivo de este artículo fue debatir cuestiones relacionadas con los servicios móviles de mensajería instantánea (MIM), en particular *WhatsApp*, y la transparencia. Basamos nuestras observaciones en dos niveles, que denominamos dilemas:

El primer dilema se refiere a la relación que dichos servicios han intentado establecer entre la privacidad de sus usuarios y la transparencia pública, apoyándose en la retórica de la protección de la privacidad para negar un entorno de transparencia en relación con los metadatos de contenido potencialmente perjudicial y el comportamiento no auténtico.

El segundo dilema se refiere a un efecto del primero, el debilitamiento de los académicos debido a la naturaleza privada de los datos disponibles para la investigación. En este último caso, aunque la transparencia metodológica es un requisito muy deseable, hay situaciones en las que la investigación exige enfoques metodológicos encubiertos, a fin de garantizar que determinados ámbitos no sean completamente impenetrables.

Estos dos dilemas han representado importantes dificultades para el avance de la investigación académica sobre *WhatsApp* en los últimos años. Aun así, los avances son notables, como pueden demostrar la mayoría de las referencias bibliográficas a lo largo de este texto.

Cabe señalar que la ética de la investigación, especialmente en las humanidades digitales, no puede reducirse a instrumentos completamente inflexibles que no respeten contextos y situaciones específicas. Por otra parte, no es nuestra intención prescribir un libro de jugadas sin normas, en el que el juego desplegado equipare a los investigadores con los radicales anticientíficos. En cambio, lo que sugerimos es que los medios para resolver estos dilemas están en manos de los legisladores y las plataformas digitales. Estos agentes pueden garantizar que la investigación científica tenga unas condiciones mínimas para funcionar, y así proporcionar a la sociedad más datos y aportaciones sobre entornos polarizados, como es el caso de los grupos de discusión política extremista en *WhatsApp*.

En este contexto, este artículo afirma que es absolutamente urgente que los Estados desarrollen modelos regulatorios para hacer frente a la propagación de la desinformación y el discurso de odio en las plataformas digitales. Si bien la principal preocupación de las empresas ha sido una lectura comprometida y controvertida del principio de libertad de expresión, se ha brindado poca o ninguna transparencia a las autoridades públicas sobre sus propias acciones y modelos de negocio. Se debe llamar a las plataformas MIMS para que expliquen de manera transparente a los usuarios cómo funciona su sistema de encriptación; informar regularmente a las autoridades y a la sociedad civil información básica sobre las cuentas prohibidas y las motivaciones de tales decisiones; también informar regularmente los metadatos de los grupos públicos y los mensajes reenviados con frecuencia; proporcionar a los usuarios metadatos sobre la circulación de los mensajes virales, sus remitentes y sus métricas de participación; y, finalmente, proporcionar una API para investigadores con metadatos claros y transparentes disponibles.

También se pueden impulsar otras acciones más heterodoxas, pero que igualmente deben brindar garantías para la libertad de expresión y la protección de datos personales. Entre ellas pueden ocurrir: la aplicación de políticas de moderación; sanciones individuales y grupales, como alertas, eliminación de contenido y eliminación de la plataforma del usuario. En todos los casos, sin embargo, es importante tener en cuenta que no se trata de adoptar métodos autocráticos para prevenir manifestaciones antidemocráticas. Lo más importante, en todos los escenarios, es fomentar plataformas de diálogo con autoridades públicas, sociedad civil e investigadores. En lugar de rodearse de un modelo opaco, quizá adoptando más transparencia llevaría a una conclusión de ganar-ganar.

6. Referencias

Abraji (2022). *O papel das plataformas digitais na proteção da integridade eleitoral em 2022*. Associação Brasileira de Jornalismo Investigativo (Abraji), Book Amazon.
https://goo.su/3stjyP

Al-Zidjaly, Najma (2017). "Memes as reasonably hostile laments: a discourse analysis of political dissent in Oman". *Discourse & society*, v. 28, n. 6, pp. 573-594.
https://doi.org/10.1177/0957926517721083

Arun, Chinmayi (2019). "On *WhatsApp*, rumours, and lynchings". *Economic & political weekly*, v. 54, n. 6.
https://www.epw.in/journal/2019/6/insight/whatsapp-rumours-and-lynchings.html

Banaji, Shakuntala; **Bhat, Ram** (2019). "*WhatsApp* vigilantes: an exploration of citizen reception and circulation of *WhatsApp* misinformation linked to mob violence in India". *Blog Media@LSE*, 11 November.
https://goo.su/XPcQ

Barbosa, Sérgio; **Milan, Stefania** (2019). "Do not harm in private chat apps: ethical issues for research on and with *Whatsapp*". *Westminster papers in communication and culture*, v. 14, n. 1, pp. 49-65.
https://doi.org/10.16997/wpcc.313

Barot, Trushar; **Oren, Eytan** (2015). *Report guide to chat apps*. Columbia Academic Commons, Tow Center for Digital Journalism Publications.
https://towcenter.gitbooks.io/guide-to-chat-apps/content

Baulch, Emma; **Matamoros-Fernández, Ariadna**; **Suwana, Fiona** (2022). "Memetic persuasion and whatsappification in Indonesia's 2019 presidential election". *New media & society*, Online first.
https://doi.org/10.1177/14614448221088274

Benevenuto, Fabricio; **Ortellado, Pablo** (2020). "WhatsApp data that could help research on misinformation in tackling misinformation: what researchers could do with social media data". *Harvard Kennedy school misinformation review*, v. 1, n. 8, pp. 6-7.
https://doi.org/10.37016/mr-2020-49

Benkler, Yochai; **Faris, Robert**; **Roberts, Hal** (2018). *Network propaganda: manipulation, disinformation, and radicalization in American politics*. Oxford, UK: Oxford University Press. ISBN: 978 0 190923624

Bennett, W. Lance; **Segerberg, Alexandra** (2012). "The logic of connective action". *Information, communication & society*, v. 15, n. 5, pp. 739-768.
https://doi.org/10.1080/1369118x.2012.670661

Bento, Gabrielly (2022). "WhatsApp baniu 2,4 milhões de contas na Índia em julho". *Olhar digital*, 5 setembro.
https://olhardigital.com.br/2022/09/05/seguranca/whatsapp-bane-24-milhoes-de-contas-na-india-em-julho

Bryant, Lauren-Valentino (2020). "The *YouTube* algorithm and the alt-right filter bubble". *Open information science*, v. 4, n. 1, pp. 85-90.
https://doi.org/10.1515/opis-2020-0007

Bursztyn, Victor S.; **Birnbaum, Larry** (2019) "Thousands of small, constant rallies: a large-scale analysis of partisan *Whatsapp* groups". In: *Proceedings IEEE/ACM International conference on advances in social networks analysis and mining 2019*, pp. 484-488.
https://doi.org/10.1145/3341161.3342905

Cesarino, Leticia (2020). "Como vencer uma eleição sem sair de casa: a ascensão do populismo digital no Brasil". *Internet & sociedade*, v. 1, n. 1, pp. 92-120.
https://revista.internetlab.org.br/serifcomo-vencer-uma-eleicao-sem-sair-de-casa-serif-a-ascensao-do-populismo-digital-no-brasil

Chagas, Viktor (2022). "*WhatsApp* and digital astroturfing: a social network analysis of Brazilian political discussion groups of Bolsonaro's supporters". *International journal of communication*, v. 16, pp. 2431-2455.
https://ijoc.org/index.php/ijoc/article/view/17296

Chagas, Viktor; **Mitozo, Isabele**; **Barros, Samuel**; **Santos, João-Guilherme**; **Azevedo, Dilvan** (2022). "The 'new age' of political participation? *WhatsApp* and call to action on the Brazilian senate's consultations on the e-cidadania portal". *Journal of information technology & politics*, v. 19, n. 3, pp. 253-268.
https://doi.org/10.1080/19331681.2021.1962779

Chagas, Viktor; **Modesto, Michelle**; **Magalhães, Dandara** (2019). "O Brasil vai virar Venezuela: medo, memes e enquadramentos emocionais no WhatsApp pró-Bolsonaro". *Esferas*, v. 14.
https://doi.org/10.31501/esf.v0i14.10374

Church, Karen; **Oliveira, Rodrigo** (2013). "What's up with *WhatsApp*? Comparing mobile instant messaging behaviors with traditional SMS". In: *Proceedings of mobile HCI 2013 - Collaboration and communication*, pp. 353-371.
https://www.ic.unicamp.br/~oliveira/doc/MHCI2013_Whats-up-with-whatsapp.pdf

Cosseti, Melissa-Cruz (2021). "O *WhatsApp* compartilha dados com o *Facebook*?". *Tecnoblog*, 8 janeiro.
https://tecnoblog.net/responde/o-whatsapp-compartilha-dados-com-o-facebook

Datafolha (2018). "Datafolha: 6 em cada 10 eleitores de Bolsonaro se informam pelo *WhatsApp*". *Veja*, 3 outubro.
https://veja.abril.com.br/politica/datafolha-eleitor-de-bolsonaro-e-o-que-mais-se-informa-por-redes-sociais

Diakopoulos, Nicholas (2014). *Algorithmic accountability: on the investigation of black boxes*. Tow Center for Digital Journalism, 3 December.
http://www.cjr.org/tow_center_reports/algorithmic_accountability_on_the_investigation_of_black_boxes.php

Evangelista, Rafael; **Bruno, Fernanda** (2019). "*WhatsApp* and political instability in Brazil: targeted messages and political radicalisation". *Internet policy review*, v. 8, n. 4.
https://doi.org/10.14763/2019.4.1434

Freitas, Miguel (2019). *WhatsApp nas eleições de 2018: o embate entre a lei, a tecnologia e o direito à privacidade*. Senado Federal.
http://legis.senado.leg.br/sdleg-getter/documento/download/bf52a4a0-ff2b-4f50-b9f8-af9b85c2a099

Garimella, Kiram; **Eckles, Dean** (2020). "Images and misinformation in political groups: evidence from WhatsApp in India". *Harvard Kennedy school misinformation review*, v. 1, n. 5.
https://doi.org/10.37016/mr-2020-030

Gil de Zúñiga, Homero; **Ardèvol-Abreu, Alberto**; **Casero-Ripollés, Andreu** (2019). "*WhatsApp* political discussion, conventional participation and activism: exploring direct, indirect and generational effects". *Information, communication & society*, v. 24, n. 2, pp. 201-218.
https://doi.org/10.1080/1369118x.2019.1642933

Gruber, Johannes B. (2022). "An R package for working with *WhatsApp* data". *GitHub*, 4 October.
https://github.com/JBGruber/rwhatsapp

Huszár, Ferenc; **Ktena, Sofia-Ira**; **O'Brien, Conor**; **Belli, Luca**; **Schlaikjer, Andrew**; **Hardt, Moritz** (2021). "Algorithmic amplification of politics on *Twitter*". *Proceedings of the National Academy of Sciences*, v. 119, n. 1.
https://doi.org/10.1073/pnas.2025334119

Iqbal, Mansoor (2022). "*WhatsApp* revenue and usage statistics 2022". *Business Fapps*.
https://www.businessofapps.com/data/whatsapp-statistics

Kabha, Robin; **Kamel, Ahmad**; **Elbahi, Moataz**; **Narula, Sumit** (2019). "Comparison study between the UAE, the UK, and India in dealing with *WhatsApp* fake news". *Journal of content, community & communication*, v. 10, n. 5, pp. 176-186.
https://doi.org/10.31620/JCCC.12.19/18

Klein-Bosquet, Oliver (2012). "El Movimiento de los Indignados: desde España a Estados Unidos". *El cotidiano*, v. 173, pp. 89-98.
https://www.redalyc.org/pdf/325/32523131010.pdf

Li, Da; **Pyke, Robert**; **Jiang, Runchao**; **Jagadeesh, Kiran** (2022). "Introducing the researcher platform: empowering independent research analyzing large-scale data from *Meta*". *Meta Research Blog*, 11 January.
https://research.facebook.com/blog/2022/1/introducing-the-researcher-platform-empowering-independent-research-analyzing-large-scale-data-from-meta

Mari, Angelica (2019). "*WhatsApp* banned nearly half a million accounts during Brazilian elections". *Zdnet*, November 20.
https://www.zdnet.com/article/whatsapp-banned-nearly-half-a-million-accounts-during-brazilian-elections

Massuchin, Michele; **Tavares, Camila**; **Mitozo, Isabele**; **Chagas, Viktor** (2021). "A estrutura argumentativa do descrédito na ciencia. Uma análise de mensagens de grupos bolsonaristas de *Whatsapp* na pandemia da Covid-19". *Fronteiras - estudos midiáticos*, v. 23, n. 2, pp. 160-174.
https://doi.org/10.4013/fem.2021.232.11

Matamoros-Fernández, Ariadna (2020). "'El negro de *WhatsApp*' meme, digital blackface, and racism on social media". *First Monday*, v. 25, n. 1.
https://doi.org/10.5210/fm.v25i12.10420

Medeiros, Ben; **Singh, Pawan** (2020). "Addressing misinformation on WhatsApp in India through intermediary liability policy, platform design modification, and media literacy". *Journal of information policy*, v. 10, pp. 276-298.
https://doi.org/10.5325/jinfopoli.10.2020.0276

Meirelles, Fernando S. (2022). *Pesquisa do uso da TI - tecnologia de informação nas empresas*. Fundação Getulio Vargas.
https://eaesp.fgv.br/sites/eaesp.fgv.br/files/u68/fgvcia_pes_ti_2022_-_relatorio.pdf

Mendonça, Ricardo-Fabrino; **Ercan, Selen A.**; **Ozguc, Umut**; **Reis, Stephanie-Lorraine-Gomes**; **Simões, Paula-Guimarães** (2019). "Protests as events: the symbolic struggles in 2013 demonstrations in Turkey and Brazil". *Revista de sociologia e política*, v. 27, n. 69.
https://doi.org/10.1590/1678987319276901

Mina, An-Xiao (2019). *Memes to movements: how the world's most viral media is changing social protest and power*. New York, NY: Penguin Random House. ISBN: 978 0 807056585

Mont'Alverne, Camila; **Mitozo, Isabele**; **Barbosa, Henrique** (2019). "*WhatsApp* e eleições: quais as características das informações disseminadas". *Le monde diplomatique Brasil*, 7 maio.
https://diplomatique.org.br/whatsapp-e-eleicoes-informacoes-disseminadas

Moura, Mauricio; **Michelson, Melissa R.** (2017). "*WhatsApp* in Brazil: mobilising voters through door-to-door and personal messages". *Internet policy review*, v. 6, n. 4.
https://doi.org/10.14763/2017.4.775

Mukherjee, Rahul (2020). "Mobile witnessing on *WhatsApp*: Vigilante virality and the anatomy of mob lynching". *South Asian popular culture*, v. 18, n. 1, pp. 79-101.
https://doi.org/10.1080/14746689.2020.1736810

Murgia, Madhumita; **Findlay, Stephanie**; **Schipani, Andres** (2019). "India: the *WhatsApp* election". *Financial Times*, 4 May.
*https://www.ft.com/content/9fe88fba-6c0d-11e9-a9a5-351eeaef6d84_*

Newman, Nic; **Fletcher, Richard**; **Kalogeropoulos, Antonis**; **Nielsen, Rasmus-Kleis** (2019). *Digital news report*. Reuters Institute; University of Oxford.
https://www.digitalnewsreport.org/survey/2019/overview-key-findings-2019

Padilha, Maria-Itayara-Coelho; **Ramos, Flávia-Regina-Souza**; **Borenstein, Miriam-Susskind**; **Martin, Cleusa-Rios** (2005). "A responsabilidade do pesquisador ou sobre o que dizemos acerca da ética em pesquisa". *Texto & contexto - enfermagem*, v. 14, n. 1, pp. 96-105.
https://doi.org/10.1590/s0104-07072005000100013

Panorama Mobile Time/Opinion Box Report (2020). *Mensageria no Brasil*. Mobile Time.
https://www.mobiletime.com.br/pesquisas/mensageria-no-brasil-fevereiro-de-2020

Passos, Paulo (2018). "Metade dos usuários acredita em noticias compartilhadas no *WhatsApp*". *Folha de São Paulo*, 26 octubre.
https://www1.folha.uol.com.br/poder/2018/10/metade-acredita-em-noticias-compartilhadas-no-whatsapp.shtml

Phillips, Whitney; **Milner, Ryan M.** (2020). *You are here: a field guide for navigating polarized speech, conspiracy theories, and our polluted media landscape*. Cambridge, MA: MIT Press. ISBN: 978 0 262539913.
https://direct.mit.edu/books/book/5041/You-Are-HereA-Field-Guide-for-Navigating-Polarized

Piaia, Victor; **Alves, Marcelo** (2020). "Abrindo a caixa preta: análise exploratória da rede bolsonarista no *WhatsApp*". *Intercom: revista brasileira de ciências da comunicação*, v. 43 n. 3, pp. 135-154.
https://doi.org/10.1590/1809-5844202037

Poder360 (2023). "Governo recebeu mais de 100 mil e-mails pelo 8 de Janeiro". *Poder360*, 6 fevereiro.
https://www.poder360.com.br/justica/governo-recebeu-mais-de-100-mil-e-mails-pelo-8-de-janeiro

Porter, Jon (2020). "*WhatsApp* says its forwarding limits have cut the spread of viral messages by 70 percent". *The verge*, 27 April.
https://www.theverge.com/2020/4/27/21238082/whatsapp-forward-message-limits-viral-misinformation-decline

Resende, Gustavo; **Melo, Philipe**; **Souza, Hugo**; **Messias, Johnnatan**; **Vasconcelos, Marisa**; **Almeida, Jussara M.**; **Benevenuto, Fabrício** (2019). "(Mis)Information dissemination in *WhatsApp*: gathering, analyzing and countermeasures". In: *Proceedings of the WWW'19 conference*, pp. 818-828.
https://homepages.dcc.ufmg.br/~fabricio/download/resende-www2019.pdf

Rossini, Patricia; **Baptista Érica-Anita**; **De-Oliveira, Vanessa-Veiga**; **Stromer-Galley, Jennifer** (2021). "Digital media landscape in Brazil: political (mis)information and participation on *Facebook* and *WhatsApp*". *Journal of quantitative description: Digital media*, v. 1.
https://doi.org/10.51685/jqd.2021.015

Rossini, Patricia; **Stromer-Galley, Jennifer**; **De-Oliveira, Vanessa-Veiga** (2020). "Dysfunctional information sharing on *WhatsApp* and *Facebook*: the role of political talk, cross-cutting exposure and social corrections". *New media & society*, v. 23, n. 8. pp. 2430-2451.
https://doi.org/10.1177/1461444820928059

Roth, Emma (2022). "*TikTok* to provide researchers with more transparency as damaging reports mount". *The Verge*, 27 September.
https://www.theverge.com/2022/7/27/23280406/tiktok-researchers-api-transparency-damaging-reports-china

Sacramento, Igor; **Paiva, Raquel** (2020). "Fake news, *WhatsApp* e a vacinação contra febre amarela no Brasil". *Matrizes*, v. 14, n. 1, pp. 79-106.
https://doi.org/10.11606/issn.1982-8160.v14i1p79-106

Saha, Punyajoy; **Mathew, Binny**; **Garimella**; **Kiran**; **Mukherjee, Animeshe** (2021). "'Short is the road that leads from fear to hate': Fear speech in Indian *WhatsApp* groups". In: *Proceedings of the Web conference 2021*, n. 4, pp. 1110-1121.
https://doi.org/10.1145/3442381.3450137

Sahafizadeh, Ebrahim; **Ladani, Behrouz** (2020). "A model for social communication network in mobile instant messagings". *IEEE transactions on computational social systems*, v. 7, n. 1, pp. 68-83.
https://doi.org/10.1109/TCSS.2019.2958968

Santos, João-Guilherme; **Freitas, Miguel**; **Aldé, Alesandra**; **Santos, Karina**; **Cunhna, Vanessa-Cristine-Cardozo** (2019). "*WhatsApp*, política mobile e desinformação: a hidra nas eleições presidenciais de 2018". *Comunicação & sociedade*. v. 41, n. 2.
https://doi.org/10.15603/2175-7755/cs.v41n2p307-334

Santos, Marcelo; **Saldaña, Magdalena**; **Tsyganova, Kesnia** (2021). "Subversive affordances as a form of digital transnational activism: The case of *Telegram*'s native proxy". *New media & society*, Online first.
*https://doi.org/10.1177/14614448211054830_*

Santos, Nina; **Chagas, Viktor**; **Marinho, Juliana** (2022). "De onde vem a informação que circula em grupos bolsonaristas no *WhatsApp*". *Intexto*, n. 53.
https://doi.org/10.19132/1807-8583202253.123603

Schaefer, Bruno-Marques; **Barbosa, Tiago-Alexandre-Leme**; **Epitácio, Sara-de-Sousa-Fernandes**; **Resende, Roberta-Carnelos** (2019). "Qual o impacto do *Whatsapp* em eleições? Uma revisão sistemática (2010-2019)". *Revista debates*, v. 13, n. 3, p. 58-88.
https://doi.org/10.22456/1982-5269.96255

Teixeira, Tarcisio; **Sabo, Paulo-Henrique**; **Sabo, Isabela-Cristina** (2017). "*WhatsApp* e a criptografia ponto-a-ponto: tendência jurídica e conflito privacidade vs. interesse público". *Revista da Faculdade de Direito da UFMG*, v. 71, p. 607-638.
https://doi.org/10.12818/p.0304-2340.2017v71p607

Tornes, Adam (2021). "Product news enabling the future of academic research with the *Twitter* API". *Twitter*, January 26.
https://developer.twitter.com/en/blog/product-news/2021/enabling-the-future-of-academic-research-with-the-twitter-api

TSE (2022). "*TSE* e *WhatsApp* celebram acordo para combate à desinformação nas eleições 2022". *TSE*, Fevereiro 15.
https://goo.su/XAU6

Valenzuela, Sebastián (2014). "Analisando o uso de redes sociais para o comportamento de protesto: o papel da informação, da expressão de opiniões e do ativismo". *Compolítica*, v. 4, n. 1, p. 13-52.
https://doi.org/10.21878/compolitica.2014.4.1.56

Vermeer, Susan A. M.; **Kruikemeier, Sanne**; **Trilling, Damian**; **De-Vreese, Class H.** (2020). "WhatsApp with politics?!: examining the effects of interpersonal political discussion in instant messaging apps". *The international journal of press/politics*, v. 26, n. 2, pp. 410-437.
https://doi.org/10.1177/1940161220925020

Vieira, Carolina-Coimbra; **Melo, Philippe-de-Freitas**; **De-Melo, Pedro O. S. Vaz**; **Benevenuto, Fabrício** (2019). "O paradoxo da viralização de informação criptografada no *WhatsApp*". In: *Anais do XXXVII Simpósio brasileiro de redes de computadores e sistemas distribuídos*, v. 37, pp. 403-416.
https://sol.sbc.org.br/index.php/sbrc/article/view/7375

Willaert, Tom; **Peeters, Stijn**; **Seijbel, Jasmin**; **Van-Raemdonck, Nathali** (2022). "Disinformation networks: a quali-quantitative investigation of antagonistic Dutch-speaking *Telegram* channels". *First Monday*, v. 27, n. 9.
https://doi.org/10.5210/fm.v27i5.12533

Wimmer, Mirian (2019). "Cidadania, tecnologia e governo digital: Proteção de dados pessoais no estado movido a dados". En: *Comitê gestor da internet no Brasil*. *TIC governo eletrônico: pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro*. *2019. ICT electronic government*, pp. 27-36.
https://cetic.br/media/docs/publicacoes/2/20200707094309/tic_governo_eletronico_2019_livro_eletronico.pdf

WhatsApp (2021). "Política de privacidade do WhatsApp". *WhatsApp*, Janeiro 4.
https://www.whatsapp.com/legal/privacy-policy/?locale=pt_BR

WhatsApp (2022). "Organizações da *Aliança Internacional de Checagem de Fatos* (*IFCN*) no *WhatsApp*". *WhatsApp*.
https://faq.whatsapp.com/528263691226435/?helpref=uf_share

Woolley, Samuel C.; **Howard, Philip N.** (eds.) (2018). *Computational propaganda: Political parties, politicians, and political manipulation on social media*. Oxford, UK: Oxford University Press. ISBN: 978 0 190931414

Wu, Yan; **Wall, Matthew** (2019). "The ties that bind: How the dominance of *WeChat* combines with *guanxi* to inhibit and constrain China's contentious politics". *New media & society*, v. 21, n. 8, pp. 1714-1733.
https://doi.org/10.1177/1461444819830072

Yahoo! Finance (2021). "Em quais países o *WhatsApp* é mais popular?". *Yahoo Finance BR*, October 18.
https://br.financas.yahoo.com/video/em-quais-pa%C3%ADses-o-whatsapp-130924324.html

YouTube (2022). "YouTube researcher program". *YouTube*.
https://research.youtube