CIVIC COMPASS

Un programa de **CIVIC HOUSE**

# **Leyes de protección de datos y sociedad civil:** navegando el impacto del RGPD

**Cecilia Galvan** (Civic House - Universidad de Buenos Aires)
**Orla Lynskey** ((Escuela de Economía y Ciencia Política de Londres)
**Katherine Nolan** (Universidad de Ulster)
**Gaston Wright** (Civic House - Universidad Torcuato Di Tella)

# Introducción[1]

En la era digital, la protección de datos es esencial para individuos, empresas y gobiernos. A medida que se recopilan, procesan y almacenan grandes cantidades de datos, garantizar la privacidad, la seguridad y el uso justo de dichos datos se ha convertido en un desafío importante. Los formuladores de políticas de todo el mundo han adoptado varias leyes de protección de datos para salvaguardar la privacidad individual y la protección de datos mientras persiguen otros objetivos, incluido el crecimiento económico y la garantía de los derechos humanos. Una regulación de protección de datos influyente es el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que ha tenido profundas implicancias para varios sectores, incluidas las organizaciones no gubernamentales (ONGs)[2] y ha servido como modelo para las leyes de protección de datos en todo el mundo.

Sin embargo, si bien dichas leyes tienen como objetivo proteger a las personas, también tienen consecuencias para la sociedad civil. A partir de insights sobre la implementación del RGPD en Europa y yuxtaponiéndolos con el caso de Brasil en América Latina, pretendemos echar luz sobre algunos de los desafíos y lecciones aprendidas. También pretendemos explicar el impacto de las estrictas leyes de protección de datos en las ONGs, centrándonos en los desafíos y las implicancias para las organizaciones sin fines de lucro con capacidad de cumplimiento limitada. Al comprender los efectos multifacéticos de las regulaciones de protección de datos, esperamos que este documento proporcione información valiosa para los formuladores de políticas sobre los riesgos de adoptar un modelo de "copiar y pegar" del RGPD sin tener en cuenta el contexto local.

El análisis procede de la siguiente manera. En la sección 1, describimos cómo funciona el RGPD. En la sección 2, presentamos algunos de los desafíos críticos asociados con el RGPD. En la sección 3, ofrecemos reflexiones iniciales sobre cómo se podrían mitigar algunos de estos desafíos. Luego, en la sección 4, profundizamos en el impacto que una ley como el RGPD puede tener en las organizaciones de la sociedad civil. En la sección 5, analizamos la Ley General de Protección de Datos (LGPD) de Brasil y sus implicaciones para las ONGs, centrándonos en el contexto particular del gobierno de Bolsonaro. Finalmente, en la sección 6, resumimos las ventajas y desventajas de los marcos integrales para la protección de datos y brindamos una serie de recomendaciones para los formuladores de políticas.

---

*1 Esta investigación fue posible gracias al generoso apoyo de la Fundación Mott y Luminate. Extendemos nuestro más sincero agradecimiento por su compromiso con el avance del conocimiento y la comprensión en este campo. Además, nos gustaría expresar nuestro agradecimiento a Katia Peirano, Asistente de Investigación de la Universidad Torcuato Di Tella, por su dedicada ayuda a lo largo de este estudio.*

*2 Schmitt, Miller, & Skiera (2021).*

# 1. Comprendiendo el RGPD

En esta sección, presentamos tres elementos clave para ayudar a comprender el RGPD. Primero, explicamos la estructura básica y el funcionamiento del RGPD. En segundo lugar, presentamos la influencia de las leyes de protección de datos de la Unión Europea en otras jurisdicciones, incluida la conexión con las normas sobre transferencias de datos según el RGPD. En tercer lugar, analizamos el contexto jurídico más amplio en que opera el RGPD.

## 1.1. Tratamiento lícito de datos

El RGPD reemplazó a la Directiva de Protección de Datos de 1995[3] que fue la primera legislación de protección adoptada a nivel de la Unión Europea.

El RGPD proporciona un marco ampliamente aplicable para la legalidad del procesamiento de datos, aunque se sitúa junto a la legislación complementaria[4] y existen exclusiones a su aplicación[5].

El RGPD se aplica al tratamiento de datos personales total o parcialmente por medios automatizados o al procesamiento de datos en sistemas de archivo[6]. La principal persona regulada según el RGPD es conocida como "responsable del tratamiento", quien puede ser una persona física o jurídica.

Las obligaciones en virtud del RGPD a las que está sujeto el responsable del tratamiento son amplias[7]. Además, se otorgan a los interesados derechos que pueden ejercer frente a los responsables del tratamiento (derechos de acceso, rectificación, supresión, limitación, portabilidad y oposición)[8].

El RGPD también crea una estructura de aplicación para supervisar la implementación de la ley y su aplicación[9]. Una parte integral de esta estructura es el rol de las autoridades independientes de protección de datos encargadas de monitorear y asegurar su cumplimiento.

---

*3 DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 24 de octubre de 1995 sobre la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos (DO L 281 de 23/11/1995, p. 31-50).*

*4 Ver Sección 2.3 debajo.*

*5 Ver Sección 3.1 debajo.*

*6 Artículo 2(1), RGPD.*

*7 Ver sección 3.2*

*8 Artículos 15-21 RGPD.*

*9 Ver sección 3.4*

## 1.2. La influencia de las leyes de protección de datos de la UE en otras jurisdicciones

La ley de protección de datos de la UE ha tenido mucha influencia en todo el mundo[10] y ha sido observada por Bradford como ejemplo del "efecto Bruselas"[11], el impacto de facto y de jure de la ley de la UE más allá de sus fronteras[12]. Varios factores contribuyen a la replicación de leyes de protección de datos de la UE en otras jurisdicciones. Un factor crucial son las normas de la UE sobre transferencias de datos fuera de la UE.

La posición por defecto según el RGPD y su Directiva predecesora es que las transferencias de datos fuera de la UE están prohibidas a menos que se cumplan ciertas condiciones[13]. Hay, en términos generales, tres formas de legitimar una transferencia de datos: confiar en una decisión de adecuación[14], garantizar que existan salvaguardias adecuadas[15] o confiar en una excepción (como el consentimiento o necesidad contractual)[16].

La Comisión Europea adopta decisiones de adecuación, que legitiman las transferencias de datos a países o territorios concretos. El RGPD faculta a la Comisión para evaluar regímenes jurídicos de estados no pertenecientes a la UE (o territorios o sectores de los mismos) y emitir un certificado de adecuación/decisión cuando considere que el país "garantiza un nivel adecuado de protección" [17]. En América Latina, Argentina[18] y Uruguay[19] fueron considerados adecuados por la Comisión en virtud de la Directiva de protección de datos. Por lo general, estas decisiones deben mantenerse bajo control regular. Sin embargo, esta política de revisión periódica no se ha aplicado de manera consistente. La primera revisión de las decisiones de adecuación adoptadas en virtud de la Directiva de protección de datos se informó el 15 de enero de 2024, y la Comisión determinó que todos los países considerados adecuados según la Directiva de protección de datos seguían proporcionando un nivel adecuado de protección[20]. La adopción de leyes que reflejen las protecciones de la Directiva de Protección de Datos o el RGPD ha influido en la toma de

---

*10 Ver, por ejemplo, Graham Greenleaf, 'Now 157 Countries: Twelve Data Privacy Laws in 2021/22' (2022) 176 Privacy Laws & Business International Report 3.*

*11 Tal fue el caso de iniciativas que luego se convirtieron en ley en Brasil, Paraguay y más recientemente en Ecuador, que adoptan en mayor o menor medida algunas normas y buenas prácticas recogidas por dicha normativa. Este hito fue precedido por otros desarrollos regionales, como la creación de las "Normas para la protección de datos personales" por parte de la Red Iberoamericana de Protección de Datos.*

*12 Anu Bradford, The Brussels Effect: How the European Union Rules the World (Oxford University Press 2020) xiv.*

*13 Artículo 44, RGPD; Artículo 25, Directiva de protección de datos.*

*14 Artículo 45, RGPD; Artículo 25, Directiva de protección de datos.*

*15 Artículo 46, RGPD; Artículo 26, apartado 2, Directiva de protección de datos.*

*16 Artículo 49, RGPD; Artículo 26, apartado 1, Directiva de protección de datos.*

*17 Artículo 45, apartado 1, del RGPD; Artículo 25, apartado 1, Directiva de protección de datos.*

*18 2003/490/CE: Decisión de la Comisión del 30 de junio de 2003 de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuada protección de datos personales en Argentina.*

*19 2012/484/UE: Decisión de Ejecución de la Comisión del 21 de agosto de 2012 de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuada protección de datos personales por parte de la República Oriental del Uruguay en lo que respecta al tratamiento automatizado de datos personales [notificada con el número C(2012) 5704].*

una decisión de adecuación por parte de la Comisión, un factor que ha llevado a que el RGPD se refleje en otras jurisdicciones.

## 1.3. Comprender el RGPD en contexto

El RGPD debe contextualizarse dentro del ordenamiento jurídico de la UE para reconocer (i) que el RGPD existe junto con otras leyes de procesamiento de datos, (ii) que el RGPD está conectado a las iniciativas de derechos fundamentales de la UE, y (iii) que el RGPD se implementa en el ámbito de los sistemas jurídicos de los Estados miembros de la UE.

Primero, el RGPD existe dentro de un panorama legal más amplio. Si bien se podría decir que el RGPD proporciona la protección básica de los datos personales en la legislación de la UE, existen leyes paralelas y cruzadas que también abordan la protección de datos, la privacidad y cuestiones relacionadas. Como complemento, existe legislación para proteger los datos personales y la privacidad en las comunicaciones electrónicas incluyendo reglas sobre el seguimiento de metadatos y el despliegue de tecnologías de seguimiento como las cookies[21]. Existe legislación separada para proteger el uso de datos personales para fines de aplicación de la ley[22], y dentro de las instituciones de la UE[23]. El Acta de Gobernanza de Datos establece reglas para cierta reutilización de datos por parte de organismos del sector público, para la intermediación de datos, servicios y en relación al altruismo de datos[24].

La Ley de Mercados Digitales[25] y la Ley de Servicios Digitales[26] recientemente adoptadas crean reglas para ciertos proveedores 'guardianes' de los servicios de plataforma más

---

*20 Informe de la Comisión al Parlamento Europeo y al Consejo sobre la primera revisión del funcionamiento del sistema de adecuación de decisiones adoptadas de conformidad con el artículo 25, apartado 6, de la Directiva 95/46/CE, Bruselas, 15.1.2024 COM(2024) 7 final. https://commission.europa.eu/system/files/2024-01/JUST_template_comingsoon_Report%20on%20the%20first%20review%20of%*

*21 DIRECTIVA 2002/58/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO del 12 de julio de 2002 sobre la tramitación de datos personales y la protección de la privacidad en el sector de las comunicaciones electrónicas (Directiva sobre privacidad y privacidad electrónica de las comunicaciones)(DO L 201 de 31/7/2002, p. 37–47) 200. Cabe señalar que se ha presentado una propuesta legislativa para reformar esta Directiva, aunque aún no se ha llegado a un acuerdo sobre la reforma.*

*22 DIRECTIVA (UE) 2016/680 DEL PARLAMENTO EUROPEO Y DEL CONSEJO del 27 de abril de 2016 sobre la protección de las personas naturales con respecto al procesamiento de datos personales por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de delitos penales o la ejecución de sanciones penales, y sobre la libre circulación de dichos datos, y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO L 119 de 4/5/2016, p. 89-131).*

*23 REGLAMENTO (UE) 2018/1725 DEL PARLAMENTO EUROPEO Y DEL CONSEJO del 23 de octubre de 2018 sobre la protección de personas físicas en lo que respecta al tratamiento de datos personales por parte de las instituciones, órganos, oficinas y agencias de la Unión y al libre movimiento de dichos datos y por el que se deroga el Reglamento (CE) n.º 45/2001 y la Decisión n.º1247/2002/CE (DO L 295 de 21/11/2018, p. 39-98).*

*24 REGLAMENTO (UE) 2022/868 DEL PARLAMENTO EUROPEO Y DEL CONSEJO del 30 de mayo de 2022 sobre la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Ley de Gobernanza de Datos)(DO L 152/1, 6/3/2022, p.1-44)*

importantes y reglas relacionadas con plataformas online, con responsabilidades adicionales para los proveedores de servicios muy grandes y los motores de búsqueda. Estas reglas de plataforma tienen ciertas superposiciones funcionales con el procesamiento de datos regido por el RGPD. La nueva Ley de Datos[27] y la propuesta de la regulación del Espacio Europeo de Datos Sanitarios[28], cuando se implemente, también se superpondrá con el RGPD.

En segundo lugar, debe entenderse que el RGPD se conecta con los derechos fundamentales de las protecciones de la UE. El RGPD expresa el derecho fundamental a la protección de datos, un derecho protegido por el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea (la "Carta"), pero en términos más generales en su materia, tiene una misión de derechos fundamentales. El artículo 1(2) del RGPD establece que "protege los derechos y libertades fundamentales de personas físicas y, en particular, su derecho a la protección de datos personales. Junto con el derecho al respeto de la vida privada en virtud del Convenio Europeo sobre Derechos Humanos, la Carta, ha desempeñado un papel crucial en el desarrollo de la legislación de protección de datos de la UE. Otros derechos, particularmente la libertad de expresión y el derecho a un recurso efectivo, son frecuentemente citados y equilibrados por el Tribunal de Justicia Europeo ("TJCE") en casos de protección de datos.

En tercer lugar, recordamos que el RGPD se implementa dentro de los regímenes legales de los Estados miembros de la UE. Aunque se trata de un reglamento de la UE, hay una serie de áreas en las que los Estados miembros tienen permitido restringir las protecciones del RGPD[29]. Además, hay áreas donde el RGPD permite niveles variables de protección de datos y los Estados miembros pueden variar el estándar RGPD en sus sistemas nacionales[30].Debido a que los Estados miembros de la UE en gran medida tienen autonomía sobre el derecho procesal nacional, también hay variaciones en la aplicación local y procedimientos de supervisión[31].

---

*25 REGLAMENTO (UE) 2022/1925 DEL PARLAMENTO EUROPEO Y DEL CONSEJO del 14 de septiembre de 2022 sobre contestabilidad y equidad de mercados en el sector digital y por la que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Ley de Mercados Digitales)(DO L 265/1 de 10/12/2022,p.1-66).*

*26 REGLAMENTO (UE) 2022/2065 DEL PARLAMENTO EUROPEO Y DEL CONSEJO del 19 de octubre de 2022 sobre un Mercado Único para Servicios digitales y modificación de la Directiva 2000/31/CE (Ley de servicios digitales)(DO L 277/1, 27/10/2022, p.1-102).*

*27 REGLAMENTO (UE) 2023/2854 DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre normas armonizadas sobre acceso equitativo y uso de datos (Ley de Datos)(DO L 2023/2854, 22/12/2023), p.1-71).*

*28 Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre el Espacio Europeo de Datos Sanitarios COM/2022/197 final.*

*29 Ver Sección 4.3 debajo.*

*30 Por ejemplo, el RGPD establece una edad predeterminada de 16 años como la edad a la que los niños pueden dar su consentimiento para el procesamiento de datos en relación con ciertos servicios de la sociedad de la información, pero los Estados miembros pueden adoptar una edad comprendida entre los 13 y los 16 años. Artículo 8(1), RGPD.*

*31 Aunque hay que tener en cuenta que la Comisión abrió una consulta para lograr cierta armonización administrativa en este espacio a principios de 2023. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13745-Further-specifying-procedural-rules-relating-to-the-enforcement-of-the-General-Data-Protection-Regulation_en*

# 2. Desafíos clave del RGPD

Hay cuatro desafíos particulares del modelo RGPD que destacamos: (i) su amplio ámbito de aplicación, (ii) el modelo único de responsabilidad, (iii) el impacto en la libertad de expresión y (iv) posibles consecuencias de aplicación de la ley.

## 2.1. Alcance

Una crítica persistente al RGPD es su alcance material demasiado amplio. Purtova llamó a la ley de protección de datos de la UE como la "ley de todo" debido a su amplio alcance[32]. Esta crítica se escucha tanto por parte de aquellos que creen que el RGPD se está extralimitando (es decir, regula inadecuadamente uso de datos, que no deberían estar sujetos a la ley) y también por parte de aquellos que sostienen que la amplitud de la aplicación de la ley socava su aplicabilidad.

El alcance material del RGPD se define en referencia al procesamiento de "datos personales". El procesamiento se entiende de manera muy amplia y se aplica esencialmente a cualquier uso de datos, incluida la recopilación de datos sin uso posterior[33]. Los datos personales se definen como "cualquier información relativa a una persona física identificada o identificable ('titular de los datos')"[34] . 'Datos personales' también tiene una interpretación amplia, y el umbral para la identificabilidad de individuos subyacentes es relativamente bajo. En particular, el TJCE ha enfatizado continuamente la importancia de adoptar una interpretación amplia para garantizar una protección adecuada de los interesados[35].

A su vez, las exclusiones a la aplicación del RGPD generalmente se interpretan de manera restrictiva. El RGPD no se aplica al procesamiento de datos personales, que queda fuera del alcance del derecho de la UE, en particular los fines de seguridad nacional de los Estados miembros[36]. Sin embargo, el TJUE ha determinado que esta excepción no se aplica cuando los proveedores de servicios contratan datos personales para fines de seguridad nacional, y se aplica la ley de la UE[37]. El RGPD no se aplica al trata-

---

*32 Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 Law, Innovation and Technology 40*

*33 Artículo 4(2), RGPD.*

*34 Artículo 4(1), RGPD.*

*35 Véase, por ejemplo, asunto C-582/14, Breyer (ECLI:EU:C:2016:779); Asunto C-434/16 Nowak (ECLI:EU:C:2017:994).*

*36 Artículo 2(a) y (b), RGPD.*

*37 Asunto C-623/17 Privacy International (ECLI:EU:C:2020:790).*

miento de datos personales "por parte de una persona física en el curso de una actividad puramente personal o doméstica"[38]

Nuevamente, esto se ha interpretado de manera restrictiva y no se aplican a la publicación de datos en línea, haciéndolos accesibles a un número indefinido de personas[39].

### 2.2. Modelo de responsabilidad

El RGPD opera principalmente con un enfoque de regulación de "talla única", y la mayoría de las obligaciones corresponden al "responsable del tratamiento de datos" regulado. Estas obligaciones son bastante onerosas y pueden implicar costos de cumplimiento, con adaptación limitada de las pequeñas y medianas empresas y sin exclusiones para entidades sin fines de lucro.

El "responsable del tratamiento" se define como "la persona física o jurídica, autoridad pública, agencia u otro organismo que, solo o conjuntamente con otros, determina los fines y medios del tratamiento de datos personales"[40] . El responsable del tratamiento es la principal entidad regulada por el RGPD, aunque las entidades que procesan datos en su nombre ("procesadores de datos") también están sujetos a algunas obligaciones. El concepto de responsable del tratamiento debe interpretarse de forma amplia según el TJCE para garantizar protección efectiva y completa de los interesados[41]. En particular, cuando más de una entidad tiene influencia sobre el tratamiento de datos, dichas entidades pueden considerarse corresponsables del tratamiento.  En una serie de casos del TJCE, se ha interpretado ampliamente que esta noción de corresponsables del tratamiento de datos significa que en algunos casos, los usuarios de redes sociales u otras herramientas en línea, como plug-ins o herramientas analíticas, puede dar lugar a que dichos usuarios sean considerados co-responsables de los datos tratados por la herramienta en cuestión[42].

Las obligaciones que enfrenta un controlador para procesar datos legalmente son importantes y relativamente complejas. Para procesar datos legalmente, los responsables del trata-

---

*38 Artículo 2(c), RGPD.*

*39 Asunto C-101/01, Bodil Lindqvist (2003), Rec. p. I-12992. Véanse también los asuntos C-212/13, Ryneš (ECLI:EU:2014:2428) y C-25/17, Jehovan todistajat (ECLI:EU:C:2018:551).*

*40 Artículo 4(7), RGPD. Nótese que, en determinados casos, el responsable del tratamiento podría estar definido en la legislación, cuando el tratamiento que se vaya a realizar está establecido en dicha legislación.*

*41 Asunto C-131/12 Google España y Google (ECLI:EU:2014:317).*

*42 Asunto C-210/16 Wirtschaftsakademie Schleswig-Holstein (ECLI:EU:C:2018:388); Asunto C-25/17 Jehová todistajat (ECLI:EU:-C:2018:551).*

miento deben poder demostrar que cumplen con los principios de protección de datos[43] y tienen una base legal para procesar datos (por ejemplo, consentimiento o una obligación legal)[44]. Existen reglas más estrictas para el procesamiento de algunas categorías especiales de datos[45]. Además, los responsables del tratamiento tienen obligaciones de transparencia y cumplimiento, que pueden implicar el requisito de designar un delegado de protección de datos[46]. Existen normas especiales que rigen las transferencias de datos fuera de la UE[47], para la seguridad de los datos y las respuestas a las violaciones de datos[48], con respecto a la toma de decisiones automatizada[49], y exigir al controlador de datos que participe en la protección por diseño y por defecto[50].

### 2.3. Relación con la libertad de expresión

Una tensión continua que se observa en la ley de protección de datos de la UE es su relación con la libertad de expresión. Formalmente, ambos son reconocidos como derechos fundamentales según la Carta de la UE, pero equilibrar estos derechos puede ser un desafío. Los críticos del RGPD han notado ciertas extralimitaciones de la norma en la libertad de expresión/acceso público a la información.

Formalmente, el RGPD reconoce la necesidad de equilibrar el derecho a la protección de datos con la libertad de expresión en una serie de disposiciones específicas. El derecho a la supresión puede limitarse cuando sea necesario para el ejercicio de la libertad de expresión[51]. Los Estados miembros deben conciliar el derecho a la protección de datos y a la libertad de expresión e información en el derecho interno, incluido el tratamiento con fines periodísticos y académicos, artísticos y literarios[52]. A tales efectos, los Estados miembros deben prever exenciones o derogaciones de muchas de las obligaciones del RGPD[53].

---

*43 Artículo 5, RGPD.*
*44 Artículo 6, RGPD.*
*45 Artículo 9, RGPD.*
*46 Artículos 12-14, RGPD; Capítulo IV, RGPD.*
*47 Capítulo V, RGPD.*
*48 Artículos 32-34, RGPD.*
*49 Artículo 22, RGPD.*
*50 Artículo 25, RGPD y Artículos 35-36, RGPD.*
*51 Artículo 17(3)(a), RGPD.*
*52 Artículo 85(1), RGPD.*
*53 Artículo 85(2), RGPD.*

El TJCE ha articulado el equilibrio entre libertad de expresión y protección de datos en el contexto de una serie de casos sobre el llamado "derecho al olvido". Establecido en Google España, el derecho al olvido faculta al interesado a que se eliminen determinadas URL de la lista del motor de búsqueda[54]. Se basa en un equilibrio entre la protección de datos y los intereses de privacidad del interesado y el interés público en la disponibilidad de la información. En Google España, de manera controvertida, el TJUE concluyó que los derechos de privacidad y protección de datos de un interesado por regla general, anulan no sólo el interés económico del operador del motor de búsqueda, sino también el interés del público en general en encontrar esa información mediante una búsqueda relacionada con el nombre del interesado"[55]. El TJCE aceptó que el interés público en la información sería más significativo en ciertos casos (por ejemplo, si el interesado era una figura pública), y esto informa la prueba de equilibrio que deben realizar los motores de búsqueda[56]. El balance entre los derechos de privacidad y de protección de datos y el derecho a la libertad de información fue más claramente explicado en el Artículo 11 de la Carta en el caso posterior de GC y otros[57]. Una vez más, se sostiene que los derechos del interesado a la privacidad y la protección de datos "anulan, como regla general, la libertad de información de los usuarios de Internet"[58].

Esta aparente priorización del derecho a la protección de datos puede sugerir una falta de respeto por el derecho a la libertad de expresión, aunque probablemente esto sea prematuro. Estos casos están enmarcados en el derecho a la libertad de información, por ejemplo, y son interpretaciones muy contextuales del equilibrio en cuestión. Sin embargo, refuerzan la necesidad de considerar la adecuada relación entre libertad de expresión y protección de datos en la adaptación de nuevas leyes de protección de datos.

### 2.4. Modelo de aplicación

El RGPD contiene una arquitectura de cumplimiento para supervisar las reglas sustantivas que protegen la información personal. Las autoridades nacionales de supervisión, el poder judicial y los interesados cumplen un rol y las consecuencias para los responsables del tratamiento de datos pueden ser importantes.

Cada Estado miembro de la UE debe tener una autoridad supervisora independiente, que esté dotada de poderes de investigación y aplicación de la ley (incluido el manejo de quejas e imponer sanciones, incluidas multas)[59]. Se ha creado un mecanismo de coordinación para

---

*54 C-131/12 Google España y Google (ECLI:EU:2014:317).*

*55 Asunto C-131/12 Google España y Google (ECLI:EU:2014:317), apartado 97.*

*56 Ibid.*

*57 Asunto C-136/17 GC y otras (ECLI: EU: C: 2019: 773), apartado 59.*

*58 Ibid, párrafo 66.*

*59 Capítulo VI, RGPD.*

permitir que las autoridades nacionales de supervisión en toda la UE cooperen[60], y la Junta de Protección de Datos de la Unión Europea se creó para supervisar la coherencia de la aplicación en toda la UE[61]. Las sanciones son potencialmente muy importantes. Se pueden imponer multas de hasta 20 millones de euros o hasta el 4% del volumen de negocios anual total a nivel mundial[62].

Los interesados tienen derecho a presentar una queja ante su autoridad supervisora local[63] o a buscar un recurso judicial (contra una autoridad supervisora o un controlador), incluyendo compensación[64]. También debe ser provista la representación colectiva de los sujetos individuales de datos por parte de las organizaciones sin fines de lucro[65].

Gran parte de las críticas al RGPD se relacionan con su aplicación. Hay dos razones principales; En primer lugar, existe una percepción de falta de cumplimiento o de falta de impacto sustancial sobre las prácticas ilegales de datos. En segundo lugar, existe la percepción de una aplicación desigual, con algunas autoridades de supervisión (particularmente los reguladores irlandeses y luxemburgueses) caracterizadas como menos probables de imponer sanciones o finalizar decisiones.

---

*60 Capítulo VII, RGPD.*
*61 Artículos 68-76, RGPD.*
*62 Artículo 83, RGPD.*
*63 Artículo 78, RGPD.*
*64 Capítulo VIII, RGPD.*
*65 Artículo 80, RGPD.*

# 3. ¿Mitigar los desafíos del RGPD?

En esta sección, consideramos dónde hay espacio para mitigar los desafíos del RGPD, con miras a las sugerencias que las organizaciones de la sociedad civil quieran presentar a los legisladores para adoptar leyes de protección de datos.

## 3.1. . Otros modelos de protección de datos

Si bien el RGPD y la Directiva de protección de datos anterior han tenido gran influencia, la protección de datos de la UE no es el único modelo de protección de datos a nivel mundial. En particular, el Convenio del Consejo de Europa para la protección de las personas en materia de Procesamiento de Datos Personales ("Convenio 108") es una alternativa notable[66].

El Convenio 108 ha dado forma a algunos de los aspectos centrales de la legislación de protección de datos de la UE: la comprensión de los datos personales, la regulación del "responsable" y obligaciones clave como los principios de protección de datos, normas relativas a categorías especiales de datos, seguridad de los datos y derechos de los interesados. Este Convenio es menos prescriptivo que el RGPD pero igualmente busca proteger los derechos fundamentales en el contexto del procesamiento de datos digitales. Muchos países de América Latina, incluidos Argentina, México y Uruguay, lo han ratificado.

Se abrió a la firma una versión modernizada del Convenio, el Convenio 108+[67], en 2018. Busca actualizar la Convención y agrega normas en relación con la legalidad del procesamiento de datos, categorías especiales adicionales de datos, derechos más específicos de los interesados y la naturaleza de las sanciones y remedios que se crearán. Ha sido ratificado por Argentina y Uruguay en América Latina.

---

*66 Convenio para la Protección de las Personas con respecto al Tratamiento Automático de Datos Personales de 1981.*
*67 https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1*

### 3.2.Supervisión independiente

Un aspecto clave de la legislación de protección de datos de la UE es el papel de la autoridad nacional de supervisión.

Con respecto a su rol, cabe señalar dos puntos importantes. En primer lugar, una autoridad reguladora independiente y con buenos recursos puede ser un control importante sobre el abuso de la ley, como el uso de la ley de protección de datos para censurar la expresión.

Dotar de recursos adecuados a las autoridades de supervisión en la UE ha sido un desafío en algunos casos, con la consecuencia de que las autoridades pueden ser subcontratadas por los controladores a quienes pretenden regular.

En segundo lugar, observamos la importancia de la independencia de esas autoridades. La independencia de las autoridades reguladoras es una cuestión de derecho primario de la UE[68]. La Comisión tiene una función de ejecución para garantizar que se mantenga dicha independencia, y se han iniciado varios casos contra Estados miembros en los que se consideró que la independencia de la autoridad pertinente estaba comprometida[69].

### 3.3. Excepciones para proteger la libertad de expresión y las PYMEs

Finalmente, el RGPD permite a los Estados miembros restringir la aplicación de sus requisitos en ciertas instancias. Cualquier país que modele sus leyes siguiendo el enfoque de la UE también debería tomar en consideración los casos en que las derogaciones podrían ser adecuadas para sus contextos nacionales o regionales.Estas normas del RGPD (las prohibiciones y los requisitos ex ante específicos) se aplican menos coherentemente en los diferentes Estados miembros.

El artículo 23 del RGPD permite restricciones de determinadas obligaciones del RGPD, siempre que tales restricciones satisfagan un análisis de derechos fundamentales (incluida la proporcionalidad)[70]. Se pueden imponer restricciones por motivos de seguri-

---

*68 Artículo 8(3), Carta.*

*69 Comisión/Alemania (C-518/07, Rec. p. I-01885); Asunto C-614/10 Comisión/Austria (ECLI:EU:2012:631); Asunto C-288/12 Comisión contra Hungría (ECLI:EU:C:2014:237).*

*70 Artículo 23 GDPR.*

dad nacional, seguridad pública, protección de la justicia independencia y procedimientos judiciales, la protección de los derechos y libertades de otros, y la ejecución de reclamaciones civiles, entre otras causales.

Además, observamos que el RGPD reconoce las diferentes posiciones de las organizaciones más pequeñas. Ciertas organizaciones que tienen menos de 250 empleados no deben asumir todas las obligaciones de mantenimiento de registros, siempre que no realicen determinados tipos de procesamiento de alto riesgo[71] . Dado el contexto de derechos humanos en el que se ubica el RGPD, el principio de proporcionalidad –en particular, la idea de que las medidas no deben ir más allá de lo necesario para lograr los propósitos declarados, pueden tener un papel que desempeñar. Sin embargo, esto aún no ha sido aclarado por los tribunales. Algunas modificaciones de la naturaleza de las obligaciones pueden ser apropiadas para el procesamiento de bajo riesgo o en pequeña escala.

*71 Artículo 30 GDPR.*

# 4. Las ONG y la gestión de datos

Habiendo reflexionado sobre algunos de los desafíos generales asociados con el RGPD, vamos a considerar cómo estos desafíos podrían ser particularmente relevantes para los actores de la sociedad civil, incluidas las ONG. Los actores de la sociedad civil, al igual que otros actores económicos, públicos o privados, es probable que estén sujetos a regulaciones de protección de datos. Aun así, la falta de capacidad administrativa, financiera y las capacidades de los recursos humanos pueden obstaculizar su habilidad para lograr sus misiones cívicas.

Los estudios sobre la sociedad civil y sus organizaciones han documentado, desde diversos enfoques, la importancia de una sociedad civil sólida para la construcción de sociedades democráticas[72]. Como se muestra arriba, algunos desafíos clave de la aplicación de leyes similares al RGPD son el alcance, los modelos de responsabilidad, su impacto en la libertad de expresión y el modelo de aplicación de la ley. Sin embargo, las ONGs difieren en tamaño, modelos de sostenibilidad, actividades y misiones al considerar a la sociedad civil como actores. En particular, como se mostró en la sección 2, un modelo basado en un material demasiado amplio en alcance como el RGPD, en combinación con burocracias que gozan de poca autonomía, pueden crear riesgos de efectos adversos sobre la libertad de expresión. Para evaluar los posibles riesgos e impactos sobre las ONGs, en esta sección primero consideramos algunas de las formas críticas en que las ONGs utilizan y gestionan datos y luego determinamos qué significaría esto para el cumplimiento de las ONGs con la legislación de protección de datos.

## 4.1. Uso y gestión de datos por parte de las ONG

En términos de uso y gestión de datos, muchas ONG han avanzado hacia la transformación digital con otros actores. Este movimiento implica el uso de sistemas SIG (Sistemas de Información Geográfica), tecnologías virtuales y móviles en el contexto de las tecnologías cívicas. ('Tecnologías cívicas' se refiere a las tecnologías y estrategias de información y comunicación adoptadas para beneficiar a los ciudadanos. El término fue pionero en el reporte de la Fundación Knight[73], que identificó diferentes propósitos de las organizaciones cívicas, incluido el crowdfunding, el intercambio P2P, los datos abiertos, la

*72 Carew Boulding ONGs, protesta política y sociedad civil. En ONGs, protesta política y sociedad civil (p. I). Cambridge: Cambridge University Press (2014).*
*73 https://knightfoundation.org/features/civictech/*

utilidad de los datos, la visualización y mapeo de datos de plataformas comunitarias, herramientas de votación y acciones de rendición de cuentas democráticas).

Algunos elementos clave de las prácticas de uso y gestión de datos de las ONGs[74] son:

i. **Diversas aplicaciones de la tecnología:** organizaciones públicas y privadas, empresas e individuos de todo el mundo utilizan una amplia gama de sistemas SIG, tecnologías virtuales y móviles para experimentar y desarrollar tecnologías cívicas. Estas tecnologías se utilizan para abordar diversos desafíos sociales y relacionados con la comunidad.

ii. **Colaboración y plataformas cívicas:** los esfuerzos de colaboración son comunes, varias partes interesadas se unen para trabajar en proyectos de tecnología cívica. Las comunidades en línea son cruciales para facilitar la colaboración y proporcionar una plataforma para las redes entre pares, movilización de partes interesadas y participación de asociaciones. Las plataformas cívicas pueden servir como incubadoras de ideas innovadoras

iii. **Análisis de datos:** los métodos de análisis de datos digitales se destacan como herramientas poderosas para desarrollar la capacidad comunitaria. Las plataformas online recopilan datos estructurados y no estructurados que pueden analizarse para obtener conocimientos e informar la toma de decisiones.

iv. **Desafíos en el compromiso impulsado por la tecnología:** el compromiso impulsado por la tecnología en las comunidades cívico tecnológicas ofrece muchas oportunidades pero presenta varios desafíos de diseño y gestión. Estos desafíos pueden incluir la privacidad y la protección de datos, la seguridad y el uso eficaz de la tecnología en contextos no comerciales.

Estas prácticas ilustran la importancia de la tecnología y el análisis de datos para las comunidades cívico tecnológicas. Existe una tensión entre el cumplimiento adecuado de las normas de protección de datos y el mantenimiento de canales deseables para la libertad de expresión. Por ejemplo, un estudio de Berdou y Shutt ha demostrado que sólo la mitad de una muestra de veinte proyectos africanos y asiáticos de tecnología cívica que actúan como "intermediarios de crowdsourcing" tenían una política de privacidad publicada. Además, registraron que seis de ellos no lograron explicar la secuencia de acciones que la información presentada desencadenaría[75]. Este estudio también

---

*74 Mačiulienė, Monika y Skaržauskienė, Aelita (2020) Creación de capacidades de comunidades tecnológicas y cívicas a través del análisis de datos digitales, Revista de Innovación y Conocimiento, Volumen 5, Número 4, 2020, páginas 244-250, ISSN 2444-569X, https://doi.org/10.1016/j.jik.2019.11.005.*

puede ser relevante para la cultura latinoamericana que se ha quedado rezagada en cuanto al desarrollo de datos regionales, marcos regulatorios de protección y donde es necesario fortalecer los canales de expresión de grupos vulnerables.

Las ONGs, en particular aquellas con recursos limitados, se encuentran en una posición única. Al no tener fines de lucro como las empresas, a menudo todavía manejan grandes cantidades de datos personales relacionados con poblaciones vulnerables. Los estrictos requisitos de las leyes de protección de datos pueden plantear desafíos a estas organizaciones, y es poco probable que algunas ONGs puedan cumplir con estas leyes.

Las organizaciones de la sociedad civil a menudo manejan una gama diversa de datos, dependiendo de su área de acción. Esto puede incluir datos personales sobre beneficiarios, donantes, voluntarios, personal, miembros de la comunidad y sujetos de investigación. Estos datos pueden incluir nombres, direcciones, datos de contacto, información de salud, datos de pago, afiliación política, intereses, ingresos y prestaciones de seguridad social. Además, las ONGs recopilan datos operativos relacionados con sus proyectos, incluidos presupuestos, cronogramas y resultados. Las ONGs también recopilan datos de campo de actividades sobre el terreno, encuestas y otras investigaciones. Por ejemplo, como está documentado[76], una ONG centrada en la salud podría recopilar datos sobre la prevalencia de enfermedades, tasas de vacunación, e infraestructura de salud en una región particular. Finalmente, un componente crítico de los datos de las ONGs son los datos de comunicación y recaudación de fondos relacionados con la divulgación, la promoción, la concientización y campañas de donantes, incluyendo retroalimentación, métricas de participación y evaluaciones de impacto[77].

Los conocimientos basados en datos ayudan a las ONGs a decidir dónde asignar recursos, qué proyectos priorizar y cómo diseñar intervenciones de manera efectiva. Las ONGs dependen de los datos para medir el impacto de sus iniciativas, asegurando que estén logrando sus objetivos y haciendo una diferencia positiva[78]. Al mantener registros de datos claros, las ONGs pueden demostrar transparencia a los donantes, las partes interesadas y las comunidades. Además, los datos son estratégicos para mejorar la asignación de los recursos. Los datos recopilados ayudan a las ONG a identificar áreas de necesidad, asegurando que los recursos se dirigen donde más se necesitan[79].

---

*75 Berdou, E. y Shutt, C. (2017) Cambiando el foco de atención: entendiendo a los intermediarios de crowdsourcing en transparencia e iniciativas de rendición de cuentas, Informe de investigación Making All Voices Count, Brighton: IDS*
*76 Dash y Mishra (2014).*
*77 Ver Iñarra (2023).*
*78 Ver Rhode, Rana, & Edwards (2017).*
*79 Véase, por ejemplo https://hazrevista.org/tercersector/2023/10/formacion-movilidad-globales-captacion-fondos-fundraising/*

El desafío de cumplir con las regulaciones de protección de datos a menudo requiere que las ONGs inviertan en tecnología, capacitación y procesos. Para las ONGs con recursos limitados, las inversiones pueden ejercer presión sobre sus presupuestos, desviando fondos de actividades básicas. Se debe tener en cuenta que el aumento de la burocracia interna que implica implementar medidas de protección de datos puede llevar a un aumento de las tareas administrativas. Es posible que las ONGs necesiten crear equipos específicos o departamentos para manejar la protección de datos, lo que lleva a posibles retrasos burocráticos en la toma de decisiones y operaciones.

Como destacan Buckley, Caulfield y Becker (2021), también existe la posibilidad de que los datos de auditorías u otras actividades de aplicación de la ley se utilicen como herramientas de represalia. Los gobiernos podrían inundar a las ONGs con investigaciones[80], no por una preocupación genuina por sus prácticas de datos, sino por abrumar e interrumpir las operaciones de la organización.

### 4.2. Implicaciones del incumplimiento para las ONGs

Como vemos arriba, el camino hacia el cumplimiento puede ser un desafío. Sin embargo, ofrece varios beneficios y aspectos positivos. Las ONGs pueden garantizar operaciones más eficientes y seguras modernizando sus operaciones de datos y mejorando los procesos de gestión de riesgos[81]. Estas mejoras pueden conducir a una mejor toma de decisiones, intervenciones más efectivas y una mayor capacidad para medir el impacto. Además, el cumplimiento de las regulaciones de protección de datos puede ser una poderosa señal de confiabilidad. En una época en la que el uso indebido de datos y las preocupaciones sobre la privacidad son rampantes, el compromiso de una ONG con la protección de datos puede diferenciarla, reforzar su reputación y fomentar una confianza más profunda con los donantes, los beneficiarios y el público en general[82].

Las implicaciones del incumplimiento de las normas de protección de datos para las ONGs son multifacéticas y pueden tener profundas consecuencias en sus operaciones y reputación. El incumplimiento de estas regulaciones se enfrenta a posibles sanciones y multas legales. Por ejemplo, según el RGPD, las organizaciones pueden recibir una multa de hasta el 4% de su facturación global anual o 20 millones de euros, lo que sea

---

*80 Un caso que podría analizarse seriamente es el de México. Consulte estas columnas para conocer un enfoque: https://elpais.com/opinion/2021-10-23/la-sociedad-civil-en-tiempos-de-amlo.html o https://www.lapoliticaonline.com/mexico/politica-mx/amlo-agencias-de-eu-son-complices-de-corrupcion-por-financiar-organizaciones-contra-la-4t/*

*81 Ver el trabajo realizado por organizaciones como Wingu en el desarrollo de infraestructura técnica especialmente orientada a las ONGs https://winguweb.org/*

*82 Buckley, Caulfield, Becker (2021).*

mayor[83]. Estas sanciones financieras podrían ser devastadoras para las ONGs, muchas de las cuales operan con presupuestos ajustados y dependen en gran medida de la financiación de donantes. Incluso donde las sanciones máximas no son probables en respuesta a infracciones menores de la ley, la mera amenaza de sanción puede afectar las decisiones operativas.

Más allá de las posibles implicaciones financieras, también existe la amenaza inminente de un deterioro de la reputación. Las ONGs, por su propia naturaleza, se basan en la confianza. Dependen de esta confianza para aumentar fondos, reclutar voluntarios y llevar a cabo sus misiones. Cualquier incumplimiento percibido de esta confianza, especialmente en la protección de datos, puede tener repercusiones duraderas. Donantes, voluntarios, y el público en general puede desconfiar de apoyar o asociarse con una ONG que haya mostrado negligencia en la protección de datos confidenciales. Esta erosión de la confianza puede suponer un desafío para las ONGs a la hora de cumplir sus misiones e incluso conduce a una disminución de las contribuciones de los donantes. Además, el incumplimiento puede tensar las relaciones con otras organizaciones. Los socios y colaboradores pueden dudar en compartir o acceder a datos con ONGs que tienen sospechas de incumplimiento, lo que limita las iniciativas conjuntas y las oportunidades de proyectos.

Además, las ONGs son susceptibles a violaciones de datos sin una protección de datos sólida y medidas de ciberseguridad. Tales violaciones podrían exponer información confidencial, incluyendo detalles de donantes, registros de empleados y datos de beneficiarios. Una violación de datos agrava el daño a la reputación y puede dar lugar a investigaciones y desafíos legales adicionales. Los órganos reguladores podrían iniciar investigaciones sobre las ONGs sospechosas de incumplimiento, lo que lleva a acciones formales de aplicación de la ley. Tales investigaciones o medidas coercitivas pueden desviar recursos críticos y atención de las actividades principales de la ONG, obstaculizando aún más su eficacia.

En resumen, si bien el camino hacia el cumplimiento de la protección de datos puede presentar desafíos, las ONGs pueden reforzar su compromiso con las operaciones éticas, mejorar la eficiencia operativa y profundizar su confianza con las partes interesadas invirtiendo en protección de datos.

Para considerar cómo las ONGs pueden responder a estas demandas contrapuestas, podemos mirar las experiencias de implementación de leyes comparables en países vecinos. Si bien los países latinoamericanos reconocen la privacidad de alguna forma en

---

*83 Artículos 83-84, GDPR.*

sus constituciones[84], varios países también han promulgado leyes de protección de datos[85], que tienen muchos puntos en común con el RGPD. Brasil es un ejemplo; Podemos examinar la experiencia brasileña como un caso de estudio.

El siguiente apartado profundizará en las complejidades de la aplicación de la nueva ley de protección de datos y cómo la relación conflictiva de la administración brasileña con ciertas ONGs destaca los riesgos de que los Estados utilicen la ley como arma para presionar a las ONGs.

*84 Véase, Rodríguez, Katitza, "Análisis comparado de las leyes y prácticas de vigilancia en América Latina", Necesarios & Proporcionados, Electronic Frontier Foundation (EFF), 2016, disponible en: https://necessaryandproportionate.org/es/análisis-comparativo-surveillance-laws-and-practices-latin-america/#resumenejecutivo, octubre de 2023.*

*85 Ver https://adc.org.ar/wp-content/uploads/2019/06/023-A-El-sistema-de-protecci%C3%B3n-de-datos-personales-en-Am%C3%A9ricaLatina- Vol.-I-12-2016.pdf*

# 5. La Ley General de Protección de Datos (LGPD) de Brasil: un análisis de su evolución e implicaciones para las ONGs [86]

La Ley General de Protección de Datos de Brasil[87](LGPD, Lei 13.709/2018), promulgada en 2018 y puesta en funcionamiento en 2020 tras dieciocho modificaciones, es un marco legal diseñado para garantizar la privacidad individual y el control sobre sus datos, ampliamente definidos. En común con el RGPD de la UE, la LGPD abarca un amplio espectro de datos personales y estrictos requisitos de consentimiento para el procesamiento de datos.

Al igual que el RGPD, un aspecto central de la LGPD es el procesamiento basado en requisitos legales específicos (incluido el consentimiento inequívoco y libre de los interesados) y transparencia en relación con la recopilación de datos y su utilización específica. La ley también anunció el establecimiento de la Autoridad Nacional de Protección de Datos de Brasil (ANPD) para supervisar y sancionar el incumplimiento, con sanciones que van desde advertencias hasta multas de hasta el 2% de los ingresos de una empresa y posible suspensión operativa. Aplicable tanto en el sector público como en el privado, la LGPD prescribe las bases jurídicas sobre las cuales los responsables del tratamiento pueden procesar datos (incluido el consentimiento y los intereses legítimos del responsable del tratamiento), además de imponer medidas generales de protección de datos, salvaguardar los derechos fundamentales de los interesados e imponer obligaciones y limitaciones en cuanto al procesamiento de datos personales.

Si bien Brasil tiene más de 40 disposiciones legales sobre privacidad y datos personales, la LGPD reemplaza y complementa el marco regulatorio sectorial existente para brindar claridad legal y certeza. Sin embargo, la transición de la adopción de la legislación a la implementación coincidió con la pandemia de COVID-19, marcada por un importante incidente relacionado con el uso de datos por el gobierno brasileño[88]. Las investigaciones revelaron esfuerzos de adquisición de datos por parte del gobierno federal y 14 gobiernos estatales para coordinar las respuestas a la pandemia que involucran acuerdos de terceros para la recopilación, manipulación y almacenamiento de

---

*86 El Sistema Interamericano de Derechos Humanos (SIDH) a través de la Convención Americana sobre Derechos Humanos (CADH); la Declaración americana de los Derechos y Deberes del Hombre (DADD); la jurisprudencia y opiniones consultivas emitidas por la Corte Interamericana de Derechos Humanos (CIDH); así como informes de casos, temáticos y por país, emitidos por la Comisión Interamericana de Derechos Humanos (CIDH) en conjunto forman el marco legal básico en América Latina.*

*87 https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm*

*88 Q&A: El Tribunal Supremo de Brasil acaba de reforzar los derechos de privacidad de datos. (2020, 20 de julio). Ver https://www.opensocietyfoundations.org/voices/q-and-a-how-civil-society-in-brazils-is-defending-privacy-rights*

datos. Este incidente destacó las vulnerabilidades gubernamentales en materia de seguridad y transparencia. Una preocupación importante fue la ausencia de herramientas de anonimización, especialmente dada la sensibilidad de los datos de salud.

En abril de 2020, el gobierno brasileño emitió la Orden Ejecutiva N° 954, que exige a las empresas de telecomunicaciones compartir datos de clientes con el Instituto Brasileño de Geografía y Estadística (IBGE) con fines estadísticos durante la pandemia de COVID-19. Esto incluía nombres, números de teléfono y direcciones. El Colegio de Abogados de Brasil y las partes implicadas presentaron demandas argumentando violaciones constitucionales.

El 24 de abril, el Supremo Tribunal Federal suspendió la orden ejecutiva, citando privacidad, preocupaciones sobre la dignidad y el debido proceso. Data Privacy Brasil contribuyó como amicus curiae[89],haciendo hincapié en la protección de datos personales como un derecho fundamental. Finalmente, el 7 de mayo, el Supremo Tribunal Federal confirmó la suspensión con una votación de 10 a 1. Los argumentos clave incluyeron la necesidad de definiciones más precisas, la colisión con la protección constitucional, la ausencia de salvaguardias fundamentales, y el carácter innecesario y desproporcionado de la recolección de los datos, dados los recursos existentes.

El fallo destacó la necesidad de especificidad en el uso de datos, cumplimiento de las normas con límites constitucionales, la implementación de salvaguardas y la exploración de alternativas menos invasivas para la investigación. La Corte Suprema[90] suspendió la implementación del programa de vigilancia sin un calendario, sentando así un precedente fundamental a nivel nacional y mundial[91].

Más allá de esta acción judicial inicial, existen perspectivas más amplias sobre la ejecución judicial en Brasil que vale la pena considerar. Investigaciones recientes[92], que analizan más de 400 decisiones de apelación en 2022 buscan discernir la aplicación por parte del poder judicial de la nueva regulación de privacidad de datos de Brasil. Surgieron cuatro tendencias destacadas: (1) los tribunales no otorgan automáticamente compensación por los datos a las víctimas de violaciones, que requieren prueba de daño tangible o intangible; (2) casi la mitad de las decisiones analizadas estaban relacionadas con el

---

*89 https://www.dataprivacybr.org/wp-content/uploads/2020/05/dpbrr_roteiro_sustentacao_stf_english_final.pdf*

*90 Caso REFERENDO NA MEDIDA CAUTELAR NA AÇÃO DIRETA DE INCONSTITUCIONALIDADE 6.387 DISTRITO FEDERAL: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2021/02/OAB-v-Bolsonaro.pdf*

*91 Para obtener más información sobre la dinámica política de las decisiones de los tribunales brasileños, consulte Lage-Freitas, A. Allende-Cid, E. Santana, O. Oliverira-Lage, I (2022, marzo) Predicción de decisiones judiciales brasileñas. En PeerJ Ciencias de la Computación.*

*92 Relatório Anual de Jurimetria 2022 https://opiceblum.com.br/wp-content/uploads/2019/07/09-relatorio-jurimetria-2022.pdf*

procesamiento de datos personales para el cobro de deudas o créditos con fines de protección; (3) los tribunales fallaron consistentemente a favor de las víctimas de fraude; y (4) los tribunales exhibieron rigor cuando los datos personales se utilizaron para fines secundarios, especialmente si los agentes procesadores carecían de medidas de transparencia. Predominantemente, las sentencias favorecieron la protección de los datos, atribuible en parte a la modificación del artículo 5 de la Constitución brasileña[93], que consagra la protección de datos personales, incluidos los digitales, como un derecho fundamental[94].

La ANPD introdujo regulaciones específicas para las pequeñas empresas[95] en enero de 2022 para perfeccionar aún más la ley. Esto tenía como objetivo equilibrar las provisiones de LGPD y los desafíos únicos de las entidades más pequeñas del sector privado. Los reguladores entendieron que las pequeñas empresas enfrentan desafíos de cumplimiento similares a los que hemos descrito para las ONGs. A través de iterativas revisiones y contribuciones de la sociedad civil, la ANPD garantizó el mejor funcionamiento de estas empresas en línea con los estándares de la ley.

Un aspecto digno de mención de la aplicación de la ley es el "enfoque receptivo" de la ANPD, que enfatiza el diálogo sobre la imposición inmediata de sanciones. Aunque aparentemente indulgente, este enfoque, respaldado por los desarrollos antes mencionados, fomenta una cultura de privacidad y mejores prácticas[96].

En conclusión, la LGPD de Brasil se esfuerza por salvaguardar la privacidad de los usuarios y el control de los datos personales, instituyendo requisitos rigurosos de consentimiento y sanciones por incumplimiento. A pesar de los desafíos iniciales de implementación, la aplicación de la ley ha sido respaldada por la Corte Suprema, sentando un importante precedente mundial. El poder judicial brasileño ha solicitado la ley de forma favorable a los reclamos iniciadas por los ciudadanos, respaldada por una enmienda constitucional que eleva la protección de datos al rango de derecho fundamental. Además, regulaciones específicas para pequeñas empresas y una postura receptiva de la ANPD subrayan aún más el carácter integral de la ley.

---

*93 Congreso brasileño aprueba enmienda a la constitución sobre protección de datos personales. (2022, 23 de febrero). https://iapp.org/news/a/brazilian-congress-passes-personal-data-protection-amendment-toconstitution/*

*94 La incorporación de un derecho a la Constitución Federal mediante enmiendas es garantía de consenso y estabilidad, ya que requiere el apoyo del 60 por ciento de los miembros de cada una de las Cámaras del Congreso, mientras que una ley ordinaria requiere la mayoría de los miembros presentes (Art. 60, Constitución Federal, Brasil).*

*95 La autoridad brasileña de protección de datos mejora la LGPD para facilitar las regulaciones para las pequeñas empresas. (2022, 31 de enero). Iapp. https://iapp.org/news/a/brazilian-data-protection-authority-improves-lgpd-to-ease-regulations-for-small-businesses/*

*96 Mari, A. (4 de agosto de 2021). El organismo brasileño de protección de datos se compromete a hacer cumplir una "regulación receptiva". ZDNET. https://www.zdnet.com/article/brazilian-data-protection-body-pledges-to-enforce-responsive-regulation/*

## 5. 1. Los efectos de la LGPD en las ONGs

En respuesta a la operacionalización de la LGPD, las organizaciones no gubernamentales (ONGs) se encontraron en una encrucijada, teniendo que equilibrar la misión de su trabajo con las exigencias de una estricta protección de datos[97].

Uno de los cambios más palpables se produjo en el ámbito de la recopilación de datos. Tradicionalmente integradas en el trabajo comunitario de base, las ONGs tuvieron que reevaluar sus métodos. Por ejemplo, una ONG dedicada al bienestar infantil en las favelas de Río de Janeiro siempre había confiado en la comunidad. Sus programas de extensión, que recopilaban datos sobre familias y niños para una mejor asignación de recursos, tuvieron que ser reestructurados. La introducción de lo digital: formularios equipados con casillas de verificación de consentimiento explícito y explicaciones detalladas en portugués se convirtió en la norma. Esto aseguró el cumplimiento de la LGPD y reforzó la confianza; sin embargo, los costos de implementación habían impactado negativamente el desempeño y capacidad financiera de la organización.

Los desafíos fueron aún más pronunciados para las ONGs que manejan datos confidenciales. Una organización que trabaja en la salud de comunidades desatendidas y opera clínicas móviles a lo largo del vasto paisaje rural de Brasil, enfrentó un doble desafío. Tenían que asegurarse de que los datos de los pacientes, a menudo recopilados en áreas remotas con conectividad limitada, se almacenaran de forma segura y educar a su personal de terreno sobre la importancia de la protección de datos. Invertir en soluciones seguras de almacenamiento en la nube era solo una parte de la ecuación; ellos también iniciaron programas de capacitación, asegurando que todos los miembros del equipo, desde médicos hasta voluntarios, comprendieran las implicaciones de la LGPD.

La recaudación de fondos, el sustento de muchas ONGs, también experimentó una evolución. Por ejemplo, las ONGs ambientalistas que trabajan en la Amazonía tenían una vasta base de datos de donantes internacionales. Con la LGPD en vigor, no podían simplemente enviar sus correos electrónicos anuales de recaudación de fondos. El proceso se volvió más complejo e implicó reconfirmar el consentimiento, explicar el uso de datos, e incluso ofrecer a los donantes una idea de cómo sus datos contribuyeron a la misión de la ONG.

---

*97 Realizamos entrevistas con importantes ONGs de Brasil que participaron en la discusión parlamentaria que condujo a la aprobación de la ley de protección de datos.Los resultados de esas entrevistas se han anonimizado en este informe. Para más información sobre el papel de la sociedad civil vis a vis LGPD ver Kira, B. Tambelli, C. (2017) Protección de datos en Brasil: Análisis crítico de la legislación brasileña. Laboratorio de Internet.*
*http://www.internetlab.org.br/wp-content/uploads/2017/03/Legal-Framework-Analysis-Brazil.pdf*

La entrevista con el director de una organización de tecnología cívica en Brasil[98] añadió evidencia de los obstáculos fundamentales de las ONGs cuando se promulga una ley restrictiva. Para esta ONG, este proceso tardó nueve meses. El director ejecutivo de la organización destacó la dificultad para rediseñar su trabajo con diferentes públicos (tuvieron que cambiar la forma en que etiquetaron el contenido y las consecuencias de la elaboración de perfiles). Además, se dieron cuenta de que las restricciones incluidas en la legislación crearon más fricciones para que los usuarios donaran, haciendo que el proceso en línea para convertirse en donante sea extraordinariamente largo y complejo. Los aspectos positivos de la nueva ley de protección de datos se convirtieron en un desafío para la supervivencia del modelo de vinculación de la organización con los usuarios, así como la promoción y sostenibilidad de esta importante organización de tecnología cívica, que promueve la democracia digital y participación en línea.

Un aspecto mencionado en la entrevista fueron las voces de los niños. Antes de que existiera la LGPD, la plataforma permitía a los niños expresar y publicar contenido. Ahora la participación y acceso a la plataforma son limitados, ya que los niños menores de 16 años requieren la autorización de sus padres[99]. Los cambios en la plataforma en respuesta a la LGPD alteraron las perspectivas para que se escuchen diferentes voces a través de la plataforma, y por lo tanto afectaron la libertad de expresión.

Estas entrevistas revelaron los desafíos que algunas ONGs experimentaron al implementar la LGPD, reforzando que los recursos organizativos y financieros para responder a la protección de datos pueden impactar significativamente en su capacidad para cumplir sus misiones cívicas.

### 5.2. El gobierno de Bolsonaro y las ONGs

Desde su creación, la LGPD de Brasil ha sido aclamada como una pieza legislativa histórica que apunta a proteger los derechos de datos de los ciudadanos brasileños. Sin embargo, en el complejo panorama político bajo la administración del presidente Jair Bolsonaro, las implicaciones de la LGPD se extendieron más allá su intención principal. Surgen dos preocupaciones fundamentales: primero, que la LGPD sea un una fuente de protección ineficaz de los datos contra la vigilancia estatal y las actividades de procesamiento de datos.

---

*98 La entrevista se realizó el 15 de agosto de 2023.*

*99 Para un resumen de la discusión legal sobre LGDP y niños y adolescentes ver https://iapp.org/news/a/el-tratamiento-de-los-datos-de-ninos-y-adolescentes-en-brasil-un-escenario-de-incertidumbres/*

En segundo lugar, surge la preocupación de que, así como el RGPD ha sido criticado por reconocer inadecuadamente la libertad de expresión, la LGPD puede usarse para restringir el discurso y reducir espacio cívico.

El gobierno de Bolsonaro es conocido por su escepticismo hacia las ONGs, particularmente aquellas que abogan por los derechos ambientales e indígenas[100]. Hay mucho en juego en la selva tropical de la Amazonía, donde las ONGs ambientalistas trabajan para combatir la deforestación y proteger los derechos indígenas. Estas ONGs a menudo recopilaban datos sobre el medio ambiente y las comunidades indígenas, su salud y sus interacciones con el mundo exterior. Estos datos fueron cruciales para la promoción, investigación y colaboración internacional. La administración de Bolsonaro ha estado frecuentemente en desacuerdo con estas ONGs ambientalistas y de derechos humanos, particularmente con aquellas que operan en la región amazónica, porque él las percibe como una interferencia en la soberanía y desarrollo económico[101] de Brasil. En 2019, el gobierno de Bolsonaro enfrentó críticas de donantes internacionales (incluidos Alemania y Noruega) por preocupaciones sobre deforestación en la Amazonía[102]. Estos países decidieron retener fondos del Fondo Amazonía, que apoya proyectos para combatir la deforestación. En respuesta, la administración de Bolsonaro ha criticado a las ONGs, sugiriendo que podrían estar detrás de los incendios forestales para empañar la imagen de Brasil.[103]

Los cambios regulatorios también han marcado el enfoque de la administración hacia las ONGs. En 2019, Bolsonaro emitió una medida provisional que le dio más control al gobierno sobre el nombramiento de representantes de ONGs en los consejos federales, una medida vista como un intento de disminuir la influencia de estas organizaciones en las políticas públicas[104]. Organizaciones globales como Human Rights Watch expresaron su preocupación por los abusos y el uso de legislación dirigida a diferentes propósitos por parte de la administración de Bolsonaro[105].

La LGPD no ha sido una salvaguarda eficaz de la protección de datos tras la crisis del procesamiento de datos por parte del gobierno de Bolsonaro y otras entidades estatales. Es importante reiterar que la LGPD creó una agencia bajo el nombre de ANPD

---

*100 https://elpais.com/internacional/2021-07-18/el-metodo-bolsonaro-un-asalto-a-la-democracia-a-camara-lenta.html*
*101 Escobar, H. (2019). "Las primeras medidas de Bolsonaro preocupan a los científicos brasileños." Ciencia, doi:10.1126/science.aaw9464*
*102 The Guardian, 16/08/2019 https://www.theguardian.com/world/2019/aug/16/norway-halts-amazon-fund-donation-dispute-brazil-deforestation-jair-bolsonaro*
*103 3 Reuters, 08/21/2019 https://www.reuters.com/article/us-brazil-politics-idUSKCN1VB1BY*
*104 Londoño, E., & Casado, L. (2019). "Bajo Bolsonaro, se reducen las protecciones del Amazonas y caen los bosques". The New York Times.*
*105 Human Rights Watch, marzo 2021 https://www.hrw.org/news/2021/03/11/crisis-brazilian-amazon*

(Autoridade Nacional de Proteção de Dados), y que la ANPD no ha sido un control eficaz de las actividades del gobierno de Bolsonaro, particularmente en relación con el proceso electoral[106]. Una investigación realizada por Coding Rights y Tactical Tech Collective ha descubierto varias prácticas en línea de campañas electorales que parecen entrar en conflicto con la ley de protección de datos existente[107]. Notablemente, los partidos políticos han estado celebrando acuerdos con empresas de marketing, categorizadas como donaciones corporativas, una táctica considerada inconstitucional por el Supremo Tribunal Federal del país en sentencia de 2015[108]. La ausencia de intervenciones por parte de la agencia de protección de datos a la luz del uso de dichos datos es preocupante. Además, existe evidencia por parte de la misma investigación sobre el uso de bases de datos externas para marketing directo en estas campañas, que plantea preocupaciones sobre la posible adquisición o uso ilegal de datos para fines no previstos. Además, las recientes modificaciones a la ley electoral y las nuevas regulaciones para el uso de publicidad electoral en línea, que permiten la promoción de contenidos, han llevado inadvertidamente a la recopilación no consentida y no divulgada de datos personales destinada a crear diversos perfiles de votantes[109].

Existe una preocupación adicional de que la LGPD pueda convertirse en una de las "armas políticas" utilizadas por la administración[110], como herramienta para ejercer presión sobre las ONGs u otras voces disidentes. En otros países latinoamericanos, estamos viendo a líderes populistas utilizar medidas legítimas existentes, leyes y regulaciones para presionar a la sociedad civil (a veces este fenómeno es descrito como la "reducción del espacio cívico"). En el contexto de una ya difícil relación con las ONGs y preocupaciones relacionadas con proyectos legislativos emergentes para regular la desinformación y ¨fake news¨, también existe el peligro de que la LGPD pueda ser utilizada como una herramienta potencial para ejercer presión. Hay una serie de factores que resaltan este riesgo. Primero, si bien la ley fue diseñada nominalmente para salvaguardar los datos y garantizar la transparencia, sus requisitos ofrecían varias vías para una aplicación rigurosa, que podría ser aplicada selectivamente. En segundo lugar, como hemos descrito, la ANPD no ha proporcionado supervisión de prácticas de datos cuestionables por parte del Estado, lo que genera preocupaciones sobre su independencia

---

*106 https://www.bnamericas.com/es/noticias/implicaciones-de-los-vetos-de-bolsonaro-a-la-ley-de-proteccion-de-datos*

*107 Consulta Pública: Codificación de Derechos y otros (2019) "Desinformación en Internet en Contextos Electorales en America Latina y el Caribe" Véase Asociación por los Derechos Civiles, https://adc.org.ar/wp-content/uploads/2019/06/Consulta-publica-desinformacion-en-contextos-electorales_contribucion-regional-AlSur.pdf*

*108 Ver https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=10329542*

*109 Ibidem.*

*110 Palau, M. (2021) Detrás de la peligrosa batalla brasileña sobre las noticias falsas. Americas Quarterly, October. https://americasquarterly.org/article/detras-de-la-peligrosa-batalla-brasilena-sobre-las-noticias-falsas/*

como agencia de protección de datos responsable. En tercer lugar, la falta de claridad sobre cómo la ley sería implementada le dio influencia política a la nueva administración para manipular aspectos de la ley. Por ejemplo, como explicó Venturini, la versión final del texto omite notablemente las sanciones administrativas propuestas inicialmente para violaciones de datos graves o recurrentes tras los vetos del presidente Bolsonaro. Estas sanciones incluían la posibilidad de suspender totalmente y prohibir de plano las actividades de tratamiento de datos de las entidades en violación. Este enfoque era similar a las medidas esbozadas en el Reglamento General de Protección de Datos de la Unión Europea. El Congreso aún debe revisar estos y otros vetos para consideración adicional[111].

A la luz de la relación polémica entre la administración de Bolsonaro y las ONGs, este es un recordatorio importante de los límites de las leyes de protección de datos y la importancia de una cuidadosa consideración de cómo se integrarán en el marco legal y político más amplio. El impacto de la LGPD se siente no sólo en los costos de cumplimiento creados sino también en el entorno político más amplio, las herramientas que los gobiernos pueden adoptar para abordar sus necesidades críticas y la incapacidad de las leyes en papel para limitar el incumplimiento estatal sin medidas efectivas y supervisión independiente.

*111 Venturini, J. (2019). ¿Bajo qué términos se protegerán los datos en Brasil?. Derechos Digitales, July. https://www.derechosdigitales.org/13499/bajo-que-terminos-se-protegeran-los-datos-en-brasil/*

## 6. Comentarios finales

La intrincada relación entre las leyes de protección de datos y la sociedad civil, particularmente las organizaciones no gubernamentales (ONGs), presenta un conjunto complejo de desafíos y oportunidades. El RGPD de la Unión Europea y la LGPD de Brasil han establecido importantes puntos de referencia en protección de datos, subrayando la importancia de salvaguardar los datos personales en la era digital. Sin embargo, los estrictos requisitos de estas regulaciones tienen profundas implicaciones para las ONGs, que a menudo operan con recursos y capacidad de cumplimiento limitados.

El amplio alcance del RGPD, su modelo único de responsabilidad, la tensión con la libertad de expresión y el modelo de aplicación de la ley presentan desafíos únicos para las ONGs. Estas organizaciones desempeñan un papel fundamental en las sociedades democráticas y su capacidad para gestionar los datos de forma eficaz suele ser crucial para sus operaciones. La transformación digital ha llevado a las ONGs a adoptar diversas tecnologías, haciendo que el análisis de datos sea parte integral de sus procesos de toma de decisiones. Sin embargo, equilibrar el cumplimiento y el mantenimiento de los canales para la libertad de expresión sigue siendo delicado.

Las ONGs, particularmente aquellas con recursos limitados, se encuentran en una posición precaria. Sin tener fines de lucro, manejan grandes cantidades de datos personales, a menudo relacionados con poblaciones vulnerables. Dada la vulnerabilidad de estas partes interesadas, la protección de datos es esencial y es crucial pensar en estrategias que apunten a implementar el nuevo marco regulatorio apoyando a las ONGs. Las implicaciones del incumplimiento son graves, con posibles consecuencias legales, sanciones y multas que pueden debilitar a estas organizaciones vitales. Además, el uso político de la legislación podría dar lugar a prácticas no democráticas.

A la luz de estos desafíos, los formuladores de políticas deben considerar la posición única de las ONGs al redactar e implementar leyes de protección de datos. Un enfoque más matizado, que incorpore exenciones u obligaciones adaptadas a las ONGs, podría aliviar algunas de estas cargas de las organizaciones. Además, proporcionar tecnología, capacitación y apoyo de recursos podría permitir a las ONGs cumplir con las normas de protección de datos sin comprometer sus actividades principales.

Mientras navegamos por este complicado terreno, es esencial aprender de la experiencia europea y de los obstáculos regulatorios en Brasil y proponer una serie de recomendaciones políticas que equilibren los imperativos de la protección de datos con el papel vital que las ONGs desempeñan en las sociedades democráticas.

Estándares de cumplimiento personalizados para ONG: los formuladores de políticas deberían considerar el estatus único de las ONGs y sus distintas necesidades de gestión de datos. Implementar un cumplimiento de estándares personalizado para las ONGs, acorde con sus limitaciones de recursos y operaciones, puede reducir la carga de cumplimiento y al mismo tiempo mantener los estándares de protección de datos. Estos estándares podrían incluir requisitos de informes simplificados y consentimiento, mecanismos que no obstaculicen la participación o exenciones para el procesamiento de tipos específicos de datos que son centrales para las actividades de las ONGs.A las pequeñas y medianas empresas del sector privado se les han concedido enfoques personalizados en otras jurisdicciones que podrían tomarse como ejemplo para las ONGs.

Desarrollo de capacidades y recursos: reconocer que las ONGs a menudo carecen de los recursos financieros y técnicos para cumplir con los estrictos requisitos de protección de datos. Los gobiernos y las organizaciones internacionales deben apoyar el desarrollo de capacidades, incluso por parte de financiadores y entidades filantrópicas globales. Este apoyo podría abarcar financiación para tecnología de protección de datos, capacitación para el personal de las ONGs y orientación sobre mejores prácticas para la gestión de datos. Al dotar a las ONGs de las herramientas y conocimientos necesarios, pueden lograr el cumplimiento sin poner en peligro sus misiones principales. Las autoridades nacionales de protección de datos pueden desempeñar un papel importante en la educación de los responsables del tratamiento de datos y en la generación de orientación y recursos para las ONGs.

Simplificación de los requisitos de presentación de informes: para salvaguardar a las ONGs del posible uso indebido de leyes de protección de datos, las autoridades responsables de la supervisión deberían simplificar solicitudes de informes de cumplimiento por parte de ONGs, y sugerimos que  las autoridades encargadas de hacer cumplir la ley, informen sobre su compromiso con las organizaciones del sector cívico en sus reportes anuales. Esta supervisión puede ayudar a garantizar que las leyes de protección de datos se apliquen de manera justa y no obstruyan el importante trabajo de las ONGs.

Diálogo entre las múltiples partes interesadas: establecer espacios específicos para participar en una empresa conjunta puede fomentar el diálogo y permitir que todas las partes interesadas participen cooperativamente en un acuerdo común. Las ONGs, las autoridades gubernamentales y los reguladores de protección de datos pueden facilitar

una comprensión mutua de los desafíos y soluciones de la protección de datos. Estos espacios pueden servir como foros para discutir posibles enmiendas o implementaciones de las leyes de protección de datos existentes que comprendan mejor las necesidades específicas de las ONGs.

Dados los riesgos asociados con el uso indebido de datos, la protección de los datos perso

nales sigue siendo primordial. Sin embargo, es igualmente importante garantizar que las leyes diseñadas para salvaguardar estos datos no obstaculicen inadvertidamente las operaciones de organizaciones que son esenciales para el tejido de nuestras sociedades democráticas.

Un enfoque equilibrado que reconozca los desafíos únicos que enfrentan las ONGs es crucial para desarrollar leyes de protección de datos que protejan el derecho a la privacidad individual y al mismo tiempo permitir que la sociedad civil prospere.

Al reconocer la importancia de la protección de datos y del trabajo de las ONGs, los responsables de la formulación de políticas deberían esforzarse por lograr este equilibrio, garantizando que la era digital se caracterice tanto por fuertes medidas de protección de datos y el florecimiento de la sociedad civil.

## Referencias


Berdou, E. and Shutt, C. (2017) **Shifting the spotlight: understanding crowdsourcing intermediaries in transparency and accountability initiatives, Making All Voices Count** Research Report, Brighton: IDS

Boulding, C. (2014). **NGOs, Political Protest, and Civil Society.** In NGOs, Political Protest, and Civil Society (p. I). Cambridge: Cambridge University Press.

Buckley, G., Caulfield, T., & Becker, I. (2021). **"It may be a pain in the backside, but..." Insights into the impact of GDPR on business after three years.** ArXiv, abs/2110.11905.

Camacho Gutiérrez, Olga y Velásquez Veloza, Lina (2022) **Iniciativas legislativas sobre privacidad y protección de datos en Argentina, Brasil, Chile, Colombia, Ecuador, México, Guatemala, Paraguay y Perú, período 2019-2021,** CELE. https://www.palermo.edu/Archivos_content/2022/cele/papers/iniciativas-legislativas-sobre-privacidad.pdf

Coding Rights and others (2019) **"Desinformación en Internet en Contextos Electorales en America Latina y el Caribe.** https://adc.org.ar/wp-content/uploads/2019/06/Consulta-publica-desinformacion-en-contextos-electorales_contribucion-regional-AlSur.pdf

Dash, Kailash Chandra and Mishra, Umakant, **Critical Considerations for Developing MIS for NGOs** (March 26, 2014). Available at SSRN: https://ssrn.com/abstract=2416294 or http://dx.doi.org/10.2139/ssrn.2416294

Escobar, H. (2019). **"Bolsonaro's first moves have Brazilian scientists worried."** Science, doi:10.1126/science.aaw9464.

Fabretti Moraes, H., & Vainzof, R. (2023, 15 de febrero). **The study analyses how Brazilian courts apply the LGPD.** https://iapp.org/news/a/study-analyzes-how-brazilian-courts-apply-the-lgpd/

Iñara, M. (2023) https://hazrevista.org/tercersector/2023/10/formacion-movilidad-globales-captacion-fondos-fundraising/

Kira, B. Tambelli, C. (2017) **Data Protection in Brazil: Critical Analysis of the Brazilian Legislation.** InternetLab. http://www.internetlab.org.br/wp-content/uploads/2017/03/Legal-Framework-Analysis-Brazil.pdf

Lage-Freitas, A. Allende-Cid, E. Santana, O. Oliverira-Lage, I (2022) **Predicting Brazilian Court Decisions.** In PeerJ Computer Science.

Londoño, E., & Casado, L. (2019). **"Under Bolsonaro, Amazon Protections Slashed and Forests Fall."** The New York Times.

Mačiulienė, Monika and Skaržauskienė, Aelita (2020) **Building the capacities of civic tech communities through digital data analytics, Journal of Innovation & Knowledge,** Volume 5, Issue 4, 2020, Pages 244-250, ISSN 2444-569X, https://doi.org/10.1016/j.jik.2019.11.005.

Mari, A. (2021, August 4). **Brazilian data protection body pledges to enforce "responsive regulation."** "https://www.zdnet.com/article/brazilian-data-protection-body-pledges-to-enforce-responsi e- regulation/

Palau, M. (2021) **Detrás de la peligrosa batalla brasileña sobre las noticias falsas.** Americas Quaterly, October.

Qamp; **A: Brazil's Highest Court Just Strengthened Data Privacy Rights.** (2020, July 20). www.opensocietyfoundations.org. https://www.opensocietyfoundations.org/voices/q-and-a-how-civil- society-in-brazils-is-defending-privacy-rights.

Rhode, Matilda & Rana, Omer & Edwards, Tim. (2017). **Data Capture & Analysis to Assess Impact of Carbon Credit Schemes.**

Rodríguez, Katitza (2016) **"Análisis comparado de las leyes y prácticas de vigilancia en América Latina",** Necesarios & Proporcionados, Electronic Frontier Foundation (EFF), 2016, disponible en: https://necessaryandproportionate.org/es/comparative-analysis-surveillance-laws-and-practices-latin-america/#resumenejecutivo , último acceso: 27 de octubre de 2023.

Schmitt, Julia and Miller, Klaus and Skiera, Bernd, T**he Impact of Privacy Laws on Online User Behavior** (October 1, 2021). HEC Paris Research Paper No MKG-2021-1437 , Available at SSRN: https://ssrn.com/abstract=3774110 or http://dx.doi.org/10.2139/ssrn.3774110

Venturini, J. (2019). **¿Bajo que términos se protegerán los datos en Brasil?. Derechos Digitales** https://www.derechosdigitales.org/13499/bajo-que-terminos-se-protegeran-los-datos-en-brasil/