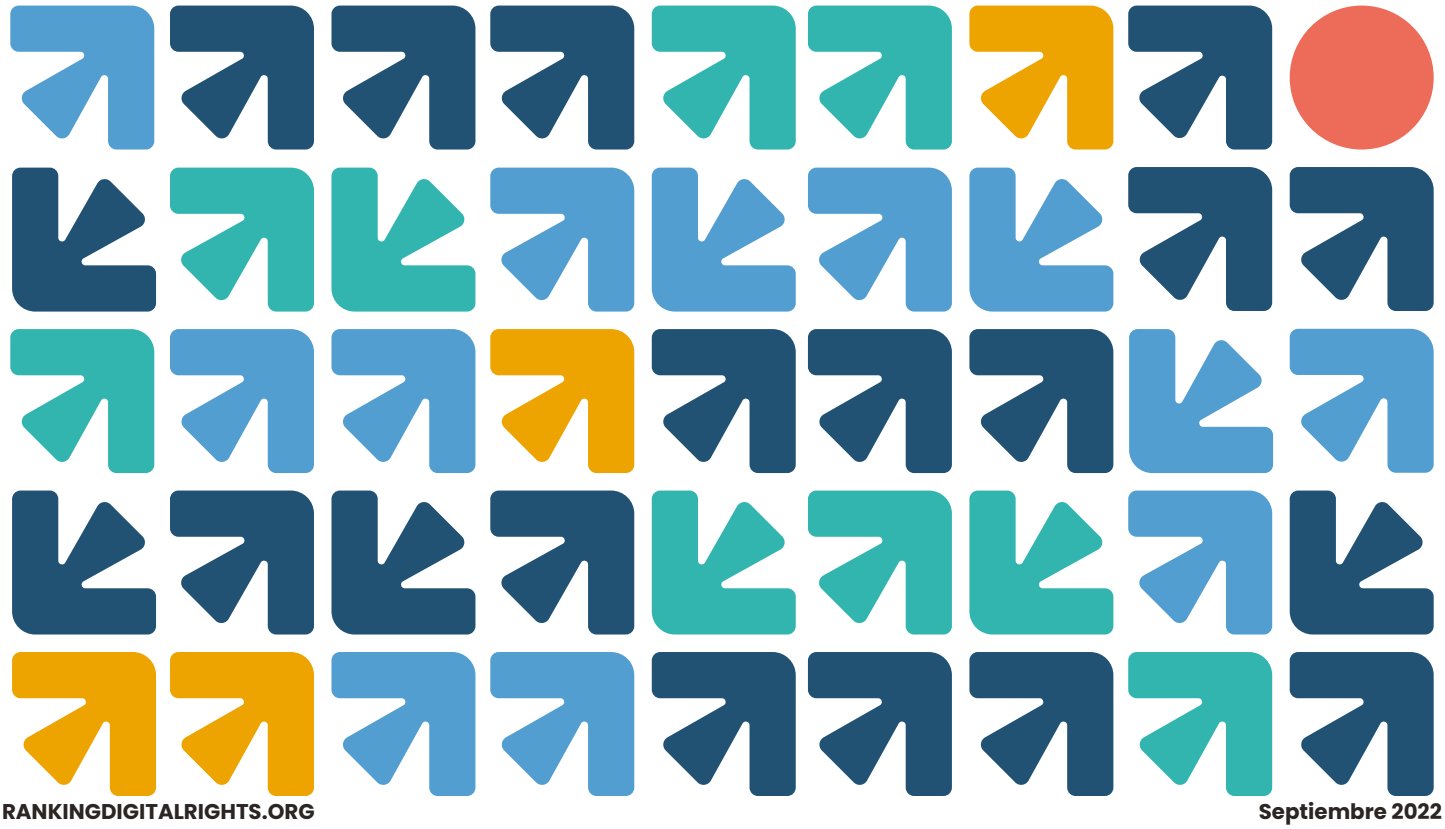
Ranking Digital Rights

Índice de Responsabilidad Corporativa 2020

Incluye guía de indicadores y glosario



Reconocimientos

Los siguientes miembros del equipo de Ranking Digital Rights (RDR) participaron en la investigación y contactándose con grupos de interés como parte de la metodología del Índice de Responsabilidad Corporativa RDR 2020:

- Amy Brouillette, directora de investigación
- Veszna Wessenauer, gerente de investigación
- Nathalie Maréchal, analista principal de políticas
- Afef Abrougui, analista de investigación
- Zak Rogoff, analista de investigación
- Jan Rydzak, jefe de participación empresarial y analista de investigación
- Jie Zhang, analista de investigación

Ver la lista completa del personal del proyecto:
https://rankingdigitalrights.org/who/

RDR quiere agradecer a los más de cien participantes que brindaron observaciones y comentarios a lo largo del proceso de elaboración de esta metodología. También queremos agradecer a Laura Reed y Andrea Hackl, exintegrantes del equipo de investigación de RDR, por sus importantes contribuciones durante la fase inicial del trabajo de expansión de nuestra metodología que empezó a inicios de 2019.

Sobre Ranking Digital Rights

Ranking Digital Rights (RDR) es una iniciativa de investigación sin fines de lucro del Instituto Open Technology de New America que trabaja con una red internacional de socios para establecer directrices globales sobre cómo las empresas del rubro de tecnología de la información y las comunicaciones (TIC) deben respetar la libertad de expresión y la privacidad.

Para saber más de RDR y el Índice de Responsabilidad Corporativa, por favor, visita:
www.rankingdigitalrights.org

Para saber más sobre New America, por favor, visita:
https://www.newamerica.org/

Para saber más sobre Open Technology Institute, por favor, visita:
https://www.newamerica.org/oti/

Para ver una lista completa de los financistas y socios del proyecto:
https://rankingdigitalrights.org/who/partners/

Índice

1. Sobre Ranking Digital Rights

Ranking Digital Rights (RDR) trabaja para promover la libertad de expresión y la privacidad en internet por medio de la creación de parámetros e incentivos globales para que las empresas respeten y protejan los derechos de los usuarios. Hacemos esto por medio de la elaboración del Índice de Responsabilidad Corporativa de Ranking Digital Rights, que evalúa los compromisos y políticas de las plataformas digitales y empresas de telecomunicaciones más poderosas del mundo, basándose en parámetros internacionales de derechos humanos. Trabajamos con empresas y también con defensores, investigadores, inversionistas y diseñadores de políticas para establecer y promover parámetros globales de responsabilidad corporativa.

El Índice de Responsabilidad Corporativa de RDR ofrece una hoja de ruta para que las empresas elaboren y operen plataformas y servicios de internet que respeten y protejan los derechos humanos. El Índice RDR 2019 clasificó a 24 empresas en 35 indicadores,[1] usando un riguroso proceso de investigación de siete pasos y una metodología abierta que revisa los mecanismos de gobernabilidad de las empresas para identificar y evitar posibles amenazas a los derechos humanos de los usuarios, junto con las políticas públicas de las empresas que afectan la libertad de expresión y la privacidad de los usuarios.

2. Sobre la metodología del Índice RDR

Los parámetros que usa el Índice RDR para medir a las empresas son el producto de más de una década de trabajo de comunidades de derechos humanos, privacidad y seguridad. Estos parámetros incluyen los Principios rectores sobre las empresas y los derechos humanos de Naciones Unidas, que afirman que así como los Gobiernos tienen la obligación de proteger los derechos humanos, las empresas también tienen la responsabilidad de respetar dichos derechos. El Índice RDR también se basa en los principios rectores de Global Network Initiative y las guías de implementación que abordan las responsabilidades específicas de las empresas de tecnologías de la información, y la comunicación relativa a la libertad de expresión y la privacidad ante solicitudes gubernamentales de restricción de contenido o la entrega de información del usuario. Además, recurre a un organismo de parámetros y normas globales emergentes en torno a la protección de datos, seguridad y acceso a la información.

La metodología del Índice RDR se ha desarrollado tras años de investigación, pruebas y consultas. Desde sus inicios, el proyecto ha participado de cerca con investigadores de todas partes del mundo. Para la elaboración de la metodología inicial, estudio piloto y el Índice RDR inaugural también nos asociamos con Sustainalytics, un importante proveedor de investigación ambiental, social y gobernabilidad (ESG) para inversionistas.

Versiones anteriores del Índice RDR:

[1] Índice RDR 2019, mayo de 2019, https://rankingdigitalrights.org/index2019/.

- En 2015, publicamos el primer Índice RDR, que clasificó a 16 empresas de internet y de telecomunicaciones en 31 indicadores.

- El Índice RDR 2017 expandió la clasificación a 22 empresas, que incluyó a todas las empresas clasificadas en 2015, y otras seis empresas más. Junto con empresas de internet y de telecomunicaciones, el Índice RDR se amplió para incluir nuevos tipos de servicios, incluidos los que elaboran software y dispositivos que llamamos "ecosistemas móviles". Como resultado, actualizamos la metodología de 2017 basándonos en una revisión detallada de los datos sin procesar del Índice RDR de 2015, y también en consultas con partes interesadas de la sociedad civil, el sector académico, inversionistas y empresas.

- El Índice RDR 2018 aplicó la misma metodología para evaluar a las mismas 22 empresas del Índice 2017. Esto nos permitió elaborar análisis comparativos del desempeño de cada empresa y dar seguimiento a tendencias generales.

- La metodología del Índice RDR 2019 hizo cambios en dos indicadores en la categoría de Gobernabilidad.[2] Estas revisiones tenían el objetivo de presentar parámetros de referencia para identificar y mitigar riesgos de derechos humanos asociados con el uso de algoritmos por parte de empresas para sus políticas y prácticas de publicidad dirigida. También actualizamos un indicador (Indicador G6) con la finalidad de fortalecer y aclarar nuestra evaluación de los mecanismos y procedimientos de reclamo y solución de las empresas.[3] Además, el Índice RDR 2019 se amplió para incluir dos nuevas empresas[4]—Deutsche Telekom y Telenor—y otros cinco servicios de la nube.

3. Sobre la revisión de la metodología del Índice RDR 2020

Desde su lanzamiento en 2015, el Índice RDR ha contribuido a mejorar la revelación que hacen las empresas de sus políticas y prácticas en diversos rubros, que incluyen un informe de transparencia, retiro de contenido, restricciones de cuentas, cierre de redes, y manejo y seguridad de la información del usuario. Sin embargo, dadas las novedades geopolíticas y tecnológicas con claras consecuencias de derechos humanos que han ocurrido en el tiempo desde que se elaboró la primera metodología del Índice RDR, ha quedado claro que la metodología se debe actualizar si se va hacer responsables a las empresas por la diversidad de potenciales amenazas en línea a los derechos humanos.

---

[2] "Indicadores de investigación del Índice de Responsabilidad Corporativa 2019", *Ranking Digital Rights*, septiembre de 2019, https://rankingdigitalderechos.org/Index2019/assets/static/download/RDRIndex2019indicators.pdf

[3] "Actualizaciones propuestas a la metodología del Índice de Responsabilidad Corporativa 2019 (borrador de consulta)", *Ranking Digital Rights,* julio de 2018, https://rankingdigitalderechos.org/wp-contenido/uploads/2018/06/2019-Index-Metodology_-Consultación-Preliminar.pdf

[4] Ver lista de empresas de 2019: https://rankingdigitalderechos.org/2019-companies/.

En enero de 2019, RDR empezó un proceso de expansión y actualización de la metodología para incluir nuevos rubros temáticos y nuevos tipos de empresas.[5] Este trabajo se ha centrado en tres rubros principales:

- **Mejoras a la metodología del Índice RDR 2019:** Actualizamos la metodología del Índice RDR 2019 para identificar las áreas claves que pueden ser actualizadas y mejoradas.

- **Incorporación de nuevos indicadores sobre publicidad dirigida y algoritmos:** Desde inicios de 2019, RDR ha estado elaborando nuevos indicadores que fijan parámetros globales de responsabilidad y transparencia sobre cómo las empresas pueden demostrar respeto por los derechos humanos en línea a medida que elaboran y muestran estas nuevas tecnologías. En octubre de 2019, RDR publicó indicadores preliminares sobre publicidad dirigida y algoritmos, sobre la base de cerca de un año de investigación interna y de la incorporación de comentarios de más de 90 expertos. El equipo de investigación de RDR hizo pruebas pilotos con estos indicadores preliminares. Los resultados de este estudio piloto se publicaron en marzo de 2020.

- **Incorporación de nuevas empresas:** A inicios de 2019, empezamos el proceso de investigación y consulta pública sobre maneras de ampliar el Índice RDR para incluir a Amazon y Alibaba. Este proceso sentó las bases para incorporar dos nuevos servicios —plataformas de comercio electrónico y "ecosistemas de asistente personal digital"— a la metodología del Índice RDR 2020.

En abril de 2020, RDR publicó una versión preliminar de la metodología final del Índice RDR 2020, que integraba el trabajo en estos tres rubros.[6] Luego iniciamos una ronda final de consulta pública para solicitar observaciones y comentarios de los grupos de interés, cuyas decisiones informadas tomamos al finalizar la metodología.

Para leer un resumen de los cambios principales a la metodología del Índice RDR 2020:
https://rankingdigitalrights.org/wp-content/uploads/2020/06/2020-methodology-revision-final-summary.pdf

Para saber más sobre nuestro proceso de elaboración de la metodología:
https://rankingdigitalrights.org/methodology-development/

[5] "Lanzamiento de Índice RDR 2019 programado para mayo, se vienen grandes planes," *Ranking Digital Rights,* febrero de 2019, https://rankingdigitalderechos.org/2019/02/13/rdr-2019-index-launch-plans//

[6] "Índice de Responsabilidad Corporativa 2020 de Ranking Digital Rights, indicadores preliminares", *Ranking Digital Rights,* abril de 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/04/2020-draft-methodology-redline-version.pdf

4. Empresas incluidas en el Índice RDR 2020

El Índice RDR 2020 evaluará a 26 empresas, enumeradas más abajo. Los investigadores examinarán las políticas y prácticas de la empresa matriz global, además de las políticas y prácticas dadas a conocer de servicios seleccionados y de empresas que funcionan a nivel local (dependiendo de la estructura empresarial).

Empresas de plataformas digitales: El Índice RDR 2020 evaluará a 14 empresas de plataformas digitales. Esto incluye a 12 empresas de plataformas digitales evaluadas con anterioridad y dos empresas nuevas (Amazon y Alibaba). Como se ha dicho antes, debido a la expansión del Índice RDR 2020 para incluir nuevos servicios ofrecidos por Amazon y Alibaba —*e*specíficamente, plataformas de comercio electrónico y ecosistemas de asistente personal digital--, hemos cambiado el nombre de la categoría "ecosistema de internet y móviles" a "plataformas digitales", cuyo alcance incluye diversos productos y servicios que ofrecen las empresas de internet, así como ecosistemas móviles, plataformas de comercio electrónico y ecosistemas de asistente personal digital.

Para cada una de estas empresas evaluamos políticas globales a nivel de grupo para indicadores relevantes además de políticas del mercado interno de las empresas (por ejemplo, evaluamos las políticas de privacidad de Facebook aplicables a los usuarios en Estados Unidos).

Para cada empresa, examinamos hasta cinco servicios, señalados a continuación:

- **Alibaba (China)** — Taobao.com (plataforma de comercio electrónico); AliGenie (ecosistema de asistente personal digital)
- **Amazon (Estados Unidos)** — Amazon.com (plataforma de comercio electrónico); Amazon Alexa (ecosistema de asistente personal digital), Amazon Drive
- **Apple (Estados Unidos)** —ecosistema móvil iOS, iMessage, iCloud
- **Baidu (China)** — Baidu Search, Baidu Cloud, Baidu PostBar
- **Facebook (Estados Unidos)** — Facebook, Instagram, WhatsApp, Messenger
- **Google (Estados Unidos)** — Search, Gmail, YouTube, ecosistema móvil Android, Google Drive
- **Kakao (Corea del Sur)** — Kakao Search, Kakao Mail, KakaoTalk
- **Mail.Ru (Rusia)** — Vkontakte, correo electrónico Mail.ru, agente de mensajería Mail.ru, Mail.Ru Cloud
- **Microsoft (Estados Unidos)** — Bing, Outlook.com, Skype, OneDrive
- **Oath (Estados Unidos)** — Yahoo Mail, Tumblr
- **Samsung (Corea del Sur)** —implementación de Android de Samsung, Samsung Cloud
- **Tencent (China)** — QZone, QQ, WeChat, Tencent Cloud
- **Twitter (Estados Unidos)** — Twitter

- **Yandex (Rusia)** — Yandex Mail, Yandex Search, Yandex Disk (almacenamiento en la nube)

Empresas de telecomunicaciones: El Índice RDR 2020 puntuará a las 12 empresas de telecomunicaciones que ya clasificamos. No se han agregado nuevas empresas de telecomunicaciones en el ciclo de investigación 2020.

Para cada una de estas empresas evaluamos políticas globales a nivel grupal para indicadores pertinentes además del servicio móvil prepago y pospago de la filial operativa del país de origen, y del servicio de banda ancha de línea fija, señalados a continuación:

- **América Móvil (México)**: Telcel (móvil prepago y pospago)
- **AT&T (Estados Unidos)**: AT&T (móvil prepago y pospago, banda ancha)
- **Axiata (Malasia):** Celcom (móvil prepago y pospago, banda ancha)
- **Bharti Airtel (India):** Airtel India (móvil prepago y pospago, banda ancha)
- **Deutsche Telekom AG (Alemania)**: Deutsche Telekom (móvil prepago y pospago, banda ancha)
- **Etisalat (Emiratos Árabes Unidos):** Etisalat UAE (móvil prepago y pospago, banda ancha)
- **MTN (Sudáfrica):** MTN South Africa (móvil prepago y pospago, banda ancha)
- **Ooredoo (Catar):** Ooredoo Qatar (móvil prepago y pospago, banda ancha)
- **Orange (Francia):** Orange France (móvil prepago y pospago, banda ancha)
- **Telefónica (España):** Movistar (móvil prepago y pospago, banda ancha)
- **Telenor ASA (Noruega):** Telenor (móvil prepago y pospago, banda ancha)
- **Vodafone (Reino Unido):** Vodafone UK (móvil prepago y pospago, banda ancha)

5. Proceso de investigación

El Índice RDR se elabora con un riguroso proceso de siete pasos de recopilación de datos, verificación y revisión. La investigación la realiza una red de más de 30 investigadores de todo el mundo. Los pasos para el Índice RDR 2020 se detallan a continuación:

- **Paso 1: Recopilación principal de datos.** En esta etapa, los investigadores principales son responsables de verificar los resultados del Índice RDR anterior (2019). Si las políticas de la empresa han cambiado, o si hay nuevos indicadores y elementos, los investigadores principales son responsables de evaluar esas políticas. Los investigadores del Paso 1 también realizarán una evaluación de cómo las políticas (actuales) se comparan con el Índice RDR anterior (2019).

- **Paso 2: Revisión secundaria:** En esta etapa, los revisores secundarios verificarán las evaluaciones proporcionadas por los investigadores principales en el Paso 1, incluido el estar de acuerdo o discrepar con el análisis hecho año a año.

- **Paso 3: Revisión y conciliación:** El equipo de RDR discutirá los resultados de los Pasos 1 y 2 para resolver todas las diferencias que surjan.

- **Paso 4: Comentarios y opiniones de las empresas.** En este paso, las empresas tienen la oportunidad de revisar la evaluación preliminar y ofrecer comentarios y opiniones al equipo de RDR. El equipo evalúa el aporte de las empresas para determinar si garantiza un cambio en la evaluación.

- **Paso 5: Procesamiento de comentarios y opiniones de las empresas.** RDR evalúa los comentarios y opiniones de las empresas, y hace todos los ajustes a las evaluaciones, según se necesite.

- **Paso 6: Revisión horizontal.** El equipo de RDR llevará a cabo una revisión horizontal, con los comentarios y opiniones de las empresas recopilados en el Paso 4, y verificará los indicadores para asegurar que han sido evaluados constantemente a través de cada empresa.

- **Paso 7: Evaluación final:** El equipo de RDR asigna evaluaciones finales. Las evaluaciones incluyen si la política o revelaciones de la empresa han cambiado con respecto a la evaluación del año anterior.

6. Evaluación y puntuación

El ciclo del Índice RDR 2020 evalúa las políticas de la empresa que han estado activas desde el 25 de enero de 2019 al 14 de septiembre de 2020. Las empresas reciben una puntuación acumulativa de su desempeño en todas las categorías del Índice RDR, y los resultados muestran cómo se desempeñaron las empresas en cada categoría e indicador.

Cada indicador tiene una lista de elementos, y las empresas reciben crédito (total, parcial o no reciben crédito) por cada elemento con el que cumplen. La evaluación incluye una evaluación de revelación para cada elemento de cada indicador, basándose en una de las siguientes posibles respuestas:

- **"Sí"** / revelación total. La revelación de la empresa cumple con el requisito del elemento.

- **"Parcial".** La revelación de la empresa ha cumplido con algunos, no con todos los aspectos del elemento, o la revelación no es suficientemente completa para satisfacer el alcance total de lo que solicita el elemento.

- **"No se encontró revelación alguna".** Los investigadores no pudieron encontrar información brindada por la empresa en su sitio web que responda a la pregunta del elemento.

- **“No”**. Existe revelación de la empresa, pero no revela específicamente a los usuarios lo que el elemento pregunta. Es diferente a la opción “no se encontró revelación alguna”, aunque ninguna aporta crédito.
- **“N/A”.** No aplicable. Este elemento no se aplica a la empresa o servicio. Los elementos marcados como N/A no se contarán a favor ni en contra de una empresa en el proceso de calificación.

Puntos

- Sí/revelación total = 100
- Parcial = 50
- No = 0
- No se encontró revelación alguna = 0
- N/A se excluye de las puntuaciones y promedios

Gobernabilidad

Los indicadores en esta categoría buscan evidencia de que la empresa tiene procesos de gobernabilidad vigentes para garantizar que se respeta el derecho humano a la libertad de expresión y la privacidad. Ambos derechos son parte de la Declaración Universal de Derechos humanos,[7] y están consagrados en el Pacto Internacional de Derechos Civiles y Políticos [8] Son aplicables en línea y fuera de línea.[9] Para que una empresa se desempeñe bien en esta categoría, la revelación de la empresa debe al menos seguir, e idealmente superar, los Principios Rectores sobre las Empresas y los Derechos Humanos[10] y otros parámetros de derechos humanos específicos para el sector centrados en libertad de expresión y privacidad, como los adoptados por Global Network Initiative.[11]

G1. Compromiso de políticas

La empresa debe publicar un **compromiso de políticas** formal de respetar los derechos humanos de los usuarios a la libertad de expresión e información, y privacidad.

Elementos:

1. ¿La empresa hace un **compromiso de políticas** de derechos humanos claramente articulado y **explícito** que incluya la libertad de expresión e información?

2. ¿La empresa hace un **compromiso de políticas** de derechos humanos claramente articulado y **explícito** que incluya la privacidad?

3. ¿La empresa revela un **compromiso de políticas** de derechos humanos claramente articulado y **explícito** de derechos humanos en su desarrollo y uso de **sistemas algorítmicos**?

Guía del indicador: Este indicador busca evidencia de que la empresa haya hecho un compromiso de políticas explícito de la libertad de expresión y la información, y la privacidad. Estos parámetros están definidos en el principio operativo 16 de los Principios

[7] "Declaración Universal de Derechos Humanos', https://www.un.org/es/universal-declaración-human-rights/index.html/

[8] "Pacto Internacional de Derechos Civiles y Políticos'', Oficina del Alto Comisionado de Derechos Humanos de Naciones Unidas: https://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx.

[9] Consejo de Derechos Humanos de Naciones Unidas, *Resolución adoptada por el Consejo de Derechos Humanos el 27 de junio de 2016 - Promoción y protección de todos los derechos humanos, civiles, políticos, económiosc, sociales y culturales, incluido el derecho al desarrollo,* disponible en: https://digitallibrary.un.org/record/845728

[10] "Principios rectores sobre las empresas y los derechos humanos', *Oficina del Alto Comisionado de Derechos humanos de Naciones Unidas* https://www.ohchr.org/documents/publicacións/guidingprincipiosbusinesshr_sp.pdf

[11] "Principios de GNI,' *Global Network Initiative*, https://globalnetworkinitiative.org/gni-principles/.

Rectores sobre las empresas y los derechos humanos de Naciones Unidas, que establece que las empresas deben adoptar políticas formales que afirmen públicamente sus compromisos con principios y parámetros de derechos humanos internacionales.[12] Las empresas también deben publicar un compromiso formal de defender los derechos humanos al elaborar y desplegar sistemas algorítmicos de tomas de decisiones, en línea con las recomendaciones del Consejo de Europa, en su *Recomendación sobre los impactos de los derechos humanos en los sistemas algorítmicos* (2020). La empresa debe revelar claramente estos compromisos en documentos de políticas formales u otras comunicaciones que reflejen las políticas oficiales de la empresa.

Posibles fuentes:

- Políticas de derechos humanos de la empresa
- Afirmaciones, informes u otras comunicaciones de la empresa que reflejen la política oficial de la empresa
- Informe anual o informe de sostenibilidad anual de la empresa
- Políticas de "principios de inteligencia artificial" de la empresa

G2. Supervisión de gobernabilidad y de gestión

El **personal directivo** de la empresa deberá ejercer **supervisión** sobre cómo sus políticas y prácticas afectan la libertad de expresión y la privacidad.

Elementos:

1. ¿La empresa **revela claramente** que la **junta directiva** ejerce **supervisión** formal de cómo las prácticas de la empresa afectan la libertad de expresión y de información?

2. ¿La empresa **revela claramente** que la **junta directiva** ejerce **supervisión** formal de cómo las prácticas de la empresa afectan la privacidad?

3. ¿La empresa **revela claramente** que un comité, equipo, programa o funcionario de **nivel ejecutivo supervisa** cómo las prácticas de la empresa afectan la libertad de expresión y de información?

4. ¿La empresa **revela claramente** que un comité, equipo, programa o funcionario de **nivel ejecutivo supervisa** cómo las prácticas de la empresa afectan la privacidad?

5. ¿La empresa **revela claramente** que un comité, equipo, programa o funcionario de **nivel gerencial supervisa** cómo las prácticas de la empresa afectan la libertad de expresión y de información?

[12] "Principios rectores sobre las empresas y los derechos humanos', *Oficina del Alto Comisionado de Derechos humanos de Naciones Unidas"*: https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_sp.pdf.

6. ¿La empresa **revela claramente** que un comité, equipo, programa o funcionario de **nivel gerencial supervisa** cómo las prácticas de la empresa afectan la privacidad?

Guía del indicador: Este indicador busca evidencia de que la empresa tiene sólida gobernabilidad y supervisión de problemas de libertad de expresión y de información, y de privacidad a todo nivel de sus operaciones. Las empresas deben revelar claramente que el personal directivo —desde junta directiva hasta nivel gerencial— supervisa y es responsable por sus políticas y prácticas que afectan a los derechos humanos.

Para recibir crédito total en este indicador, las empresas deben revelar claramente que en todo nivel de mando (junta directiva, ejecutivo, gerencial) hay supervisión clara de los problemas de libertad de expresión y privacidad. A nivel de la junta directiva, esta supervisión podrá incluir un directorio u otra explicación pública de cómo la junta ejerce la supervisión de estos asuntos. Por debajo del nivel de la junta directiva, puede incluir una unidad de la empresa programa o persona que informe al ejecutivo o nivel gerencial. El comité, programa, equipo, funcionario, etc. debe identificar específicamente libertad de expresión y privacidad en la descripción de sus responsabilidades.

Posibles fuentes:
- Lista de integrantes de la junta directiva
- Documentos de gobernabilidad de la empresa
- Informe de sostenibilidad de la empresa
- Organigrama de la empresa
- Políticas de derechos humanos de la empresa
- Documentos de Global Network Initiative (si la empresa es miembro)

G3. Implementación interna

La empresa debe tener mecanismos vigentes para implementar sus compromisos con la libertad de expresión y la privacidad dentro de la empresa.

Elementos:

1. ¿La empresa **revela claramente** que brinda capacitación a sus trabajadores sobre asuntos de libertad de expresión y privacidad?

2. ¿La empresa **revela claramente** que brinda capacitación a sus trabajadores sobre asuntos de privacidad?

3. ¿La empresa **revela claramente** que mantiene un **programa de informantes** para sus trabajadores a través del cual los trabajadores pueden informar de asuntos relacionados con cómo la empresa trata los derechos de libertad de expresión e información de los usuarios?

4. ¿La empresa **revela claramente** que mantiene un **programa de informantes** para

sus trabajadores a través del cual los trabajadores pueden informar de asuntos relacionados con cómo la empresa trata los derechos de privacidad de sus usuarios?

Guía del indicador: El indicador G2 evalúa si el personal directivo de una empresa se compromete a supervisar asuntos de libertad de expresión y privacidad. Este indicador, G3, evalúa si la empresa revela si es que estos compromisos están institucionalizados en la empresa, y cómo los institucionaliza. Más específicamente, este indicador busca revelar si la empresa ayuda a los trabajadores a entender la importancia de la libertad de expresión y la privacidad, y cómo los ayuda. Cuando los trabajadores escriben un código informático para un producto nuevo, revisan solicitudes de datos de usuario o responden preguntas sobre cómo usar un servicio, actúan de maneras que pueden afectar directamente la libertad de expresión y la privacidad de los usuarios. Tenemos la expectativa de que las empresas revelen información sobre si ofrecen capacitación que informe a los trabajadores sobre su rol en el respeto a los derechos humanos que dan a los trabajadores un medio para expresar sus preocupaciones con respecto a los derechos humanos.

Una empresa solamente recibe crédito en este indicador si revela claramente información sobre capacitación a sus trabajadores sobre libertad de expresión y privacidad, y si existe un programa de informante que aborde estos asuntos. La revelación debería especificar que la capacitación de los trabajadores y los programas internos de informantes abarcan la libertad de expresión y privacidad. Las empresas pueden recibir crédito en este indicador si el programa de informantes de una empresa no menciona específicamente los reclamos relacionados con la libertad de expresión y privacidad en tanto la empresa haya hecho compromisos con esos principios en otra parte de una manera que deje en claro que la empresa consideraría estos reclamos a través de su programa de informantes.

Posibles fuentes:

- Código de conducta de la empresa
- Manual de los trabajadores
- Organigrama de la empresa
- Informe de sostenibilidad/responsabilidad corporativa de la empresa
- Publicaciones en el blog de la empresa

G4. Revisión exhaustiva en derechos humanos

G4(a). Evaluación del impacto: Gobiernos y regulaciones

Las empresas deben ejercer una revisión exhaustiva de manera frecuente, integral y creíble a través de sólidas **evaluaciones de impacto de los derechos humanos** para identificar cómo las regulaciones y políticas gubernamentales afectan la libertad de expresión e información, y la privacidad, y para mitigar los riesgos que suponen estos impactos en las jurisdicciones en que las empresas operan.

Elementos:

1. ¿La empresa **evalúa** cómo las leyes afectan la libertad de expresión y de información en las jurisdicciones donde funciona?

2. ¿La empresa **evalúa** cómo las leyes afectan la privacidad en jurisdicciones donde funciona?

3. ¿La empresa **evalúa** los riesgos de libertad de expresión e información asociados con productos y servicios existentes en las jurisdicciones donde funciona?

4. ¿La empresa **evalúa** los riesgos de privacidad asociados con productos y servicios existentes en las jurisdicciones donde funciona?

5. ¿La empresa **evalúa** los riesgos de libertad de expresión e información asociados con una nueva actividad, incluido el lanzamiento y adquisición de nuevos productos, servicios o empresas, o entrada a nuevos mercados o jurisdicciones?

6. ¿La empresa **evalúa** los riesgos de privacidad asociados con una nueva actividad, incluido el lanzamiento y adquisición de nuevos productos, servicios o empresas, o entrada a nuevos mercados o jurisdicciones?

7. ¿La empresa realiza evaluación adicional cada vez que las **evaluaciones de riesgo** de la empresa identifican problemas?

8. ¿Los **altos ejecutivos** o miembros de la **junta directiva** de la empresa revisan y toman en cuenta los resultados de las **evaluaciones** y la revisión exhaustiva en su toma de decisiones?

9. ¿La empresa realiza **evaluaciones** con un calendario regular?

10. ¿Las **evaluaciones** de la empresa están garantizadas por un **tercero** externo?

11. ¿El **tercero** externo que garantiza la **evaluación** está acreditado con un parámetro de derechos humanos relevante y confiable, por parte de una organización fiable?

Guía del indicador: Este indicador examina si las empresas llevan a cabo evaluaciones de riesgos de derechos humanos frecuentes, sólidas y responsables de regulaciones y políticas gubernamentales en las jurisdicciones en las que las empresas funcionan. Estas evaluaciones deben ser parte de las actividades formales y sistemáticas de revisión exhaustiva con el objetivo de asegurar que sus decisiones y prácticas no causen, contribuyan ni exacerben perjuicios a los derechos humanos. Las evaluaciones permiten que las empresas identifiquen posibles riesgos a los derechos de libertad de expresión y privacidad de los usuarios, y tomar medidas para mitigar posibles perjuicios si se identifican.

Nótese que este indicador no tiene la expectativa de que las empresas publiquen resultados detallados de sus evaluaciones de impacto en derechos humanos, pues las evaluaciones pueden incluir información delicada. En cambio, tiene la expectativa de que las empresas

revelen que realizan evaluaciones de riesgos de los derechos humanos y brindan información sobre qué comprende su proceso de evaluación de riesgos de los derechos humanos.

Posibles fuentes:

- Informes de responsabilidad corporativa/de sostenibilidad de la empresa
- Política de derechos humanos de la empresa
- Informes de evaluación de Global Network Initiative

G4(b). Evaluación del impacto: Procesos para aplicación de políticas

La empresa debe ejercer una revisión exhaustiva de manera frecuente, integral y creíble a través de sólidas **evaluaciones de impacto de derechos humanos** para identificar cómo sus procesos para aplicar políticas que afectan los derechos fundamentales de los usuarios a la libertad de expresión y de información, y a la privacidad, y a no ser discriminados, y para mitigar cualquier riesgo que supongan esos impactos.

Elementos:

1. ¿La empresa **evalúa** riesgos a la libertad de expresión y la información por la aplicación de sus términos de servicio?

2. ¿La empresa realiza **evaluaciones de riesgos** de la aplicación de sus políticas de privacidad?

3. ¿La empresa **evalúa** los riesgos de discriminación asociados con sus procesos para aplicar sus **términos de servicio**?

4. ¿La empresa **evalúa** los riesgos de **discriminación** asociados con los procesos para aplicar sus **políticas de privacidad**?

5. ¿La empresa lleva a cabo evaluaciones adicionales cada vez que las **evaluaciones de riesgo** de la empresa identifican problemas?

6. ¿Los **altos ejecutivos** o miembros de la **junta directiva** de la empresa revisan y tienen en cuenta los resultados de las **evaluaciones** y revisión exhaustiva en su toma de decisiones?

7. ¿La empresa realiza evaluaciones con un calendario regular?

8. ¿Las **evaluaciones** de la empresa están garantizadas por un **tercero** externo?

9. ¿El **tercero** externo que garantiza la **evaluación** está acreditado con un parámetro relevante y reputado de derechos humanos de una organización confiable?

Guía del indicador: Este indicador examina si las empresas revelan que realizan evaluaciones de riesgos de derechos humanos sólidas, frecuentes y responsables del impacto de sus políticas sobre de derechos fundamentales de los usuarios a la libertad de expresión, privacidad y a no ser discriminados. Estas evaluaciones deben ser parte de las actividades formales y sistemáticas de revisión exhaustiva de la empresa que tienen el objetivo de garantizar que las decisiones y prácticas de una empresa no causen, contribuyan ni exacerben perjuicios a los derechos humanos. Las evaluaciones permiten a las empresas identificar posibles riesgos de sus propias políticas con los derechos de expresión y de información, privacidad y no discriminación de los usuarios, y tomar medidas para mitigar posibles perjuicios si se identifican.

Nótese que este indicador no tiene la expectativa de que las empresas publiquen resultados detallados de sus evaluaciones de impacto en los derechos humanos, pues las evaluaciones pueden incluir información delicada. En cambio, tiene la expectativa de que las empresas deben revelar que realizan evaluaciones de riesgos de los derechos humanos y brindan información sobre qué comprende su proceso de evaluación de riesgos de los derechos humanos.

Posibles fuentes:

- Informe anual o informe de sostenibilidad anual de la empresa
- Políticas de derechos humanos de la empresa
- Informes de evaluación de Global Network Initiative

G4(c) Evaluación del impacto: Publicidad dirigida

Las empresas deben ejercer una revisión exhaustiva frecuente, integral y creíble a través de sólidas **evaluaciones de impacto de derechos humanos**, para identificar cómo todos los aspectos de sus políticas y prácticas de **publicidad dirigida** afectan los derechos fundamentales de los usuarios a la expresión y de información, de privacidad y a no ser discriminados, y de mitigar todos los riesgos que suponen estos impactos.

Elementos:

1. ¿La empresa **evalúa** riesgos a la libertad de expresión y de información asociados con sus políticas y prácticas de **publicidad dirigida**?

2. ¿La empresa **evalúa** riesgos a la privacidad asociados con sus políticas y prácticas de **publicidad dirigida**?

3. ¿La empresa **evalúa** riesgos a la discriminación asociados con sus políticas y prácticas de **publicidad dirigida**?

4. ¿La empresa realiza evaluaciones adicionales cada vez que las **evaluaciones de riesgo** de la empresa identifican problemas?

5. ¿Los **altos ejecutivos** o miembros de la **junta directiva** de la empresa revisan y tienen en cuenta los resultados de **evaluaciones** y revisión exhaustiva en su toma de decisiones?

6. ¿La empresa realiza **evaluaciones** con un calendario regular?

7. ¿Las **evaluaciones** de la empresa están garantizadas por un **tercero** externo?

8. ¿El **tercero** externo que garantiza la **evaluación** está acreditado con un parámetro de derechos humanos relevante y confiable, por parte de una organización fiable?

Guía del indicador: La publicidad dirigida puede tener efectos adversos en los derechos humanos, específicamente en los derechos a la libertad de información y discriminación[13] de los usuarios. La discriminación ocurre cuando las plataformas permiten que terceros anunciantes muestren publicidad diferente a diferentes usuarios sobre la base de información revelada e inferida, incluida pertenencia a categorías protegidas (raza, etnia, edad, identidad y expresión de género, orientación sexual, salud, discapacidad, etc.). La discriminación no necesita ser inmediatamente ilegal ni perjudicial para que produzca efectos perjudiciales a escala, tanto a nivel poblacional o en el transcurso de la vida de una persona. Considerando el hecho de que las publicidades dirigidas son menos transparentes que otras formas de publicidad y los significativos incentivos financieros de las empresas para implementar tecnología rápidamente, se deben tener en cuenta estos posibles perjuicios a los derechos en las evaluaciones de riesgos.

Este indicador examina si es que las empresas revelan si llevan a cabo evaluaciones de riesgos de derechos humanos frecuentes, sólidas y responsables del impacto de la publicidad dirigida sobre los derechos fundamentales de los usuarios a la libertad de expresión y de información, privacidad y a no ser discriminados. Estas evaluaciones deben ser parte de las actividades formales y sistemáticas de revisión exhaustiva que tienen el objetivo de garantizar que las decisiones y prácticas de una empresa no causen, contribuyan ni exacerben perjuicios de los derechos humanos. Las evaluaciones permiten a las empresas identificar posibles riesgos de políticas y prácticas de publicidad dirigida sobre los derechos humanos de los usuarios y tomar medidas para mitigar posibles perjuicios si se identifican.

Nótese que este indicador no tiene la expectativa de que las empresas publiquen resultados detallados de sus evaluaciones de impacto en derechos humanos, pues las evaluaciones pueden incluir información delicada. En cambio, tiene la expectativa de que las empresas

[13] "Situaciones de riesgo de derechos humanos: Publicidad dirigida", *Ranking Digital Rights*, febrero de 2019: https://rankingdigitalrights.org/wp-content/uploads/2019/02/Human-Rights-Risk-Scenarios-targeted-advertising.pdf.

deben revelar que realizan evaluaciones de riesgos de los derechos humanos y brindan información sobre qué comprende su proceso de evaluación de riesgos de los derechos humanos.

Posibles fuentes:

- Informe anual o informe de sostenibilidad anual de la empresa
- Políticas de derechos humanos de la empresa
- Informes de evaluación de Global Network Initiative

G4(d). Evaluación del impacto: Sistemas algorítmicos

Las empresas deben realizar una revisión exhaustiva frecuente, integral y creíble, a través de sólidas **evaluaciones de impacto de derechos humanos**, para identificar cómo todos los aspectos de sus políticas y prácticas relacionadas con la elaboración y uso de **sistemas algorítmicos** afectan los derechos fundamentales de los usuarios a la libertad y expresión y de información, a la privacidad y a **no ser discriminados**, y de mitigar todos los riesgos que suponen estos impactos.

Elementos:

1. ¿La empresa **evalúa** riesgos a la libertad de expresión e información asociados con su elaboración y uso de **sistemas algorítmicos**?

2. ¿La empresa **evalúa** riesgos a la privacidad asociados con su elaboración y uso de **sistemas algorítmicos**?

3. ¿La empresa **evalúa** riesgos de **discriminación** asociados con su elaboración y uso de **sistemas algorítmicos**?

4. ¿La empresa realiza evaluación adicional cada vez que las **evaluaciones de riesgo** de la empresa identifican problemas?

5. ¿Los **altos ejecutivos** o miembros de la **junta directiva** de la empresa revisan y toman en cuenta los resultados de las **evaluaciones** y la revisión exhaustiva en su toma de decisiones?

6. ¿La empresa realiza **evaluaciones** con un calendario regular?

7. ¿Las **evaluaciones** de la empresa están garantizadas por un **tercero** externo?

8. ¿El **tercero** externo que garantiza la **evaluación** está acreditado con un parámetro de derechos humanos relevante y confiable, por parte de una organización fiable?

Guía del indicador: Hay diversas maneras en que los sistemas algorítmicos pueden suponer perjuicios a los derechos humanos.[14] La elaboración de estos sistemas puede depender de información del usuario, a menudo sin conocimiento o consentimiento explícito ni informado del sujeto de datos, lo que constituye una violación a la privacidad. Esos sistemas también pueden causar o contribuir con perjuicios a la expresión y la información. Además, el objetivo de muchos sistemas de toma de decisiones algorítmicas es automatizar la personalización de las experiencias de los usuarios sobre la base de información del usuario recopilada o inferida, lo que puede causar o contribuir con la discriminación. Por tanto, las empresas deben llevar a cabo evaluaciones de riesgos de derechos humanos relacionados con su elaboración y uso de algoritmos, como sostiene el Consejo de Europa en su *Recomendación a los impactos de los derechos humanos de los sistemas algorítmicos* (2020).

Este indicador examina si las empresas llevan a cabo evaluaciones de riesgos de derechos humanos sólidas, frecuentes y responsables que evalúen sus políticas y prácticas relativas a su elaboración y utilización de sistemas algorítmicos. Estas evaluaciones deben ser parte de las actividades formales y sistemáticas de revisión exhaustiva con el objetivo de asegurar que sus decisiones y prácticas no causen, contribuyen ni exacerben perjuicios a los derechos humanos. Las evaluaciones permiten que las empresas identifiquen posibles riesgos a los derechos de libertad de expresión y privacidad de los usuarios, y que tomen medidas para mitigar posibles perjuicios si se identifican.

Nótese que este indicador no tiene la expectativa de que las empresas publiquen resultados detallados de sus evaluaciones de impacto en derechos humanos, pues las evaluaciones pueden incluir información delicada. En cambio, tiene la expectativa de que las empresas revelen que realizan evaluaciones de riesgos de los derechos humanos y brindan información sobre qué comprende su proceso de evaluación de riesgos de los derechos humanos.

Posibles fuentes:

- Informe anual o informe de sostenibilidad anual de la empresa
- Políticas de derechos humanos de la empresa
- Informes de evaluación de Global Network Initiative

G4(e) Evaluación del impacto: Calificación cero

Si la empresa se compromete con la **calificación cero** debe ejercer una revisión exhaustiva frecuente, integral y creíble, tales como sólidas **evaluaciones de impacto en los derechos humanos,** para identificar cómo todos los aspectos de su políticas y prácticas de calificación cero afectan a los derechos fundamentales de los usuarios a la libertad de expresión y la información, la privacidad, y a no ser discriminados, y para mitigar cualquier

[14] "Situaciones de riesgo de los derechos humanos: Algoritmos, aprendizaje automático y toma de decisiones automatizada", *Ranking Digital Rights*, julio de 2019: https://rankingdigitalrights.org/wp-content/uploads/2019/07/Human-Rights-Risk-Scenarios_-algorithms-machine-learning-automated-decision-making.pdf..

riesgo que supongan esos impactos.

Elementos:

1. ¿La empresa evalúa riesgos a la libertad de expresión y la información asociados con sus programas de **calificación cero**?

2. ¿La empresa evalúa riesgos a la privacidad asociados con sus programas de **calificación cero**?

3. ¿La empresa evalúa riesgos a la discriminación asociados con sus programas de **calificación cero**?

4. ¿La empresa realiza evaluación adicional cada vez que las **evaluaciones de riesgo** de la empresa identifica problemas?

5. ¿Los **altos ejecutivos** o miembros de la **junta directiva** de la empresa revisan y toman en cuenta los resultados de las **evaluaciones** y la revisión exhaustiva en su toma de decisiones?

6. ¿La empresa realiza evaluaciones con un calendario regular?

7. ¿Las **evaluaciones** de la empresa están garantizadas por un **tercero** externo?

8. ¿El **tercero** externo que garantiza la **evaluación** está acreditado con un parámetro de derechos humanos relevante y confiable, por parte de una organización fiable?

Guía del indicador: "Calificación cero" se refiere a programas —que pueden ser ofrecidos por empresas de telecomunicaciones y por plataformas, en asociación con empresas de telecomunicaciones— que brindan acceso a algunos servicios o plataformas en línea sin afectar el plan de datos de una persona. Muchos proveedores de telecomunicaciones, incluidas empresas calificadas por RDR, ofrecen esos programas, ya sea como único proveedor del programa o en sociedad con plataformas de medios sociales, como "Free Basics" de Facebook. Ese tipo de programas son una forma de priorización de red que mina los principios de neutralidad en la red —y puede generar diversos posibles perjuicios a los derechos humanos, incluido socavar el derecho a la libertad de expresión y de información. Además, Global Voices Advox ha identificado Free Basics de Facebook como un "mecanismo rentable para recopilar datos de los usuarios" (Global Voices, 2017), que plantea serios problemas de privacidad sobre el programa. Los programas de calificación cero también pueden ser discriminatorios en el sentido de que dan prioridad a algunos tipos de datos sobre otros, ya sea sobre la base del protocolo en cuestión (HTTP, HTTPS, VoIP, etc.) o sobre la base del contenido (es decir, dar prioridad a un sitio de red social sobre otro). Esta discriminación (contra tipos de datos) puede a su vez llevar a perjuicios de los derechos humanos que afectan a las personas basándose en sus características personales, incluido el género, raza o etnia, idioma(s) que hablan y muchos otros rasgos.

Este indicador examina si las empresas realizan evaluaciones sólidas, frecuentes y responsables sobre el impacto de los efectos de los programas de calificación cero en los derechos humanos de los usuarios. Las empresas que ofrecen estos programas deberían realizar evaluaciones de cómo estos programas pueden impactar los derechos de los usuarios a la expresión y la información, la privacidad y a no ser discriminados. Estas evaluaciones deberían ser parte de las actividades formales y sistemáticas de revisión exhaustiva de la empresa que tienen el objetivo de garantizar que las decisiones y prácticas de una empresa no causen, contribuyan ni exacerben perjuicios a los derechos humanos. Las evaluaciones permiten a las empresas identificar posibles riesgos de los programas de calificación cero y tomar medidas para mitigar posibles perjuicios si se identifican.

Nótese que este indicador no tiene la expectativa de que las empresas publiquen resultados detallados de sus evaluaciones de impacto en derechos humanos, pues las evaluaciones pueden incluir información delicada. En cambio, tiene la expectativa de que las empresas revelen que realizan evaluaciones de riesgos de los derechos humanos y brindan información sobre qué comprende su proceso de evaluación de riesgos de los derechos humanos.

Posibles fuentes:

- Informe anual o informe de sostenibilidad anual de la empresa
- Políticas de derechos humanos de la empresa
- Informes de evaluación de Global Network Initiative

G5. Participación y responsabilidad de los grupos de interés

La empresa debe **incluir** a diversos **grupos de interés** en el impacto de la empresa en la libertad de expresión y la información, privacidad, y riesgos potenciales relacionados con perjuicios a los derechos humanos, como la **discriminación**.

Elementos:

1. ¿La empresa integra una o más **iniciativas multipartidarias** que abordan una amplia gama de maneras en que los derechos fundamentales de los usuarios a la libertad de expresión y la información, la privacidad y a no ser discriminados pueden verse afectados en el curso de las operaciones de la empresa?

2. Si la empresa no integra una o más **iniciativas multipartidarias**, ¿la empresa integra alguna organización que participa sistemáticamente y de manera frecuente con grupos de interés que no son del sector y no son gubernamentales sobre la libertad de expresión y los problemas de privacidad?

3. Si la empresa no integra ninguna de estas organizaciones, ¿la empresa revela que inicia o participa en reuniones con **grupos de interés** que representan, defiendan o

que son personas cuyos derechos a la libertad de expresión y la información, y la privacidad se ven directamente impactados por los negocios de la empresa?

Guía del indicador: Este indicador busca evidencia de que la empresa participa y es responsable con sus grupos de interés, sobre todo con quienes enfrentan riesgos de derechos humanos en relación con sus actividades en línea. Tenemos la expectativa de que la participación de los grupos de interés sea un componente fundamental de la elaboración y el proceso de evaluación del impacto que realiza una empresa. La participación de los grupos de interés debe llevarse a cabo en diversos asuntos relacionados con la libertad de expresión y de información, privacidad y derechos relacionados de los usuarios, incluido un proceso de la empresa para elaborar los términos de servicio, las políticas de privacidad y de identidad, así como las políticas de uso de algoritmos y las políticas que rigen la publicidad dirigida, junto con las prácticas de aplicación para esas políticas. La participación de los grupos de interés y los mecanismos de responsabilidad deben incluir diversas maneras en que se pueden violar los derechos de los usuarios: solicitudes gubernamentales, acciones de otros terceros a través de productos y servicios de las empresas, o de las propias empresas. Las empresas que reciben crédito total en este indicador no solamente participarán con los grupos de interés, sino que también se comprometen con los procesos de responsabilidad, tales como las evaluaciones independientes supervisadas por entidades cuyas decisiones finales no están controladas solamente por las empresas.

Participar con los grupos de interés, sobre todo los que operan en ambientes de alto riesgo, puede ser delicado. Una empresa puede no sentirse cómoda de revelar públicamente detalles específicos sobre qué grupos de interés consulta, dónde o cuándo se reúnen y qué analizan. Aunque alentamos a las empresas a brindar detalles que no sean delicados sobre la participación de los usuarios, como mínimo buscamos que exista una revelación pública de que una empresa participa con grupos de interés que son o representan a usuarios cuyos derechos a la libertad de expresión y la privacidad están en riesgo. Una manera en que el público sepa si una empresa emprende este tipo de participación y que esta participación genera resultados es a través de su intervención en una iniciativa multipartidaria cuyo objetivo no es solamente crear un espacio seguro para la participación, sino también permitir que las empresas hagan compromisos, que les den su apoyo para que los cumplan y hagan que las empresas se responsabilicen por esto. Los mecanismos de responsabilidad plena y creíble requieren gobernabilidad multipartidaria en el que las empresas solas no controlan la toma de decisiones con respecto a procesos de responsabilidad y participación, sino que comparten autoridad en la toma de decisiones con representantes de otros grupos de interés.

Si una empresa recibe crédito total en el Elemento 1, automáticamente recibirá crédito total en el Elemento 2 y el Elemento 3. Nótese que, como el ámbito del trabajo de Global Network Initiative se centra en solicitudes gubernamentales y que al menos la mitad de la metodología de RDR aborda amenazas de los derechos humanos que no se originan en los Gobiernos, para el Índice RDR 2020, la pertenencia al GNI (sin evidencia de participación y responsabilidad en otros riesgos de los derechos humanos además de los planteados por los

Gobiernos) tendrá como resultado solamente crédito parcial para el Elemento 1 de este indicador.

Posibles fuentes:

- Informe de sostenibilidad/responsabilidad corporativa de la empresa
- Informe anual de la empresa
- Blog de la empresa
- Preguntas frecuentes o centro de ayuda de la empresa

G6. Solución y peticiones

G6(a). Solución

La empresa debe tener mecanismos de **reclamo** y **solución** claros y previsibles para abordar problemas de libertad de expresión y privacidad de los usuarios.

Elementos:

1. ¿La empresa **revela claramente** que tiene **mecanismo(s) de reclamo** que permiten a los usuarios presentar quejas si sienten que sus derechos a la libertad de expresión y la información derechos se han visto afectados negativamente por las políticas o prácticas de la empresa?

2. ¿La empresa **revela claramente** que tiene **mecanismo(s) de reclamo** que permiten a los usuarios presentar quejas si sienten que su privacidad se ha visto afectada negativamente por las políticas o prácticas de la empresa?

3. ¿La empresa **revela claramente** sus procedimientos para brindar **solución** a los **reclamos** relacionados con la libertad de expresión y de información?

4. ¿La empresa **revela claramente** sus procedimientos para brindar **solución** a los **reclamos** relacionados con la privacidad?

5. ¿La empresa **revela claramente** plazos para sus procedimientos de **reclamo** y **solución**?

6. ¿La empresa **revela claramente** la cantidad de quejas recibidas con relación a la libertad de expresión?

7. ¿La empresa **revela claramente** la cantidad de quejas recibidas con relación a la privacidad?

8. ¿La empresa **revela claramente** evidencia de que brinda **solución** para **reclamos sobre** libertad de expresión?

9. ¿La empresa **revela claramente** evidencia de que brinda **solución** para **reclamos** sobre privacidad?

Guía del indicador: Los derechos humanos solamente se pueden proteger y respetar si las personas son compensadas cuando creen que sus derechos han sido violados. Este indicador examina si las empresas brindan esos mecanismos de solución y si es que han revelado públicamente los procesos para responder a reclamos de personas que creen que la empresa ha violado o facilitado directamente violaciones a su libertad de expresión o privacidad.

Tenemos la expectativa de que las empresas revelen claramente el mecanismo o mecanismos de reclamo que permiten a los usuarios presentar quejas si sienten que su libertad de expresión y su privacidad han sido transgredidas por las políticas o prácticas de la empresa. Para recibir crédito total en el Elemento 1, los mecanismos de reclamo de una empresa no tienen que afirmar explícitamente que se aplican a quejas relacionadas con libertad de expresión y privacidad. Sin embargo, debe estar claro que este mecanismo se puede usar para presentar cualquier reclamo relacionado con los derechos humanos. También tenemos la expectativa de que los mecanismos de reclamo de una empresa estén claramente accesibles a los usuarios. Además, la empresa debe explicar sus procesos para brindar una solución a este tipo de quejas, y revelar evidencia de que así lo hace. Las empresas deben describir plazos claros para abordar cada etapa de los procesos de reclamo y solución. Estos parámetros están definidos en el Principio 31 de los Principios Rectores sobre las Empresas y los Derechos Humanos de Naciones Unidas, que afirma que las empresas deben publicar procedimientos de solución claros, accesibles y previsibles.[15]

Posibles fuentes:

- Términos de servicio de la empresa o acuerdos de usuario equivalentes
- Políticas de contenido de la empresa
- Políticas de privacidad de la empresa, guías de privacidad o sitio de recursos de privacidad
- Informe de sostenibilidad/responsabilidad corporativa de la empresa
- Preguntas frecuentes o centro de ayuda de la empresa
- Informe de transparencia de la empresa (por la cantidad de quejas recibidas)
- Políticas de publicidad de la empresa

G6(b). Proceso para peticiones de moderación de contenido

La empresa debe ofrecer a los usuarios mecanismos de **peticiones** claros y predecibles, y procesos para presentar **acciones de moderación de contenido**.

Elementos:

[15] "Principios rectores sobre las empresas y derechos humanos", *Oficina del Alto Comisionado de Derechos Humanos de Naciones Unidas*, 2011, https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_sp.pdf..

1. ¿La empresa **revela claramente** que brinda a los **usuarios afectados** la capacidad de **apelar acciones de moderación de contenido**?

2. ¿La empresa **revela claramente** que **notifica** a los usuarios que se ven **afectados** por una **acción de moderación de contenido**?

3. ¿La empresa **revela claramente** un plazo para **notificar** a los **usuarios afectados** cuando emprende una **acción de moderación de contenido**?

4. ¿La empresa **revela claramente** si es que las **peticiones** no están permitidas?

5. ¿La empresa **revela claramente** su proceso para revisar **peticiones**?

6. ¿La empresa **revela claramente** sus plazos para revisar **peticiones**?

7. ¿La empresa **revela claramente** que esas peticiones son revisadas por al menos un humano no involucrado en la **acción de moderación de contenido** original?

8. ¿La empresa **revela claramente** qué rol tiene la automatización en la revisión de **peticiones**?

9. ¿La empresa **revela claramente** que los **usuarios afectados** tienen una oportunidad de presentar información adicional que será considerada en la revisión?

10. ¿La empresa **revela claramente** que brinda a los **usuarios afectados** una declaración que contenga la razón para su decisión?

11. ¿La empresa **revela claramente** evidencia de que aborda las **peticiones** de moderación de contenido?

Guía del indicador: Sin importar con cuánto cuidado una plataforma elabora sus términos de servicio, los errores son inevitables en la exigente y subjetiva tarea de moderación de contenido. Esto es particularmente cierto cuando la moderación de contenido se despliega rápidamente por medio del uso de automatización. Para respetar los derechos de los usuarios a la libertad de expresión y de información, las empresas deben ofrecer un sistema de peticiones sólido y transparente que permita a los usuarios apelar las decisiones tomadas por la empresa que influyan directamente en la capacidad de los usuarios de ejercer esos derechos. Las empresas deben revelar claramente sus procesos para apelar las acciones de moderación de contenido, que incluyan la posibilidad de permitir a los usuarios afectados a que apelen inmediatamente esa acción. Un proceso de apelaciones sólido debe incluir la supervisión de un revisor humano y dar a los usuarios afectados una oportunidad para presentar información adicional. Las empresas también deben ofrecer un plazo claro para revisar las apelaciones y revelar claramente las circunstancias en que las apelaciones no son posibles.

Para recibir crédito total en este indicador, las empresas deben informar a los usuarios cómo presentar una apelación y describir qué ocurre una vez que se inicia la tramitación de la apelación. Esto incluye notificar a los usuarios de sus opciones de apelación en cuanto la empresa toma una acción inicial sobre su contenido, y aclarar el rol de los moderadores automatizados y humanos independientes en el proceso de apelación, revelar claramente la razón para una decisión de apelaciones en el plazo involucrado y especificar las circunstancias en que el proceso de apelaciones no esté disponible. Las empresas también deberían demostrar claramente que responden las apelaciones con publicación de datos sobre las apelaciones recibidas y el resultado de esas decisiones.

Posibles fuentes:

- Términos de servicio de la empresa o acuerdos del usuario
- Políticas de privacidad de la empresa
- Informe de sostenibilidad de la empresa

Libertad de expresión e Información

Los indicadores en esta categoría buscan evidencia de que la empresa demuestra que respeta el derecho a la libertad de expresión y la información, como establece la Declaración Universal de Derechos humanos,[16] el Pacto Internacional de Derechos Civiles y Políticos,[17] y otros instrumentos de derechos humanos internacionales. Las políticas y prácticas reveladas de la empresa demuestran qué hace para evitar colaborar con acciones que pueden interferir con este derecho, salvo cuando esas acciones sean legítimas, proporcionadas o por un objetivo justificable. Las empresas que se desempeñan bien en este indicador demuestran un sólido compromiso público con la transparencia, no solamente en términos de cómo responde a solicitudes gubernamentales y de otros, sino también de cómo determinan, comunican y aplican reglas y prácticas comerciales privadas que afectan el derecho fundamental de los usuarios a la libertad de expresión y de información.

F1. Acceso a políticas

F1(a). Acceso a términos de servicio

La empresa debe ofrecer **términos de servicio** que sean **fáciles de encontrar** y **fáciles de comprender**.

Elementos:

1. ¿Los **términos de servicio** de la empresa son **fáciles de encontrar**?

[16] "Declaración Universal de Derechos Humanos", https://www.un.org/es/universal-declaración-human-rights/index.html//.
[17] "Pacto Internacional de Derechos Civiles y Políticos", Oficina del Alto Comisionado de Derechos Humanos de Naciones Unidas, https://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx,

2. ¿Los **términos de servicio** están disponibles en el idioma principal que hablan los usuarios en la jurisdicción de la empresa?

3. ¿Los **términos de servicio** están presentados de **manera comprensible**?

Guía del indicador: Los términos de servicio de una empresa definen la relación entre el usuario y la empresa. Estos términos contienen reglas sobre actividades y contenido prohibidos, y las empresas también pueden tomar acción contra los usuarios por violar las reglas descritas en los términos. Considerando esto, tenemos la expectativa de que las empresas garanticen que sus términos sean fáciles de acceder y de comprender.

Este indicador evalúa si para los usuarios es fácil ubicar los términos de la empresa. Un documento que sea fácil de encontrar se ubica en la página de inicio de la empresa o servicio, a uno o dos clics de la página de inicio o en un lugar lógico en el que los usuarios pueden esperar encontrarlo. El uso de combinaciones de lugares o colores que hacen menos notorio a un texto o enlace, o que hacen que sea difícil de encontrar en una página web, significa que el documento no es fácilmente accesible. Los términos de servicio de una aplicación nunca deben estar "a más de dos toques" al usar la aplicación (por ejemplo, incluir una opción de "Privacidad"/" Protección de datos" en la funcionalidad del menú de la aplicación). Los términos también deben estar disponibles en los principales idiomas del mercado principal de operaciones. Además, esperamos que una empresa tome medidas para ayudar a los usuarios a entender la información presentada en sus documentos. Esto incluye, sin limitarse a, ofrecer resúmenes, consejos o pautas que expliquen qué significan los términos, con encabezados, tamaño de fuente legible u otras características gráficas que ayuden a los usuarios a entender el documento, o escribir los términos con sintaxis fácilmente legible.

Posibles fuentes:
- Términos de servicio, términos de uso, términos y condiciones de la empresa, etc.
- Políticas de uso de la empresa, pautas comunitarias, reglas, etc. que sean aceptables.

F1(b). Acceso a políticas de contenido publicitario

La empresa debe ofrecer **políticas de contenido publicitario** que sean **fáciles de encontrar** y **fáciles de comprender**.

Elementos:

1. ¿Las **políticas de contenido publicitario** de la empresa son **fáciles de encontrar**?

2. ¿Las **políticas de contenido publicitario** de la empresa están disponibles en el idioma principal que hablan los usuarios en la jurisdicción de la empresa?

3. ¿Las **políticas de contenido publicitario** de la empresa están presentadas de **manera comprensible**?

4. (Para **ecosistemas móviles**): ¿La empresa **revela claramente** que solicita que las aplicaciones disponibles en su **tienda de aplicaciones** brinden a los usuarios las **políticas de contenido publicitario**?

5. (Para **ecosistemas de asistente digital personal**): ¿La empresa **revela claramente** que solicita que las **habilidades** disponibles en su **tienda de habilidades** brinden a los usuarios las **políticas de contenido publicitario**?

Guía del indicador: Las empresas que permiten cualquier tipo de publicidad en sus servicios o plataformas deben revelar claramente las reglas sobre qué tipo de contenido publicitario está prohibido, por ejemplo, anuncios que discriminen a personas o grupos basándose en atributos personales como edad, religión, género y etnia. Las empresas deben ser transparentes sobre estas reglas para que tanto usuarios como anunciantes puedan entender qué tipos de contenido publicitario no están permitidos, por lo que deben ser responsables por el contenido publicitario que aparezca en sus servicios o plataformas.

Por lo tanto, las empresas deben hacer que estas reglas sean fáciles de encontrar (E1), fáciles de comprender (E3) y que estén disponibles en los principales idiomas del mercado local de la empresa (E2). Las empresas que operan ecosistemas móviles (Apple iOS, Google Android e implementación de Android de Samsung) y ecosistemas de asistente personal digital (Alexa de Amazon, AliGenie de Alibaba) deben permitir a los usuarios elegir qué aplicaciones o habilidades descargar sobre la base de su participación (o no) en redes de publicidad. Por lo tanto, el Elemento 4 y el Elemento 5 preguntan si la empresa revela un requisito para que las aplicaciones o habilidades disponibles en su tienda de aplicaciones o tienda de habilidades brinden a los usuarios las políticas de contenido publicitario.

Posibles fuentes:
- Políticas de publicidad de la empresa
- Centro de ayuda de negocios de la empresa
- Términos de uso de la empresa

F1(c). Acceso a políticas de publicidad dirigida

La empresa debe ofrecer **políticas de publicidad dirigida** que sean **fáciles de encontrar** y **fáciles de comprender**.

Elementos:

1. ¿Las **políticas de publicidad dirigida** de la empresa son **fáciles de encontrar**?

2. ¿Las **políticas de publicidad dirigida** están disponibles en el idioma o idiomas principales que hablan los **usuarios** en mercado local de la empresa?

3. ¿Las **políticas de publicidad dirigida** están presentada de **manera comprensible**?

4. (Para **ecosistemas móviles**): ¿La empresa **revela claramente** que solicita que las **aplicaciones** disponibles a través de su **tienda de aplicaciones** brinden a los usuarios las **políticas de publicidad dirigida**?

5. (Para **ecosistemas de asistente digital personal**): ¿La empresa **revela claramente** que solicita que las **habilidades** disponibles en su **tienda de habilidades** brinden a los usuarios las **políticas de contenido publicitario?**

Guía del indicador: Además de brindar políticas de contenido publicitario accesibles (Indicador F1b), las empresas también deben revelar claramente sus políticas de publicidad dirigida. La capacidad de los anunciantes u otros terceros para llegar a los usuarios con contenido personalizado —basándose en su comportamiento de navegación, información de ubicación y otros datos y características que se infieren a partir de eso[18]— puede determinar significativamente (o en algunos casos, distorsionar) el ecosistema en línea de un usuario. La selección de sujetos, que puede incluir contenido pagado y no pagado, puede ampliar las desigualdades sociales fuera de línea y puede ser abiertamente discriminatoria. También puede resultar en "burbujas de filtro" y ampliar contenido problemático, e incluso contenido creado con el objetivo de inducir a error o difundir falsedades.[19]

Por lo tanto, las empresas que permiten a los anunciantes y otros terceros dirigirse a sus usuarios con publicidad o contenido personalizado deberían publicar políticas de selección de sujetos que los usuarios puedan comprender y encontrar fácilmente, y que estén disponibles en los principales idiomas en los que opera la empresa. Los usuarios deben poder acceder y comprender estas reglas para tomar decisiones informadas con datos suficientes sobre el contenido publicitario que reciben. Para ecosistemas móviles y ecosistemas de asistente personal digital, las empresas pueden revelar un requisito para que las aplicaciones y las habilidades que estén disponibles por medio de sus tiendas de aplicaciones o tiendas de habilidades brinden a los usuarios políticas de publicidad dirigida que sean accesibles.

Posibles fuentes:

- Políticas de publicidad de la empresa
- Centro de ayuda de la empresa
- Términos de uso de la empresa

F1(d). Acceso a políticas de uso de sistemas algorítmicos

[18] Para saber más sobre políticas de inferencia de datos, ver la Sección 6.2 del "Estudio piloto y lecciones aprendidas 2020", *Ranking Digital Rights*, 16 de marzo de 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

[19] "Indicadores preliminares: Parámetros de transparencia y responsabilidad para publicidad dirigida y sistemas de toma de decisiones algorítmicas", *Ranking Digital Rights*, octubre de 2019: https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-Targeted-advertising-algorithms.pdf.

La empresa debe ofrecer políticas relacionadas con su uso de **algoritmos** que los usuarios puedan **encontrar** y **comprender fácilmente**.

Elementos:

1. ¿Las **políticas de uso de sistemas algorítmicos** de la empresa son **fáciles de encontrar**?

2. ¿Las **políticas de uso de sistemas algorítmicos** están disponibles en los idiomas principales que hablan los usuarios en el mercado local de la empresa?

3. ¿Las **políticas de uso de sistemas algorítmicos** están presentadas de **manera comprensible**?

Guía del indicador: El uso de sistemas algorítmicos puede tener efectos adversos sobre derechos humanos fundamentales, y específicamente, sobre el derecho a la libertad de expresión y la información, y sobre el derecho a no ser discriminados.[20] Además de comprometerse claramente con respetar y proteger los derechos humanos mientras elaboran e implementan estas tecnologías (*ver Indicador G1, Elemento 3*), las empresas también deben publicar políticas que describan claramente los términos sobre cómo usan sistemas algorítmicos en sus servicios y plataformas. Así como tienen políticas de términos de servicio o acuerdos del usuario que resumen los términos sobre qué tipo de contenido o actividades están prohibidas, las empresas que usan sistemas algorítmicos con el potencial de causar perjuicios a los derechos humanos también deberían publicar políticas claras y accesibles que afirmen la naturaleza y funciones de estos sistemas. Como expresa el Consejo de Europa en su *Recomendación sobre los impactos de los sistemas algorítmicos en los derechos humanos* (2020), estas políticas deben ser fáciles de encontrar, estar presentadas en lenguaje simple y contener opciones para que los usuarios gestionen configuraciones.

Nótese que en este indicador estamos buscando políticas que expliquen términos sobre cómo la empresa implementa sistemas algorítmicos en sus plataformas y servicios. También buscamos que las empresas revelen términos que definan cómo elaboran y prueban sistemas algorítmicos, lo que se aborda en el Indicador P1b.

Posibles fuentes

- Políticas de uso de sistemas algorítmicos
- Guías para elaborar sistemas algorítmicos
- Políticas de privacidad o políticas de datos
- Centro de ayuda

[20] "Escenarios de riesgo de derechos humanos: Algoritmos, aprendizaje digital y toma de decisiones automatizada", *Ranking Digital Rights*, julio de 2019: https://rankingdigitalrights.org/wp-content/uploads/2019/07/Human-Rights-Risk-Scenarios_-algorithms-machine-learning-automated-decision-making.pdf

F2. Notificación de cambios de políticas

F2(a). Cambios a los términos de servicio

La empresa debe **revelar claramente** que **notifica directamente** a los usuarios cada vez que cambie sus términos de servicio, antes de que estos cambios estén vigentes.

Elementos:

1. ¿La empresa **revela claramente** que **notifica directamente** a los usuarios sobre todos los cambios a sus **términos de servicio**?

2. ¿La empresa **revela claramente** cómo **notificará directamente** a los usuarios de los cambios?

3. ¿La empresa **revela claramente** el plazo en el cual **notifica directamente** a los **usuarios** de los cambios antes de que estos estén vigentes?

4. ¿La empresa tiene un **archivo público** o **registro de cambios**?

Guía del indicador: Es común que las empresas cambien sus términos de servicio a medida que sus negocios evolucionan. Sin embargo, estos cambios, que pueden incluir reglas sobre actividades y contenidos prohibidos, pueden tener un impacto significativo en los derechos de libertad de expresión y de información de los usuarios. Por lo tanto, nuestra expectativa es que las empresas se comprometan a notificar a los usuarios cuando cambien estos términos y de ofrecer a los usuarios información que los ayude a entender qué significan estos cambios.

Este indicador evalúa si las empresas revelan claramente el método y plazo para notificar a los usuarios sobre los cambios a sus términos de servicio. Nuestra expectativa es que las empresas se comprometan a notificar de estos cambios directamente a los usuarios antes de que entren en vigencia. El método de notificación directa puede variar según el tipo de servicio, esperamos que las empresas notifiquen directamente a los usuarios de una manera que a los usuarios les asegure poder acceder. Para servicios que contengan cuentas de usuario, la notificación directa puede involucrar el envío de un correo electrónico o un mensaje de texto. Para servicios que no requieran una cuenta de usuario, la notificación directa puede incluir la publicación de una notificación destacada en donde los usuarios acceden a ese servicio. Este indicador también busca evidencia de que una empresa brinda públicamente registros disponibles de términos anteriores para que las personas puedan entender cómo los términos de la empresa han evolucionado a lo largo del tiempo.

Posibles fuentes:

- Términos de servicio de la empresa

F2(b). Cambios a políticas de contenido publicitario

La empresa debe **revelar claramente** que **notifica directamente** a los **usuarios** cuando cambia sus **políticas de contenido publicitario,** antes de que estos cambios estén vigentes.

Elementos:

1. ¿La empresa **revela claramente** que **notifica directamente** a los **usuarios** sobre cambios a sus **políticas de contenido publicitario**?

2. ¿La empresa **revela claramente** cómo **notificará directamente** a los **usuarios** de estos cambios?

3. ¿La empresa **revela claramente** el plazo en el cual **notifica directamente** a los **usuarios** de los cambios antes de que estos cambios estén vigentes?

4. ¿La empresa tiene un **archivo público** o **registro de cambios**?

5. (Para **ecosistemas móviles**): ¿La empresa **revela claramente** que pide a las aplicaciones disponibles en su **tienda de aplicaciones** que **notifiquen** a los **usuarios** cuando los **aplicaciones** cambien sus **políticas de contenido publicitario**?

6. (Para **ecosistemas digitales personales**): ¿La empresa **revela claramente** que pide a las **habilidades** disponibles en su **tienda de habilidades** que **notifiquen** a los **usuarios** cuando cambien las **habilidades** de sus **políticas de contenido publicitario**?

Guía del indicador: Es común que las empresas cambien sus políticas de contenido publicitario a medida que sus negocios y servicios evolucionan. Sin embargo, estos cambios, que pueden incluir revisión de reglas sobre contenido y actividades prohibidos, pueden afectar la libertad de expresión y de información de los usuarios, así como su derecho a no ser discriminados. Por lo tanto, las empresas deben comprometerse a notificar a los usuarios cuando cambien estos términos y de brindar información a los usuarios que los ayude a comprender qué significan esos cambios.

Este indicador evalúa si las empresas revelan claramente el método y plazo para notificar a los usuarios sobre los cambios antes de que los cambios estén vigentes. El método de notificación directa puede variar según el tipo de servicio; tenemos la expectativa de que las empresas notifiquen directamente a los usuarios de manera que a los usuarios les asegure poder acceder. Para servicios que contengan cuentas de usuario, la notificación directa puede incluir enviar un correo electrónico o un mensaje de texto. Para servicios que no requieran una cuenta de usuario, la notificación directa puede incluir la publicación una notificación destacada en donde los usuarios acceden a ese servicio. Este indicador también busca evidencia de que una empresa brinda registros públicamente disponibles de términos anteriores para que las personas puedan entender cómo los términos de la empresa han evolucionado a lo largo del tiempo.

Posibles fuentes:

- Políticas, guías, términos de uso, etc. de publicidad
- Publicidad o Centro de Ayuda de la empresa

F2(c). Cambios a políticas de publicidad dirigida

La empresa debe **revelar claramente** que **notifica directamente** a los **usuarios** cuando cambia sus **políticas de publicidad dirigida**, antes de que estos cambios estén vigentes.

Elementos:

1. ¿La empresa **revela claramente** que **notifica directamente** a los **usuarios** sobre los cambios a sus **políticas de publicidad dirigida**?

2. ¿La empresa **revela claramente** cómo **notificará directamente** a los **usuarios** de los cambios?

3. ¿La empresa **revela claramente** el plazo en el cual **notifica directamente** a los **usuarios** de cambios antes de que estos cambios estén vigentes?

4. ¿La empresa tiene un **archivo público** o **registro de cambios**?

5. (Para **ecosistemas móviles**): ¿La empresa **revela claramente** que pide a los **aplicaciones** disponibles en su **tienda de aplicaciones** que **notifiquen directamente** a los **usuarios** cuando los **aplicaciones** cambien sus **políticas de publicidad dirigida**?

6. (Para **ecosistemas digitales personales**): ¿La empresa **revela claramente** que pide a las **habilidades** disponibles en su **tienda de habilidades** que **notifiquen** a los **usuarios** cuando las **habilidades** cambien sus **políticas de publicidad dirigida**?

Guía del indicador: Es común que las empresas cambien sus políticas de publicidad dirigida a medida que sus negocios y servicios evolucionan. Sin embargo, estos cambios pueden afectar la libertad de expresión y de información de los usuarios, así como su derecho a no ser discriminados. Por tanto, las empresas deben comprometerse a notificar a los usuarios cuando cambien estos términos y a brindar a los usuarios información que los ayude a entender qué significan estos cambios.

Este indicador evalúa si las empresas revelan claramente el método y plazo para notificar a los usuarios sobre los cambios antes de que los cambios estén vigentes. El método de notificación directa puede variar según el tipo de servicio; tenemos la expectativa de que las empresas notifiquen directamente a los usuarios de una manera que a los usuarios les asegure poder acceder. Para servicios que contengan cuentas de usuario, la notificación directa puede incluir enviar un correo electrónico o un mensaje de texto. Para servicios que no requieran una cuenta de usuario, la notificación directa puede incluir publicar una

notificación destacada donde los usuarios acceden a ese servicio. Este indicador también busca evidencia de que una empresa brinde registros públicamente disponibles de términos anteriores para que las personas puedan entender cómo los términos de la empresa han evolucionado con el tiempo.

Posibles fuentes:

- Políticas, guías, términos de uso, etc. de publicidad
- Publicidad o Centro de Ayuda de la empresa

F2(d). Cambios a políticas de uso de sistemas algorítmicos

La empresa debe **revelar claramente** que **notifica directamente** a los **usuarios** cuando cambie sus **políticas de uso de sistemas algorítmicos**, antes de que estos cambios estén vigentes.

Elementos:

1. ¿La empresa **revela claramente** que **notifica directamente** a los **usuarios** sobre cambios a sus **políticas de uso de sistemas algorítmicos**?

2. ¿La empresa **revela claramente** cómo **notificará directamente** a los **usuarios** de los cambios?

3. ¿La empresa **revela claramente** el plazo en el cual **notifica directamente** a los **usuarios** de los cambios antes de que estos cambios estén vigentes?

4. ¿La empresa tiene un **archivo público** o **registro de cambios**?

Guía del indicador: Cuando las empresas cambian sus políticas de uso de algoritmos, estos cambios pueden afectar la libertad de expresión y de información de los usuarios, así como su derecho a no ser discriminados. Por lo tanto, las empresas deben comprometerse a notificar a los usuarios cuando cambien estas políticas y a brindar a los usuarios información que les ayude a comprender qué significan estos cambios. Este parámetro está en línea con la *Recomendación de los impactos de los sistemas algorítmicos en derechos humanos* del Consejo de Europa (2020).

Este indicador evalúa si las empresas revelan claramente el método y plazo para notificar a los usuarios sobre cambios antes de que los cambios estén vigentes. El método de notificación directa puede variar según el tipo de servicio; tenemos la expectativa de que las empresas notifiquen directamente a los usuarios de una manera que a los usuarios les asegure poder acceder. Para servicios que contengan cuentas de usuario, la notificación directa puede incluir el envío de un correo electrónico o mensaje de texto. Para servicios que no requieran una cuenta de usuario, la notificación directa puede incluir la publicación de una notificación destacada en donde los usuarios accedan a ese servicio. Este indicador también busca evidencia de que una empresa brinda registros públicamente disponibles de términos anteriores para que las personas puedan entender cómo los términos de la empresa han evolucionado a lo largo del tiempo.

Posibles fuentes

- Políticas de uso de sistemas algorítmicos
- Guías para elaborar sistemas algorítmicos
- Políticas de privacidad o políticas de datos
- Centro de ayuda

F3. Proceso para aplicación de políticas

F3(a). Proceso para aplicación de términos de servicio

La empresa debe **revelar claramente** las circunstancias bajo las cuales puede restringir **contenido** o **cuentas de usuario**.

Elementos:

1. ¿La empresa **revela claramente** qué tipos de **contenido** o actividades no permite?

2. ¿La empresa **revela claramente** por qué puede **restringir la cuenta de un usuario**?

3. ¿La empresa **revela claramente** información sobre los procesos que usa para identificar **contenido** o **cuentas** que violan las reglas de la empresa?

4. ¿La empresa **revela claramente** cómo usa **sistemas algorítmicos** para señalizar **contenido** que puede violar las reglas de la empresa?

5. ¿La empresa **revela claramente** si alguna autoridad gubernamental recibe consideración prioritaria cuando **marca** **contenido** para ser restringido por violar las reglas de la empresa?

6. ¿La empresa **revela claramente** si alguna entidad privada recibe consideración prioritaria cuando **marca** **contenido** para ser restringido por violar las reglas de la empresa?

7. ¿La empresa **revela claramente** sus procesos para aplicar sus reglas una vez que se detecten violaciones?

Guía del indicador: Es esperable que las empresas fijen reglas que prohíban algún contenido o actividades, como discurso tóxico o comportamiento malicioso. Sin embargo, cuando las empresas elaboran y aplican reglas sobre qué pueden hacer y decir las personas en internet —o si pueden acceder a un servicio— deben hacerlo de tal manera que sea transparente y responsable.

Por lo tanto, tenemos la expectativa de que las empresas revelen claramente qué son esas reglas y cómo las aplican. Esto incluye información sobre cómo las empresas se enteran de material o actividades que violan sus términos. Por ejemplo, las empresas pueden depender

de contratistas externos para revisar contenido o la actividad de los usuarios. También pueden depender de mecanismos comunitarios para señalizar contenido que permita a los usuarios señalar el contenido de otros usuarios o actividad para que la empresa lo revise. También pueden implementar sistemas algorítmicos para detectar y señalar filtraciones, en cuyo caso, las empresas deben explicar cómo se usan estos sistemas y en qué tipos de contenido. Tenemos la expectativa de que las empresas revelen claramente si tienen una política de garantizar la prioridad o brindar consideración expeditiva con cualquier autoridad gubernamental o miembros de organizaciones privadas u otras entidades que identifiquen su afiliación organizativa cuando denuncien contenido o usuarios por presuntamente violar las reglas de la empresa. Para ecosistemas móviles, tenemos la expectativa de que las empresas revelen los tipos de aplicaciones que restringirían. Para ecosistemas de asistentes personales digitales, tenemos la expectativa de que las empresas revelen los tipos de habilidades y resultados de búsquedas que restringirían. En esta revelación, la empresa también debe ofrecer ejemplos que ayuden a los usuarios a entender qué significan estas reglas.

Posibles fuentes:

- Términos de servicio, acuerdos de usuario de la empresa
- Política de uso aceptable de la empresa, normas comunitarias, guías de contenido, políticas sobre comportamiento abusivo o documento similar que explique las reglas que los usuarios deben seguir
- Centro de asistencia, de ayuda o preguntas frecuentes de la empresa

F3(b). Reglas y aplicación de contenido publicitario

La empresa debe **revelar claramente** las políticas que rigen qué tipo de contenido publicitario está prohibido.

Elementos:

1. ¿La empresa **revela claramente** qué tipo de **contenido publicitario** no permite?

2. ¿La empresa **revela claramente** si **pide** que todo el **contenido publicitario** esté claramente especificado como tal?

3. ¿La empresa **revela claramente** los procesos y tecnologías que usa para identificar **contenido publicitario** o **cuentas** que violen las reglas de la empresa?

Guía del indicador: Las empresas deben revelar claramente sus políticas sobre qué tipo de contenido publicitario está prohibido en una plataforma o servicio, y sus procesos para aplicar estas reglas. Específicamente, este indicador pregunta si las empresas revelan claramente qué tipos de contenido publicitario están prohibidos, si la empresa revela un requisito de que todo el contenido publicitario esté claramente identificado como tal, y si revela sus procesos para aplicar estar reglas.

Posibles fuentes:

- Portal de anunciantes, políticas de publicidad, políticas sobre publicidad política de la empresa
- Términos de servicio de la empresa, contrato del usuario
- Políticas de uso de la empresa, pautas comunitarias, reglas, etc. que sean aceptables
- Centro de asistencia, centro de ayuda o preguntas frecuentes de la empresa

F3(c). Reglas y aplicación de la publicidad dirigida

La empresa debe **revelar claramente** sus políticas que rigen qué tipo de **publicidad dirigida** está prohibida.

Elementos:

1. ¿La empresa **revela claramente** si permite que **terceros** se dirijan a sus **usuarios** con **contenido publicitario**?

2. ¿La empresa **revela claramente** qué tipos de **parámetros dirigidos** no están permitidos?

3. ¿La empresa **revela claramente** que no permite que los **anunciantes** se dirijan a personas específicas?

4. ¿La empresa **revela claramente** que las **categorías de audiencia publicitaria** generadas **algorítmicamente** son evaluadas por revisores humanos antes de que se usen?

5. ¿La empresa **revela claramente** información sobre los procesos y tecnologías que usa para identificar **contenido publicitario** o **cuentas** que violen las reglas de la empresa?

Guía del indicador: La capacidad de los anunciantes u otros terceros para llegar a los usuarios con contenido personalizado —basándose en su comportamiento de navegación, información de ubicación y otros datos y características que se infieren a partir de eso[21]— puede determinar significativamente el ecosistema en línea de un usuario. La selección de sujetos, que puede incluir contenido pagado y no pagado, puede ampliar las desigualdades sociales fuera de línea y puede ser abiertamente discriminatoria. También puede resultar en "burbujas de filtro" y ampliar contenido problemático, incluido contenido con el objetivo de inducir a error o difundir falsedades.[22]

---

[21] Para saber más sobre políticas de inferencia de datos, sección 6.2 de este informe. "Estudio piloto y lecciones aprendidas 2020", *Ranking Digital Rights*, 16 de marzo de 2020: https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf

[22] "Indicadores preliminares: Parámetros de transparencia y responsabilidad para publicidad dirigida y sistemas de toma de decisión algorítmica", *Ranking Digital Rights*, octubre de 2019: https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-Targeted-advertising-algorithms.pdf.

Por lo tanto, las empresas que permiten a los anunciantes y otros terceros dirigirse a sus usuarios con publicidad o contenido personalizado deben tener políticas claras que describan sus reglas de orientación de publicidad. Las empresas deben revelar claramente si permiten que terceros se dirijan a sus usuarios con anuncios personalizados u otros tipos de contenido patrocinado, y revelar claramente qué parámetros de selección de sujetos — como usar algunos tipos de categorías de audiencia, como edad, ubicación u otras características del usuario—no están permitidas. Las empresas también deben revelar sus procesos para identificar violaciones a las reglas de selección de sujetos.

Posibles fuentes:

- Portal de anunciantes, políticas de publicidad, políticas sobre publicidad política de la empresa
- Políticas de uso aceptables de la empresa
- Centro de asistencia, centro de ayuda o preguntas frecuentes de la empresa

F4. Datos sobre aplicación de políticas

F4(a). Datos sobre restricciones de contenido para aplicar términos de servicio

La empresa debe **revelar claramente** y publicar frecuentemente datos sobre el volumen y la naturaleza de las acciones tomadas para **restringir contenido** que viole las reglas de la empresa.

Elementos:

1. ¿La empresa publica datos sobre cuánto **contenido** **restringe** por haber violado las reglas de la empresa?

2. ¿La empresa publica datos de cuánto **contenido** **restringe** basándose en qué regla se haya violado?

3. ¿La empresa publica datos de cuánto **contenido** restringe basándose en el formato de contenido? (por ejemplo, texto, imagen, video, video en vivo)?

4. ¿La empresa publica datos de cuánto **contenido** ha **restringido** basándose en el método usado para identificar la violación?

5. ¿La empresa publica estos datos al menos cuatro veces al año?

6. ¿Los datos se pueden exportar como un archivo de **datos estructurados**?

Guía del indicador: Las empresas pueden y deben establecer reglas claras sobre qué tipos de contenido no están permitidos en sus plataformas o servicios. Este indicador tiene la

expectativa de que las empresas revelen públicamente datos sobre las acciones que toman para restringir o censurar contenido por violaciones a las reglas de la empresa. Publicar estos datos es un primer paso esencial para que las empresas se hagan responsables de aplicar sus propias reglas y por las acciones que toman para moderar contenido en sus plataformas y servicios.

Las empresas deben publicar datos sobre la cantidad agregada de contenido que restringe, retira o —en el caso de las empresas de telecomunicaciones — bloquea o filtra, como resultado de violaciones a los términos de servicio. También deben desglosar estos datos por violación y por método —como programa comunitario para señalizar contenido o automatización—a través de los cuales se detectó la violación a las reglas. Las empresas también deben publicar estos datos al menos cuatro veces al año, en línea con los Principios de Santa Clara, y en un archivo de datos estructurados.

Posibles fuentes:

- Informe de transparencia de la empresa
- Informe de aplicación de las reglas comunitarias de la empresa, informe de guías de aplicación de la comunidad, etc.

F4(b). Datos sobre restricciones de cuenta para aplicar términos de servicio

La empresa debe **revelar claramente** y publicar con frecuencia datos sobre el volumen y naturaleza de las acciones tomadas para **restringir cuentas** que violen las reglas de la empresa.

Elementos

1. ¿La empresa publica datos sobre el número total de **cuentas restringidas** por violar las reglas de la empresa?

2. ¿La empresa publica datos sobre la cantidad de **cuentas restringidas** basándose en qué regla se violó?

3. ¿La empresa publica datos sobre la cantidad de **cuentas restringidas** basándose en el método usado para identificar la violación?

4. ¿La empresa publica estos datos al menos cuatro veces al año?

5. ¿Los datos se pueden exportar como un archivo de **datos estructurados**?

Posibles fuentes:

- Informe de transparencia de la empresa

Guía del indicador: Las empresas pueden y deben establecer reglas claras sobre qué tipos de contenido o actividades no están permitidos en sus plataformas o servicios. Este indicador tiene la expectativa de que las empresas revelen públicamente datos sobre las acciones que toman para aplicar estas reglas. Publicar estos datos es un primer paso esencial para que las empresas se hagan responsables de aplicar sus propias reglas y por las acciones que toman para moderar contenido en sus plataformas y servicios.

Las empresas deben publicar datos sobre la cantidad de cuentas que restringen como resultado de violaciones a sus términos de servicio. También deben desglosar estos datos de acuerdo con la violación y de acuerdo con el método —tales como programa comunitario para señalizar contenido o automatización— a través de los cuales se detectó la violación a las reglas. Las empresas también deben publicar estos datos al menos cuatro veces al año, en línea con los Principios de Santa Clara, y en un archivo de datos estructurados.

Posibles fuentes:

- Informe de transparencia de la empresa

F4(c). Datos sobre contenido publicitario y aplicación de políticas de publicidad dirigida

La empresa debe **revelar claramente** y publicar frecuentemente datos sobre el volumen y naturaleza de acciones tomadas para **restringir contenido publicitario** que viole las **políticas de contenido publicitario** de la empresa y las **políticas de publicidad dirigida**.

Elementos

1. ¿La empresa publica la cantidad total de **anuncios publicitarios** que **restringió** para aplicar sus **políticas de contenido publicitario**?

2. ¿La empresa publica la cantidad de **anuncios publicitarios** que **restringió** basándose en qué regla de **contenido publicitario** se violó?

3. ¿La empresa publica el número total de **anuncios publicitarios** que **restringió** para aplicar sus **políticas de publicidad dirigida**?

4. ¿La empresa publica la cantidad de **anuncios publicitarios** que **restringió** basándose en qué regla de **publicidad dirigida** se violó?

5. ¿La empresa publica estos datos al menos una vez al año?

6. ¿Los datos se pueden exportar como un archivo de **datos estructurados**?

Guía del indicador: Los indicadores F3(c) y F3(d) piden a las empresas que revelen claramente reglas sobre qué tipo de contenido publicitario y de orientación de publicidad está prohibido, respectivamente, y que describan sus procesos para aplicar estas reglas.

Este indicador, F4(c), pide a las empresas que publiquen evidencia de que están aplicando estas reglas. Las empresas deben publicar datos sobre el número total de anuncios publicitarios que elimina como resultado de violaciones a las políticas de contenido publicitario, y también deben desglosar estos datos de acuerdo con la regla que se haya violado. Las empresas también deben brindar evidencia de que están aplicando sus políticas de orientación de publicidad por medio de la publicación de datos sobre cuántos anuncios publicitarios eliminaron por violar las reglas de selección de sujetos, y qué regla se violó. Las empresas también deben publicar estos datos al menos una vez al año en un archivo de datos estructurados.

Posibles fuentes:

- Informe de transparencia de la empresa

F5. Proceso para responder a solicitudes de terceros de restringir contenido o cuentas

F5(a). Proceso para responder a solicitudes gubernamentales

La empresa debe **revelar claramente** su proceso para responder a **solicitudes gubernamentales** (incluidas órdenes judiciales) para eliminar, filtrar o restringir **contenido** o **cuentas**.

Elementos:

1. ¿La empresa **revela claramente** su proceso para responder **solicitudes gubernamentales no judiciales**?
2. ¿La empresa **revela claramente** su proceso para responder **órdenes judiciales**?
3. ¿La empresa **revela claramente** su proceso para responder **solicitudes gubernamentales** de jurisdicciones extranjeras?
4. ¿Las explicaciones de la empresa **revelan claramente** la base legal bajo la cual cumpliría con **solicitudes gubernamentales**?
5. ¿La empresa **revela claramente** que realiza revisión exhaustiva con las **solicitudes gubernamentales** antes de decidir cómo responder?
6. ¿La empresa se compromete a desestimar las **solicitudes gubernamentales** inapropiadas o demasiado generales?
7. ¿La empresa brinda una guía o ejemplos claros de implementación de su proceso de respuesta a **solicitudes gubernamentales**?

Guía del indicador: Con frecuencia, las empresas reciben solicitudes de Gobiernos de eliminar, filtrar o restringir acceso a contenido y cuentas. Estas solicitudes pueden venir de agencias gubernamentales, autoridades y cortes (nacionales y extranjeras). Nuestra expectativa es que las empresas revelen públicamente sus procesos para responder este

tipo de solicitudes. Las empresas deben revelar las razones legales por las que cumplirían con una orden gubernamental, y también revelar un compromiso claro de desestimar solicitudes demasiado generales.

Nótese que nuestra definición de "solicitudes gubernamentales" incluye las que llegan a través de un proceso "no judicial", como órdenes de aplicación de las autoridades, y de casos civiles interpuestos por privados a través de cortes civiles. Las solicitudes de retiro de contenido realizadas a través de procesos organizados como la Ley de Derechos de Autor de la Era Digital de Estados Unidos y la disposición europea del Derecho al Olvido están definidas como "procesos privados" y se evalúan en el Indicador F5(b), más abajo.

Posibles fuentes:

- Informe de transparencia de la empresa
- Guía de aplicación de la ley de la empresa
- Informes anuales de la empresa

F5(b). Proceso para responder a solicitudes privadas

La empresa debe **revelar claramente** su proceso para responder a **solicitudes** para eliminar, filtrar o restringir **contenido** o **cuentas** que llegan por medio de **procesos privados**.

Elementos:

1. ¿La empresa **revela claramente** su proceso para responder **solicitudes** para eliminar, filtrar o restringir **contenido** o **cuentas** hechas a través de **procesos privados**?

2. ¿Las explicaciones de la empresa **revelan claramente** la base bajo la cual pueden cumplir con las **solicitudes** hechas a través de **procesos privados**?

3. ¿La empresa **revela claramente** que ejecuta con revisión exhaustiva las **solicitudes** hechas a través de **procesos privados** antes de decidir cómo responder?

4. ¿La empresa se compromete a desestimar **solicitudes** inapropiadas o demasiado generales hechas a través de **procesos privados**?

5. ¿La empresa brinda guías o ejemplos claros de implementación de sus procesos de respuesta a **solicitudes** hechas a través de **procesos privados**?

Guía del indicador: Además de las solicitudes de Gobiernos y otro tipo de autoridades, las empresas pueden recibir solicitudes de eliminar o restringir acceso a contenido y cuentas a través de procesos privados. Este tipo de solicitudes puede llegar a través de procesos formales establecidos por ley (por ejemplo, solicitudes hechas de acuerdo con la Ley de Derechos de Autor de la Era Digital de Estados Unidos, la disposición europea del Derecho al Olvido, etc.) o por acuerdos autorregulados (por ejemplo, acuerdos de la empresa para bloquear algunos tipos de materiales o imágenes, como a través del Código de Conducta

sobre Desinformación de la Unión Europea). Nótese que este indicador no contempla que las solicitudes privadas sean solicitudes hechas a través de ningún proceso judicial, que están consideradas como solicitudes "gubernamentales" (Indicador F5a).

Este indicador evalúa si la empresa revela claramente cómo responde a solicitudes de eliminación, filtración o restricción de contenido o cuentas hechas a través de estos tipos de procesos privados (Elemento 1). La empresa debe revelar la base para cumplir con este tipo de solicitudes (Elemento 2), y si se conduce con la revisión exhaustiva en estas solicitudes antes de decidir cómo responder (Elemento 3). También tenemos la expectativa de que las empresas se comprometan a desestimar solicitudes demasiado generales para eliminar contenido o cuentas hechas a través de procesos privados (Elemento 4), y a publicar ejemplos claros que ilustren cómo una empresa gestiona este tipo de solicitudes (Elemento 5).

Posibles fuentes:

- Informe de transparencia de la empresa
- Centro de ayuda o de asistencia de la empresa
- Publicaciones en el blog de la empresa
- Política de la empresa sobre derecho de autor y propiedad intelectual

F6. Datos sobre solicitudes gubernamentales para restringir contenido y cuentas

La empresa debe publicar frecuentemente datos sobre **solicitudes gubernamentales** (incluidas órdenes judiciales) para eliminar, filtrar o restringir **contenido** y **cuentas**.

Elementos:

1. ¿La empresa desglosa la cantidad de **solicitudes** que recibe por país?
2. ¿La empresa enumera la cantidad de **cuentas** afectadas?
3. ¿La empresa enumera cuánto **contenido** o la cantidad de URL afectadas?
4. ¿La empresa enumera los tipos de asunto asociados con los **solicitudes** que recibe?
5. ¿La empresa enumera la cantidad de **solicitudes** que llegan de diferentes autoridades legales?
6. ¿La empresa enumera la cantidad de **solicitudes** que recibe a sabiendas de funcionarios gubernamentales de restringir **contenido** o **cuentas** a través de **procesos no oficiales**?
7. ¿La empresa enumera la cantidad de **solicitudes** que ha cumplido?

8. ¿La empresa publica las **solicitudes** originales o revela que brinda copias al **archivo público de terceros**?

9. ¿La empresa publica estos datos al menos una vez al año?

10. ¿Los datos se pueden exportar como un archivo de **datos estructurados**?

Guía del indicador: Con frecuencia, las empresas reciben solicitudes de Gobiernos de eliminar, filtrar o restringir contenido o cuentas. Nuestra expectativa es que las empresas publiquen frecuentemente datos sobre el número y tipo de solicitudes gubernamentales que recibe, y la cantidad de esas solicitudes con las que cumple. Las empresas pueden recibir estas solicitudes a través de procesos oficiales, como una orden judicial, o a través de canales informales, como el sistema de una empresa para señalizar contenido con la finalidad de permitir que privados denuncien cualquier contenido que viole los términos de servicio. Las empresas deben ser transparentes sobre la naturaleza de estas solicitudes. Si una empresa sabe que viene una solicitud de una entidad gubernamental o una corte, la empresa debe revelarlo como parte de sus informes de solicitudes gubernamentales. Revelar estos datos ayudan al público a tener una mejor comprensión de las relaciones entre empresas y Gobiernos para vigilar contenido en línea, y ayuda al público a responsabilizar a empresas y Gobiernos por sus obligaciones de respetar y proteger los derechos de libertad de expresión.

En algunos casos, la ley puede evitar que una empresa revele información mencionada en los elementos de este indicador. Por ejemplo, tenemos la expectativa de que las empresas publiquen números exactos en vez de rangos de números. Reconocemos que a veces las leyes evitan que las empresas actúen así, y los investigadores documentarán situaciones en que ese sea el caso. Sin embargo, una empresa perderá puntos si no logra cumplir con los parámetros en todos los elementos mencionados arriba. Esto representa una situación en que la ley causa que las empresas no cumplan con las mejores prácticas, y alentamos a las empresas a defender leyes que les permitan respetar totalmente los derechos de libertad de expresión y de privacidad de los usuarios.

Posibles fuentes:

- Informe de transparencia de la empresa

F7. Datos sobre solicitudes privadas para restringir contenido o cuentas

La empresa debe publicar frecuentemente datos sobre solicitudes para eliminar, filtrar o restringir acceso a **contenido** o **cuentas** que lleguen a través de **procesos privados**.

Elementos:

1. ¿La empresa desglosa la cantidad de solicitudes para restringir **contenido** o **cuentas** que recibe a través de **procesos privados**?

2. ¿La empresa enumera la cantidad de **cuentas** afectadas?

3. ¿La empresa enumera cuánto **contenido** o URL se ve afectado?

4. ¿La empresa enumera las razones de eliminación asociadas con las solicitudes que recibe?

5. ¿La empresa **revela claramente** los **procesos privados** que hicieron solicitudes?

6. ¿La empresa enumera con cuántas solicitudes cumple?

7. ¿La empresa publica las solicitudes originales o revela que brinda copias al **archivo público de un tercero**?

8. ¿La empresa publica estos datos al menos una vez al año?

9. ¿Los datos se pueden exportar como un archivo de **datos estructurados**?

10. ¿La empresa **revela claramente** que sus informes abarcan todo tipo de solicitudes que recibe a través de **procesos privados**?

Guía del indicador: Las empresas reciben frecuentemente solicitudes para eliminar, filtrar o restringir contenido o cuentas a través de procesos privados, como solicitudes hechas de acuerdo con la Ley de Derechos de Autor de la Era Digital de Estados Unidos, la disposición europea del Derecho al Olvido, etc. o a través de acuerdos autorregulados (por ejemplo, acuerdos de la empresa para bloquear algunos tipos de imágenes). Tenemos la expectativa de que las empresas publiquen frecuentemente datos sobre el número y tipo de solicitudes recibidas a través de estos procesos privados, y la cantidad de esas solicitudes con las que cumple.

Posibles fuentes:
- Informe de transparencia de la empresa

F8. Notificación al usuario sobre restricciones de contenido y cuenta

La empresa debe **revelar claramente** que **notifica** a los **usuarios** cuando restringe **contenido** o **cuentas**.

Elementos:

1. Si la empresa aloja **contenido** generado por el usuario, ¿la empresa **revela claramente** que notifica a los **usuarios** que generaron el **contenido** cuando lo restringe?

2. ¿La empresa **revela claramente** que notifica a los usuarios que intentan acceder a **contenido** que ha sido restringido?

3. ¿En su notificación, la empresa **revela claramente** una razón para la **restricción de contenido** (legal o de otra manera)?

4. ¿La empresa **revela claramente** que notifica a los usuarios cuando restringe su **cuenta**?

Guía del indicador: El indicador F3 examina la revelación de la empresa de restricciones sobre qué pueden publicar o hacer los usuarios en un servicio. Este indicador, F8, se centra en si la empresa revela claramente que notifica a los usuarios cuando toma este tipo de acciones (ya sea por aplicación de sus términos de servicio o por solicitudes de restricción de terceros). La decisión de una empresa de restringir o eliminar acceso a contenido o cuentas puede tener un impacto significativo en el derecho a la libertad de expresión y acceso a información de los usuarios. Por lo tanto, tenemos la expectativa de que una empresa revele que notifica a los usuarios cuando elimine contenido, restringe la cuenta de un usuario o restringe la capacidad de los usuarios para acceder a un servicio. Si una empresa elimina contenido que un usuario ha publicado, tenemos la expectativa de que la empresa informe a ese usuario sobre la decisión. Si otro usuario intenta acceder a contenido que la empresa ha restringido, tenemos la expectativa de que la empresa notifique a ese usuario sobre la restricción de contenido. También tenemos la expectativa de que las empresas especifiquen razones para sus decisiones. Esta revelación debe ser parte de las explicaciones de las empresas de sus prácticas de restricción a contenido y acceso.

Posibles fuentes:

- Términos de servicio de la empresa, políticas de uso que sean aceptables
- Normas comunitarias de la empresa
- Página de asistencia, centro de ayuda o preguntas frecuentes de la empresa
- Guías de la empresa para programadores
- Políticas de derechos humanos de la empresa

F9. Gestión de red (empresas de telecomunicaciones)

La empresa debe **revelar claramente** que no **prioriza**, bloquea ni retrasa algunos tipos de tráfico, **aplicaciones**, **protocolos** o **contenido** por ninguna razón que vaya más allá de asegurar la calidad del servicio y la confiabilidad de la red.

Elementos:

1. ¿La empresa **revela claramente** un **compromiso de políticas** de que no **prioriza**, bloquea ni retrasa algunos tipos de tráfico, **aplicaciones**, **protocolos** o **contenido** por razones más allá de garantizar la calidad de servicio y confiabilidad de la red?

2. ¿La empresa interviene en prácticas, como brindar **programas de calificación cero**, que **priorizan** el tráfico de red por razones que van más allá de garantizar la calidad de servicio y confiabilidad de la red?

3. Si la empresa interviene en prácticas de **priorización** de la red por razones que van más allá de garantizar la calidad del servicio y confiabilidad de la red, ¿**revela claramente** su objetivo de hacerlo?

Guía del indicador: Este indicador evalúa si las empresas de telecomunicaciones revelan claramente si realizan prácticas que afectan el flujo de contenido a través de sus redes, como ahogar o dar forma al tráfico. Tenemos la expectativa de que estas empresas se comprometan públicamente a evitar priorización o degradación del contenido. En algunos casos, una empresa puede realizar prácticas legítimas de dar forma al tráfico para garantizar el flujo de tráfico a través de sus redes. Tenemos la expectativa de que la empresa lo revele públicamente y que explique su objetivo de hacerlo. Las empresas pueden realizar priorización pagada o prácticas de calificación cero, lo que no entraría en prácticas ilegítimas de gestión de redes. Una empresa puede tener una declaración en su sitio web de que se compromete a neutralidad de la red, por ejemplo, pero también ofrecer un cero como calificación.

Posibles fuentes:
- Gestión de red de la empresa o políticas de gestión de tráfico
- Informes anuales de la empresa

F10. Cierre de la red (empresas de telecomunicaciones)

La empresa debe **revelar claramente** las circunstancias bajo las cuales **cierra o restringe acceso a la red** o acceso a **protocolos**, servicios o **aplicaciones** específicos en la red.

Elementos:

1. ¿La empresa **revela claramente** la razón o razones por las que puede cerrar el servicio a una zona o grupo de usuarios en particular?

2. ¿La empresa **revela claramente** por qué podría restringir el acceso a **aplicaciones** o **protocolos** específicos (por ejemplo, VoIP, mensajería) en una zona o grupo de usuarios en particular?

3. ¿La empresa **revela claramente** su proceso para responder a **solicitudes gubernamentales** de **cerrar una red o restringir acceso a un servicio**?

4. ¿La empresa **revela claramente** un compromiso de desestimar **solicitudes gubernamentales** de **cerrar una red o restringir acceso a un servicio**?

5. ¿La empresa **revela claramente** que notifica directamente a los usuarios cuando **cierra una red o restringe acceso a un servicio**?

6. ¿La empresa **revela claramente** la cantidad de **solicitudes** de **cierres de red** que recibe?

7. ¿La empresa **revela claramente** la autoridad legal específica que hace las **solicitudes**?

8. ¿La empresa **revela claramente** la cantidad de **solicitudes gubernamentales** con las que ha cumplido?

Guía del indicador: El cierre de las redes es una amenaza creciente a los derechos humanos. El Consejo de Derechos Humanos de Naciones Unidas ha condenado los cierres de red como una violación de derechos humanos internacionales y pidió a los Gobiernos que se abstuvieran de tomar estas acciones.[23] Pero cada vez más, los Gobiernos están ordenando a las empresas de telecomunicaciones que cierren sus redes,[24] lo que a su vez pone presión a las empresas a tomar acciones que violen su responsabilidad de respetar los derechos humanos. Tenemos la expectativa de que las empresas revelen totalmente las circunstancias bajo las cuales toman tal acción, que denuncien las solicitudes que reciben para tomar esas acciones, y que revelen compromisos de desestimar o mitigar los efectos de las órdenes gubernamentales.

Posibles fuentes:
- Términos de servicio de la empresa
- Informe de transparencia de la empresa
- Guías de aplicación de la ley de las empresas
- Políticas de derechos humanos de la empresa

F11. Políticas de identidad

La empresa no debe **solicitar** a los usuarios que confirmen su identidad con su **documento de identificación oficial** ni otras formas de identificación que podrían estar conectadas con su identidad fuera de línea.

1. ¿La empresa **pide** a los usuarios que confirmen su identidad con su **documento de identificación oficial** o con otras formas de identificación que podrían estar conectadas con su identidad fuera de línea?

Guía del indicador: La capacidad de comunicarse anónimamente es esencial para la libertad de expresión en línea y fuera de línea. Usar el nombre verdadero en línea o solicitar a los usuarios que proporcionen a la empresa información que los pueda identificar facilita un vínculo entre las actividades en línea y una persona específica. Esto presenta riesgos a los derechos humanos para quienes, por ejemplo, expresan opiniones que no sean iguales a las opiniones de un Gobierno o que participan en activismo que un Gobierno no permite. También presenta riesgos para las personas perseguidas por creencias religiosas u orientación sexual.

---

[23] "Promoción, protección y disfrute de derechos humanos en internet", Consejo de Naciones *Undas* (32° sesión) 27 de junio de 2016: https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement.

[24] "#KeepItOn", *Access Now,* https://www.accessnow.org/keepiton/, ultimo acceso 2 de abril de 2020.

Por lo tanto, tenemos la expectativa de que las empresas revelen si piden a los usuarios que confirmen su identidad con sus identificaciones oficiales u otras formas de identificación que pueden estar conectadas con su identidad fuera de línea. Otras formas de identificación pueden incluir tarjetas de crédito y números de teléfono registrados. Reconocemos que los usuarios tal vez deban ofrecer información que podría estar conectada con su identidad fuera de línea para poder acceder a funciones pagadas de diversos productos y servicios. Sin embargo, los usuarios deben poder acceder a funciones que no pidan un pago sin necesidad de brindar información que pueda estar vinculada con su identidad fuera de línea. En algunos casos, los números de teléfono pueden estar vinculados a la identidad fuera de línea de un usuario, por ejemplo, en contextos legales en que los usuarios de prepago deban registrarse con su identificación. Cuando proporcionar un número de teléfono sea necesario para contar con el servicio (por ejemplo, en el caso de aplicaciones de mensajería instantánea), las empresas deben recibir crédito total, a menos que pidan a los usuarios que utilicen sus nombres reales o presenten documentos que vincularían su nombre a su identidad fuera de línea. Los servicios que pidan a los usuarios proporcionar un número de teléfono para fines que no son necesarios para brindar el servicio no recibirán crédito: por ejemplo, algunos servicios pueden solicitar números de teléfono con fines de realizar autenticación de dos pasos. Sin embargo, esto debe ser optativo, y a los usuarios se les debe ofrecer otras opciones de autenticación de dos pasos.

Este indicador es aplicable a empresas de plataformas digitales y servicios móviles prepago (para empresas de telecomunicaciones).

Posibles fuentes:

- Términos de servicio de la empresa o documento equivalente
- Centro de ayuda de la empresa
- Página de inscripción de una empresa

F12. Sistemas algorítmicos de clasificación, recomendación y clasificación de contenido

Las empresas deben **revelar claramente** cómo se **clasifica, califica o recomienda** el **contenido** en línea de los usuarios.

Elementos:

1. ¿La empresa **revela claramente** si usa **sistemas algorítmicos** para **clasificar, recomendar o calificar** el **contenido** al que los **usuarios** pueden acceder a través de su plataforma?

2. ¿La empresa **revela claramente** cómo implementa los **sistemas algorítmicos** para **clasificar, recomendar o calificar** **contenido**, incluidas las variables que influyen en estos sistemas?

3. ¿La empresa **revela claramente** qué opciones tienen los usuarios para controlar las variables que toman en **cuenta** los **sistemas algorítmicos de conservación, recomendación o calificación de contenido**?

4. ¿La empresa **revela claramente** si los **sistemas algorítmicos** se usan para **conservar, recomendar o calificar contenido** automáticamente por defecto?

5. ¿La empresa **revela claramente** que los usuarios pueden elegir usar **sistemas automatizados de conservación, recomendación o calificación de contenidos**?

Guía del indicador: Los sistemas algorítmicos de conservación, recomendación y calificación de contenido tienen un rol crítico en dar forma a qué contenido e información pueden ver y acceder los usuarios en línea. Además, los sistemas que están optimizados de acuerdo con la participación del usuario pueden tener el efecto de priorizar contenido controvertido y provocador, incluyendo contenido que no esté protegido por derechos humanos internacionales. Con el tiempo, depender de sistemas algorítmicos de conservación y recomendación optimizados de acuerdo con la participación puede alterar los ecosistemas de noticias e información de países o comunidades enteras. Estos sistemas pueden manipularse para propagar desinformación o distorsionar el ecosistema de información, que a su vez puede generar abusos de los derechos humanos.

Por lo tanto, las empresas deben ser transparentes sobre su uso de sistemas automatizados de conservación, recomendación y calificación, incluidas las variables que influyen en esos sistemas. Las empresas deben publicar información sobre si usan sistemas algorítmicos para conservar, recomendar y calificar contenido. También deben revelar cómo funcionan estos sistemas, qué opciones tienen los usuarios para controlar cómo estos sistemas usan su información, si es que esos sistemas están puestos automáticamente por defecto, o si los usuarios pueden "elegir usar" que el sistema algorítmico conserve automáticamente su contenido.

Posibles fuentes:

- Políticas de derechos humanos de la empresa
- Políticas de inteligencia artificial de la empresa, incluidos principios, marco y guía de uso de inteligencia artificial
- Páginas de ayuda que describan cómo las configuraciones de ajustes, las configuraciones de páginas de inicio, resultados de búsqueda, recomendaciones, intereses del usuario o temas se ven afectados por algoritmos

F13. Agentes de software automatizado ("bots")

Las empresas deben **revelar claramente** las políticas que rigen el uso de **agentes de software automatizado ("bots")** en sus plataformas, productos y servicios, y cómo aplican esas políticas.

Elementos:

1. ¿La empresa **revela claramente** las reglas que rigen el uso de **bots** en su plataforma?

2. ¿La empresa **revela claramente** que pide a los **usuarios** que etiqueten claramente todo el **contenido** y **cuentas** que se produzcan, difundan o funcionen con la asistencia de un **bot**?

3. ¿La empresa **revela claramente** sus procesos para aplicar sus **políticas de bots**?

4. ¿La empresa **revela claramente** datos sobre el volumen y naturaleza de **contenido** del usuario y **cuentas restringidas** por violar las **políticas de bots** de la empresa?

Guía del indicador: Las plataformas de medios sociales suelen permitir a los usuarios crear agentes de software automatizado, o "bots", que automatizan diversas acciones que la cuenta de un usuario puede tomar, como publicar o impulsar contenido (retuitear, por ejemplo). Hay muchos usos de bots inocuos y hasta positivos, por ejemplo, los artistas usan bots de Twitter con el fin de hacer parodia.[25] También hay usos más problemáticos que muchas empresas prohíben o no recomiendan, como cuando los partidos políticos o sus suplentes usan botnets para promocionar algunos mensajes o inflar artificialmente el alcance de un candidato para manipular el discurso público y los resultados. En algunas plataformas de medios sociales, se pueden usar bots o redes de bots coordinadas ("botnets") para acosar a los usuarios ("brigadas"), ampliar artificialmente contenido (retuiteo masivo, etc), y distorsionar el discurso público en la plataforma. Algunos expertos han solicitado que las empresas pidan a quienes usan bots que los etiqueten explícitamente como bots, con la finalidad de ayudar a detectar esas distorsiones.[26]

Por lo tanto, las empresas que permiten bots deben tener políticas claras que rijan el uso de bots en sus plataformas. Deben revelar si es que piden que se etiqueten como tal el contenido y cuentas que se producen, difunden o funcionan con asistencia de un bot. También deben aclarar su proceso para aplicar sus políticas de bots, y hasta publicar datos sobre el volumen y naturaleza de contenido y cuentas que están restringidos por violar estas reglas.

Posibles fuentes:

- Políticas de plataforma para programadores
- Reglas de automatización o bots
- Informes de transparencia

---

[25] *Thinkpiece Bot*, Twitter, https://twitter.com/thinkpiecebot, ultimo acceso, 2 de abril de 2020.

[26] Engler, A. (22 de enero de 2020): El caso sobre los requisitos de transparencia de la inteligencia artificial. Brookings Institution https://www.brookings.edu/research/the-case-for-ai-transparency-requirements/, último acceso, 2 de abril de 2020.

Privacidad

Los indicadores en esta categoría buscan que haya evidencia de que, en sus políticas y prácticas reveladas, la empresa demuestra maneras concretas de que respeta el derecho a la privacidad de los usuarios, como se articula en la Declaración Universal de Derechos Humanos,[27] el Pacto Internacional de Derechos Civiles y Políticos,[28] y otros instrumentos de derechos humanos internacionales. Las políticas y prácticas reveladas de la empresa demuestran cómo trabaja para evitar contribuir con acciones que pueden interferir con la privacidad de los usuarios, salvo cuando esas acciones sean legítimas, proporcionadas o por un objetivo justificable. También demostrarán un fuerte compromiso para proteger y defender la seguridad digital de los usuarios. Las empresas que se desempeñan bien en estos indicadores demuestran un fuerte compromiso público con la transparencia, no solamente en términos de cómo responden a solicitudes gubernamentales y otros, sino también de cómo determinan, comunican y aplican reglas privadas y prácticas comerciales que afectan la privacidad de los usuarios.

P1. Acceso a las políticas que afectan la privacidad de los usuarios

P1(a). Acceso a las políticas de privacidad

La empresa debe ofrecer **políticas de privacidad** que sean **fáciles de encontrar** y **fáciles de comprender**.

Elementos:

1. ¿Las **políticas de privacidad** de la empresa son **fáciles de encontrar**?
2. ¿Las **políticas de privacidad** están disponibles en el idioma principal que hablan los usuarios en la jurisdicción de la empresa?
3. ¿Las políticas están presentadas de **manera comprensible**?
4. (Para **ecosistemas móviles**): ¿La empresa revela que solicita que los **aplicaciones** disponibles a través de su **tienda de aplicaciones** brinden a los **usuarios** la **política de privacidad**?
5. (Para **ecosistemas de asistente digital personal**): ¿La empresa revela que solicita que las **habilidades** disponibles a través de su **tienda de habilidades** brinden a los **usuarios** la **política de privacidad**?

[27] "Declaración Universal de Derechos Humanos", *Naciones Unidas*, https://www.un.org/es/universal-declaración-human-rights/index.html/, último acceso, 2 de abril de 2020.
[28] "Pacto Internacional de Derechos Civiles y Políticos", Oficina del Alto Comisionado de Derechos Humanos de Naciones Unidas: https://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx, último acceso 2 de abril de 2020.

Guía del indicador: Las políticas de privacidad abordan cómo las empresas recopilan, gestionan, usan y aseguran la información sobre los usuarios al igual que información brindada por los usuarios. Teniendo esto en cuenta, las empresas deben asegurar que los usuarios puedan ubicar fácilmente estas políticas y hacer un esfuerzo para ayudar a los usuarios a comprender qué significan. Este indicador tiene la expectativa de que las empresas publiquen políticas de privacidad que sean fáciles de encontrar, estén disponibles en los principales idiomas que se hablan en el mercado local de la empresa, y que sean fáciles de comprender. Si la empresa ofrece múltiples productos y servicios, debe estar claro a qué productos y servicios se aplican las políticas de privacidad.

Un documento que sea "fácil de encontrar" debe estar accesible en la página de inicio del sitio web de la empresa o servicio. Debe estar a uno o dos clics de la página de inicio o en un lugar lógico en el que los usuarios pueden esperar encontrarlo. Los términos también deben estar disponibles en el idioma o idiomas principales del mercado local. Además, tenemos la expectativa de que una empresa tome medidas para ayudar a los usuarios a comprender la información presentada en sus políticas. Esto incluye, sin limitarse, a ofrecer resúmenes, consejos o pautas que expliquen qué significan los términos, con encabezados, tamaño de fuente legible u otras características gráficas que ayuden a los usuarios a entender el documento, o escribir los términos con sintaxis fácilmente legible.

Posibles fuentes:
- Políticas de privacidad de la empresa
- Políticas de uso de datos de la empresa

P1(b). Acceso a las políticas de elaboración de los sistemas algorítmicos

La empresa debe ofrecer las **políticas de elaboración de los sistemas algorítmicos** de manera que sean **fáciles de encontrar** y **fáciles de comprender**.

Elementos:

1. ¿Las **políticas de elaboración de los sistemas algorítmicos** de la empresa son **fáciles de encontrar**?

2. ¿Las **políticas de elaboración de los sistemas algorítmicos** están disponibles en los principales idiomas que hablan los usuarios?

3. ¿Las **políticas de elaboración de los sistemas algorítmicos** están presentadas de **manera comprensible**?

Guía del indicador: La elaboración y prueba de los sistemas algorítmicos pueden plantear riesgos a la privacidad, sobre todo cuando las empresas luego usan la información recopilada sobre los usuarios para elaborar, entrenar y probar estos sistemas sin el

consentimiento informado del sujeto interesado.[29] Las empresas deben revelar claramente las políticas que describen la elaboración y pruebas de los sistemas algorítmicos de una manera que los usuarios puedan acceder, leer y comprender, para que los usuarios puedan tomar decisiones informadas sobre si usar los productos y servicios de una empresa.

Posibles fuentes:

- Políticas de uso de sistemas algorítmicos
- Guías para elaborar sistemas algorítmicos
- Políticas de privacidad o políticas de datos

P2. Notificación de cambios

P2(a). Cambios a las políticas de privacidad

La empresa debe **revelar claramente** que **notifica directamente** a los usuarios cuando cambie sus **políticas de privacidad**, antes de que estos cambios estén vigentes.

Elementos:

1. ¿La empresa **revela claramente** que **notifica directamente** a los **usuarios** sobre todos los cambios a sus **políticas de privacidad**?

2. ¿La empresa **revela claramente** cómo **notificará directamente** a los **usuarios** de los cambios?

3. ¿La empresa **revela claramente** el plazo en el cual **notifica directamente** a los **usuarios** de los cambios antes de que estén vigentes?

4. ¿La empresa tiene un **archivo público** o **registro de cambios**?

5. (Para **ecosistemas móviles**): ¿La empresa **revela claramente** que solicita que las aplicaciones vendidos a través de su **tienda de aplicaciones** notifiquen a los **usuarios** cuando la aplicación cambie su **política de privacidad**?

6. (Para **ecosistemas de asistente digital personal**): ¿La empresa **revela claramente** que solicita que las **habilidades** disponibles en su **tienda de habilidades** notifiquen a los **usuarios** cuando la **habilidad** cambie su **política de privacidad**?

[29] Zuboff, S. (2019). La era del capitalismo de la vigilancia: La lucha por un futuro humano en las nuevas fronteras del poder, Nueva York, NY, Estados Unidos, PublicAffairs; Nathalie Maréchal. La publicidad dirigida esta arruinando internet y destrozando el mundo, https://www.vice.com/en_us/article/xwjden/targeted-advertising-is-ruining-the-internet-and-breaking-the-world, *Vice Motherboard,* 16 de noviembre de 2018; "Escenarios de riesgos de derechos humanos: Algoritmos, aprendizaje automático y toma de decisiones automatizada", *Ranking Digital Rights*, julio de 2019: https://rankingdigitalrights.org/wp-content/uploads/2019/07/Human-Rights-Risk-Scenarios_-algorithms-machine-learning-automated-decision-making.pdf..

Guía del indicador: Las empresas cambian frecuentemente sus políticas de privacidad a medida que sus negocios evolucionan. Sin embargo, estos cambios pueden afectar los derechos de privacidad del usuario al cambiar qué información del usuario las empresas pueden recopilar, compartir y almacenar. Por lo tanto, tenemos la expectativa de que las empresas se comprometan a notificar a los usuarios cuando cambien estas políticas y de brindar a los usuarios información para ayudarlos a comprender qué significan estos cambios.

Este indicador busca que haya una revelación clara de parte de las empresas sobre su método y plazo para notificar a los usuarios sobre cambios a las políticas de privacidad. Tenemos la expectativa de que las empresas se comprometan *directamente* a notificar a los usuarios antes de que los cambios estén vigentes. El método de notificación directa puede variar basándose en el tipo de servicio. Para los servicios que requieran una cuenta de usuario, la notificación directa puede involucrar el envío de un correo electrónico o un mensaje de texto. Para servicios que no requieran una cuenta de usuario, la notificación directa puede incluir la publicación de una notificación destacada en el lugar donde los usuarios acceden a ese servicio. Este indicador también busca evidencia de que una empresa dispone públicamente los registros de los términos anteriores para que las personas puedan entender cómo los términos de la empresa han evolucionado a lo largo del tiempo.

Posibles fuentes:

- Políticas de privacidad de la empresa
- Políticas de uso de datos de la empresa

P2(b). Cambios a las políticas de los sistemas algorítmicos

La empresa debe **revelar claramente** que **notifica directamente** a los **usuarios** cuando cambie sus **políticas de elaboración de los sistemas algorítmicos**, antes de que estos cambios estén vigentes.

Elementos:

1. ¿La empresa **revela claramente** que **notifica directamente** a los **usuarios** sobre todos los cambios a sus **políticas de elaboración de los sistemas algorítmicos**?

2. ¿La empresa **revela claramente** cómo **notificará directamente** a los **usuarios** de los cambios?

3. ¿La empresa **revela claramente** el plazo en el cual **notifica directamente** a los **usuarios** de los cambios antes de que estos cambios estén vigentes?

4. ¿La empresa tiene un **archivo público** o **registro de cambios**?

Guía del indicador: Las empresas pueden cambiar sus políticas de elaboración de los sistemas algorítmicos a medida que su negocio evoluciona. Sin embargo, estos cambios

pueden tener un impacto significativo en el derecho a la privacidad de los usuarios. Por lo tanto, tenemos la expectativa de que las empresas se comprometan a notificar a los usuarios cuando cambien estas políticas y a brindar a los usuarios información que les ayude a comprender qué significan estos cambios, tal como establece el Consejo de Europa en su *Recomendación sobre los impactos a los derechos humanos de los sistemas algorítmicos* (2020).

Este indicador busca que exista una revelación clara por parte de las empresas de su método y plazo para notificar a los usuarios sobre los cambios a las políticas de privacidad. Tenemos la expectativa de que las empresas se comprometan a notificar *directamente* a los usuarios antes de que los cambios estén vigentes. Este método de notificación directa puede variar basándose en el tipo de servicio. Para los servicios que requieran una cuenta de usuario, la notificación directa puede involucrar el envío de un correo electrónico o un mensaje de texto. Para los servicios que no requieran una cuenta de usuario, la notificación directa puede incluir la publicación de una notificación destacada en el lugar donde los usuarios acceden a ese servicio. Este indicador también busca evidencia de que una empresa dispone públicamente los registros de los términos anteriores para que las personas puedan entender cómo los términos de la empresa han evolucionado a lo largo del tiempo.

Posibles fuentes:

- Políticas de uso de algoritmos de la empresa
- Políticas de privacidad o políticas de datos

P3. Recopilación e inferencia de la información del usuario

P3(a). Recopilación de la información del usuario

La empresa debe **revelar claramente** qué **información del usuario recopila** y cómo.

Elementos:

1. ¿La empresa **revela claramente** qué tipos de **información del usuario recopila**?

2. Por cada tipo de **información del usuario** que la empresa **recopila**, ¿la empresa **revela claramente** cómo recopila esa información del usuario?

3. ¿La empresa **revela claramente** que **limita la recopilación** de **información del usuario** a lo que es directamente pertinente y necesario para lograr el objetivo de su servicio?

4. (Para **ecosistemas móviles**): ¿La empresa **revela claramente** que evalúa si las **políticas de privacidad** de **aplicaciones** de terceros disponibles a través de su **tienda de aplicaciones** revelan qué **información del usuario recopilan** las aplicaciones?

5. (Para **ecosistemas móviles**): ¿La empresa **revela claramente** que evalúa si los **aplicaciones** de terceros disponibles a través de su **tienda de aplicaciones limitan la recopilación** de **información del usuario** a lo que es directamente pertinente y necesario para lograr el objetivo de la aplicación?

6. (Para **ecosistemas de asistente digital personal**): ¿La empresa **revela claramente** que evalúa si las **políticas de privacidad** de las **habilidades** de terceros disponibles a través de su **tienda de habilidades** revela qué **información del usuario** las habilidades **recopilan**?

7. (Para **ecosistemas de asistente digital personal**): ¿La empresa **revela claramente** que evalúa si las **habilidades** de terceros disponibles a través de su **tienda de habilidades limita la recopilación** de **información del usuario** a lo que es directamente pertinente y necesario para lograr el objetivo de la habilidad?

Guía del indicador: Las empresas recopilan una amplia gama de información personal de los usuarios, desde detalles personales y perfiles de cuenta a actividades y ubicación del usuario. Tenemos la expectativa de que las empresas revelen claramente qué información del usuario recopilan y cómo la recopilan. También tenemos la expectativa de que las empresas se comprometan con el principio de minimización de datos y de demostrar cómo este principio da forma a sus prácticas referentes a información del usuario. Si las empresas recopilan múltiples tipos de información, tenemos la expectativa de que brinden detalles sobre cómo gestionan cada tipo de información. Para ecosistemas móviles y de asistente digital personal, tenemos la expectativa de que la empresa revele claramente si las políticas de privacidad de las aplicaciones o las habilidades de asistente digital personal disponibles en su tienda de aplicaciones móviles o tienda de habilidades del asistente digital personal especifican qué información del usuario recopilan las aplicaciones o habilidades y si esas políticas cumplen con principios de minimización de datos.

Posibles fuentes:
- Políticas de privacidad de la empresa
- Página web de la empresa o sección sobre protección de datos o recopilación de datos

P3(b). Inferencia de la información del usuario

La empresa debe **revelar claramente** qué **información del usuario infiere** y cómo.

Elementos:

1. ¿La empresa **revela claramente** todos los tipos de **información del usuario** que **infiere** basándose en **información recopilada del usuario**?

2. Por cada tipo de **información del usuario** que la empresa **infiere**, ¿la empresa **revela claramente** cómo **infiere** esa **información del usuario**?

3. ¿La empresa **revela claramente** que limita la **inferencia** de **información del usuario** a lo que es directamente pertinente y necesario para lograr el objetivo de su servicio?

Guía del indicador: Además de recopilar información sobre los usuarios, las empresas también aplican analíticas de grandes datos para hacer inferencias o predicciones sobre los usuarios basándose en la información recopilada. Estos métodos se pueden usar para hacer inferencias sobre preferencias o atributos de los usuarios (como raza, género, orientación sexual) y opiniones (incluidas opiniones políticas), o para predecir comportamientos del consumidor. Sin suficiente transparencia y control del usuario sobre su inferencia de datos, los usuarios no pueden predecir, comprender ni refutar las inferencias invasivas de la privacidad e inferencias no verificables.[30]

Además de revelar la información que recopilan, las empresas deben revelar qué información infieren y cómo la infieren. También deben comprometerse a inferir solamente información que sea pertinente y necesaria para brindar el servicio. Por ejemplo, las empresas no deben tratar de inferir la religión, orientación sexual ni condición de salud de los usuarios (como asignarles una categoría de audiencia basándose en esta característica) a menos que la información sea directamente necesaria de alguna manera para lograr el objetivo de su servicio.

Posibles fuentes:
- Políticas de privacidad y políticas de cookies de la empresa
- Página web de la empresa o sección sobre protección de datos o recopilación de datos

P4. Difusión de información del usuario

La empresa debe **revelar claramente** qué **información del usuario difunde** y a quién.

Elementos:

1. Por cada tipo de **información del usuario** que la empresa recopila, ¿la empresa **revela claramente** si **difunde** esa información del usuario?

2. Por cada tipo de **información del usuario** que la empresa **difunde**, ¿la empresa **revela claramente** los tipos de **terceros** a los cuales **difunde** esa información del usuario?

3. ¿La empresa **revela claramente** que puede **difundir información del usuario** a Gobierno(s) o autoridades legales?

[30] Para saber más, ver: Wachter, Sandra y Mittelstadt, Brent, Derecho a inferencias razonables: Repensando la ley de protección de datos en la era de los grandes datos y la inteligencia artificial (5 de octubre de 2018). Columbia Business Law Review, 2019(2), https://ssrn.com/abstract=3248829

4. Por cada tipo de **información del usuario** que la empresa **difunde**, ¿la empresa **revela claramente** los nombres de todos los **terceros** a los cuales **difunde** información del usuario?

5. (Para **ecosistemas móviles**): ¿La empresa **revela claramente** que evalúa si las **políticas de privacidad** de **aplicaciones** de **terceros** que están disponibles a través de su **tienda de aplicaciones** revelan qué **información del usuario difunden** las aplicaciones?

6. (Para **ecosistemas móviles**): ¿La empresa **revela claramente** que evalúa si las **políticas de privacidad** de **aplicaciones** de **terceros** disponibles a través de su **tienda de aplicaciones** revelan los tipos de **terceros** a quienes **difunde información del usuario**?

7. (Para **ecosistemas de asistente personal digital**): ¿La empresa **revela claramente** que evalúa si las **políticas de privacidad** de **habilidades** de **terceros** disponibles a través de su **tienda de habilidades** revela qué **información del usuario difunden** las habilidades?

8. (Para **ecosistemas de asistente digital personal**): ¿La empresa **revela claramente** que evalúa si las **políticas de privacidad** de **habilidades** de **terceros** disponibles a través de su **tienda de habilidades** revela los tipos de **terceros** a quienes **difunde información del usuario**?

Guía del indicador: Las empresas recopilan una amplia gama de información personal de los usuarios, desde nuestros detalles personales y perfiles de cuenta a nuestras actividades de navegación y ubicación. A menudo, las empresas también difunden esta información con terceros, incluidos anunciantes, Gobiernos y autoridades legales. Tenemos la expectativa de que las empresas revelen claramente qué información del usuario (como la define RDR) difunde y a quién se la difunde, Las empresas deben especificar si difunden información del usuario con Gobiernos y con entidades comerciales. Para ecosistemas móviles, tenemos la expectativa de que la empresa revele claramente si las políticas de privacidad de las aplicaciones disponibles en sus aplicaciones especifiquen qué información del usuario difunden las aplicaciones a terceros. Las empresas que operan ecosistemas de asistente digital personal deben solicitar que las habilidades de terceros disponibles en su tienda de habilidades revelen claramente qué tipos de información del usuario difunde, y los tipos de terceros a quienes la difunde.

Posibles fuentes:
- Políticas de privacidad de la empresa
- Políticas de la empresa relativas a difusión de datos, interacción con terceros

P5. Objetivo de recopilar, inferir y difundir información del usuario

La empresa debe **revelar claramente** por qué **recopila**, **infiere** y **difunde información del usuario**.

Elementos:

1. Por cada tipo de **información del usuario** que la empresa **recopila**, ¿la empresa **revela** claramente el objetivo de la **recopilación**?

2. Por cada tipo de **información del usuario** que la empresa **infiere**, ¿la empresa **revela claramente** el objetivo de la **inferencia**?

3. ¿La empresa **revela claramente** si combina **información del usuario** de diversos servicios de la empresa, y revela por qué lo hace, en el caso de que así sea?

4. Por cada tipo de **información del usuario** que la empresa **difunde**, ¿la empresa **revela claramente** su objetivo para **difundir**?

5. ¿La empresa **revela claramente** que limita su uso de **información del usuario** al objetivo por el cual fue **recopilada** o **inferida**?

Guía del indicador: Tenemos la expectativa de que las empresas revelen claramente el objetivo para recopilar, difundir e inferir cada tipo de información del usuario que recopila, difunde e infiere. Además, muchas empresas tienen u operan diversos productos y servicios, y tenemos la expectativa de que las empresas revelen claramente cómo se puede difundir o combinar la información del usuario entre servicios. Las empresas también deben comprometerse públicamente con el principio de la limitación de uso —es decir, deben declarar públicamente en sus políticas que solamente usan los datos para los objetivos para los que fue especificado— en línea con las guías de privacidad de la OECD, el Reglamento General de Protección de Datos y otros marcos de trabajo, para la información del usuario que recopilan y la que infieren.

Posibles fuentes:

- Políticas de privacidad de la empresa

P6. Retención de información del usuario

La empresa debe **revelar claramente** por cuánto tiempo **retiene** la **información del usuario**.

Elementos:

1. Por cada tipo de **información del usuario** que la empresa recopila, ¿la empresa **revela claramente** por cuánto tiempo **retiene** esa información del usuario?

2. ¿La empresa **revela claramente** qué **información anonimizada del usuario** retiene?

3. ¿La empresa **revela claramente** el proceso para **anonimizar** la **información del usuario**?

4. ¿La empresa **revela claramente** que elimina toda la **información del usuario** después de que los usuarios cancelan su cuenta?

5. ¿La empresa **revela claramente** el plazo en el cual elimina la **información del usuario** después de que los usuarios cancelan su cuenta?

6. (Para **ecosistemas móviles**): ¿La empresa **revela claramente** que evalúa si las **políticas de privacidad** de los **aplicaciones** de **terceros** disponibles a través de su **tienda de aplicaciones** revelan cuánto tiempo retienen la **información del usuario**?

7. (Para **ecosistemas móviles**): ¿La empresa **revela claramente** que evalúa si las **políticas de privacidad** de los **aplicaciones** de **terceros** disponibles a través de su **tienda de aplicaciones** declaran que toda la **información del usuario** es eliminada cuando los usuarios cancelan sus cuentas o eliminan la **aplicación**?

8. (Para **ecosistemas de asistente digital personal**): ¿La empresa **revela claramente** que evalúa si las **políticas de privacidad** de **habilidades** de **terceros** disponibles en su **tienda de habilidades** revelan cuánto tiempo retienen la **información del usuario**?

9. (Para **ecosistemas de asistente digital personal**): ¿La empresa **revela claramente** que evalúa si las **políticas de privacidad** de **habilidades de terceros** disponibles a través de su **tienda de habilidades** declaran que toda la **información del usuario** es eliminada cuando los usuarios cancelan sus cuentas o eliminan la **habilidad**?

Guía del indicador: Así como tenemos la expectativa de que las empresas revelen qué información recopilan y difunden sobre nosotros, también tenemos la expectativa de que las empresas revelen claramente cuánto tiempo la retienen y hasta qué grado eliminan los identificadores de la información del usuario que almacenan. Además, los usuarios también deben poder entender qué ocurre con su información cuando eliminan sus cuentas. En algunos casos, las leyes o regulaciones pueden solicitar a las empresas que retengan alguna información por un periodo determinado. En estos casos, las empresas deben revelar claramente estas regulaciones a los usuarios. Las empresas que eligen retener información del usuario por periodos extendidos también deben tomar medidas para garantizar que los datos no estén vinculados a un usuario específico. Reconociendo los debates actuales sobre la eficacia de los procesos de "anonimización" y la creciente sofisticación en torno a prácticas de "reidentificación", consideramos que retirar los elementos de identificación es una medida positiva que pueden tomar las empresas para proteger la privacidad de sus usuarios.

Además, si las empresas recopilan múltiples tipos de información, tenemos la expectativa de que revelen claramente cuánto tiempo retienen cada tipo de información. Para ecosistemas móviles y asistentes digitales personales, tenemos la expectativa de que las empresas revelen si las políticas de privacidad de las aplicaciones móviles y habilidades de los asistentes digitales personales disponibles en su tienda de aplicaciones declaran cuánto

tiempo la aplicación o habilidad retiene información del usuario y si toda la información del usuario es eliminada si los usuarios cancelan o eliminan la aplicación o la habilidad.

Posibles fuentes:

- Políticas de privacidad de la empresa
- Sitio web de la empresa o sección sobre protección de datos o recopilación de datos

P7. Control de los usuarios sobre su propia información de usuario

La empresa debe **revelar claramente** a los **usuarios** qué **opciones tienen para controlar** la **recopilación**, **inferencia**, **retención** y uso que hace la empresa de la **información del usuario**.

Elementos:

1. Por cada tipo de **información del usuario** que la empresa **recopila**, ¿la empresa **revela claramente** si los **usuarios** pueden controlar la **recopilación** de esta **información del usuario** que hace la empresa?

2. Por cada tipo de **información del usuario** que la empresa **recopila**, ¿la empresa **revela claramente** si los **usuarios** pueden eliminar esta **información del usuario**?

3. Por cada tipo de **información del usuario** que la empresa **infiere** basándose en la **información recopilada**, ¿la empresa **revela claramente** si los **usuarios** pueden controlar si la empresa puede intentar **inferir** esta **información del usuario**?

4. Por cada tipo de **información del usuario** que la empresa **infiere** basándose en la **información recopilada**, ¿la empresa **revela claramente** si los **usuarios** pueden eliminar esta **información del usuario**?

5. ¿La empresa **revela claramente** que brinda a los **usuarios** **opciones para controlar** cómo se usa su **información del usuario** para **publicidad dirigida**?

6. ¿La empresa **revela claramente** qué **publicidad dirigida** está inhabilitada por defecto?

7. ¿La empresa **revela claramente** que brinda a los **usuarios** **opciones para controlar** cómo se usa su **información del usuario** para la elaboración de **sistemas algorítmicos**?

8. ¿La empresa **revela claramente** si usa **información del usuario** para elaborar **sistemas algorítmicos** por defecto, o no?

9. (Para **ecosistemas móviles** y **ecosistemas de asistente digital personal**): ¿La empresa **revela claramente** que brinda a los **usuarios** **opciones para controlar** las funciones de **geolocalización** del dispositivo?

Guía del indicador: Tenemos la expectativa de que las empresas revelen claramente qué opciones tienen los usuarios para controlar la información que las empresas recopilan, retienen e infieren sobre ellos. Permitir que los usuarios controlen qué información referida a ellos recopila, infiere y retiene una empresa debe significar dar a los usuarios la capacidad de eliminar tipos específicos de información del usuario sin solicitarles que eliminen toda su cuenta. Por lo tanto, tenemos la expectativa de que las empresas revelen claramente si los usuarios tienen la opción de eliminar tipos específicos de información del usuario. Además, tenemos la expectativa de que las empresas permitan a los usuarios controlar el uso de su información para los fines de publicidad dirigida y elaboración de sistemas algorítmicos. La publicidad dirigida necesita amplia recopilación, retención e inferencia de la información del usuario y, por lo tanto, las empresas deben revelar claramente si los usuarios tienen opciones de controlar cómo se usa su información para estos fines.

Para ecosistemas móviles y ecosistemas de asistentes digitales personales, tenemos la expectativa de que las empresas revelen claramente qué opciones tienen los usuarios para controlar la recopilación de la información de su ubicación. La ubicación de un usuario cambia frecuentemente y muchos usuarios llevan sus dispositivos móviles casi a todas partes, lo que hace que la recopilación de este tipo de información sea particularmente delicada. Además, las configuraciones de ubicación en ecosistemas móviles y ecosistemas de asistentes digitales personales pueden influir en cómo otros productos y servicios acceden a la información de su ubicación. Por ejemplo, las aplicaciones móviles o los ecosistemas de las habilidades de asistentes digitales personales permitirían a los usuarios controlar la información de su ubicación. Sin embargo, si el dispositivo en el cual esas aplicaciones móviles o las habilidades de asistentes digitales personales recopilan datos de geolocalización por defecto y no brindan a los usuarios una manera de inhabilitar esto, los usuarios podrían quedarse sin poder limitar la recopilación de la información de su ubicación que recopilan las aplicaciones móviles o habilidades de asistente digital personal. Por estas razones, tenemos la expectativa de que las empresas revelen que los usuarios pueden controlar cómo interactúa su dispositivo con la información de su ubicación.

Posibles fuentes:

- Políticas de privacidad de la empresa
- Página de configuraciones de la empresa, tableros de privacidad
- Centro de ayuda de la empresa

P8. Acceso de los usuarios a su propia información de usuario

Las empresas deben permitir que los usuarios obtengan toda su **información de usuario** que la empresa tenga.

Elementos:

1. ¿La empresa **revela claramente** que los usuarios pueden obtener una copia de su **información de usuario**?

2. ¿La empresa **revela claramente** qué **información del usuario** pueden obtener los **usuarios**?

3. ¿La empresa **revela claramente** que los **usuarios** pueden obtener su **información del usuario** en un formato de **datos estructurados**?

4. ¿La empresa **revela claramente** que los **usuarios** pueden obtener toda la **información del usuario**, tanto pública como privada, que una empresa tiene sobre ellos?

5. ¿La empresa **revela claramente** que los **usuarios** pueden acceder a la lista de **categorías de audiencia publicitaria** a la cual la empresa los ha asignado?

6. ¿La empresa **revela claramente** que los **usuarios** pueden obtener toda la información que una empresa ha **inferido** sobre ellos?

7. (Para **ecosistemas móviles**): ¿La empresa **revela claramente** que evalúa si las **políticas de privacidad** de **aplicaciones** de **terceros** disponibles a través de su **tienda de aplicaciones** revelan que los **usuarios** pueden obtener toda la **información de usuario** referida a ellos que tienen las aplicaciones?

8. (Para **ecosistemas de asistente digital personal**): ¿La empresa **revela claramente** que evalúa si las **políticas de privacidad** de **habilidades de terceros** disponibles a través de su **tienda de habilidades** revelan que los **usuarios** pueden obtener toda la **información de usuario** referida a ellos que la habilidad tiene?

Guía del indicador: Los usuarios deben tener la capacidad de obtener toda la información pública e interna que las empresas tienen referida a ellos, incluida la información que una empresa ha usado para hacer inferencias o predicciones sobre los usuarios**.** Tenemos la expectativa de que las empresas revelen claramente qué opciones tienen los usuarios para obtener esta información, qué datos contiene este registro, y en qué formatos pueden obtenerla los usuarios. Las empresas también deben poder facilitar que los usuarios accedan a la lista de categorías publicitarias a las que han sido asignados. Con la finalidad de dirigir anuncios, las empresas suelen asignar a cada usuario a una determinada cantidad de categorías de audiencia. Los anunciantes pueden luego elegir a qué categoría de audiencia quieren dirigirse. Los usuarios deben poder saber a qué categorías de audiencia los ha asignado la empresa, basándose en información que la empresa ha recopilado o inferido sobre los usuarios.

Para ecosistemas móviles, tenemos la expectativa de que la empresa revele a los usuarios si las aplicaciones disponibles en su tienda de aplicaciones especifican que los usuarios pueden obtener toda la información del usuario que la aplicación tiene sobre ellos. Tenemos la expectativa de que las empresas que operan tiendas de habilidades de asistentes digitales personales fijen los parámetros mínimos que deben cumplir las habilidades de terceros alojados en su plataforma. Así como tenemos la expectativa de que las propias empresas revelen que los usuarios pueden obtener un registro de su propia

información de usuario de la empresa, las tiendas de habilidades de asistentes digitales personales deben solicitar que las habilidades ofrezcan una revelación similar en su tienda.

Posibles fuentes:

- Políticas de privacidad de la empresa
- Configuraciones de cuenta de la empresa
- Centro de ayuda de la empresa
- Publicaciones en el blog de la empresa

P9. Recopilación de información del usuario a partir de terceros

La empresa debe **revelar claramente** cuáles son sus prácticas con respecto a la **información del usuario** que recopila desde sitios web o **aplicaciones** de terceros a través de **medios técnicos**, así como la **información del usuario** que recopila a través de **medios no técnicos**.

Elementos:

1. (Para **plataformas digitales**) ¿La empresa **revela claramente** qué **información del usuario** recopila de sitios web de terceros a través de **medios técnicos**?
2. (Para **plataformas digitales**) ¿La empresa **explica claramente** cómo recopila **información del usuario** de **terceros** a través de **medios técnicos**?
3. (Para **plataformas digitales**) ¿La empresa **revela claramente** su objetivo para recopilar **información del usuario** a partir de **terceros** a través de **medios técnicos**?
4. (Para **plataformas digitales)** ¿La empresa **revela claramente** cuánto tiempo retiene la **información del usuario** que recopila a partir de **terceros** a través de **medios técnicos**?
5. (Para **plataformas digitales)** ¿La empresa **revela claramente** que respeta las señales generadas por el usuario de elegir que no se recopilen sus datos?
6. ¿La empresa **revela claramente** qué **información del usuario** recopila a partir de **terceros** a través de **medios no técnicos**?
7. ¿La empresa **revela claramente** cómo recopila **información del usuario** a partir de **terceros** a través de **medios no técnicos**?
8. ¿La empresa **revela claramente** su objetivo para recopilar **información del usuario** a partir de **terceros** a través de **medios no técnicos**?
9. ¿La empresa **revela claramente** cuánto tiempo retiene la **información del usuario** que recopila a partir de terceros a través de **medios no técnicos**?

Guía del indicador: Tenemos la expectativa de que las empresas revelen qué información sobre los usuarios recopilan de terceros, que puede implicar información recopilada de

sitios web o aplicaciones de terceros a través de medios técnicos, por ejemplo, a través de cookies, plugins o widgets, o a través de medios no técnicos, por ejemplo, a través de acuerdos contractuales. Las empresas también pueden adquirir información del usuario a través de medios no técnicos, inclusive como parte de un acuerdo contractual, y estos datos adquiridos pueden volverse parte de un "expediente digital" que las empresas pueden tener de sus usuarios, que luego pueden ser la base para información del usuario inferida o difundida. Las empresas deben ser transparentes y responsables sobre estas prácticas para que los usuarios puedan entender si las empresas están rastreando sus actividades, y cómo las rastrean, aunque no estén alojadas en el sitio web de una empresa o cuando la persona no use un servicio o plataforma en particular.

Posibles fuentes:

- Políticas de privacidad de la empresa
- Políticas de la empresa sobre terceros o políticas de cookies

P10. Proceso para responder a solicitudes de información del usuario

P10(a). Proceso para responder a solicitudes gubernamentales

La empresa debe **revelar claramente** su proceso para responder a las **solicitudes gubernamentales** de **información del usuario**.

Elementos:

1. ¿La empresa **revela claramente** su proceso para responder a **solicitudes gubernamentales no judiciales**?

2. ¿La empresa **revela claramente** su proceso para responder a **órdenes judiciales**?

3. ¿La empresa **revela claramente** su proceso para responder a **solicitudes gubernamentales** de jurisdicciones extranjeras?

4. ¿Las explicaciones de la empresa **revelan claramente** la base legal en virtud de la cual puede cumplir con **solicitudes gubernamentales**?

5. ¿La empresa **revela claramente** que realiza una revisión exhaustiva de las **solicitudes gubernamentales** antes de decidir cómo responder?

6. ¿La empresa se compromete a desestimar **solicitudes gubernamentales** inapropiadas o demasiado generales?

7. ¿La empresa brinda guías o ejemplos claros de implementación de sus procesos para **solicitudes gubernamentales**?

Guía del indicador: Cada vez más, las empresas reciben solicitudes gubernamentales de entregar información del usuario. Estas solicitudes pueden venir de agencias

gubernamentales o cortes (nacionales y extranjeras). Tenemos la expectativa de que las empresas revelen públicamente su proceso para responder a las solicitudes gubernamentales, junto con la base para cumplir con estas solicitudes. Las empresas también deben comprometerse públicamente a desestimar solicitudes gubernamentales inapropiadas o demasiado generales.

En algunos casos, la ley puede evitar que una empresa revele información mencionada en los elementos de este indicador. Los investigadores documentarán las situaciones en que este sea el caso, pero de todas maneras una empresa perderá puntos si no logra cumplir con todos los elementos. Esto representa una situación en la que la ley causa que las empresas no sean competitivas, y exhortamos a las empresas a abogar por leyes que les permitan respetar plenamente los derechos de los usuarios a la libertad de expresión y privacidad.

Posibles fuentes:

- informe de transparencia de la empresa
- Guías de aplicación de la ley de la empresa
- Políticas de privacidad de la empresa
- Informe de sostenibilidad de la empresa
- Publicaciones de blog de la empresa

P10(b). Proceso para responder a solicitudes privadas

La empresa debe **revelar claramente** su proceso para responder a solicitudes de **información del usuario** que lleguen a través de **procesos privados**.

Elementos:

1. ¿La empresa **revela claramente** su proceso para responder a solicitudes hechas a través de **procesos privados**?

2. ¿Las explicaciones de la empresa **revelan claramente** la base en virtud de la cual puede cumplir con las solicitudes hechas a través de **procesos privados**?

3. ¿La empresa **revela claramente** que ejecuta con revisión exhaustiva las solicitudes hechas a través de **procesos privados** antes de decidir cómo responder?

4. ¿La empresa se compromete a desestimar solicitudes inapropiadas o demasiado generales hechas a través de **procesos privados**?

5. ¿La empresa brinda guías o ejemplos claros de la implementación de sus procesos para responder solicitudes hechas a través de **procesos privados**?

Guía del indicador: Cada vez más, las empresas reciben solicitudes privadas de entregar información del usuario. A menudo, son solicitudes informales de información del usuario de una entidad no gubernamental que no incluye ni se hace a través de un proceso legal formal. Según la Fundación Wikimedia —que publica informes de transparencia con datos

sobre la cantidad de solicitudes de este tipo que recibe—, las solicitudes privadas de información del usuario incluyen casos en los que otra empresa les envía una carta o correo electrónico para solicitar "información no pública" sobre uno de sus usuarios. Esto podría incluir la dirección IP o dirección de correo electrónico del usuario.

Este indicador tiene la expectativa de que las empresas revelen sus procesos para gestionar este tipo de solicitudes. Las empresas deben explicar las razones para cumplir con este tipo de solicitudes, y comprometerse a desestimar solicitudes demasiado generales.

Posibles fuentes:
- Informe de transparencia de la empresa
- Guías de aplicación de la ley de la empresa
- Políticas de privacidad de la empresa
- Publicaciones del blog de la empresa

P11. Datos sobre solicitudes de información del usuario

P11(a). Datos sobre solicitudes gubernamentales de información del usuario

La empresa debe publicar frecuentemente datos sobre **solicitudes gubernamentales** de **información del usuario**.

Elementos:

1. ¿La empresa enumera la cantidad de **solicitudes gubernamentales** que recibe por país?

2. ¿La empresa enumera la cantidad de **solicitudes gubernamentales** que recibe de información almacenada del usuario y **acceso a las comunicaciones en tiempo real**?

3. ¿La empresa enumera la cantidad de cuentas afectadas?

4. ¿La empresa enumera si una solicitud buscaba acceder a **contenido** de comunicaciones o a información que **no correspondía a contenido** de comunicaciones, o ambos?

5. ¿La empresa identifica la autoridad legal específica o el tipo de proceso legal a través del cual se hacen las solicitudes de las autoridades y de los organismos de seguridad nacional?

6. ¿La empresa incluye **solicitudes gubernamentales** provenientes de **órdenes judiciales**?

7. ¿La empresa enumera la cantidad de **solicitudes gubernamentales** con las que cumplió, desglosadas por categoría de solicitud?

8. ¿La empresa enumera qué tipos de **solicitudes gubernamentales** no debe revelar por ley?

9. ¿La empresa informa de estos datos al menos una vez al año?

10. ¿Los datos se pueden exportar como un archivo de **datos estructurados**?

Guía del indicador: Con frecuencia, las empresas reciben solicitudes de Gobiernos de entregar información del usuario. Estas solicitudes pueden llegar de agencias gubernamentales o cortes (nacionales y extranjeras). Tenemos la expectativa de que las empresas publiquen frecuentemente datos sobre la cantidad y tipo de estas solicitudes que reciben y con cuántas cumplen. Las empresas deben revelar datos sobre las solicitudes que reciben por país, incluidas las solicitudes de su Gobierno y Gobiernos extranjeros, y también las que llegan de autoridades y cortes. También tenemos la expectativa de que la revelación de las empresas indique la cantidad de cuentas afectadas por estas solicitudes y que delineen por categoría las solicitudes con las cuales la empresa ha cumplido. Reconocemos que a veces las leyes no permiten a las empresas revelar las solicitudes de información del usuario que son hechas por los Gobiernos. Sin embargo, en estos casos tenemos la expectativa de que las empresas informen qué tipos de solicitudes gubernamentales están impedidas de revelar por ley. Las empresas también deben informar de estos datos una vez al año y deben garantizar que los datos se puedan exportar como un archivo de datos estructurados.

En algunos casos, la ley puede impedir que una empresa revele información mencionada en este indicador. Por ejemplo, tenemos la expectativa de que las empresas publiquen cantidades exactas más que rangos de números. Reconocemos que a veces las leyes no permiten que las empresas lo hagan así, y los investigadores documentarán las situaciones en que este sea el caso. Pero una empresa perderá puntos si no logra cumplir con todos los elementos. Esto representa una situación en que la ley causa que las empresas no cumplan con las mejores prácticas, y alentamos a las empresas que alienten leyes les permitan respetar totalmente los derechos de libertad de expresión y de privacidad de los usuarios.

Posibles fuentes:
- Informe de transparencia de la empresa
- Informe de aplicación de la ley de la empresa
- Informe de sostenibilidad de la empresa

P11(b). Datos sobre solicitudes privadas de información del usuario

La empresa debe publicar frecuentemente datos sobre las solicitudes de **información del usuario** que llegan a través de **procesos privados.**

Elementos:

1. ¿La empresa enumera la cantidad de solicitudes que recibe de **información del usuario** que llegan a través de **procesos privados**?

2. ¿La empresa enumera la cantidad de solicitudes de **información del usuario** que llegan a través de **procesos privados** con los que cumplió?

3. ¿La empresa informa de estos datos al menos una vez al año?

4. ¿Los datos se pueden exportar como un archivo de **datos estructurados?**

Guía del indicador: Cada vez más, las empresas reciben solicitudes privadas de entregar información del usuario. Esas solicitudes son a menudo solicitudes informales de información del usuario de una entidad no gubernamental que no incluyen ni llega a través de ningún proceso legal formal. Según la Fundación Wikimedia —que publica informes de transparencia con datos sobre la cantidad de solicitudes de este tipo que recibe—, las solicitudes privadas de información del usuario incluyen casos en los que otra empresa les envía una carta o correo electrónico para solicitar "información no pública" sobre uno de sus usuarios. Esto podría incluir la dirección IP o dirección de correo electrónico del usuario.

Así como las empresas deben publicar datos sobre las solicitudes gubernamentales que reciben para entregar información del usuario, las empresas deben publicar datos sobre solicitudes de información del usuario que reciben (y con las que cumplen) que llegan a través de cualquier proceso privado. Tenemos la expectativa de que las empresas publiquen frecuentemente datos sobre la cantidad y tipo de tales solicitudes que reciben, y la cantidad de esas solicitudes con las que cumplen. Las empresas también deben informar estos datos una vez al año y asegurarse de que se puedan exportar en un archivo de datos estructurados.

Posibles fuentes:
- Informe de transparencia de la empresa
- Informe de sostenibilidad de la empresa
- Informe de responsabilidad social corporativa

P12. Notificación a los usuarios sobre las solicitudes de terceros de información del usuario

La empresa debe **notificar** a los usuarios hasta donde permita la ley cuando su **información de usuario** haya sido **solicitada por Gobiernos** y otros **terceros**.

Elementos:

1. ¿La empresa **revela claramente** que notifica a los usuarios cuando **entidades gubernamentales (incluidos cortes u otros entes judiciales) piden** su **información de usuario**?

2. ¿La empresa **revela claramente** que **notifica** a los usuarios cuando recibe solicitudes de su **información de usuario** a través de **procesos privados**?

3. ¿La empresa **revela claramente** situaciones en las que podría no **notificar** a los usuarios, incluida una descripción de los tipos de **solicitudes gubernamentales** que la ley le prohíbe revelar a los usuarios?

Guía del indicador: Tenemos la expectativa de que las empresas revelen claramente un compromiso de notificar a los usuarios cuando los Gobiernos y otros terceros soliciten datos sobre sus usuarios. Reconocemos que este aviso puede no ser posible en casos donde existe una investigación en curso. Sin embargo, tenemos la expectativa de que las empresas especifiquen qué tipo de solicitudes la ley les impide revelar.

Posibles fuentes:
- Informe de transparencia de la empresa
- Guías de aplicación de la ley de la empresa
- Políticas de privacidad de la empresa
- Políticas de derechos humanos de la empresa

P13. Supervisión de seguridad

La empresa debe **revelar claramente** información sobre sus procesos institucionales para garantizar la seguridad de sus productos y servicios.

Elementos:

1. ¿La empresa **revela claramente** que tiene sistemas vigentes para limitar y dar seguimiento al acceso de sus trabajadores a **información del usuario**?

2. ¿La empresa **revela claramente** que tiene un equipo de seguridad que lleva a cabo auditorías de seguridad a los productos y servicios de la empresa?

3. ¿La empresa **revela claramente** que encarga a terceros las auditorías de seguridad realizadas a sus productos y servicios?

Guía del indicador: Como las empresas gestionan y almacenan inmensas cantidades de información sobre los usuarios, deben tener vigentes medidas de seguridad claras para garantizar que esta información se conserve de forma segura. Tenemos la expectativa de que las empresas revelen claramente que tienen sistemas vigentes para limitar y dar seguimiento al acceso de sus trabajadores a la información del usuario. También tenemos la expectativa de que la empresa revele claramente que usa equipos de seguridad internos y externos para realizar auditorías de seguridad a sus productos y servicios.

Posibles fuentes:
- Políticas de privacidad de la empresa
- Guía de seguridad de la empresa

P14. Tratamiento a las vulnerabilidades de seguridad

La empresa debe abordar las **vulnerabilidades de seguridad** cuando las descubre.

Elementos:

1. ¿La empresa **revela claramente** que tiene un mecanismo a través del cual los **investigadores de seguridad** pueden presentar las **vulnerabilidades** que descubren?

2. ¿La empresa **revela claramente** el plazo en el que revisará denuncias de **vulnerabilidades**?

3. ¿La empresa se compromete a no iniciar acción legal contra los **investigadores** que denuncian **vulnerabilidades** dentro de los términos del mecanismo de denuncia de la empresa?

4. (Para ecosistemas móviles y **ecosistemas de asistente digital personal**)¿La empresa **revela claramente** que las **actualizaciones de software**, **parches** de seguridad, componentes adicionales o extensiones se descargan por un canal **encriptado**?

5. (Para ecosistemas móviles y empresas de telecomunicaciones) ¿La empresa **revela claramente** qué **modificaciones** ha hecho a un **sistema operativo móvil**, y si es que las ha hecho?

6. (Para ecosistemas móviles, **ecosistemas de asistente digital personal** y empresas de telecomunicaciones) ¿La empresa **revela claramente** qué efecto tienen esas modificaciones en la capacidad de la empresa de enviar **actualizaciones de seguridad** a los usuarios, si es que tienen efecto?

7. (Para ecosistemas móviles y **ecosistemas de asistente digital personal**) ¿La empresa **revela claramente** la fecha a partir de la cual continuará ofreciendo **actualizaciones de seguridad** para el **dispositivo/sistema operativo**?

8. (Para ecosistemas móviles y **ecosistemas de asistente digital personal**) ¿La empresa se compromete a ofrecer **actualizaciones de seguridad** para el sistema operativo y demás software fundamental por un mínimo de cinco años tras el lanzamiento?

9. (Para ecosistemas móviles, **ecosistemas de asistente digital personal** y empresas de telecomunicaciones) Si la empresa usa un sistema operativo adaptado de un sistema existente, ¿la empresa se compromete a ofrecer **parches de seguridad** en el término de un mes desde que una **vulnerabilidad** se anuncia al público?

10. (Para **ecosistemas de asistente digital personal**): ¿La empresa **revela claramente** qué **modificaciones** ha hecho, si es que ha hecho modificaciones, al **sistema operativo de un asistente digital personal**?

11. (Para **ecosistemas de asistente digital personal**): ¿La empresa **revela claramente** qué efecto han tenido esas modificaciones, si es que ha habido efectos, en la capacidad de la **empresa de enviar actualizaciones de seguridad a los usuarios?**

Guía del indicador: El código informático no es perfecto. Cuando las empresas toman conocimiento sobre vulnerabilidades que pueden poner en riesgo a los usuarios y su información, deben tomar acciones para mitigar esos problemas. Esto incluye garantizar que las personas puedan hacer llegar a la empresa cualquier vulnerabilidad que descubran. Creemos que es especialmente importante que las empresas brinden a los usuarios políticas clara sobre cómo y cuándo los usuarios recibirán actualizaciones de seguridad. Además, como los proveedores de telecomunicaciones pueden alterar los sistemas operativos móviles de fuente abierta, tenemos la expectativa de que estas empresas revelen información que pueda afectar la capacidad de un usuario de acceder a estas actualizaciones fundamentales.

Posibles fuentes:
- Políticas de privacidad de la empresa
- Guía de seguridad de la empresa
- Foros de "ayuda" de la empresa

P15. Filtración de datos

La empresa debe revelar públicamente información sobre sus procesos para responder a las **filtraciones de datos**.

Elementos:

1. ¿La empresa **revela claramente** que notificará a las autoridades pertinentes sin que haya una demora injustificada cuando ocurra una **filtración de datos**?

2. ¿La empresa **revela claramente** su proceso para notificar los datos a quienes pueden verse afectados por una **filtración de datos**?

3. ¿La empresa **revela claramente** qué medidas tomará para enfrentar el impacto de una **filtración de datos** de sus usuarios?

Guía del indicador: Las empresas deben tener vigentes procesos claramente revelados para abordar las filtraciones de datos, incluidas políticas claras para notificar a los usuarios afectados. Como las filtraciones de datos pueden resultar en amenazas significativas a la seguridad financiera o personal de alguien, además de exponer información privada, las empresas deben hacer que estos procesos estén disponibles para el público. Así, las personas pueden tomar decisiones informadas y evaluar los posibles riesgos antes de suscribirse a un servicio o de brindarle su información a una empresa.

Confiamos en que las empresas tengan políticas formales vigentes con respecto a su manejo de filtración de datos cuando ocurren, si es que ocurren, y hacer que esta información sobre las políticas y compromisos sea pública antes de que ocurra una filtración.

Posibles fuentes:

- Términos de servicio o políticas de privacidad de la empresa
- Guía de seguridad de la empresa

P16. Encriptación de la comunicación del usuario y contenido privado (plataformas digitales)

La empresa debe **encriptar** la comunicación de los usuario y el **contenido** privado para que los **usuarios** puedan controlar quién tiene acceso.

Elementos:

1. ¿La empresa **revela claramente** que la transmisión de comunicaciones del usuario está **encriptada** por defecto?

2. ¿La empresa **revela claramente** que la transmisión de las comunicaciones del usuario está **encriptada** con llaves únicas?

3. ¿La empresa **revela claramente** que los usuarios pueden asegurar su contenido privado con **encriptación de extremo a extremo**, o **encriptación total del disco** (cuando sea aplicable)?

4. ¿La empresa **revela claramente** que la **encriptación de extremo a extremo**, o **encriptación total del disco**, está habilitada por defecto?

Guía del indicador: La encriptación es una herramienta importante para proteger la libertad de expresión y la privacidad. El relator especial de Naciones Unidas sobre Libertad de Expresión ha afirmado sin lugar a dudas que la encriptación y el anonimato son esenciales para el ejercicio y protección de los derechos humanos.[31] Tenemos la expectativa de que las empresas revelen claramente qué comunicaciones del usuario están encriptadas por defecto, que las transmisiones están protegidas por la "reserva perfecta de aquí hacia adelante", que los usuarios tienen la opción de activar la encriptación de extremo a extremo, y si está habilitada por defecto. Para ecosistemas móviles y ecosistemas de asistente digital personal, tenemos la expectativa de que las empresas revelen claramente que permiten la encriptación total del disco.

Posibles fuentes:

[31] "Informe sobre encriptación, anonimato y marco de los derechos humanos",*Oficina del Alto Comisionado de Naciones Unidas para Derechos Humanos,* https://www.ohchr.org/en/issues/freedomopinion/pages/callforsubmission.aspx, último acceso 2 de abril de 2020.

- Términos de servicio o políticas de privacidad de la empresa
- Guía de seguridad de la empresa
- Centro de ayuda de la empresa
- Informes de sostenibilidad de la empresa
- Blog oficial empresa o comunicados de prensa

P17. Seguridad de la cuenta (plataformas digitales)

La empresa debe ayudar a los usuarios a mantener sus **cuentas** seguras.

Elementos:

1. ¿La empresa **revela claramente** que implementa métodos de autenticación avanzados para evitar el acceso fraudulento?

2. ¿La empresa **revela claramente** que los usuarios pueden ver la actividad reciente de su cuenta?

3. ¿La empresa **revela claramente** que **notifica a los usuarios** sobre actividad inusual de la cuenta y posible acceso no autorizado a sus cuentas?

Guía del indicador: Las empresas deben ayudar a los usuarios a mantener sus cuentas seguras. Deben revelar claramente que usan técnicas de autenticación avanzadas para evitar el acceso no autorizado a las cuentas e información del usuario. También confiamos que las empresas brinden a los usuarios herramientas que les permitan asegurar sus cuentas y saber cuando sus cuentas puedan estar comprometidas.

Posibles fuentes:
- Centro de seguridad de la empresa
- Páginas de ayuda de la empresa o página de asistencia comunitaria
- Página de configuraciones de cuenta de la empresa
- Blog de la empresa

P18. Información e instrucción a usuarios sobre potenciales riesgos

La empresa debe publicar información para ayudar a los usuarios a defenderse de **riesgos de ciberseguridad**.

Elementos:

1. ¿La empresa publica materiales prácticos que instruya a los usuarios sobre cómo protegerse de **riesgos de ciberseguridad** relevantes para sus productos o servicios?

Guía del indicador: Como las empresas tienen enormes cantidades de datos de los usuarios, a menudo son blanco de actores maliciosos. Tenemos la expectativa de que las empresas ayuden a los usuarios a protegerse de esos riesgos. Esto puede incluir publicar materiales sobre cómo configurar autenticación avanzada de la cuenta o adaptar las configuraciones de privacidad, cómo evitar el software malicioso, *phishing* y ataques de ingeniería social, cómo evitar o abordar el *bullying* o el acoso en línea, y qué significa la "navegación segura". Las empresas deben presentar estas pautas con un lenguaje claro, idealmente acompañado de material visual, imágenes, diseñados para ayudar a los usuarios a entender la naturaleza de los riesgos que las empresas y los usuarios pueden enfrentar. Estos materiales pueden tomar muchas formas, incluidos consejos, tutoriales, guías instructivas, preguntas frecuentes u otros recursos presentados de una manera que los usuarios puedan comprender fácilmente.

Posibles fuentes:

- Centro de seguridad de la empresa
- Páginas de ayuda de la empresa o página de asistencia comunitaria
- Blog de la empresa

Glosario

Nota: *Este no es un glosario general. Las definiciones y explicaciones que aparecen a continuación fueron escritas específicamente para guiar a los investigadores en evaluar a las empresas de tecnología de la información y la comunicación en los indicadores de este proyecto de investigación.*

Acceso a las comunicaciones en tiempo real — Vigilancia de una conversación u otra comunicación electrónica en "tiempo real" mientras se lleva a cabo la conversación, o interceptación de datos en el mismo momento en que se transmite. También se le llama "intervención telefónica". Considera la diferencia entre una solicitud de interceptación y una solicitud de datos archivados. Una interceptación brinda a las autoridades acceso a futuras comunicaciones, mientras una solicitud para datos archivados brinda acceso a las autoridades a registros de comunicaciones ocurridas en el pasado. El Gobierno estadounidense puede obtener acceso a las comunicaciones en tiempo real a través de la Ley de Interceptaciones y la Ley de Registro, ambas integrantes de la Ley de Privacidad de Comunicaciones Electrónicas (ECPA, por su nombre en inglés); el Gobierno ruso puede hacerlo a través del Sistema para Actividades Operativas de Investigación (SORM, por su nombre en inglés).

Acción de moderación de contenido — La moderación de contenido es la práctica de ocultar el contenido generado por el usuario y que es publicado en sitios de internet, medios sociales y otros medios en línea, con la finalidad de determinar si el contenido es apropiado para un sitio web, lugar o jurisdicción determinado. El proceso puede tener como resultado que el contenido sea eliminado o restringido por un moderador que actúa como agente de la plataforma o sitio web en cuestión. Cada vez más, además de moderadores humanos, las empresas usan sistemas algorítmicos para moderar contenido en sus plataformas. Fuente: "Moderación de contenido," Enciclopedia de Grandes Datos, https://doi.org/10.1007/978-3-319-32001-4_44-1.

Actualización de seguridad — Reparación dada a conocer ampliamente para una vulnerabilidad específica de un producto y relacionada con la seguridad. Las vulnerabilidades de seguridad se califican por su gravedad: críticas, importantes, moderadas o bajas.

Actualización de software — Una actualización de software (a veces llamado parche de software) es una descarga gratuita para una aplicación o paquete de software que brinda reparaciones para características que no funcionan como deberían funcionar o agrega mejoras y compatibilidad de software menores. Una actualización también puede incluir actualizaciones de unidades que mejoran el funcionamiento del hardware o periféricos, o agregan respaldo para nuevos modelos de periféricos.

Actualización fundamental (de software) — Reparación lanzada ampliamente para una vulnerabilidad específica de un producto y relacionada con la seguridad. Las

vulnerabilidades de seguridad se califican por su severidad: críticas, importantes, moderadas o bajas.

Ahogar — Manera terminante de dar forma al tráfico en la que el operador de la red reduce la velocidad del flujo de paquetes a través de una red. Los operadores móviles pueden ahogar el tráfico para aplicar límites a la cantidad de datos transferidos.

Algoritmos: Un algoritmo es un conjunto de instrucciones usadas para procesar información y entregar un resultado según lo estipulado en las instrucciones. Los algoritmos pueden ser simples partes de código, pero también pueden ser increíblemente complejos, y "codificar miles de variables a través de millones de puntos de datos". En el contexto de las empresas de internet, móviles y de telecomunicaciones, algunos algoritmos —por su complejidad, la cantidad y tipo de información del usuario que se les ingresa, y la función de toma de decisiones para las que sirven— tienen consecuencias significativas para los derechos humanos de los usuarios, incluidas la libertad de expresión y la privacidad. Leer más en: "Responsabilidad algorítmica: Manual básico" de Data & Society.

Altos ejecutivos — Director ejecutivo y demás miembros del equipo ejecutivo como aparecen en el sitio web de la empresa u otros documentos oficiales, como su informe anual. Si no hay una lista del equipo ejecutivo definido por la empresa, se consideran altos ejecutivos a otras posiciones con nivel de jefe y las que están en las posiciones más altas de gestión (por ejemplo, vicepresidente ejecutivo, dependiendo de la empresa).

Anonimizar (información del usuario) — Esto se refiere a información del usuario que las empresas recopilan y retienen, pero solamente después de retirar u ocultar toda información que los pueda identificar. Esto significa retirar identificadores explícitos como nombres, dirección de correo electrónico y cualquier número de identificación oficial, así como identificadores como direcciones IP, cookies y números únicos de dispositivos.

Anunciante — Una persona o entidad que ha creado o pagado por contenido publicitario. Típicamente, el anunciante determina los parámetros de selección de sujetos para cada anuncio publicitario.

Anuncio publicitario — Mensaje que un anunciante ha pagado a una empresa para mostrar a un subgrupo de sus usuarios, que consiste en contenido publicitario y parámetros de selección de sujetos.

Aplicación — Programa independiente o porción de software diseñado para cumplir un objetivo particular; aplicación de software, sobre todo si un usuario la descarga a un dispositivo móvil.

Archivo público — Recurso públicamente disponible que contiene versiones anteriores de las políticas de una empresa, como los términos de servicio o la política de privacidad, o que explica exhaustivamente todas las rondas de cambios que la empresa hace a esas políticas.

Archivo público de terceros— De manera ideal, las empresas publican información sobre las solicitudes que reciben para que el público tenga una mejor comprensión de cómo se restringe el contenido en la plataforma. Las empresas pueden brindar información sobre las solicitudes que reciben del archivo de un tercero, como Lumen (antes conocido como Chilling Effects o "efecto negativo"), que es un proyecto de investigación independiente que gestiona una base de datos públicamente disponible de solicitudes de eliminación de contenido en línea. Este tipo de depósito ayuda a los investigadores y al público a entender qué tipo de contenido se ha pedido que se elimine, y para tener mayor comprensión de solicitudes legítimas e ilegítimas. Ver: https://cyber.harvard.edu/research/lumen.

Bot — Cuenta en línea automatizada en la que todas o sustancialmente todas las acciones o publicaciones de esa cuenta no resultan de la acción de una persona.

Botnet — Red de bots coordinada que actúa de común acuerdo, por lo general porque está bajo el control de la misma persona o entidad.

Categorías de audiencia publicitaria — Grupos de usuarios, identificados con la finalidad de emitir publicidad dirigida, que comparten algunas características o intereses, tales como que están determinados sobre la base de información del usuario que una empresa ha recopilado o inferido.

Cierre o restricción de acceso a la red — Cierre de red se refiere a la interrupción intencional de internet o comunicaciones electrónicas, incluidos servicios de telecomunicaciones como telefonía celular y mensajes SMS. Esto incluye un cierre general de todos los servicios celulares o de internet dentro de una zona geográfica y el bloqueo dirigido de servicios específicos, tales como las redes sociales o aplicaciones de mensajería.

Compromiso de políticas —Declaración disponible públicamente que representa la política oficial de la empresa que ha sido aprobada en los niveles más altos de la empresa.

Conservar, recomendar o calificar — La práctica de usar algoritmos, aprendizaje automático y otros sistemas de toma de decisiones automatizadas para gestionar, dar forma y regir el flujo de contenido e información en una plataforma, por lo general de una manera que está personalizada para cada usuario individual.

Contenido — La información contenida en comunicaciones por cable, oral o electrónica (por ejemplo, una conversación que tiene lugar por teléfono o cara a cara, el texto escrito y transmitido en un mensaje SMS o correo electrónico).

Contenido publicitario — Todo contenido que alguien ha pagado para que una empresa muestre a sus usuarios.

Cookie(s) — "Las cookies son una tecnología web que permite a los sitios web reconocer tu navegador. Originalmente, las cookies fueron diseñadas para permitir que los sitios

ofrecieran carritos de compra en línea, guardar preferencias o mantener tu sesión en un sitio. También permiten rastrear y hacer perfiles, para que los sitios puedan reconocerte y saber más de a dónde vas, qué dispositivos usas y qué te interesa – aunque no tengas cuenta en ese sitio o no hayas iniciado sesión". Fuente: https://ssd.eff.org/en/glossary/cookies

Cuenta / cuenta de usuario — Grupo de datos asociados con un usuario en particular de un sistema informático, servicio o plataforma. Como mínimo, la cuenta de usuario comprende un nombre de usuario y una contraseña, que se usan para autenticar el acceso del usuario a sus datos.

Dar forma al tráfico — Configurar el flujo de tráfico a través de una red. Puede incluir hacer más lentos algunos tipos de tráfico, con reservas. Se puede usar para dar forma al tráfico con fines de un manejo legítimo de redes (por ejemplo, dar prioridad a tráfico VoIP antes que al tráfico web normal para facilitar comunicación en tiempo real) o por razones que responden a principios de neutralidad en la red (por ejemplo, reducir intencionalmente el tráfico del video para disuadir a los usuarios de utilizar aplicaciones con gran ancho de banda).

Datos anónimos — Datos que de ninguna manera están relacionados con otra información que permitiría que se identificara a un usuario. La naturaleza amplia de esta definición que se usa en el proyecto de Ranking Digital Rights es necesaria para reflexionar sobre varios hechos. Primero, analistas especializados pueden "desanonimizar" grandes conjuntos de datos. Esto hace que sea imposible cumplir con casi todas las promesas de anonimización. En esencia, ningún dato vinculado con un "identificador anónimo" es anónimo. Más bien, suelen ser datos pseudónimos que se pueden conectar con la identidad fuera de línea del usuario. Segundo, los metadatos pueden ser más o igualmente reveladores de las asociaciones e intereses de un usuario que los datos de contenido, por lo que estos datos son de vital interés. Tercero, las entidades que tienen acceso a muchas fuentes de datos, tales como los agentes de datos y Gobiernos, pueden juntar una o más fuentes de datos que revelan información sobre los usuarios. Por lo tanto, los agentes más sofisticados pueden usar los datos que parecen anónimos para construir una mayor imagen de un usuario.

Datos de ubicación— Información recopilada por una red o servicio sobre dónde está o estuvo ubicado el teléfono u otro dispositivo del usuario —por ejemplo, rastrear la ubicación de un teléfono móvil a partir de los datos recopilados por las estaciones base en una red de telefonía móvil o a través del posicionamiento de GPS o de las redes inalámbricas.

Datos estructurados — "Datos en campos fijos dentro de un registro o archivo. Las bases de datos relacionales y las hojas de cálculo son ejemplos de datos estructurados. Aunque los datos en archivos XML no están fijos en un lugar como los registros de bases de datos tradicionales, están estructurados porque los datos están etiquetados y se les puede identificar con precisión". A la inversa, los datos no estructurados son datos que "no están ubicados en lugares fijos. El término generalmente se refiere a texto sin formato, que es ubicuo. Los ejemplos son documentos de procesamiento de palabras, archivos PDF,

mensajes de correo electrónico, blogs, páginas web y sitios sociales". Fuente: PC Mag Encyclopedia.
"datos estructurados" http://www.pcmag.com/encyclopedia/term/52162/structured-data.
"datos no estructurados" http://www.pcmag.com/encyclopedia/term/53486/unstructured-data.

Despliegue / desplegar — Serie de anuncios de productos relacionados que se llevan a cabo con el tiempo; el proceso de hacer parches, actualizaciones de software y mejoras de software disponibles para usuarios finales.

Difusión / difundir — La empresa permite que un tercero acceda a la información del usuario, ya sea porque da libremente la información a un tercero (o al público o a otros usuarios) o porque la vende a un tercero.

Discriminación — Para los propósitos del Índice RDR, la discriminación se refiere a la práctica de tratar a personas, empresas o productos particulares de manera diferente, sobre todo de manera injusta. Fuente: diccionario de inglés comercial de Cambridge: https://dictionary.cambridge.org/dictionary/english/discrimination.

Dispositivo / dispositivo portátil / dispositivo móvil — Objeto físico, como un smartphone o un teléfono básico, que se usa para acceder a las redes de telecomunicaciones que ha sido diseñado para que el usuario lo lleve y use en diversos lugares.

Documentación — La empresa provee registros que los usuarios pueden consultar, como un registro de cambios a los términos de servicio o documentos de política de privacidad.

Documentos de políticas por niveles — Términos de servicio y políticas de privacidad que están divididas en secciones con hipervínculos, que permiten a los usuarios navegar directamente a la sección que tienen interés en ver.

Ecosistema de asistente personal digital — Un ecosistema de asistente digital personal consiste en una interfaz accionada por inteligencia artificial instalada en dispositivos digitales que puede interactuar con los usuarios por medio de texto o voz para acceder a información en internet y realizar algunas tareas con datos personales difundidos por los usuarios. Los usuarios pueden interactuar con ecosistemas de asistentes digitales personales a través de **habilidades**, las que se encuentran disponibles a través de terceros programadores/proveedores o el propio asistente digital personal.

Ecosistema móvil — Conjunto indivisible de bienes y servicios que ofrece una empresa de dispositivos móviles, que comprende el hardware del dispositivo, sistema operativo, tiendas de aplicaciones y cuentas de usuario.

Encriptación — En esencia, oculta el contenido de comunicaciones o archivos de tal manera que solamente pueda verlo el destinatario a quien estaba dirigido. El proceso usa un algoritmo para convertir el mensaje (texto sin formato) en un formato codificado (texto

cifrado) para que quien quiera que vea el mensaje lo vea como una serie aleatoria de caracteres. Solamente alguien con la clave de encriptación apropiada puede desencriptar el mensaje, revertir el texto cifrado en texto sin formato. Los datos pueden estar encriptados cuando se guardan y cuando están en una transmisión.

Por ejemplo, los usuarios pueden encriptar los datos de su disco duro para que solamente el usuario con la clave de encriptación pueda descifrar los contenidos del disco. Además, los usuarios pueden enviar un mensaje de correo electrónico encriptado, lo que impediría que alguien viera el contenido del correo electrónico mientras el mensaje se mueve por la red para llegar al destinatario a quien estaba dirigido. Con encriptación en tránsito (por ejemplo, cuando un sitio web usa HTTPS), la comunicación entre un usuario y un sitio web está encriptada, para que los externos, como el proveedor de servicio de internet del usuario, solamente puedan ver la visita inicial al sitio web, pero no lo que el usuario comunica en ese sitio web ni las subpáginas que el usuario visita.
Para más información, ver este recurso: http://www.explainthatstuff.com/encryption.html.

Encriptación de extremo a extremo — Con la encriptación de extremo a extremo, solamente el remitente y el destinatario pueden leer el contenido de las comunicaciones encriptadas. Los terceros, incluida la empresa, no podrán desencriptar el contenido.

Encriptación total del disco — Encriptación completa de todos los datos almacenados en un dispositivo físico, de tal manera que solamente el usuario puede acceder al contenido al suministrar la contraseña, o contraseñas, generada por el usuario u otros medios de desencriptación (huella digital, código de autenticación de dos factores, autentificador físico, etc.).

Equipo / programa — Unidad definida dentro de una empresa que tiene responsabilidad sobre cómo los productos o servicios de la empresa se intersecan, en este caso, con la libertad de expresión o privacidad.

Evaluación del impacto en los derechos humanos (evaluación de riesgos de derechos humanos) — La evaluación de riesgos de derechos humanos es un enfoque sistemático a la revisión exhaustiva. Una empresa lleva a cabo estas evaluaciones o revisiones para ver cómo sus productos, servicios y prácticas empresariales afectan la libertad de expresión y la privacidad de sus usuarios.

Para más información sobre la Evaluación del impacto en los derechos humanos y de mejores prácticas para llevarla a cabo, revisa esta página especial alojada en el Centro de Recursos de Negocios y Derechos Humanos:
https://business-humanrights.org/en/un-guiding-principles/implementation-tools-examples/implementation-by-companies/type-of-step-taken/human-rights-impact-assessments

El Instituto Danés para los Derechos Humanos ha elaborado una herramienta relacionada con la Evaluación de cumplimiento de derechos humanos

(https://hrca2.humanrightsbusiness.org), y la organización Business for Social Responsibility (BSR) ha elaborado una guía útil para llevar a cabo una evaluación de riesgos de derechos humanos: http://www.bsr.org/en/our-insights/bsr-insight-article/how-to-conduct-an-effective-human-rights-impact-assessment

Para una guía específica del sector de tecnologías de la información y la comunicación, ver el extracto del capítulo del libro ("Negocios, derechos humanos e internet: Marco para la Implementación") de Michael Samway en el sitio web del proyecto en: http://rankingdigitalrights.org/resources/readings/samway_hria.

Explícito — La empresa declara específicamente su apoyo a la libertad de expresión y la privacidad.

Fácil de encontrar — Los términos de servicio o la política de privacidad están a uno o dos clics de la página de inicio de la empresa o servicio, o están en un lugar lógico donde es probable que los usuarios los encuentren.

Fácil de entender / manera comprensible — La empresa ha tomado medidas para ayudar a los usuarios a entender sus términos de servicio y política de privacidad. Esto incluye, entre otros, brindar resúmenes, consejos u orientación que expliquen qué significan los términos, con encabezados de sección, tipo de letra legible u otras características gráficas para ayudar a los usuarios a entender el documento, o redactar los términos con sintaxis legible.

Filtración de datos — Una filtración de datos ocurre cuando una parte no autorizada adquiere acceso a la información del usuario que una empresa recopila, retiene o procesa de alguna manera, y que compromete la integridad, seguridad o confidencialidad de esa información.

Funcionalidad básica — Las funciones o características más esenciales de un producto o servicio. Por ejemplo, la funcionalidad básica de un smartphone incluiría hacer y recibir llamadas, mensajes de texto y correos electrónicos, descargar y ejecutar aplicaciones y acceder a internet.

Funcionario –Trabajador de jerarquía responsable de un conjunto explícito de riesgos e impactos, en este caso, privacidad y libertad de expresión.

Geolocalización — Identificación de la ubicación geográfica en el mundo real de un objeto, como una fuente de radar, teléfono móvil o terminal computacional conectada a internet. La geolocalización se puede referir a la práctica de evaluar la ubicación o a la propia ubicación evaluada.

Grupos de interés — Personas que tienen un "interés" porque de alguna manera se ven afectadas por las acciones o decisiones de una empresa. Nótese que interesado no es lo

mismo que “titulares de derechos” y que hay diferentes tipos de grupos de interés; los directamente afectados, e “grupos de interés intermediarios”, cuyo rol es defender los derechos de los grupos de interés directos. Los titulares de derechos son las personas cuyos derechos humanos pueden verse directamente impactados. Interactúan con la empresa y sus productos y servicios a diario, por lo general como trabajadores, clientes o usuarios. Los usuarios intermediarios incluyen a personas y organizaciones informadas y que pueden hablar en nombre de los titulares de derechos, como organizaciones de la sociedad civil, grupos activistas, académicos, formadores de opinión y diseñadores de políticas” (p. 10 de 28). Fuente: Compromiso de las partes interesadas en la revisión exhaustiva en materia de derechos humanos: desafíos y soluciones para empresas de TIC de BSR, septiembre de 2014:
http://www.bsr.org/reports/BSR_Rights_Holder_Engagement.pdf

Habilidades — Las habilidades son capacidades del asistente digital personal activadas por voz que permiten a los usuarios realizar algunas tareas o interactuar con contenido en línea usando dispositivos equipados con un asistente digital personal. Las habilidades de un ecosistema de asistente personal digital son similares a las aplicaciones del ecosistema móvil: los usuarios pueden habilitar o inhabilitar habilidades incorporadas o instalar habilidades elaboradas por terceros a través de tiendas similares a las tiendas de aplicaciones.

Identificación oficial — Documento oficial con o sin fotografía emitida oficialmente que puede usarse para probar la identidad de una persona. Esto incluye identificación oficial o cualquier otra forma de documentación que identifica a la persona por ubicación física, familia o comunidad. Esto también incluye números de teléfono, que en muchas jurisdicciones están conectados a la identidad fuera de línea de una persona.

Inferencia de datos — Las empresas pueden hacer inferencias y predicciones sobre los comportamientos, preferencias y vida privada de sus usuarios por medio del uso de analíticas de “grandes datos” y tecnologías algorítmicas de toma de decisiones. Estos métodos se pueden usar para hacer inferencias sobre preferencias o atributos del usuario (por ejemplo, raza, género, orientación sexual), opiniones (por ejemplo, posturas políticas), o para predecir comportamientos (por ejemplo, para presentar anuncios publicitarios). Sin suficiente transparencia y control del usuario sobre la inferencia de datos, los usuarios no pueden predecir, entender ni refutar las inferencias invasivas de la privacidad e inferencias no verificables. Ver: Wachter, Sandra y Mittelstadt, Brent. “Derecho a inferencias razonables: Reconsiderar la ley de protección de datos en la era de los grandes datos y la inteligencia artificial”, Columbia Business Law Review, 2019(2), https://ssrn.com/abstract=3248829.

Información del usuario — Todo dato relacionado con una persona identificable, o que se puede vincular a esa persona si se combinan conjuntos de datos o se utilizan técnicas de minería de datos. Como explicación adicional, la información del usuario son todos los datos que documentan las características o actividades de un usuario. Esta información puede estar o no vinculada a una cuenta de usuario específica. Esta información incluye,

sin limitarse a, correspondencia personal, contenido generado por el usuario, preferencias y configuraciones de cuenta, datos de registro y acceso, datos sobre las actividades o preferencias de un usuario recopilada de terceros, ya sea a través de rastreo de comportamiento o adquisición de datos, y todas las formas de metadatos. La información del usuario nunca se considera anónima, excepto cuando está incluida exclusivamente como base para generar mediciones globales (por ejemplo, número de usuarios activos por mes). Por ejemplo, la declaración: 'Nuestro servicio tiene un millón de usuarios activos por mes' contiene datos anónimos pues no da suficiente información para saber quiénes son ese millón de usuarios.

Información recopilada del usuario — Información del usuario que una empresa observa directamente o adquiere de un tercero.

Iniciativa multipartidaria — Una organización creíble formada por varios grupos de interés que incluye y está regida por miembros de al menos otros tres grupos interesados además de la industria: sociedad civil, inversionistas, académicos, representantes de usuarios o clientes en general, comunidad de técnicos y Gobierno. Su modelo de financiamiento se deriva de más de un tipo de fuente (empresas, Gobiernos, fundaciones, donaciones públicas, etc.). Su independencia, rigor y profesionalismo son muy altos, con fuerte participación de organizaciones de derechos humanos que tienen sólido historial de independencia de control corporativo y gubernamental. Global Network Initiative es un ejemplo de iniciativa multipartidaria dedicada a la libertad de expresión y la privacidad en el sector de tecnologías de la información y la comunicación.

Inteligencia artificial — La inteligencia artificial tiene una gran variedad de usos y significados. Para fines de la metodología de RDR, la inteligencia artificial se refiere a los sistemas que se parecen, llevan a cabo o imitan funciones que típicamente necesitan inteligencia. Los ejemplos incluyen software de reconocimiento facial, procesamiento natural del lenguaje y otros, y cuyo uso por las empresas de internet, móviles y de telecomunicaciones tienen consecuencias en los derechos de libertad de expresión y privacidad de las personas. Ver: https://privacyinternational.org/sites/default/files/2018-04/Privacy%20and%20Freedom%20of%20Expression%20%20In%20the%20Age%20of%20Artificial%20Intelligence.pdf

Investigador de seguridad — Alguien que estudia cómo garantizar los sistemas técnicos y las amenazas a la seguridad informática y de red para encontrar una solución.

Junta directiva —La supervisión a nivel directivo debe incluir a los miembros de la junta que tengan supervisión directa sobre los asuntos relacionados con la libertad de expresión y la privacidad. No tiene que ser un comité formal, pero la responsabilidad de los directivos de supervisar las prácticas de la empresa en estos asuntos debe estar claramente articulada y revelada en el sitio web de la empresa.

Marca automatizada — Marca que se origina con un sistema algorítmico. Ver también: marca enviada por humanos.

Medios no técnicos — Las empresas pueden adquirir información del usuario a través de medios no técnicos, como a través de compras, acuerdos de difusión de datos y otras relaciones contractuales con terceros. Estos datos adquiridos pueden volverse parte de un "expediente digital" que las pueden tener de sus usuarios, que luego pueden formar la base de información del usuario inferida y difundida.

Medios técnicos — Las empresas despliegan diversas tecnologías, como cookies, widgets y botones para rastrear la actividad de los usuarios en sus servicios y en sitios y servicios de terceros. Por ejemplo, una empresa puede insertar contenido en el sitio web de un tercero y recopilar información del usuario cuando un usuario pone "me gusta" o interactúa de otra manera con este contenido.

Mejora de software — Una mejora de software es una nueva versión de un software que ofrece una mejora o cambio significativo a la versión actual.

Métricas de participación — Números que describen la popularidad de un contenido o cuenta en la plataforma, por ejemplo, seguidores, conexiones, contactos, amigos, comentarios, "me gusta", retuiteos, etc.

Minimización de datos — Según el principio de minimización de datos, las empresas deben limitar la recopilación de información del usuario a lo que es relevante y necesario para lograr un objetivo claramente especificado. *Ver también: limitación de uso (ya definido).*

Modificaciones a un sistema operativo móvil — Cambios hechos a la versión estándar de un sistema operativo móvil que pueden afectar la funcionalidad básica, la experiencia del usuario o el proceso de mostrar actualizaciones de software. Las funcionalidades básicas son las funciones o características más esenciales de un producto o servicio. Por ejemplo, una funcionalidad básica de un smartphone incluye hacer y recibir llamadas telefónicas, mensajes de texto y correos electrónicos, descargar y ejecutar aplicaciones, y acceder a internet. Esto se aplica a smartphones Android fabricados por empresas además de Google.

Nivel gerencial —Comité, programa, equipo o funcionario que no es parte del directorio de la empresa ni del equipo ejecutivo.

No rastrear — También conocido por las siglas "DNT" (por la frase en inglés "Do not track"), se refiere a una configuración en las preferencias del navegador de un usuario que comunica a empresas o terceros que no lo "rastreen". En otras palabras, cada vez que un usuario abre un sitio web, se comunica a todas las partes involucradas en presentar la página (que suelen ser muchas, sobre todo anunciantes) que no recopilen ni guarden ninguna información de la visita del usuario a esa página. Sin embargo, es solamente una solicitud por cortesía, pues una empresa puede ignorar una solicitud de no rastrear, y muchas la ignoran.

Notificar / notificación — La empresa se comunica con los usuarios o informa a los usuarios sobre algo relacionado con la empresa o servicio.

Notificar directamente / notificación directa — Cuando una empresa cambia o actualiza sus políticas aplicables a un servicio en particular, tenemos la expectativa de que la empresa notifique a los usuarios de esos cambios a través del servicio. El método de notificación directa puede variar según el tipo de servicio. Para servicios que contengan cuentas de usuario, la notificación directa puede incluir el envío de un correo electrónico o mensaje de texto. Para servicios que no requieran una cuenta de usuario, la notificación directa puede incluir publicar un aviso destacado en la página principal en la que los usuarios acceden al servicio.

Opciones para controlar — La empresa brinda al usuario un mecanismo directo y fácil de entender para elegir o no elegir recopilación, uso o difusión de datos. "Elegir" (opt-in) significa que la empresa no recopila, usa ni difunde datos para un propósito determinado hasta que los usuarios señalen explícitamente que quieran que se haga. "No elegir" (opt-out) significa que la empresa usa los datos para un propósito determinado por defecto, pero que dejará de recopilar una vez que el usuario le diga a la empresa que deje de hacerlo. Nótese que esta definición es potencialmente controvertida, pues muchos defensores de la privacidad creen que solamente "elegir" constituye control aceptable. Sin embargo, para los propósitos de RDR, hemos elegido considerar "no elegir" como una forma de control.

Órdenes judiciales — Órdenes emitidas por un juzgado o corte, tanto en casos penales como civiles.

Parámetros de selección— Condiciones, por lo general establecidas por el anunciante, que determinan a qué usuarios se les mostrará el contenido publicitario en cuestión. Puede incluir demografía, ubicación, comportamiento, intereses, conexiones y otra información del usuario.

Parche — Pieza de software diseñada para actualizar un programa informativo o los datos de apoyo, para repararlo o mejorarlo. Esto incluye reparar las vulnerabilidades seguridad y otros fallos, con parches conocidos como *bugfixes* (reparación de fallos), y mejorar la facilidad de uso del programa computacional, aplicación o sistema operativo.

Participar / participación — Son las interacciones entre la empresa y los grupos de interés. Las empresas o grupos de interés pueden iniciar estas interacciones, y pueden tomar diversos formatos, incluidos mensajes, otra comunicación, etc.

Participación de los grupos de interés — Se refiere a las interacciones entre la empresa y los grupos de interés. Las empresas o los grupos de interés pueden iniciar estas interacciones, y pueden tomar diversos formatos, incluidas reuniones, otras comunicaciones, etc.

Petición — Para los objetivos de RDR, esta definición de peticiones incluye los procesos a través de los cuales los usuarios solicitan un cambio formal a una moderación de contenido o decisión de restringir una cuenta que hace una empresa.

Plataforma — En el sentido más general, una plataforma informática es toda pieza informática u objeto de código preexistente diseñado para ejecutarse según sus restricciones y que usa sus servicios. El término plataforma informática puede referirse a diferentes niveles de abstracción, incluida una arquitectura de hardware, un sistema operativo (OS) y bibliotecas de ejecución.[1] En total, se puede decir que es la etapa en que los programas informáticos se pueden ejecutar.

Plataformas digitales — Para los objetivos de la metodología del Índice RDR, las plataformas digitales se refieren a una categoría del Índice RDR que incluye internet y empresas de ecosistema móvil, así como empresas que operan servicios de comercio electrónico y ecosistemas de asistente digital personal.

Políticas de bots — Documento que resume las reglas que rigen el uso de bots de una empresa para generar contenido, divulgar contenido o realizar otras acciones. Pueden ser parte de los términos de servicio de una empresa u otro documento.

Políticas de contenido publicitario — Documentos que definen las reglas de una empresa que rigen qué contenido publicitario está permitido en la plataforma.

Políticas de elaboración de sistemas algorítmicos — Documentos que resumen las prácticas de una empresa relacionadas con la elaboración y pruebas de algoritmos, aprendizaje automático y toma de decisiones automatizadas.

Políticas de privacidad — Documentos que definen las prácticas de una empresa que incluyen la recopilación y uso de información, sobre todo información sobre los usuarios.

Políticas de publicidad dirigida — Documentos que definen las reglas de una empresa que rigen qué parámetros de publicidad dirigida están permitidos en la plataforma.

Políticas de uso de sistemas algorítmicos — Documentos que resumen las prácticas de una empresa que incluyen el uso de algoritmos, aprendizaje automático y la toma de decisiones automatizadas.

Priorización — La priorización ocurre cuando un operador de red "gestiona su red de una manera que beneficie un contenido, aplicaciones, servicios o dispositivos particulares" (p. 7 de 400). Para los propósitos de RDR, esta definición de priorización incluye la decisión de una empresa de bloquear el acceso a una aplicación, servicio o dispositivo particular. Fuente: Reglas de internet abierta de la Comisión Federal de Comunicaciones de Estados Unidos de 2015 (p. 7 de 400): https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf.

Procesos no oficiales — Procesos o canales a través de los cuales el Gobierno hace pedidos o solicitudes de restricciones de contenido o cuenta en vez de procesos oficiales, como ley o regulación. Por ejemplo, un funcionario local puede hacer una orden o protestar por algún contenido a través de un canal informal.

Procesos privados — Solicitudes hechas a través de un proceso privado más que un proceso judicial o gubernamental. Las solicitudes privadas de restricción de contenido pueden venir de un ente autorregulatorio como Internet Watch Foundation, o un sistema de notificación y cierre, como la Ley de Derechos de Autor de la Era Digital estadounidense. Para mayor información sobre la notificación y cierre, y también para la Ley de Derechos de Autor de la Era Digital específicamente, ver pp. 40-52 de 211 de "Fomentar la libertad en línea: el papel de los intermediarios de internet", UNESCO, http://unesdoc.unesco.org/images/0023/002311/231162e.pdf.

Las solicitudes privadas de datos de los usuarios suelen ser informales y no implican que exista un proceso legal formal. Según la Fundación Wikimedia, que elabora informes de transparencia que revelan datos sobre la cantidad de este tipo de solicitudes que recibe, las solicitudes privadas de información del usuario incluyen casos en los que otra empresa les envía una carta o correo electrónico en la que solicita "información no pública" sobre uno de sus usuarios. Esto podría incluir una dirección IP y correo electrónico del usuario.

Programa de calificación cero — "Calificación cero" se refiere a la práctica de no cobrar a los usuarios por datos usados para acceder a algunos servicios o plataformas en línea. La calificación cero es considerada una forma de priorización de la red que socava el principio de neutralidad de la red.

Programa de informantes — Programa a través del cual los trabajadores de las empresas pueden denunciar cualquier presunta actividad ilícita que vean dentro de la empresa, incluyendo asuntos relacionados con los derechos humanos. Suele tomar la forma de línea de ayuda anónima y suele ser responsabilidad de un jefe de cumplimento o jefe de conformidad.

Programador / programador de terceros — Persona, o grupo de personas, que crean un programa de software o aplicación que se distribuye a través de la tienda de aplicaciones de la empresa.

Protocolo — Conjunto de reglas que rigen el intercambio o la transmisión de datos entre dispositivos.

Publicidad dirigida — También se le conoce como "publicidad basada en intereses" o "publicidad personalizada", y se refiere a la práctica de transmitir anuncios a la medida a los usuarios según su historial de navegación, información de ubicación, perfiles y actividades en medios sociales, y características demográficas y otras funciones. La publicidad dirigida depende de prácticas de recopilación de muchos datos, que pueden

incluir rastrear las actividades de los usuarios por internet con cookies, widgets y otras herramientas de rastreo, para crear perfiles de usuario detallados.

Reclamo — RDR toma la definición de reclamo a partir de los Principios Rectores de Naciones Unidas sobre Negocios y Derechos Humanos: "percepción de una injusticia que afecte a los derechos reivindicados por una persona o grupo de personas sobre la base de una ley, un contrato, promesas explícitas o implícitas, prácticas tradicionales o nociones generales de justicia de las comunidades agraviadas" (p. 33 de 43.) Fuente: "Principios rectores sobre las empresas y los derechos humanos: Puesta en práctica del marco de Naciones Unidas para 'proteger, respetar y remediar'" 2011: https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_sp.pdf.

Recopilar / recopilación — Todos los medios a través de los cuales una empresa puede reunir información sobre los usuarios. Por ejemplo, una empresa puede recopilar esta información directamente en diversas situaciones, incluyendo cuando los usuarios publican contenido para difusión pública, enviar números de teléfono para verificación de cuentas, transmitir información personal en conversaciones privadas entre ellos, etc. Una empresa también puede recopilar esta información indirectamente, por ejemplo, con un archivo de datos de registro, información de la cuenta, metadatos y otra información relacionada que describa a los usuarios o documente sus actividades.

Red publicitaria — Empresa o servicio que conecta a anunciantes con sitios web que quieren alojar anuncios publicitarios. La función clave de una red publicitaria es agrupar la oferta de espacio publicitario de editores y hacerla coincidir con la demanda de anunciantes.

Registro de cambios — Registro que describe los cambios específicos en un documento, en este caso, un documento de términos de servicio o de política de privacidad.

Requerir — Requerimiento que puede ocurrir cuando un usuario se suscribe a una cuenta o más adelante, a solicitud de una empresa.

Restricción de contenido — Acción que toma la empresa que hace que un caso de contenido generado por el usuario se vuelva invisible o menos visible en la plataforma o servicio. Esta acción puede incluir eliminar el contenido totalmente o tomar una forma menos absoluta, como ocultarlo solamente a algunos usuarios (por ejemplo, habitantes de un país o personas menores de una determinada edad), lo que limita la capacidad de los usuarios a interactuar con ese contenido (con lo que sería imposible marcar "me gusta"), agregarle algo que lo contrarreste (por ejemplo, información correctiva sobre publicaciones contra las vacunas) o reducir la cantidad de amplificación que ofrecen los sistemas de conservación proporcionados por la plataforma.

Restricción de cuenta / restringir la cuenta de un usuario — Limitación, suspensión, desactivación, eliminación o cancelación de la cuenta o permisos de la cuenta de un usuario específico.

Retención de la información del usuario — Una empresa puede recopilar datos y luego eliminarlos. Si la empresa no los elimina, los datos quedan "retenidos". El tiempo entre la recopilación y eliminación es el "periodo de retención". Esos datos pueden caer dentro de nuestra definición de "información del usuario", o pueden ser anónimos. Hay que tener en cuenta que los datos realmente anónimos de ninguna manera se pueden relacionar con un usuario, identidad, comportamiento o preferencia de un usuario, lo cual es algo que no suele suceder.

Revelar claramente — La empresa presenta o explica sus políticas o prácticas en sus materiales visibles para el público de una forma que sea fácil de encontrar y comprender para los usuarios.

Riesgos de ciberseguridad —Situaciones en las que la seguridad, privacidad u otros derechos relacionados de un usuario pueden verse amenazados por un actor malicioso (como, por ejemplo, delincuentes, informantes o Estados) que pueden obtener acceso no autorizado a datos del usuario por medio de hackeo, *phishing* u otras técnicas engañosas.

Secretismo hacia adelante / secretismo perfecto hacia adelante — Método de encriptación usado sobre todo en el tráfico web HTTPS y en aplicaciones de mensajería, en el que se genera un nuevo par de llaves para cada sesión (HTTPS), o para cada mensaje intercambiado entre las partes (aplicaciones de mensajería). De esta manera, si un adversario obtiene una llave de desencriptación, no podrá desencriptar transmisiones anteriores o futuras ni mensajes en la conversación. El secreto hacia adelante es diferente a la encriptación de extremo a extremo, que se refiere a datos que se encriptan mientras "descansan" en servidores remotos de la empresa. Para leer más, visita "Presionar para secreto perfecto hacia adelante", de Electronic Frontier Foundation.

Señales generadas por el usuario — Muchas empresas permiten a los usuarios "elegir no usar" el rastreo por medio de la configuración de diversas cookies específicas para la empresa. Si un usuario elimina cookies para proteger la privacidad, entonces se le rastrea hasta que vuelve a configurar la cookie de "elegir no usar". Además, algunas empresas pueden solicitar a un usuario que instale un componente adicional para el navegador para impedir el rastreo. Esos dos escenarios comunes son ejemplos de usuarios que se ven obligados a usar señales que son específicas para la empresa, y por lo tanto no cuentan. En cambio, una señal generada por el usuario viene del usuario y es un mensaje universal de que el usuario no debe ser rastreado. La primera opción para las señales generadas por el usuario es el encabezado "No rastrear" (referido antes), pero esta redacción deja la puerta abierta a medios futuros para que los usuarios señalen que no quieren ser rastreados.

Señalización hecha por humanos — Señalización originada por un ser humano, el cual puede ser un usuario, trabajador o contratista de empresa, trabajador o representante gubernamental, o trabajador o representante humano de una entidad privada. Ver también: señalización automatizada.

Señalizador — Persona o entidad que alerta a una empresa que un contenido o cuenta puede estar violando las reglas de la empresa. Este proceso puede ocurrir dentro de la plataforma o a través de un proceso externo. Los señalizadores incluyen a usuarios, sistemas algorítmicos, personal de la empresa, Gobiernos y otras entidades privadas.

Señalizar — Proceso de alertar a una empresa de que un contenido o cuenta puede estar violando las reglas de la empresa, o la señal que transmite esta información a la empresa. Este proceso puede ocurrir dentro de la plataforma o a través de un proceso externo. Los señalizadores incluyen a usuarios, sistemas algorítmicos, personal de la empresa, Gobiernos y otras entidades privadas.

Sin contenido — Datos sobre un caso de comunicación o sobre un usuario. Las empresas pueden usar diferentes términos para referirse a estos datos, como metadatos, información básica del suscriptor, datos de transacción sin contenido, datos de cuenta o información del cliente.

En Estados Unidos, la Ley de Comunicaciones Almacenadas define las comunicaciones o los registros del cliente sin contenido como "nombre, dirección, registros de conexión telefónica local y de larga distancia o registros de hora y duración de sesiones; duración del servicio (incluida fecha de inicio) y tipos de servicio utilizado; número de teléfono o instrumento u otro número de identidad del suscriptor (incluida toda dirección de red temporalmente asignada), y medios y fuentes de pago por el servicio (incluido todo número de tarjeta de crédito o cuenta bancaria)". El Manual sobre la ley europea de protección de datos de la Unión Europea afirma: "La confidencialidad de las comunicaciones electrónicas concierne al contenido de una comunicación y también a datos de tráfico, como la información de quién se comunica con quién, cuándo y cuánto tiempo, y datos de ubicación, como desde dónde se comunicaron esos datos". Ver:
"Título 18 del Código § 2703 de Estados Unidos. Revelación requerida de comunicaciones o registros de clientes", Instituto de Información Legal de la Facultad de Derecho de Cornell, https://www.law.cornell.edu/uscode/text/18/2703.
"Manual sobre ley europea de protección de datos", Corte Europea de Derechos Humanos, https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf.

Sistema algorítmico — Sistema que usa algoritmos, aprendizaje automático o tecnologías relacionadas para automatizar, optimizar o personalizar procesos de toma de decisiones.

Sistema algorítmico de conservación, recomendación y clasificación de contenido — Sistema que usa algoritmos, aprendizaje automático y otros sistemas de toma de decisiones automatizadas para gestionar, dar forma y regir el flujo de contenido e información en una plataforma, por lo general hecho de una forma personalizada para cada usuario individual.

Sistema operativo — Software que respalda las funciones básicas de una computadora, como la programación de tareas, ejecución de aplicaciones y control de unidades periféricas. Un sistema operativo móvil es el sistema operativo de un dispositivo móvil, como smartphone o tablet.

Software malicioso / malware — Término amplio usado para referirse a diversas formas de software hostil o invasivo, como virus informáticos, gusanos, troyanos, *ransomware*, software espía, software publicitario o *adware*, *scareware* y otros programas maliciosos. Puede tomar la forma de código ejecutable, texto, contenido activo u otro software.

Solicitudes gubernamentales — Incluye solicitudes de ministerios o agencias estatales, autoridades y órdenes judiciales en casos penales y civiles.

Solicitudes gubernamentales no judiciales — Solicitudes que vienen de entidades gubernamentales que no son entes judiciales, juzgados ni cortes. Pueden incluir solicitudes de ministerios, agencias, departamentos de Policía, agentes policiales (que actúen en calidad oficial) y otras oficinas, autoridades o entes gubernamentales no judiciales.

Solución — "La solución puede incluir disculpas, restitución, rehabilitación, compensación financiera o no financiera y sanciones punitivas (ya sean penales o administrativas, como multas), y también la prevención de daños a través de mandatos judiciales o garantías de no repetición, por ejemplo. Los procedimientos para la disposición de soluciones deben ser imparciales, estar protegidas de corrupción y libres de intentos políticos o de otra índole que puedan influir en el resultado" (p. 22 de 27).

Fuente: "Informe del representante especial del secretario general en asuntos de derechos humanos y empresas transnacionales y otras empresas, John Ruggie. Principios rectores en negocios y derechos humanos: Implementando el marco de trabajo de Naciones Unidas: 'Protección, respeto y solución", 2011.
http://business-humanrights.org/sites/default/files/media/documents/ruggie/ruggie-guiding-principles-21-mar-2011.pdf

Supervisión / supervisar — Ya sean los documentos de gobernabilidad de la empresa o los procesos de toma de decisiones asignan a un comité, programa, equipo o funcionario la autoridad formal de supervisar con una función particular. Este grupo o persona tiene la responsabilidad de realizar esta función y se evalúa según el grado con el que cumple esa responsabilidad.

Supervisión a nivel ejecutivo — El comité ejecutivo o un miembro del equipo ejecutivo de una empresa supervisa directamente los asuntos relacionados con la libertad de expresión y la privacidad.

Tecnologías publicitarias — Son los sistemas algorítmicos de la toma de decisiones que determinan a qué usuarios se les mostrará un contenido publicitario específico. Esta determinación puede tener en cuenta los parámetros de selección fijados por el anunciante, o pueden ser totalmente automatizados.

Tienda de aplicaciones —Plataforma a través de la cual una empresa hace que sus propias aplicaciones y las creadas por programadores de terceros estén disponibles para ser

descargados. Una tienda de aplicaciones (o mercado de aplicaciones) es una plataforma de distribución digital para software de computadora, a menudo en un contexto móvil.

Tienda de habilidades —Plataforma a través de la cual una empresa hace disponibles para descarga sus propias habilidades, así como las creadas por terceros programadores. Una tienda de habilidades (o mercado de habilidades) es una forma de plataforma de distribución digital para software informático.

Toma de decisiones automatizadas — Tecnología que toma decisiones sin supervisión o aporte humano significativo en el proceso de toma de decisiones, como a través del uso de inteligencia artificial o algoritmos.

Terceros – "Parte" o entidad diferente al usuario o la empresa. Para los propósitos de esta metodología, los terceros pueden incluir organizaciones gubernamentales, cortes u otros privados (por ejemplo, una empresa, una ONG o una persona individual).

Términos de servicio — También se le puede llamar términos de uso, términos y condiciones, etc. Los términos de servicio "a menudo brindan los principios básicos necesarios de cómo se deben usar diversos servicios en línea", como establece EFF, y representan un acuerdo legal entre la empresa y el usuario. Las empresas pueden tomar acciones contra los usuarios y su contenido basándose en la información en los términos del servicio. Fuente: Electronic Frontier Foundation, "Términos de (ab)uso" https://www.eff.org/issues/terms-of-abuse

Uso/ limitación de objetivo — Según el principio de minimización de uso u objetivo, las entidades que gestionan la información del usuario deben declarar su objetivo de hacerlo así y deben limitar el uso de esta información a cualquier otro objetivo a menos que reciban el consentimiento del usuario. *Ver también el principio de minimización de datos (arriba).*

Usuario afectado — El usuario que publicó un contenido que fue restringido por una acción de moderación o el usuario asociado con una cuenta de usuario que fue restringida por una acción de moderación y, en caso de ser aplicable, el usuario que emitió la marca que llevó a considerar ese contenido o cuenta para una acción de moderación.

Un tema relacionado es el "periodo de retención". Por ejemplo, una empresa puede recopilar datos de registro continuamente, pero purga (elimina) los datos una vez por semana. En este caso, el periodo de retención de datos es de una semana. Sin embargo, si no se especifica el periodo de retención, se debe asumir por defecto que los datos no se eliminan nunca, y el periodo de retención es indefinido. En muchos casos, los usuarios pueden querer que se retengan sus datos mientras usen activamente el servicio, pero querrían que se eliminaran (por lo tanto, que no se retuvieran) cuando dejaran de usar el servicio, si es que dejaran de usarlo. Por ejemplo, los usuarios pueden querer que el servicio de una red social conserve todos sus mensajes privados, pero cuando el usuario sale de la red puede querer que todos sus mensajes privados se eliminen.

Usuarios — Personas que usan un producto o servicio. Incluye personas que publican o transmiten contenido en línea, y también a quienes tratan de acceder o recibir el contenido. Para los indicadores de la categoría de libertad de expresión, esto incluye programadores de terceros que crean aplicaciones que están alojadas o se distribuyen a través del producto o servicio de una empresa.

Vulnerabilidad de seguridad — Debilidad que permite a un atacante reducir la seguridad de la información de un sistema. Una vulnerabilidad es la intersección de tres elementos: susceptibilidad o defecto de un sistema, acceso de un atacante al defecto y capacidad de atacante de explotar el defecto.

Widget — Parte de un código que permite a un usuario o una empresa insertar aplicaciones y contenido de un sitio web o servicio en el sitio o servicio de un tercero. En algunos casos, las empresas usan widgets en el sitio web de un tercero y recopilan información sobre los visitantes de ese sitio web sin su conocimiento.

Ranking Digital Rights