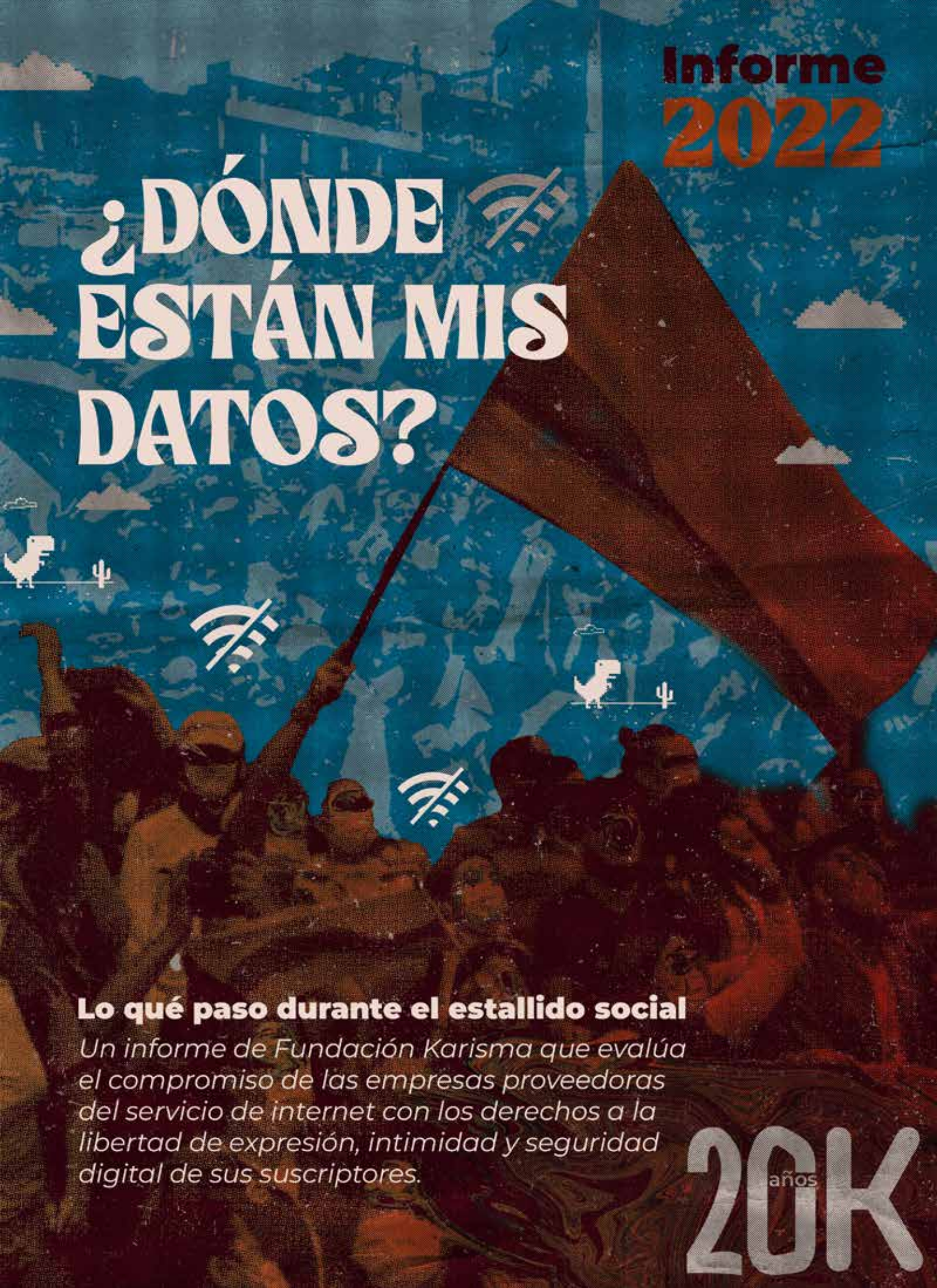


Informe
2022

¿DÓNDE ESTÁN MIS DATOS?

Lo qué paso durante el estallido social

Un informe de Fundación Karisma que evalúa el compromiso de las empresas proveedoras del servicio de internet con los derechos a la libertad de expresión, intimidad y seguridad digital de sus suscriptores.

20K años

Un informe de:

Fundación Karisma 20 años

Autores:
Carolina Botero Cabrera
María Alejandra Medina
Investigación:
María Alejandra Medina
Revisión:
Alejandra Martínez
Diagramación y diseño gráfico:
Daniela Moreno
Carolina Salazar

Bogotá, Colombia

Marzo de 2023

INFORME
2022

¿Dónde están mis datos?

Resumen ejecutivo

El 2021 no solo fue un año de reapertura económica y de transición post pandemia; también estuvo marcado por el paro nacional y el intenso ciclo de movilizaciones y protestas sociales a lo largo y ancho del país. En este contexto, sin precedentes recientes, la séptima edición de este, nuestro informe anual *"¿Dónde están mis datos?",* ofrece una mirada adicional a la habitual e incorpora asuntos sobre el papel de los proveedores de servicios de internet (PSI) en escenarios de crisis y transformación social.

Más allá de esta decisión metodológica, ratificamos la necesidad de mantener los ejes de evaluación sobre los compromisos de los PSI. Para este informe, evaluamos a Claro, Movistar, ETB, EmCali, UNE-Tigo, Directv; también a Hughesnet y Skynet por segundo año consecutivo, y por primera vez a Wom, anteriormente Avantel. Compromisos en materia de transparencia, libertad de expresión, intimidad y seguridad digital. Así como en nuestra versión anterior integramos nuevos ejes para documentar la forma en que las medidas desplegadas por el gobierno nacional para la contención de la pandemia impactaron en los compromisos de las empresas, este año damos una una mirada sobre contextos especiales como la movilización social.

En esa oportunidad, también analizamos cómo los PSI evolucionaron frente a estos criterios y a las recomendaciones formuladas en informes pasados. Sobre el desempeño de 2021 vimos que en relación con criterios de evaluación tradicionales no se presentaron muchos cambios, mientras que en algunos criterios nuevos si evidenciamos algunos retrocesos.

Para esta última versión de ¿Dónde están mis datos?, varias empresas mantuvieron su desempeño, incluso aquellas que todavía no reportan información evaluada por este informe en su informe anual de transparencia, o de políticas de protección de datos con mínimos que están previstos en la ley. Las novedades más relevantes fueron documentadas en torno a neutralidad de la red, acceso directo, en información sobre solicitudes de gobierno.

1. Los resultados del informe

Para la evaluación de 2022 subimos el nivel de exigencia para los indicadores de publicidad (en el sentido de hacer pública la información) y claridad en todos los ejes temáticos.

En esta oportunidad la empresa que mejor puntaje obtuvo, en general, fue Movistar, seguida por Tigo y posteriormente por ETB y Claro que comparten un puntaje similar.

TABLA GENERAL

Tabla evaluación desempeño en 2021

	Claro	EMCALI	Movistar	tigo	eTb	DIRECTV	WOM	HughesNet	SkyNet
COMPROMISOS POLÍTICOS	2	2	4	3	2	3	0	0	0
INTIMIDAD	1	0	3	2	1	2	1	0	0
LIBERTAD DE EXPRESIÓN	3	1	4	2	3	1	3	2	0
SEGURIDAD DIGITAL	3	2	4	4	3	2	2	2	2

1 COMPROMISOS POLÍTICOS

TABLA GENERAL

Tabla evaluación desempeño en 2021

	Claro	EMCALI	Movistar	tigo	eTb	DIRECTV	WOM	HughesNet	SkyNet
COMPROMISOS POLÍTICOS	2	2	4	3	2	3	0	0	0
1.1. Política de género									
1.2. Política de accesibilidad									
1.3. Informes de transparencia									

2 INTIMIDAD

TABLA GENERAL

Tabla evaluación desempeño en 2021

	Claro	EMCALI	Movistar	tigo	eTb	DIRECTV	WOM	HughesNet	SkyNet
INTIMIDAD	1	0	3	2	1	2	1	0	0
2.1. Políticas de protección de datos									
2.2. Informa la obligación legal de retención de datos									
2.3 Acceso directo									
2.4. Informa las razones para responder a solicitudes de información del sector público									
2.5. Procedimiento de entrega de datos al sector público									
2.6. Notifica a las personas sobre la entrega de datos a entidades públicas									
2.7 Criterios para el tratamiento de datos en relación con aliados comerciales									

TABLA GENERAL

Tabla evaluación desempeño en 2021

3 LIBERTAD DE EXPRESIÓN

	Claro	EMCALI	Movistar	tigo	eTb	DIRECTV	WOM	HughesNet	SkyNet
LIBERTAD DE EXPRESIÓN	3	1	4	2	3	1	3	2	0
3.1. Informa sobre la obligación legal de bloqueo									
3.2 Procedimientos de bloqueo (incluye obligación contractual)									
3.3. Guía sobre comportamientos no permitidos									

4 SEGURIDAD DIGITAL

TABLA GENERAL

Tabla evaluación desempeño en 2021

	Claro	EMCALI	Movistar	tigo	eTb	DIRECTV	WOM	HughesNet	SkyNet
SEGURIDAD DIGITAL	3	2	4	4	3	2	2	2	2
4.1. Informa de fuga de datos personales y acciones de mitigación									
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web									

1.1. Compromisos políticos

En materia de género y accesibilidad se destacan particularmente Movistar y Tigo, seguidos de DirecTV.

En relación con los informes de transparencia, Movistar y Tigo obtienen el mejor puntaje. Informan sobre todos los criterios esperados y de forma desagregada. ETB, Claro y DirecTV mantienen el mismo puntaje del año anterior en este criterio.

En relación con la neutralidad de la red, destacamos los casos de Movistar, Tigo, Wom y Hughesnet que además de publicar sus prácticas de gestión del tráfico, con el fin de asegurar la calidad en sus servicios y la seguridad, hacen expreso su compromiso por proteger dicho principio. Sin embargo, ninguna empresa hizo referencia, en los documentos revisados, a la aplicación de este compromiso en relación con las caídas de internet y las solicitudes del Estado durante un año de movilización social y Paro Nacional.

1.2. Intimidad

En el primer criterio de evaluación sobre protección de datos debemos indicar que en comparación con los hallazgos del año anterior no se produjeron cambios, por tanto Movistar, Tigo, DirecTV y Wom recibieron el mejor puntaje, seguidos por Claro, ETB y Hughesnet con el mismo puntaje.

Sobre la evaluación en materia de retención de datos tanto Movistar como Tigo informan que están obligadas por ley a retener datos en indicación del marco legal, mientras que ETB menciona en su política de tratamiento de datos que retiene datos sin indicación del marco legal. Así como ETB y DirecTV mejoraron en cuanto a qué tipo de datos retienen. La mayoría de las empresas, excepto Movistar, no dicen o no son claras respecto al tiempo en el que retienen datos.

En relación a si informan a las personas usuarias de los servicios de estas empresas sobre la existencia del acceso directo que efectúa la Fiscalía General de la Nación para interceptar comunicaciones, resaltamos que en este criterio de evaluación se destaca el caso de Movistar por la claridad en la información que entrega de este tema. También identificamos que después

de haberlo reportado durante varios años, Claro y Tigo no reportaron esta información para este período de evaluación.

En relación con las solicitudes de datos por parte de entidades públicas, procedimiento de entrega y notificación a las personas sobre dichos eventos, durante el 2021 los PSI no efectuaron cambios significativos en sus políticas y procesos sobre entrega de datos en comparación con la información que ya ofrecían. En estos criterios destacamos a DirecTV y a Movistar; ambas sobresalen por sus avances en términos de claridad y publicidad de estos procesos. Adicionalmente ninguna PSI reportó, relacionó o se pronunció sobre riesgos o afectaciones a la privacidad de las personas usuarias de los servicios en consecuencia del contexto de movilización social en el país.

1.3. Libertad de expresión

En materia de libertad de expresión la evaluación muestra que los PSI tienen una menor gestión comparado con lo que hacen en materia de protección de la privacidad de las personas usuarias. En este eje se analiza la forma como los PSI enfrentan la obligación legal de bloqueo de contenidos en internet y el procedimiento que siguen. En nuestra revisión encontramos que Claro, Movistar, Tigo, ETB y Wom informan sobre la ejecución de órdenes de bloqueo de sitios web o URL.

EMCALI y Hughesnet informan que bloquean sitios web o URL solo en el caso de circulación de contenido de abuso sexual infantil. Skynet no provee información sobre ninguno de estos criterios.

Encontramos que ningún PSI informó sobre las solicitudes del gobierno de bloqueo o las caídas de internet que se relacionarán con los contextos de movilización social, solo Tigo reportó un hito en el número agregado de solicitudes de bloqueo en junio de 2021, pero no brinda información adicional sobre este aumento por lo que no es posible indagar la causa.

1.4 Seguridad digital

Encontramos que todos los PSI evaluados han implementado el protocolo https en sus sitios web.

De otra parte, en relación con la evaluación sobre si las compañías informan las fugas de datos personales y acciones de mitigación en caso de que se presenten, si tienen protocolos de notificación a las autoridades cuando suceden fallas de seguridad que comprometen los datos personales de las personas usuarias de los servicios, así como si las notifican sobre estos sucesos luego de que hayan desplegado las debidas medidas de mitigación, encontramos que Movistar y Tigo son las únicas que cuentan con un protocolo y documentación para realizar acciones de mitigación y bloqueos. Mientras que Claro y ETB describen medidas de seguridad de forma general pero no proveen información concreta sobre mitigación de riesgos o seguimiento a estas contingencias.

2. Mantuvimos los criterios para evaluar la evolución en transparencia

Es necesario recordar que en 2020 subimos los niveles de exigencia para (i) contenido del informe de transparencia, (ii) los mínimos aceptables en la políticas de tratamiento de datos, (iii) en los procesos de entrega de datos al sector público, (iv) en materia de bloqueos y su procedimiento. Haber subido los estándares afectó la calificación que todas las empresas recibían. Para 2021 añadimos nuevos criterios en el eje de transparencia (neutralidad de la red) e intimidad (acceso directo). En 2022 la metodología para este eje no surtió ningún cambio, lo que permitió hacer una trazabilidad y comparabilidad con los criterios específicos introducidos en el 2020 y en el 2021.

Índice]

Sobre el informe

El 2021 estuvo marcado por jornadas de protesta y movilización social que se retomaron el 28 de abril, tras el paro nacional de 2019- 2020, y que se extendieron durante el resto del año. El "estallido social", nombre que acuñó la opinión pública nacional para denominar al paro nacional y las movilizaciones, se caracterizó por una grave crisis de los derechos humanos ante las graves violaciones a la libertad de expresión, la violencia contra periodistas, el uso de la fuerza y la falta de debida diligencia, la violencia basada en género, la violencia étnico-racial, irregularidades en el debido proceso y denuncias de desaparición, principalmente entre abril y junio de 2021.

La Comisión Interamericana de Derechos Humanos (CIDH) presentó un informe de "Observaciones y recomendaciones de la visita de trabajo de la CIDH a Colombia"[1] realizada del 8 al 10 de junio de 2021 en el que documentó una larga lista de observadas violaciones a los derechos humanos y los obstáculos identificados para la garantía del derecho de protesta, en el que incluyeron consideraciones sobre Internet como espacio de protesta.

Se reconoció a internet como instrumento para "desplegar el potencial del derecho a la libertad de expresión y el acceso a la información durante las protestas", "como medio de interacción y organización para aquellas personas que salieron a manifestarse", como herramienta para "comunicar incidentes y hacer denuncias abiertas, muchas veces en tiempo real, sobre posibles excesos en el uso de la fuerza, además de solicitar la protección de sus derechos".

Al mismo tiempo, la CIDH conoció de "prácticas de "ciberpatrullaje" orientadas a un monitoreo proactivo de contenidos presuntamente falsos sobre el desarrollo de las protestas". Ante la CIDH el Estado reportó la identificación -y posiblemente la solicitud de bloqueo- a "al menos 154 noticias falsas y más de 2.300 publicaciones que contienen amenazas a la vida o la integridad física". Situación frente a la cual la Comisión

1 Disponible en https://www.oas.org/es/cidh/informes/pdfs/ObservacionesVisita_cidh_Colombia_spA.pdf

manifestó la preocupación ante “perfilamiento de personas usuarias de redes sociales”, “interrupciones del servicio de Internet en el contexto de las protestas”, solicitudes de bloqueo desproporcionadas y falta de un marco jurídico para solicitar el bloqueo de dichos contenidos.

La movilización social significó una presión sobre la Internet que se reflejó por ejemplo en la necesidad de acceso a la información, se materializó para muchas personas en la preocupación por censura y bloqueo de contenidos en internet, también, la preocupación por la vigilancia del estado desproporcionada y la necesidad de transparencia frente a las razones de las caídas de internet durante las protestas. Adicionalmente, en Colombia, la tecnología se consolidó como herramienta de denuncia y difusión de información sobre lo que sucedía en las calles.

En mayo de 2022, la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos publicó el informe “Interrupciones del acceso a Internet: tendencias, causas, implicaciones jurídicas y efectos en una serie de derechos humanos”[2] sobre el fenómeno de las caídas de Internet, analizando cuándo y por qué estos son impuestos y examinando cómo llegan a socavar una serie de derechos humanos, principalmente el derecho a la libertad de expresión. De acuerdo con este Informe, “casi la mitad de todas las caídas de internet registradas por grupos de la sociedad civil durante los últimos seis años fueron aplicadas durante protestas y en medio de tensiones políticas para sofocar las manifestaciones acerca de un enorme abanico de reivindicaciones sociales, políticas y económicas”.

Desde la Fundación Karisma mediante este informe, sumándonos a otras organizaciones a nivel internacional, hacemos un llamado a la transparencia en contextos de protesta dado que hay presiones por parte de los Estados para restringir la libertad de expresión, acceder de manera irregular a datos y conducir a violaciones de otros derechos humanos.

2 En cumplimiento de la resolución 47/16 del Consejo de Derechos Humanos. Disponible en https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/341/58/PDF/G2234158.pdf? Open Element

¿Dónde están mis datos? Vistazo a nuestro informe

Como ha hecho cada año desde 2016 la Fundación Karisma publica nuevamente su informe "¿Dónde están mis datos?" con el que se propone analizar cómo las principales empresas proveedoras del servicio de internet y telefonía celular en Colombia dicen cumplir sus obligaciones en materia de derechos humanos. Se trata de un ejercicio que es replicado por otros países de la región y a nivel internacional por organizaciones especializadas en derechos humanos.[3]

Desde entonces, el objetivo de este informe ha sido proveer una herramienta que facilite a las personas usuarias el proceso de toma de decisión cuando contratan dichos servicios, y además ofrecer un instrumento que facilite la comprensión de aspectos de la tecnología que cada vez más deben ser de interés general para las personas.

"¿Dónde están mis datos?" analiza cómo protegen nuestros derechos a la libertad de expresión, intimidad y seguridad digital las siete compañías de internet y telefonía celular más importantes en el país: Claro, Movistar, Tigo, Etb, DirecTv, Emcali, Wom así como las empresas de internet satelital Hughesnet y Skynet por su rol para conectar a la ruralidad.

El informe evalúa lo que estas compañías dicen hacer a la hora de respetar el ejercicio de los derechos de las personas que usan sus servicios. No se pretende verificar si en efecto cumplen lo que dicen hacer.

Queremos agradecer a las empresas que hicieron esfuerzos adicionales para atender las recomendaciones de nuestro informe en versiones anteriores, que apuntan, tal y como hemos sostenido en estos últimos siete años, a fortalecer conjuntamente el ejercicio de derechos en internet cuando se apoya en actores que juegan un rol determinante en su realización: los proveedores de acceso a internet.

3 Nos referimos en concreto a los informes de la Electronic Frontier Foundation titulado "Who has your back?" y el informe anual de Ranking Digital Rights titulado "The Ranking Digital Rights Telco Giants Scorecard 2022".

Principales hallazgos

Tal y como anunciamos anteriormente en esta, la séptima versión del informe, mantuvimos los actores evaluados y los criterios de evaluación para así identificar la evolución en los diferentes ejes evaluados en el sector de proveedoras del servicio de internet. Solo cambió Avantel que ahora es Wom, sobre las demás compañías proveeremos un comparativo sobre su desempeño, no sin antes dejar de recordar que nuestra evaluación se orienta en la revisión del contenido de políticas, documentos y compromisos públicos que se encuentran disponibles en los sitios web de cada proveedor de acceso a internet. La metodología no permite establecer si los compromisos se cumplen.

En la edición de este año al tiempo que evaluaremos a los PSI, mencionaremos casos que documentamos durante el año en el que se reactivó significativamente la movilización social en Colombia y la revisión de la implementación progresiva de mejoras en dichas políticas y documentos en aras de garantizar plenamente los derechos de las personas suscriptoras de sus servicios. Dicha documentación la incluiremos, cuando aplique, en una sección *de contexto e interés*.

1. Eje de compromisos políticos

1.1. Políticas de género y políticas de accesibilidad

Buscamos incentivar y reconocer buenas prácticas de los PSI en materia de equidad de género, promoción y respeto por la diversidad. Valoramos positivamente las compañías que se comprometen mediante políticas, programas y prácticas con la inclusión y la equidad. Estamos convencidas de que solo las empresas que tienen este tipo de medidas pueden abordar los desafíos en materia de la tecnología en un ambiente más equitativo.

En dicha evaluación verificamos si, por ejemplo, los PSI cuentan con políticas sobre selección y contratación de su personal que activamente promueva la selección de mujeres así como de poblaciones y comunidades minoritarias o

diversas en el sector de las Tecnologías de la Información y las Comunicaciones (TIC). Si cuentan con políticas de desarrollo de carreras y capacitación de su personal, si tienen políticas favorables al equilibrio familiar y laboral, así como políticas dedicadas a prevenir y gestionar casos de abuso y acoso sexual en el trabajo, y la promoción de imágenes publicitarias no sexistas.

En materia de accesibilidad buscamos identificar políticas que explícitamente declaren el compromiso del PSI con la promoción e implementación de ajustes razonables, en el marco de sus operaciones internas como en la oferta de sus servicios comerciales, que integren especialmente a las personas con discapacidad y les permita el acceso y consulta de los contenidos que publican estas compañías en sus sitios web.

En materia de género, se destacan particularmente **Claro** y **Movistar**, seguidos por **Tigo**, **ETB** y **DirecTV** que comparten un puntaje similar. En accesibilidad , lo hacen **Movistar** y **Emcali**, seguidos por **DirecTV**. En comparación con el año anterior, no hubo un cambio significativo en este criterio, algunas compañías que ya tenían buenas prácticas reforzaron sus políticas y programas con enfoque de género, mientras que las compañías que no tenían estos compromisos en el 2020, siguen sin avanzar en su adopción para el 2021.

Para 2021, **Claro,** mantiene en la actualización de su Código de Ética, acciones para garantizar la adopción de mejores prácticas laborales que promuevan el empleo inclusivo, la equidad de género y la diversidad. Por ejemplo, campañas sobre la importancia del respeto a los Derechos Humanos, la inclusión laboral, la diversidad y la igualdad de género, la igualdad de oportunidades, principios de no violencia basada en el género ni acoso, y la inclusión en el lugar de trabajo sin discriminación.

Movistar publica diversas políticas que abordan por completo los ítems evaluados como conciliación de la vida personal y laboral, ambiente de trabajo libre de acoso y discriminación, lenguaje y comunicación inclusiva, no sexista o discriminatoria, entre otras.

Por su parte, **DirecTV** en comparación con el desempeño de 2020, mejoró en criterios específicos como carreras con

enfoque de género y equilibrio familiar laboral, además tiene planes de trabajo para ampliar la representación de grupos LGBTI, de personas con discapacidad y mujeres tanto en sus operaciones como en su comunidad de personas usuarias. Sin duda, la inclusión y los compromisos de las compañías deben avanzar a la inclusión de grupos vulnerables que enfrentan barreras para insertarse en el mercado laboral, como es la comunidad LGBTQ+, y un enfoque de género más amplio, tal y como lo advertimos en el informe anterior.

Movistar, **Tigo UNE** y **Emcali** recibieron puntaje favorable por hacer disponible en su sitio web la configuración accesible para personas con limitación visual. Sin embargo, solo **Movistar** se compromete explícitamente con la accesibilidad para la interacción de las personas usuarias con sus productos, por ejemplo para personas con discapacidad auditiva ofrecen video atención con intérprete en lengua de señas, online, desde móvil o computador. **Claro** no recibe puntaje, pero se reconoce que implementaron en unos de sus productos asistentes de voz.

Las empresas podrían avanzar con compromisos sobre la accesibilidad, como parte de sus apuestas a la inclusión, dado que se espera que mejoren en el acceso igualitario a la información y los servicios ya no solo para personas con discapacidades física, sino también con diferencias en la manera de pensar y aprender, no solo en el diseño de sus páginas web sino también en sus productos.

1.2. Informes de transparencia

La ley colombiana no obliga a los PSI a presentar informes de transparencia o informes periódicos, está práctica se mantiene como voluntad de las empresas. Sin embargo, las exigencias del Estado y de la sociedad civil en materia de responsabilidad empresarial, en particular en materia de derechos humanos, ha ido en aumento. Efectivamente, es innegable que la actual tendencia regulatoria global hacía la regulación del sector de las telecomunicaciones tiene como uno de sus principios la transparencia y por tanto, un importante rol del reporte de información y los informes de transparencia de los PSI.

Para las empresas del sector privado que facilitan la tecnología

digital, los informes de transparencia se han convertido en el instrumento por excelencia para responder por su responsabilidad corporativa respecto del impacto de los derechos humanos. Los Principios Guías para los Negocios y los Derechos Humanos[4] de la Organización de las Naciones Unidas (UNGP por su sigla en inglés) se ha convertido en el marco en el cual desarrollan obligaciones para estas empresas.

Los informes de transparencia se encuentran en una etapa de transformación rápida, no solo por el número y la diversidad de reportes, sino también por el aumento en el debate público y académico sobre cuáles pueden ser las buenas prácticas para su reporte. Además, hay una tendencia regulatoria de los Estados para generar obligaciones legales a las empresas intermediarias de internet como vimos recientemente en el Digital Service Act Package -DSA- en Europa y que antes ya habían intentado países como México, es frecuente que en esas propuestas regulatorias los informes de transparencia tengan un rol.

Las razones por las que una compañía opta por elaborar un informe de transparencia pueden ser diversas: y entre ellas puede que quieran señalar los valores de la empresa, aliviar los temores sobre su impacto en la privacidad y la libertad de expresión, concienciar a diferentes actores sobre este tema, afianzar la rendición de cuentas, también puede tener como fin competir con otras empresas[5]. En todo caso, es en los UNGP donde encontramos la obligación derivada de normas de derecho internacional de informar sobre su posible impacto en los derechos humanos de las personas. Estos principios ofrecen a las empresas instrumentos para prevenir y mitigar el impacto de posibles violaciones a los derechos humanos a los que hayan contribuido directa o indirectamente[6].

Para este año no cambiamos la metodología de evaluación, pero si subimos el nivel de exigibilidad frente a la publicación

4 https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

5 https://na-production.s3.amazonaws.com/documents/Transparency_Reporting_Guide_and_Template-Final.pdf

6 https://www.palermo.edu/Archivos_content/2021/cele/papers/Human-Rights-Impact-Assessments.pdf

y reporte de información relevante de riesgos e impactos a los derechos humanos. Asimismo, la forma en que las compañías comunican de manera clara un compromiso público y explícito con la garantía de derechos humanos como la libertad de expresión y la privacidad.

El aumento en la exigencia de este criterio responde también a un contexto internacional de ascenso en las solicitudes por parte de gobiernos a empresas de telecomunicaciones y al aumento del debate sobre los impactos de la moderación de contenidos. En el contexto nacional durante el período de evaluación también hubo un riesgo para los Derechos Humanos en el marco del estallido social de la Protesta Nacional de 2021.

En efecto, la importancia del acceso a la información, la libertad de expresión, la privacidad, la seguridad y la protección de los datos de las personas usuarias de los servicios de internet es una preocupación para estas últimas, no solo por el rol de las empresas PSI como intermediarias frente al Estado, también por sus propias acciones. En esta evaluación buscamos identificar cómo las compañías identificaron y gestionaron los riesgos y afrontan las presiones estatales.

1.2.1. Solicitudes de datos del suscriptor, bloqueos de URL, interceptaciones de las telecomunicaciones

La ley colombiana no obliga a los PSI a publicar informes de transparencia o informes periódicos sobre los requerimientos que las autoridades hacen a las compañías, en relación con los datos de las personas que usan los servicios o sobre los bloqueos de contenidos o cuentas. Sí tienen obligación de entregar información pero sobre los planes de internet y telefonía celular o las prácticas de gestión de tráfico. Sin embargo, dar información sobre lo que sucede con los datos que recolectan se ha convertido en una buena práctica internacional especialmente entre las empresas del sector de las TIC, y a su vez, una necesidad de diferentes grupos de interés, especialmente en contextos de riesgos a los derechos humanos, como lo fue el 2021 en el marco de la protesta social en Colombia.

Ahora bien, como responsables del tratamiento de datos personales, los PSI sí tienen obligaciones de informar con claridad qué datos recogen y cómo los usan, así como de tener una

política de tratamiento de datos que advierta los eventos en que debe entregar los datos de sus suscriptores al Estado.[7] Sin embargo, esta obligación parece insuficiente si consideramos el apetito por los datos personales que múltiples actores tienen en esta época.

El Comité de Política de la Economía Digital de la OCDE en 2020 advirtió que "una gobernanza adecuada y salvaguardias sobre la forma en que los gobiernos acceden a los datos personales en poder de entidades privadas son una parte importante de la creación de confianza y la minimización de las barreras a los flujos de datos"[8] y por lo que publicó orientaciones políticas de alto nivel para el acceso de los gobiernos a los datos personales en poder del sector privado[9].

En esta reciente evaluación de ¿Dónde están mis datos? nos concentramos con tres tipos de peticiones o solicitudes que pueden elevar las entidades del Estado a los PSI que son: (i) la entrega de datos de las personas suscriptoras,[10] (ii) las solicitudes de interceptaciones a líneas telefónicas fijas[11] y (iii) los bloqueos de URL o sitios web que legalmente pueden ser restringidas con ocasión de los siguientes subtipos: la prevención del abuso sexual infantil en línea,[12] combatir la ilegalidad en los juegos de suerte y azar,[13] protección al consumidor, por derechos de autor, las órdenes de tipo judicial y administrativas, y las emitidas en el marco de los estados de emergencia.[14]

7 Obligaciones que se encuentran enmarcadas por la Ley 1581 de 2012 y el decreto 1377 de 2013 especialmente.
8 Disponible en https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm
9 Disponible en https://www.oecd.org/mcm/C-MIN-2020-7-FINAL.en.pdf
10 Art. 15 de la Constitución, Ley Estatutaria 1266 de 2008, Ley 1581 de 2012, Art. 244 de la Ley 906 de 2004 (búsqueda selectiva en bases de datos), modificado por la Ley 1908 de 2018; numeral 9 del Art. 277 de la Constitución Política (solicitud del Procurador General de la Nación); Arts. 631 y 684 del Estatuto Tributario (DIAN) y Cobro Coactivo de entidades públicas (Ley 1066 de 2006). Art. 44 de la Ley Estatutaria 1621 de 2013 (inteligencia y contrainteligencia); Art. 4 del Decreto 1704 de 2012 (interceptación legal).
11 Art. 1 del Decreto 1704 de 2012.
12 Según lo contenido en el art 7 y art 8 de la Ley 679 de 2001; art. 5 y art. 6 del Decreto 1524 de 2002
13 Según lo ordena el art. 38 de la Ley 643 de 2001.
14 Según el art. 8 de la Ley 1341 de 2009.

Frente a la tendencia de ampliar el bloqueo de contenidos como forma de controlar lo que sucede en Internet, nos interesa que las empresas hablen de las causales de solicitud de bloqueo que hacen los estados y que pueden impactar la privacidad y libertad de expresión de las personas usuarias de sus servicios y productos de las PSI. Si las empresas de manera pública y accesible, informan sobre las causales, relacionan el número de solicitudes recibidas por mes o año, las autoridades que efectúan estos pedidos, así como la relación de cuáles y cuántas solicitudes fueron atendidas de manera favorable y cuál terminó siendo su extensión en el tiempo, como sociedad podemos hacer un seguimiento a esta situación y tenemos una herramienta para proteger ese espacio público.

Una medida importante para que desde la sociedad civil podamos hacer un seguimiento a esta situación y podamos contar con una herramienta para proteger ese espacio público, es que las empresas, de manera pública y accesible, informen sobre las causales, relacionen el número de solicitudes recibidas por mes o año, las autoridades que efectúan estos pedidos, así como la relación de cuáles y cuántas solicitudes fueron atendidas de manera favorable y cuál terminó siendo su extensión en el tiempo.

En 2022, **Movistar** sigue siendo la empresa con el mejor puntaje para estos criterios específicos, aun cuando bajo en la puntuación respecto al año pasado al disminuir la facilidad en el acceso al informe de transparencia de Telefónica, dado que la información ya no se aloja en el sitio web de Movistar Colombia. Movistar informa con detalle el marco legal en que se justifica cada orden sobre solicitud de datos, bloqueos e interceptaciones de líneas telefónicas, define a su vez para cada tipo de solicitud las autoridades con facultad para elevarlas ante la compañía, y el número de solicitudes aceptadas y rechazadas por año incluyendo los eventos de bloqueo ante la declaración de estados de emergencia o excepción. **Tigo** le sigue en calificación, y luego **Claro** y **DirecTV** con un mismo puntaje en este eje.

Tigo mejoró desde 2021, y para 2022 presenta mayor granularidad en las solicitudes de datos al clasificar por tipo de requerimiento (datos biográficos, registros llamadas, ubicación antena, documentos contrato, registros IP e Historial IMEI),

y por autoridad (FIscalía, Policía, Entidades Inteligencia, Juzgados, Ejército y otras entidades). En 2022 la empresa entregó información sobre promedios de órdenes de bloqueo de URL o sitios web solo para páginas bloqueadas con material de abuso sexual infantil, sin embargo no se conoce el número total en el año ni más información desagregada.

Claro informa sobre la ocurrencia de cada evento, el marco legal en que se justifica cada orden, las autoridades con facultad para elevarlas ante la compañía, pero a la hora de proveer estadísticas desagregadas sólo lo hace en relación con las órdenes de bloqueo y los cuatro subtipos en que ésta se puede justificar al igual que el año anterior.

En el caso de **ETB** para 2022 su informe de "transparencia de datos", relaciona que provee información desagregada sobre las solicitudes de datos del suscriptor así como las órdenes de bloqueo de URL o sitios web que fueron recibidas, desagregando en ambos eventos por autoridad solicitante, y por solicitudes procedentes *vs* las solicitudes recibidas.

Después de la pandemia, por dos años consecutivos compañías como **DirecTV, EmCali, Avantel, ahora Wom,** y **Skynet** no publicaron informes de transparencia con información que permitiese evaluar su desempeño en este eje.

DirecTV sigue publicando el procedimiento de bloqueo que se refiere en exclusivo a contenido asociado con el abuso sexual infantil.

Hughesnet no cuenta con un informe de transparencia o sostenibilidad, pero en su política de tratamiento de datos informa que efectúa procesos de 'filtrado' de contenidos de abuso sexual infantil.

De contexto e interés

Nos parece relevante destacar que **Movistar** es la única empresa que reporta información sobre interceptaciones de líneas telefónicas, indica información como las normas aplicables en Colombia, define autoridades que pueden hacer la solicitud, y número de solicitudes aceptadas y rechazadas por año, aun cuando han sido cero desde 2017 hasta 2021, exceptuando 2018 con dos solicitudes. Mientras que **Claro** menciona el marco

legal de interceptación pero no desagrega ni da el dato global de solicitudes recibidas.

Movistar, de nuevo, señala que sobre la interceptación de líneas móviles no se reportan datos pues "la Fiscalía General de la Nación en Colombia, por ser la autoridad competente de conformidad con la Constitución y la Ley, realiza las interceptación de manera directa sobre las líneas móviles".

Como lo señalamos en el informe del 2021[15], la ausencia de solicitudes de interceptación de comunicaciones para líneas fijas confirma no solo que predominan las comunicaciones por vía celular, sino que es un indicio que permite entender por qué las autoridades han acudido cada vez menos al mecanismo tradicional de interceptación de comunicaciones vía los PSI (y que estos documentan en sus informes de transparencia cada vez menos) acudiendo en su lugar al acceso directo. En la sección sobre acceso directo, profundizaremos en este tema y su impacto en la privacidad.

1.2.2. Caídas de internet y transparencia en un contexto de movilización social

Después de la pandemia se sentó un precedente claro de cómo en contextos especiales de emergencia resulta importante la transparencia frente a cómo los PSI abordan y gestionan los diferentes riesgos que se pueden presentar en el cumplimiento de sus compromisos políticos y la prestación de sus servicios, esta tendencia exige dar un foco a los informes de transparencia a coyunturas especiales de alto impacto, criterio que evaluaremos en próximos informes.

Como referencia para este análisis se tomó la definición de caídas de internet o interrupciones del acceso a Internet como:

> "bloqueos totales de la conectividad a Internet o de la accesibilidad a los servicios afectados. No obstante, los gobiernos recurren cada vez más a limitar el ancho de banda o restringir el servicio móvil a redes 2G, lo que oficialmente mantiene el acceso a Internet, pero dificulta en gran

15 Puede consultarse aquí https://web.karisma.org.co/donde-estan-mis-datos-2021/

> medida su uso efectivo. En particular, la limitación del ancho de banda interfiere con la capacidad de compartir y ver grabaciones de video y transmisiones en directo. Otra intervención consiste en limitar la disponibilidad de algunos sitios web y servicios y restringir el acceso a determinados canales de comunicación mientras se mantiene la interrupción del acceso al resto de Internet. (...) En algunos casos, además de impedirse el acceso a Internet, también se interrumpe por completo el servicio de las redes de telefonía, por lo que se deja a la población sin ningún canal de comunicación electrónica directa"[16].

Descripción del fenómeno que nos permite ubicar el rol y la relación de los PSI con este tipo de situaciones que, como ya se ha citado en este informe, ponen en riesgo diferentes derechos humanos lo que exige transparencia y garantía de buenas prácticas.

En este informe no evaluamos bajo ningún criterio específico el reporte de información en relación al contexto nacional de Colombia de protesta y movilización social por parte de las compañías. Lo que si queríamos identificar es si algún PSI en el marco del cumplimiento de sus políticas, programas y prácticas, abordó esa coyuntura nacional. Adicionalmente, hicimos una búsqueda de información pública, oficial de las empresas y de fácil acceso para validar como contestaron ante este contexto de riesgo a los derechos digitales como la libertad de expresión y la privacidad.

Sin embargo, lo que se encontró es que ningún PSI en Colombia reportó información específica o relacionada con los derechos humanos, la movilización social y el uso de los servicios que ofrecen. Como señalamos en septiembre de 2021 en el informe "Pistolas contra Celulares", "las empresas también deberían ofrecer más información sobre lo que sucede con su infraestructura para explicar las razones de los fallos (justo al momento de publicar este comunicado las empresas

16 Interrupciones del acceso a Internet: tendencias, causas, implicaciones jurídicas y efectos en una serie de derechos humanos Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. Disponible en https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/341/58/PDF/G2234158.pdf?OpenElement

mencionadas en el informe de Netblocks informaron: Movistar que tienen fallos en la infraestructura[17] y Emcali indica[18] que no tiene servicio de internet celular y el fijo funciona bien)"[19] .

Recordamos que los problemas de conexión a internet que reportó la ciudadanía en el contexto de movilización social, específicamente el 4 y 5 de mayo en Cali, exigieron que los PSI y el Ministerio TIC dieran una explicación pública sobre las causas de dichas interrupciones, fuera por origen en fallas en la infraestructura de internet o por el alto tráfico en las redes. Como indicamos en nuestro informe: Pistolas contra Celulares se conoció "que había afectaciones en su red producto del hurto de cables y la imposibilidad de repararlos debido a los problemas de orden público que sacudieron a Cali ese día. Esto permitió entender la falla informada por Netblocks y también establecer que las fallas que se presentaban en sitios como Siloé no responden a problemas en la infraestructura de las empresas operadoras de internet en el país"[20].

Lo que se espera hasta al momento por parte de los PSI, y conforme con la tendencia internacional en términos de transparencia, es que reconozcan los desafíos, riesgos o amenazas a los derechos a la información, la libertad de expresión, la privacidad, entre otros, que representan las caídas de internet. En este sentido, aunque durante el Paro Nacional sucedieron caídas de internet, no encontramos información o pronunciamientos por parte de las compañías evaluadas frente a este contexto, puntualmente en lo que respecta a la garantía, posibles riesgos o impacto en los derechos humanos de las personas usuarias de los servicios de PSI. Tampoco encontramos una asociación o información de contexto entre las "solicitudes de datos del suscriptor, solicitudes de bloqueos, interceptaciones de las telecomunicaciones" y esa coyuntura nacional.

Si bien, entendemos que hubo un contexto de tensión nacional,

17 https://twitter.com/carobotero/status/1389968589017526273?s=20
18 https://twitter.com/EMCALIoficial/status/1389950916732858371?s=20
19 Disponible en https://web.karisma.org.co/paronacionalcolombia-fallas-de-internet-bloqueos-de-redes-censura-de-contenidos-realidades-y-retos-para-el-ejercicio-de-los-derechos-humanos-en-los-contextos-digitales/
20 Disponible en https://web.karisma.org.co/wp-content/uploads/2021/09/Informe-Pistolas-vs-Celulares.pdf

si es necesario que las políticas de derechos humanos, los procesos claros y legales para tramitar las solicitudes de los Estados, e incluso la debida diligencia o mapeo de riesgos para contrarrestar las presiones de los gobiernos se implementen con transparencia y sobre todo en circunstancias de presión social.

La propia CIDH, en el mencionado informe "Observaciones y recomendaciones de la visita de trabajo de la CIDH a Colombia"[21] incluyó entre sus recomendaciones al Estado: "Brindar proactiva y periódicamente información sobre el funcionamiento de las redes Internet con el fin de que las denuncias sobre eventuales interrupciones y bloqueos sean contrastables con información técnica actualizada y accesible", esta requiere la participación activa de las empresas.

Para dar un ejemplo, de acuerdo con la evaluación anual realizada por Ranking Digital Rights (RDR) algunas compañías en 2021, como América Móvil en México y MTN en Sudáfrica ofrecieron en sus informes de transparencia " nuevos datos sobre sus procesos de gestión de las demandas de bloqueo y caídas de internet"[22], RDR reconoce que los datos suministrados siguen siendo incompletos pero, se celebra que en estos casos se ofrezcan datos. Otro ejemplo fue Telenor que en Myanmar reportó a las personas usuarias el corte de internet solicitado por el gobierno en 2020[23].

Queremos destacar la importancia de lo anterior dado que "en el contexto de protesta social pacífica, la libertad de expresión y otros derechos asociados se ejercen en el entorno en línea y a través de las tecnologías de información y comunicación que son usadas para apoyar, habilitar y facilitar los derechos de asociación y protesta en línea y fuera de línea[24].

21 Disponible en https://www.oas.org/es/cidh/informes/pdfs/ObservacionesVisita_cidh_Colombia_spA.pdf

22 Puede consultarse aquí: https://rankingdigitalrights.org/tgs22/key-findings/transparency-improves-on-shutdowns-but-telcos-still-weak-on-free-expression

23 Tomado de https://www.business-humanrights.org/es/%C3%BAltimas-noticias/telenor-quits-myanmar-as-regime-pressures-telco-operators/

24 "The rights to freedom of peaceful assembly and of association in the digital age: APC submission to the United Nations Special Rapporteur on the rights to freedom of peaceful assembly and of association", dispo-

Instamos a los PSI a impulsar una mayor transparencia y responsabilidad en torno a actividades como cortes o caídas de internet u otro tipo de prácticas que desencadenan una tensión entre sus obligaciones legales para con el Estado y sus responsabilidades en materia de derechos humanos para con sus clientes.

Entendemos que los PSI tienen estrechas relaciones con los gobiernos, que están altamente reguladas, su negocio depende de permisos otorgados por los Estados y que en algunos casos son total o parcialmente propiedad del Estado. Los gobiernos son sus reguladores, pero también suelen ser algunos de sus principales clientes. Como también es evidente que no hay un marco jurídico suficientemente claro sobre cómo y cuándo los gobiernos pueden solicitar legalmente interrupciones de la red, ni sobre cómo los funcionarios pueden exigir responsabilidades a los proveedores, como lo señaló Global Network Initiative (GNI) en marzo de 2022[25].

Sin embargo, para enfrentar estos desafíos y aún así cumplir con los compromisos de respeto a los derechos humanos se elaboróun conjunto inicial de buenas prácticas que fueron el resultado de varios estudios de caso adelantados por GNI. Con base en este proceso se estableció que el sector de las telecomunicaciones en general puede adelantar algunas acciones cuando se enfrenta a interrupciones del servicio:[26]

1) Aclarar sus obligaciones legales, recabar la experiencia de asesores jurídicos y expertos externos para informar a las personas usuarias de lo que los gobiernos pueden exigir adecuadamente y orientar sus próximos pasos.

2) Adoptar procesos claros y documentados. Documentar y escalar las demandas, utilizando políticas y procedimien-

nible en https://www.apc.org/en/pubs/rights-freedom-peaceful-assembly-and-association-digital-age-apc-submission-unitednations y "The promotion and protection of human rightsin the context of peaceful protests:Submission to the Office of the HighCommissioner for Human Rights by theAssociation for Progressive Communications", disponible en https://www.apc.org/sites/default/files/APCSubmissionOHCHRThematicReportNewTechnologiesAndAssemblies_2019 1015.pdf

25 Tomado de https://globalnetworkinitiative.org/wp-content/uploads/2022/03/UN-Submission-Internet-Shutdowns.pdf

26 Tomado de https://www.lawfareblog.com/five-ways-telecommunications-companies-can-fight-internet-shutdowns

tos debidamente establecidos, puede dar a las empresas margen de maniobra a la hora de hacer frente a las órdenes gubernamentales.

3) Reducir el impacto de las solicitudes de cortes de internet. Por ejemplo, reducir la duración o el alcance geográfico de una interrupción, o tratar de eximir de su efecto a infraestructuras como los hospitales.

4) Aumentar la transparencia. Aunque las empresas pueden estar legalmente limitadas en su capacidad de comunicar sobre las caídas, hay una variedad de medios por los que pueden aumentar la transparencia. Cuando no tienen prohibida la comunicación, pueden notificar a las personas usuarias las interrupciones impuestas por el gobierno.

5) Colaborar con los aliados. Son diferentes los grupos de interés afectados por los cortes de internet al ser desproporcionados, por lo que las PSI pueden apoyar la defensa de la transparencia en estas solicitudes.

Cuando ha sucedido, es frecuente que las leyes que rigen las interrupciones otorguen a los gobiernos una amplia autoridad para ordenar interrupciones por motivos imprecisos, a menudo al amparo de estrictas órdenes de silencio. Por eso es tan difícil para el público comprender si las empresas están haciendo todo lo posible para luchar contra las interrupciones de la red. Pero un grupo cada vez mayor de empresas está abriendo sus operaciones al escrutinio de las personas expertas en derechos humanos y proporcionando información crítica en cumplimiento de sus compromisos con los derechos humanos.

Por último, recordamos a los PSI que en 2022 la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos[27] señaló, entre diferentes consideraciones para la detección y prevención de las interrupciones del acceso a Internet y respuesta a estas que:

27 Interrupciones del acceso a Internet: tendencias, causas, implicaciones jurídicas y efectos en una serie de derechos humanos Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. Disponible en https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/341/58/PDF/G2234158.pdf?OpenElement

- Las empresas deben explorar todas las medidas legales para impugnar la aplicación de las interrupciones. La transparencia es fundamental para detener las interrupciones del servicio y limitar sus consecuencias perjudiciales. Las empresas que aplican las restricciones, o se ven afectadas por ellas, suelen ser las primeras, y a veces las únicas, que pueden ofrecer información precisa sobre la naturaleza de la interrupción del acceso a Internet y su alcance.

- Es fundamental que las prácticas para documentar y elevar las demandas dentro de las empresas estén claramente establecidas, protocolos para revelar información sobre dichas interrupciones.

- Las empresas estatales están sujetas a normas aún más estrictas, dada su obligación directa de proteger.

- Siempre que sea posible, las empresas deberían colaborar con las partes interesadas locales e internacionales para mitigar los daños.

1.2.3. Neutralidad de la Red

Desde 2011, Colombia ha establecido regulaciones para garantizar la neutralidad de la Red[28], principio que prohíbe a los proveedores de servicios de internet interferir en cómo las personas utilizan internet, siempre y cuando ese uso sea legal[29].

El concepto de neutralidad de red no ha sido unificado, sin embargo, se basa en principios que buscan asegurar que los PSI brinden servicios competitivos y transparentes y que les permitan a las personas elegir un servicio acorde con sus necesidades. Para lograr esto, se garantiza que las redes permanezcan abiertas y permitan el flujo libre de contenidos de varios proveedores y el acceso de las personas usuarias a ellos[30].

28 Tomado de la Ley 1450 de 2011, y la Resolución 3502 de 2011.

29 Fundación Karisma (2017). *Neutralidad de la red y ofertas comerciales en Colombia. Análisis de la regulación.* https://web.karisma.org.co/fundacion-karisma-publica-informe-sobre-neutralidad-de-la-red-en-colombia/ pg. 8

30 Carboni O., Labate C. América Latina por una red neutral: el principio de neutralidad in Chile y Brasil. Revista FAMECOS: mídia, cultura e tecnolo-

Principios que en Colombia se adaptaron en la Resolución 3502 de 2011: libre elección, no discriminación, transparencia e información.[31]

Libertad de elección hace referencia al derecho de las personas usuarias de los servicios de telecomunicaciones a utilizar, enviar, recibir u ofrecer cualquier contenido y servicio en línea a través, además, de cualquier tipo de tecnología digital. Y se prohíbe a los PSI su limitación arbitraria. En cuanto a no discriminación, se refiere a que los PSI brindarán un trato igualitario a los contenidos y aplicaciones sin diferenciar en razón del contenido, su autor, origen, formato, etc. Transparencia, en términos de neutralidad de la red, obliga a los PSI a proveer información sobre sus políticas de gestión del tráfico. Y el cuarto, información, reconoce el deber de las compañías de internet de suministrar información sobre las condiciones de prestación del servicio en términos de velocidad, calidad, prácticas de gestión del tráfico según el plan de navegación, entre otros.[32]

Las Prácticas de Gestión del Tráfico (PGT), a través de las cuales los PSI pueden intervenir en el tráfico de internet para "reducir o mitigar los efectos de la congestión sobre la red" o "asegurar la calidad del servicio a las personas usuarias", entre otros, deben ser razonables y no discriminatorias. Ello quiere decir que la gestión razonable hace alusión a las medidas que asumen los PSI para garantizar que la conectividad del usuario final no se vea afectada por la congestión de la red, y debe ser transparente. Así mismo, de acuerdo con la Comisión de Regulación de Comunicaciones (CRC), "estas medidas no sólo deben ser proporcionales, apropiadas para cada situación particular, y evitar la discriminación injustificada de tráfico o contenidos, sino que deben ser objeto de revisión periódica por parte de los mismos PSI y las autoridades correspondientes, según se considere necesario"[33].

---

gia, vol. 25, núm. 2, ID28507, 2018

31 Art. 3 Resolución 3502 de 2011

32 Art. 3 Resolución 3502 de 2011

33 CRC, 2022. Estudio del estado dela neutralidad de la red en Colombia. https://www.crcom.gov.co/system/files/Biblioteca%20Virtual/Estado%20de%20la%20Neutralidad%20de%20Red%20en%20Colombia%202021/Estudio_Neutralidad_CRC_2021.pdf

Al igual que en el 2021, en nuestra evaluación consultamos el contenido de las PGT y observamos, que todos los proveedores del servicio de internet (a excepción de **Skynet**) las publican en sus sitios web, con alguna variación en términos de claridad y facilidad en su búsqueda. Para este criterio específico, no hubo cambios significativos.

Destacamos particularmente los casos de **Claro**, **Movistar**, **Tigo**, **Wom** y **Hughesnet** que además de publicar sus prácticas de gestión del tráfico hacen expreso su compromiso por proteger el principio de neutralidad de la red. Asimismo, **Tigo** explica ampliamente la gestión de tráfico con un lenguaje no técnico y usa diferentes materiales para facilitar la compresión de las políticas, ante la necesidad de las personas usuarias de que estás medidas sean más claras. De acuerdo con información solicitada por la CRC a el Ministerio TIC y a la Superintendencia de Industria y Comercio (SIC), hasta marzo de 2022 no reportaron casos de violación a la neutralidad de la red[34].

En un próximo informe, además del compromiso con la naturalidad de la red y la evaluación sobre si publica o no la Política de Gestión del Tráfico, será necesario valorar en la metodología, qué se entiende como prácticas de gestión de tráfico razonables y cómo los cambios en los servicios de las PSI pueden representar retos de cara a los principios de neutralidad de la red.

De contexto e interés

En marzo de 2022 la CRC publicó el Estudio del Estado de la Neutralidad en la red en Colombia, que tuvo el "objetivo de conocer el panorama internacional y nacional en torno a la neutralidad de red y su importancia, así como conocer la aproximación de las múltiples partes interesadas frente a dicha temática en Colombia mediante un proceso de participación abierta"[35].

En el informe citado se reconoció y definió cómo se han presentado grandes cambios en términos de evolución

34 Radicados 2021816084, 2021816103

35 CRC, 2022. Estudio del estado dela neutralidad de la red en Colombia. https://www.crcom.gov.co/system/files/Biblioteca%20Virtual/Estado%20de%20la%20Neutralidad%20de%20Red%20en%20Colombia%202021/Estudio_Neutralidad_CRC_2021.pdf

tecnológica, de mercado y de modelos de negocio que han llevado a una constante transformación en la diversidad de ofertas y servicios, y que pueden representar retos para la neutralidad de la red, como: 1) Priorización: Las vías rápidas (fast lanes); 2) Throttling o limitación del ancho de banda; 3) Tethering, es más conocido como "compartir datos" o "compartir conexión a Internet" y 4) el Zero-rating (también llamado tasa cero o tarifa cero).

Respecto a este último, el Zero-rating se define como la práctica de no cobrar a las personas usuarias por los datos utilizados para acceder a determinados servicios o plataformas en línea. La tarificación cero se considera en algunos países un tipo de priorización de la red que socava el principio de neutralidad de la red.

Por ejemplo, **Wom** menciona en relación a su PGT sus planes de Zero-rating. Sin embargo, **Claro**, **ETB**, **Movistar** y **Tigo** también ofrecen estos servicios en planes pospago y prepago, pero no los mencionan en relación a sus declaraciones de neutralidad de la red.

Ahora bien, en términos de transparencia y considerando que en Colombia ha venido evolucionando con planes que son ampliamente demandados por las personas usuarias de servicios móviles, lo que se puede exigir ante estos servicios es la debida diligencia sobre el impacto en derechos humanos -libertad de expresión e información, a la privacidad y a la no discriminación- y los principios de neutralidad de la red periódicamente, para mitigar cualquier riesgo planteado por esos impactos.

Después de la discusión en 2021 sobre la neutralidad de la red en relación con los decretos[36] que previeron la posibilidad de priorizar el tráfico de internet en caso de que fuese necesario para privilegiar la navegación de contenidos sobre "servicios de salud, páginas gubernamentales y del sector público, el desarrollo de actividades laborales", en el marco de la emergencia sanitaria, y posteriormente su fallo[37], la Corte Constitucional recogió dichas

36 Decreto 464 de 2020 renovado en el tiempo por el Decreto 555 de 2020.

37 Que puede verse aquí https://www.corteconstitucional.gov.co/relatoria/2020/C-151-20.htm

preocupaciones y aclaró que la previsión sobre la priorización del tráfico no significaba instaurar en la práctica un mecanismo de bloqueo de contenidos. La CRC con el Estudio del Estado de la Neutralidad , concluyó que " las disposiciones generales en torno a la neutralidad de red, siguen siendo válidas y aplicables a nuestro contexto bajo los principios de libre elección de las personas, no discriminación de contenidos, transparencia e información de gestión de tráfico"[38].

Desde el 2022 la Corte Constitucional está estudiando una demanda de inconstitucionalidad presentada por la organización El Veinte a la parte final del primer parágrafo del artículo 56 de la Ley 1450 de 2011 en el que se establece una excepción al principio de neutralidad que consiste en autorizar a los PSI a hacer ofertas de acuerdo con las necesidades de los segmentos de mercado o de las personas que usan sus servicios de acuerdo con perfiles de uso y consumo, sin que esto se entienda como discriminación. Para quienes demandan, esta autorización atenta contra los artículos 13, 15, 20, 75, 83 y 333 de la Constitución Política, los artículos 11 y 13 de la Convención Americana sobre Derechos Humanos y los artículos 17 y 19 del Pacto Internacional de Derechos Civiles y Políticos[39].

Al respecto, desde la Fundación Karisma consideramos que "no todos los planes de zero rating limitan el acceso a internet y al derecho a acceder a la información y la cultura. Por eso pedimos declarar la constitucionalidad condicionada, evitando los planes que pueden impactar negativamente la libertad de expresión"[40]. La excepción en el artículo de neutralidad de la red debe revisarse en tanto no genere una vulneración a la estructura de Internet, el pluralismo informativo y la libertad de expresión de las personas usuarias, que ven limitados los medios para acceder y compartir ideas e información, como también una limitación

38 CRC, 2022. Estudio del estado dela neutralidad de la red en Colombia. https://www.crcom.gov.co/system/files/Biblioteca%20Virtual/Estado%20de%20la%20Neutralidad%20de%20Red%20en%20Colombia%202021/Estudio_Neutralidad_CRC_2021.pdf

39 Disponible en https://web.karisma.org.co/demanda-en-contra-de-la-excepcion-al-principio-de-neutralidad-en-la-red-establecido-en-el-articulo-56-de-la-ley-1450-de-2011/

40 Disponible en https://web.karisma.org.co/la-corte-constitucional-nos-convoco-a-una-audiencia-publica-sobre-neutralidad-en-la-red%EF%BF%BC/

a la competencia entre las aplicaciones. Incluso debe evaluarse si esto facilita el perfilamiento y segmentación de las personas usuarias, lo cual da paso al tratamiento de datos personales sensibles, sin que estas personas tengan pleno conocimiento sobre su uso[41]. Está decisión y este debate continuará en 2023, por lo que se espera se avance en reconocer como nuevas prácticas y servicios de las PSI aplican y se mantienen dentro de los principios de neutralidad de la red.

2. Eje de intimidad

2.1. Políticas de protección de datos

El debate mundial sobre la privacidad, así como las reformas regulatorias necesarias para la garantía de este derecho, se han concentrado hasta el momento en las plataformas de redes sociales, olvidando un poco los PSI como quienes pueden acceder a información como nuestra ubicación, nuestra información personal, los mensajes SMS, el historial de navegación web y el uso de aplicaciones.

En este sentido, mientras avanza la discusión y los ajustes necesarios al marco legal, cuando hablamos de empresas de telecomunicaciones, buscamos evaluar cuáles son las diferentes prácticas que implementan las PSI para ser activamente transparentes en el manejo de datos de las personas usuarias.

El marco legal de protección de datos exige a los encargados del manejo de información personal y sensible, que adopten medidas para informar a los titulares acerca de los detalles relacionados con el recabamiento, el uso, el almacenamiento y la posible compartición de sus datos personales. Para cumplir con esta obligación, es necesario que se establezca una política de privacidad clara y accesible para toda persona que utiliza los servicios de los PSI. Esta política deberá estar disponible para su consulta por parte de las personas interesadas.

Pese a que ha habido progresos sustanciales en esta materia, creemos que todavía se requiere de un mayor nivel de

41 Disponible en https://web.karisma.org.co/demanda-en-contra-de-la-excepcion-al-principio-de-neutralidad-en-la-red-establecido-en-el-articulo-56-de-la-ley-1450-de-2011/

desagregación y granularidad en la información que se provee sobre los datos objeto de tratamiento y su compartición con terceras partes (del sector público y privado).

Por ejemplo, la granularidad y desagregación de los tipos de información que recopilan los PSI puede incluir, pero sin limitarse a, correspondencia personal, contenido generado por la persona usuaria, preferencias y configuración de la cuenta, datos de registro y acceso, datos sobre las actividades o preferencias de un usuario recopilados de terceros, ya sea a través del seguimiento del comportamiento o de la compra de datos, y todas las formas de metadatos, es decir una transparencia amplia sobre los diferentes tipos de datos que obtienen.

En este sentido, es necesario avanzar a una visión extensiva de los datos y a la protección no solo a "la información sustantiva contenida en las comunicaciones", sino también a los metadatos, que pueden "dar una mejor idea del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona que la información obtenida accediendo al contenido de una comunicación privada"[42] .

De acuerdo con Ranking Digital Rights, una política de privacidad que defina "información personal" como "información sobre usted que sea personalmente identificable, como su nombre, dirección, dirección de correo electrónico o número de teléfono, y que no esté disponible públicamente de otro modo" es más restrictiva[43]. Si bien anticipamos esta visión y hacía dónde debemos avanzar en protección de datos, para esta evaluación, solo revisamos si hay definiciones claras sobre los tipos de datos que recopilan las empresas.

En comparación con los hallazgos del año anterior no hubo cambios,[44] **Movistar**, **Tigo, DirecTV** y **Wom** recibieron el mejor puntaje, seguidos en la calificación por **Claro**, **ETB** y **Hughesnet,** con el mismo puntaje.

Movistar clasifica los datos que recoge en:datos demográficos, datos económicos, datos biométricos, datos de servicios,

42 CIDH, Estándares para una Internet Libre, Abierta e Incluyente, párr. 189, OEA/Ser.L/V/II CIDH/RELE/INF.17/17 (15 de marzo de 2017)

43 Disponible en https://rankingdigitalrights.org/bts22/indicators/P3a

44 Puede verse aquí https://web.karisma.org.co/donde-estan-mis-datos-2021/

datos comerciales y datos de localización. A su vez indica algunas finalidades como el cálculo de riesgo económico o crediticio, la publicación de directorios, y la prevención y control de fraudes, también para fines comerciales o publicitarios en Colombia o en el exterior haciendo la salvedad de siempre contar con la autorización de la persona usuaria. Describe algunos terceros que podrán tener acceso a éstos y en dicho caso para satisfacer qué finalidad en concreto.

Wom no informa en su política qué datos concretos recoge, no obstante quisiéramos reconocer que enlista de manera clara todas las finalidades de datos personales por grupo de interés: recursos humanos; proveedores; clientes y prospectos comerciales. También señala que comparte datos con terceros con fines comerciales a nivel nacional y en el extranjero contando con las autorizaciones de cada una de las personas titulares.

Por su parte, **Emcali** mantiene la misma política de protección de datos, que divide para clientes, proveedores y empleados, por lo que no es clara y tampoco especifica qué tipo de datos recoge y cuáles son sus usos. Tampoco señala si comparte o no dichos datos con terceros y en caso afirmativo, para qué fines en concreto.

Las empresas que evaluamos proporcionaron pocos detalles sobre cómo recopilan datos directamente de las personas usuarias o qué comparten y con quién. También revelaron muy poco, o en algunos casos no reportan nada, sobre cómo recopilan información de las a través de terceros, como por ejemplo de intermediarios de datos o instituciones financieras.

Un criterio específico en el que no vimos mayores cambios y genera alarma, es que algunas de los PSI evaluadas no avanzan en la aclaración y definición exhaustivas sobre qué información personal utilizan, con qué finalidades, las razones por las cuales recolectan cada tipo de dato, cómo y con quienes las comparten. Es importante avanzar en políticas de protección de datos que no sean incompletas, confusas o dispersas de manera que dificulten la comprensión clara de lo que la empresa recopila, las fuentes de esta información, los usos de estos datos, el intercambio de información con terceros, entre otros. Por ejemplo, si las empresas recopilan varios tipos de información, esperamos que proporcionen detalles sobre cómo manejan cada tipo de información.

Incluso, a nivel internacional ya se habla no solo de estos criterios de transparencia en las políticas de tratamiento de datos, sino de la posibilidad de que las personas accedan a sus datos personales y se proporcionen activamente herramientas sencillas para eliminarlos o determinar cómo se utilizan, más allá de la autorización. Adicionalmente, aunque este año no evaluamos si las empresas se comprometen con el principio de minimización de datos y si demuestran cómo este principio determina sus prácticas en relación con la información de las personas usuarias, nos parece relevante identificar si las empresas avanzan en este sentido en Colombia y por tanto estamos analizando sí incluirlo para futuras evaluaciones.

2.2. Retención de datos

En esta sección revisamos la forma como los operadores informan que desarrollan su obligación de retención de datos, cuáles son los que retienen y por cuánto tiempo. No revisamos el resultado de la actividad de retención de datos.

Como hemos señalado desde informes pasados, cuando hablamos de retención de datos nos referimos específicamente a la obligación que tienen los PSI de conservar hasta por cinco años y entregar de manera *inmediata* a las autoridades de inteligencia y a la Fiscalía General, la información que producen en la prestación del servicio de telecomunicaciones. Es decir hablamos de un marco normativo que a la fecha no ha cambiado.

Para esta edición nuevamente la mayoría de los operadores informan sobre el cumplimiento de la ley -con o sin la indicación del marco legal al que hacen referencia-, o publican que deben retener los datos de las personas que se suscriben a sus servicios. A continuación, el resumen de marco legal que incluimos en el informe pasado y que se mantiene vigente y sin modificaciones.

En dicho caso, las compañías de telecomunicaciones deben colaborar con la Fiscalía General de la Nación para entregar, en el marco de una investigación penal, los siguientes datos:[45]

45 Decreto 1704 de 2012, artículo 4.

- Los datos de la persona suscriptora, tales como identidad, dirección de facturación y tipo de conexión. Además deben conservarla por cinco años.
- Información específica contenida en sus bases de datos, tal como sectores, coordenadas geográficas y potencia, entre otras, que contribuya a determinar la ubicación geográfica de los equipos terminales o dispositivos que intervienen en la comunicación. Deben suministrarla en tiempo real en caso de que se requiera.

La ley de Inteligencia y contrainteligencia obliga a los operadores a entregar a agencias de inteligencia:[46]

- El historial de comunicaciones de los abonados telefónicos vinculados, es decir, de las personas que contratan sus servicios.
- Los datos técnicos de identificación de las personas que suscriben sus servicios y sobre los que recae su operación,
- La localización de las celdas en que se encuentran las terminales y cualquier otra información que contribuya a su localización.

Sin embargo, de toda la información que pueden producir los operadores sobre la actividad de los teléfonos celulares, no está claro exactamente qué entregan a las autoridades de investigación penal e inteligencia cuando deben cumplir con estas normas. Por eso, en este criterio nos preocupamos por cómo informan (i) a las personas usuarias sobre la existencia de esta obligación, (ii) sobre qué datos retienen en concreto, (iii) sobre el tiempo por el cual los retienen.

Además de las normas de retención de datos que acabamos de exponer, la Fiscalía puede realizar la "búsqueda selectiva en bases de datos"[47] y las autoridades, en general, pueden solicitar datos personales sin autorización de la persona titular, siempre que sea en ejercicio de sus funciones.[48] No está claro cómo funcionan en la práctica cada una de estas facultades ni cómo se relacionan entre ellas.

46 Ley 1621 de 2013, artículo 44.
47 Ley 906 de 2004. Código de Procedimiento Penal. Artículo 244.
48 Ley 1581 de 2012. Artículos 10 y 13.

Sobre los datos que conservan para entregar a las autoridades en investigaciones penales o de inteligencia o el tiempo que dura la retención, los operadores no introdujeron cambios en 2021 en comparación con la información que ya proveían para 2020. En general las empresas en Colombia no son claras en los detalles en torno al cumplimiento de esta obligación legal.

Movistar y **Tigo** informan que están obligadas por ley a retener datos con indicación del marco legal. **ETB** y **DirecTv** mencionan en su política de tratamiento de datos que retiene datos sin indicación del marco legal. Ninguna advierte el tiempo por el cual retiene datos y la mayoría de los operadores no informan o son ambiguos en el tipo de datos que retiene.

Al igual que en 2021, **Movistar** cita a plenitud el marco legal que justifica la retención de datos. Incluyen la Ley 906 de 2004 (art. 235), Ley 1621 de 2013 (art. 44), y el Decreto 1704 de 2012 (art. 18). Ese marco legal describe el tiempo de retención que se extiende hasta por cinco años, el tipo de datos que son retenidos (metadatos como el historial de comunicaciones de las personas que suscriben sus servicios, su identificación, datos que faciliten su localización, entre otros).

Cuando se trata de detallar el tiempo por el que hace la retención de dichos datos, **Tigo** continúa señalando que lo hará por un periodo superior al autorizado por la persona titular de los datos sin la advertencia de un plazo determinado en el tiempo. **ETB** mantiene una fórmula más bien genérica para señalar, por ejemplo, que retendrá los datos por el tiempo que sea necesario hacerlo.

Por último, ni **EmCali, Wom, Hughesnet** o **Skynet** relacionan información sobre el deber legal de retención de datos, sobre el tipo de datos que retienen, ni el tiempo por el que lo hacen.

2.3. Acceso directo

Los estándares internacionales de derechos humanos obligan a que la interceptación de las comunicaciones requiera por mandato legal que una autoridad competente emita una orden que está sujeta a parámetros estrictos de motivación fundada y razonable, y que en su confección atienda además un test de proporcionalidad en el que se justifique el qué, para

qué y por cuánto tiempo de una medida que impacta en la privacidad de las personas.

Dicha orden de acceso a las comunicaciones se remite a los proveedores de servicios de internet que pueden validar y analizar su contenido y forma y, en caso de hallarla deficiente o arbitraria, pueden oponerse a su ejecución. La intermediación le da a estas empresas un rol en la garantía de los derechos fundamentales de las personas que contratan sus servicios.

Como indicamos en el informe de 2021, el acceso directo, por su parte, faculta a las autoridades a tener acceso a las comunicaciones de las personas prescindiendo del rol de los PSI, esta situación suele ir acompañada de desregulación o ambigüedad legal que no cumple con los estándares internacionales de protección a los derechos humanos. En el acceso directo las empresas están obligadas a dejar una puerta abierta en su infraestructura sin que tengan capacidad de negarse (puede llegar a ser una condición para funcionar en determinados países[49]), o de denunciarlo públicamente, tal y como lo han manifestado algunos proveedores internacionales de acceso a internet como Vodafone, Telenor, Millicom y Telia.[50]

Recordamos la importancia de que las compañías reporten estos sucesos, tal y como lo puso de presente la organización Privacy International en su intervención[51] ante el Relator Especial para la Libertad de Expresión de la ONU en 2016, donde destacó el valor que tienen los informes de transparencia de las compañías proveedoras de acceso a internet para visibilizar

49 Consultar la publicación de Katitza Rodríguez y Veridiana Alimonti en el Blog de la Electronic Frontier Foundation en donde se recoge un extracto a la explicación de Telecom sobre por qué no puede oponerse al acceso directo “some governments may require direct access into companies’ infrastructure for the purpose of intercepting communications and/or accessing communications-related data. This can leave the company without any operational or technical control of its technology”. Disponible aquí https://www.eff.org/deeplinks/2021/02/when-law-enforcement-wants-your-private-communications-what-legal-safeguards-are

50 En el blog de la Freedom Coalition Online tanto Lisl Brunner y Patrick Hiselius informan en detalle al respecto. La entrada puede consultarse aquí https://freedomonlinecoalition.com/blog/blog-2-direct-access-systems-and-the-right-to-privacy-by-lisl-brunner-and-patrik-hiselius/

51 Se puede leer acá https://www.ohchr.org/Documents/Issues/Expression/Telecommunications/PrivacyInternational.pdf

este tipo de prácticas en los casos en que no pueden denunciar públicamente su despliegue. De acuerdo con diferentes casos recolectados por esta organización, las empresas son quienes han permitido en varias partes del mundo identificar en qué países se ejecutan actividades de acceso directo sin supervisión ni control legal.

En junio de 2021 GNI solicitó al Gobierno de Indonesia suspender el Reglamento nº 5/2020 al ser incompatible con los principios internacionales de derechos humanos. GNI[52] expresó su preocupación por los acuerdos de "acceso directo" que dan a las autoridades gubernamentales "un acceso sin restricciones a los datos de los usuarios, eliminando de paso la capacidad de los intermediarios para revisar, examinar y proporcionar transparencia en torno a dicho acceso. Dada la posibilidad de que dicho acceso dé lugar a abusos, [....] contemplar la posibilidad de un acceso más invasivo y directo".

En Colombia, el Decreto 1704 de 2012 sobre interceptación de las comunicaciones prevé que "[l]os proveedores de redes y servicios de telecomunicaciones (...) deberán implementar y garantizar en todo momento la infraestructura tecnológica necesaria que provea los puntos de conexión y *de acceso* a la captura del tráfico de las comunicaciones que cursen por sus redes". Aunque esta no es una previsión lo suficientemente precisa como para responder a la pregunta sobre si la práctica del acceso directo para interceptar las comunicaciones de las personas se encuentra o no consagrada en Colombia, el hecho de que se ha mencionado durante los últimos años por algunos PSI colombianos como la base legal para que la interceptación de comunicaciones en la red celular ya no pase por su control, hace pensar que efectivamente existe. Es decir, aunque la ley no es clara sobre el despliegue de esta modalidad de vigilancia de las comunicaciones, lo que nos dicen los informes de transparencia es que así se ha hecho.

Para 2022, en este criterio de evaluación a los PSI se retrocede no solo en número de compañías que manifiestan el acceso directo, que pasó de tres a dos, sino la información sobre el marco normativo aplicable, que pasó de dos a una. Adicionalmente,

52 Se puede leer acá https://globalnetworkinitiative.org/mr5-indonesia/

ninguna empresa expresa su posición de manera explícita respecto a su postura o rol ante este tipo de eventos.

Merecen reconocimiento **Movistar,** que mantiene la claridad con que manifiesta este tipo de realidad frente al acceso directo y **Tigo** también al reportar que hay acceso directo por parte de autoridades en ejercicio de sus competencias.

Movistar ha reportado en su informe de transparencia desde 2017 que, sobre interceptación de las telecomunicaciones "[s]olo se incluyen los requerimiento sobre líneas fijas. Líneas móviles: No se reportan interceptaciones sobre líneas móviles. *La Fiscalía General de la Nación en Colombia, por ser la autoridad competente de conformidad con la Constitución y la Ley, realiza las interceptaciones de manera directa* sobre las líneas móviles".[53] (Subrayado propio).

Tigo, por su parte, ha decidido manifestar en su informe de "requerimientos de datos personales por terceros y bloqueos de contenido" que "entregamos información personal o damos *acceso directo* a bases de datos o sistemas que contienen información personal a nuestro cargo a autoridades en ejercicio de sus competencias"(Subrayado propio).

Como lo hemos advertido en el 2022[54], que en Colombia exista acceso directo de la Fiscalía a las redes de los PSI sin un marco jurídico claro, sin mediar evaluación de impacto en la privacidad de las personas, sin controles ni mecanismos de seguimiento y sanción a los abusos, y sin que tampoco haya tenido lugar un análisis profundo sobre su constitucionalidad o compatibilidad con el marco jurídico nacional y compromisos asumidos por el Estado colombiano en materia de derechos humanos, es motivo de preocupación.

A su vez, como alertamos desde el informe anterior, la ausencia de controles contrasta con el ejercicio de transparencia que poco a poco han decidido llevar adelante los PSI que son quienes nos ofrecen algún indicio sobre su desarrollo.

53 Consultar los informes desde 2016 para Colombia aquí https://www.telefonica.com/es/sostenibilidad-innovacion/privacidad-seguridad/informe-de-transparencia/

54 Puede verse aquí https://web.karisma.org.co/donde-estan-mis-datos-2021/

2.4. Solicitudes de datos por parte de entidades públicas, procedimiento de entrega y notificación a las personas sobre dichos eventos

La Ley de Protección de Datos permite la entrega de datos personales a entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial sin autorización de la persona titular de los datos.[55] Las autoridades que reciben la información deben guardarla en reserva, usarla solo para los fines para los cuales la recibieron, deben informar a los titulares del dato sobre el uso que le dan y tomar medidas de seguridad para protegerla.[56] Las empresas reciben cada vez más demandas gubernamentales para que entreguen información sobre las personas usuarias de sus servicios. Estas demandas pueden proceder de organismos gubernamentales o de tribunales.

En este eje de evaluación esperamos que las empresas provean información sobre los procedimientos que han diseñado y que siguen internamente a la hora de entregar los datos de las personas que se suscriben a sus servicios a las entidades públicas que los solicitan.

Por *procedimiento interno* nos referimos al proceso de consideración sobre la legalidad y procedencia del pedido antes que al procedimiento desde un punto de vista técnico. Es decir, se trata de establecer si la empresa tiene procedimientos alineados con los derechos humanos.

Mediante estos procesos internos, además de esperar que sean públicos y claros, se espera que los PSI se comprometan públicamente a oponerse a las demandas gubernamentales inapropiadas o demasiado amplias. Si bien este último elemento no hace parte de la calificación de nuestra evaluación, si revisamos si las empresas manifiestan límites y criterios a otros grupos de interés para aceptar o rechazar estas solicitudes de datos, y de esta manera garantizar procesos proporcionales, definidos y legales para la protección de los derechos humanos de las personas usuarias.

55 Ley 1581 de 2012 art. 10 y 13

56 Corte Constitucional. Sentencia C-748 de 2011. M.P. Jorge Ignacio Pretelt Chaljub.

Por *notificación a las personas usuarias* buscamos identificar si los PSI avisan a sus suscriptores de la entrega de sus datos personales a las autoridades facultadas para requerir acceso a estos. Se trata de promover una buena práctica que aún no tiene recepción legal en Colombia.

Con frecuencia se nos indica que dicha notificación no es compatible con la confidencialidad que revisten las investigaciones preliminares de tipo penal, sin embargo, consideramos que esta afirmación no puede ser llevada a extremos y que -como sucede en otros países de la región como Chile- tal restricción como mínimo debería ser excepcional y limitada a delitos graves, pero entendemos que en este campo existe una discusión que debe darse. En cuanto a notificación revisamos que las PSI se comprometan a hacerlo en tanto el marco normativo no lo impida, es decir que sea la excepción el no notificar y no la regla general en el proceso, esto en razón de que hay diferentes procedimientos de solicitud de datos de las personas, diferentes autoridades que las llevan a cabo y sobre diferentes tipos de datos, la restricción y reserva no puede ser extensiva a cualquier tipo de solicitud.

Nuevamente durante 2022 los PSI no efectuaron cambios significativos en sus políticas sobre entrega de datos en comparación con la información que ya ofrecían en 2020.

Al igual que informe de 2021, sobre el procedimiento o protocolo para atender solicitudes de entrega de datos de sus suscriptores con criterios más o menos definidos se destacan **Movistar**, **Tigo**, **DirecTV** y **ETB**.

Por su cuenta, **Claro** solo describe cuáles son las autoridades facultadas para elevar este tipo de solicitudes, sin detallar un procedimiento en este sentido. **Wom**, **EmCali, Hughesnet** y **Skynet** no proporcionan ninguna información al respecto.

Queremos resaltar que tanto **Movistar** como **Tigo,** tienen los protocolos de trámite para las solicitudes de entrega de datos más fáciles de comprender. Describen en flujos de procesos el paso a paso en que las tramitan, y suelen incluir una fase de validación sobre su procedencia y legalidad.

Si bien en el reporte de 2021 reconocimos que por ejemplo, en el contexto particular de Covid-19 en 2020, **Tigo** reportó solo

para ese año que durante la emergencia y bajo el argumento de mitigar los efectos de ésta, las autoridades solicitaron bases de datos personales como una de las medidas excepcionales que se tomaron en la lucha contra el Covid- 19. Situación frente a la cual la compañía afirma que "cada uno de estos requerimientos fueron atendidos asegurando que la información sobre la cual teníamos influencia permaneciera protegida y el derecho a la intimidad de los distintos grupos de interés fuera respetado"[57].

Para este informe, y evaluando el desempeño de las empresas durante el 2021 en el contexto de protesta, buscamos pronunciamientos o consideraciones en los informes, políticas y documentos de las compañías alguna particularidad o garantía de protección en el marco de los procesos regulares para la atención de solicitudes de datos por parte de autoridades. Lo que encontramos es que ninguna reportó información o expresó una posición de la empresa frente a esta coyuntura.

Movistar por su parte, señala que en la validación de la procedencia de las solicitudes de acceso a sus datos personales, aplica los principios de: confidencialidad en su trámite, exhaustividad y fundamentación de la orden, proporcionalidad y neutralidad política de la misma, respuesta diligente en su trámite y seguridad en la entrega de los datos. Adicionalmente, ofrece materiales prácticos en lenguaje no técnico para entender el proceso de atención de las solicitudes. Sin embargo, no demuestra en su proceso la notificación a las personas usuarias cuando es posible, y tampoco ofrece mecanismos de garantía de derechos.

Nuevamente ninguna compañía con excepción de **DirecTV** se compromete públicamente a notificar a sus suscriptores de la entrega de sus datos al sector público, compromiso que advierte, se hará siempre y cuando ésto sea posible. Habría que advertir que el alcance de este informe no permite verificar su cumplimiento, por tanto sería deseable que **DirecTV** acompañará a esta política con la indicación del número de veces que ha notificado de esto a las personas, de lo contrario es

57 https://assets.tigocloud.net/j1bxozgharz5/4o30TqaSceMRe2eUApq5bh/bbb9107944f2e50958941471f44a4aa1/REQUERIMIENTOS_DE_DATOS_PERSONALES_POR_TERCEROS_2022.pdf

muy posible que se tratara del trasplante de una práctica que tiene su matriz en Estados Unidos, pero que no tiene efectos prácticos en países como Colombia.

En caso en que los PSI en Colombia se enfrenten ante una situación en la que la ley hace que las empresas no alcancen las mejores prácticas, es decir que las normas aplicables impidan revelar información sobre el proceso de atención de solicitudes de datos, impulsamos a las empresas a abogar por leyes que les permitan respetar plenamente los derechos de las personas usuarias a la privacidad, así como otros derechos que puedan verse afectados por estas solicitudes.

También a revisar y ajustar sus procesos internos para hacer las solicitudes más específicas frente a qué tipo de información solicita, qué periodicidad tienen esas solicitudes, qué marco jurídico las sustenta, qué entidades solicitan los datos, y si se notifica o no a las personas usuarias sobre estas solicitudes. En este sentido, solicitar a las autoridades ser más específicos, claros, proporcionales, y permitir a los PSI revisar dichas solicitudes.

3. Eje sobre libertad de expresión

3.1. Obligación legal de bloqueo y el procedimiento de bloqueo

El bloqueo de sitios web o URL son medidas de excepción que deben estar reguladas en la ley. Órdenes de este tipo sólo proceden como medida de protección de un derecho humano u otro interés legítimo.[58]

En Colombia, la protección de esos intereses legítimos ha dado paso, que sepamos, a cuatro subtipos de bloqueo legal en particular, y que son: el bloqueo de sitios web en que circulan contenidos sobre el abuso sexual infantil en línea por

58 Esto es así según el estándar interamericano fijado por la Relatoría para la Libertad de Expresión de la Organización de Estados Americanos. Al respecto se puede visitar el informe "Estándares para una Internet Libre, Abierta e Incluyente", que se puede consultar aquí http://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf

el Ministerio TIC,[59] el bloqueo para combatir la ilegalidad en los juegos de suerte y azar por Coljuegos,[60] por derechos de autor por la Dirección Nacional de Derechos de Autor, y las órdenes de bloqueo de tipo judicial y administrativo como por ejemplo medidas cautelares en una tutela, y las órdenes de bloqueo que tienen lugar durante los estados de emergencia y excepción.[61]

También existen eventos en que los PSI advierten en los términos y condiciones de prestación de sus servicios que podrían llegar a bloquear sitios web o URL por razones de tipo contractual. En este tipo de escenarios, pedimos a los PSI implementar procedimientos de reclamo en favor de las personas usuarias.

En nuestra evaluación nos interesa verificar, en concreto, que los PSI reconozcan que llevan a cabo este tipo de medidas y que cuentan con un procedimiento para tramitarlas, esto con el fin de entender cómo las empresas gestionan estas solicitudes, y sobre todo cómo protegen el derecho a la libertad de expresión. Explicar el procedimiento es un acto de transparencia en la manera en cómo se ejecuta el bloqueo, independientemente de si su origen es de tipo legal o contractual.

En la explicación de dicho procedimiento también verificamos si se prevé un paso de notificación a las personas usuarias de sus servicios sobre el tipo de bloqueo efectuado, el marco legal y la razón en que éste se motiva.

Durante 2022 los PSI no efectuaron cambios significativos en sus políticas sobre entrega de datos en comparación con la información que ya ofrecían en 2020 y 2021.

Sobre el procedimiento o protocolo para atender solicitudes de bloqueo de sus suscriptores con criterios más o menos definidos se destacan **Movistar**, **Tigo**, **DirecTV** y **ETB**. Sin embargo, consideramos que no son procesos claros que garanticen la protección de riesgos al derecho de libertad de expresión por solicitudes del gobierno.

59 Según lo contenido en el art 7 y art 8 de la Ley 679 de 2001; art. 5 y art. 6 del Decreto 1524 de 2002
60 Según lo ordena el art. 38 de la Ley 643 de 2001.
61 Según el art. 8 de la Ley 1341 de 2009.

Por su cuenta, **Claro** solo describe cuáles son las autoridades facultadas para elevar este tipo de solicitudes, sin detallar un procedimiento en este sentido. Nuevamente **EmCali, Hughesnet, Skynet** y ahora **Wom** no proporcionan ninguna información al respecto.

En la explicación de dicho procedimiento también verificamos si se prevé un paso de notificación a las personas usuarias de sus servicios sobre el tipo de bloqueo efectuado, el marco legal y la razón en que éste se motiva. En este caso **Tigo** tienen mecanismos de aviso, y ponen como ejemplo el de abuso sexual infantil.

En nuestra revisión encontramos que **Claro**, **Movistar**, **Tigo**, **ETB** y **Wom** informan sobre la ejecución de órdenes de bloqueo de sitios web o URL.

Claro, **ETB**, **DirecTv**, **Wom**, **Emcali** y **Hughesnet** informan que bloquean sitios web o URL solo en el caso de circulación de contenido de abuso sexual infantil. **Skynet** no provee información sobre ninguno de estos criterios.

Movistar informa a plenitud sobre todos los tipos de bloqueo de sitios web o URL que puede efectuar. Cuenta con un procedimiento detallado para tramitar solicitudes de bloqueos de sitio web y URL. También notifica a sus suscriptores del tipo de bloqueo que efectúa en cada caso, anunciado el soporte legal en que se motiva cada uno.

Claro es el único PSI que informa expresamente en su informe de transparencia que no efectúa bloqueos de sitios web o URL de naturaleza contractual. Sin embargo, pese a contar con un procedimiento de bloqueo, no anuncia a las personas usuarias de sus servicios sí en los asos de bloqueo de un sitio web o URL informa han sido bloqueados, o la razón de ello.

Tigo cuenta con un procedimiento detallado de bloqueo, así como informa que notifica a las personas usuarias de sus servicios cuando un bloqueo de sitio web o URL ha tenido lugar, Además señala que informa el motivo en que dicha medida se justifica señalando que “en los casos que medie orden judicial o administrativa se realizará, se realiza la verificación de que la autoridad que emite la decisión cuenta con la competencia

legal para hacerlo"[62]. Adicionalmente, si bien este año no informaron sobre un contexto particular en el 2021, como sí lo hicieron en el 2020, sobre lo sucedido en la pandemia, se destaca que sí indicaron que durante junio de 2021 fue el mes con más sitios reportados a bloquear por el Ministerio TIC.

Wom avisa que lleva a cabo bloqueos de sitio web o URL de naturaleza contractual sin proveer información sobre si cuenta o no con procedimientos de reclamo para que las personas suscriptoras que estimen que se trató de un procedimiento arbitrario puedan solicitar una revisión de dicha medida. Esta compañía dice que cuenta con un procedimiento para dar trámite a este tipo de eventos pero no informa en qué consiste.

Se identificó que uno de los tipos de solicitudes de bloqueo de contenidos en línea en las que las autoridades no judiciales tienen el poder de solicitar la eliminación de contenido reportado para 2021 por las PSI, es principalmente el abuso sexual infantil. Por un lado, instamos a las empresas a reportar si existen solicitudes de bloqueo en los otros temas - aun cuando sea cero-, así como también a compartir con mayor granularidad el estado de dichas solicitudes, si son aceptadas, si están en revisión o si fueron rechazadas. Esto para que el panorama de solicitudes de bloqueo esté más claro y para que se pueda hacer una mayor análisis de la injerencia estatal en la moderación de contenidos.

Lo anterior en el sentido en que solo con más información y con más transparencia se puede evaluar si las tendencias en estas solicitudes por autoridades en Colombia tiene un comportamiento particular en años como el 2021 de movilización social, en los que se presenta una mayor vulnerabilidad y sensibilidad de estos mecanismos al poder afectar derechos como la libertad de expresión, el acceso a la información y la participación política. Durante estos periodos la información cobra mucha importancia, así como la responsabilidad de las PSI de respetar los principios de neutralidad de la red y garantizar que en la prestación de los servicios, no se restrinja que las personas puedan informarse y comunicarse.

62 Disponible en https://assets.tigocloud.net/j1bxozgharz5/4o30TqaSceMRe2eUApq5bh/bbb9107944f2e50958941471f44a4aa1/REQUERIMIENTOS_DE_DATOS_PERSONALES_POR_TERCEROS_2022.pdf

De contexto e interés

Las reglas de moderación de contenido es un tema que está cambiando constantemente y que con el crecimiento del alcance de internet, así como la cantidad de personas usuarias y la multiplicidad de fuentes de información, la garantía de la libertad de expresión y el derecho al acceso a la información exigen a más actores una apropiada gestión de sus servicios, sus operaciones, su infraestructura, sus modelos de negocio y su respuesta a contextos desafiantes, tal como lo demostró la pandemia, los conflictos armados, contextos de inestabilidad política, las elecciones, entre otros.

Por esta razón, los PSI adquieren una mayor responsabilidad ante un aumento del flujo de información en internet, así como un incremento en las solicitudes de bloqueo de contenidos por parte de los Estados y las pretensiones de supervisión de contenidos en el espacio digital. Lo identificado por el Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) es que en Colombia en la "última década todos los años, el Congreso de la República dicta normas que de alguna u otra manera legislan los contornos del derecho a la libertad de expresión"[63], con un importante porcentaje que tiende a limitarla.

Por ejemplo, el Proyecto de Ley sobre regulación del buen uso y funcionamiento de redes sociales y sitios web presentado en 2018[64], o recientemente el Proyecto de Ley de 2021 sobre trabajo sexual en el que incluian disposiciones desproporcionadas y ambiguas sobre sobre cualquier contenido en línea y en medios de comunicación que se refieran a cualquier asunto sexual[65].

Hasta el momento hemos abordado el tema de garantía a la libertad de expresión desde la proporcionalidad, legalidad y transparencia de las solicitudes de bloqueo de contenidos y

63 Disponible en https://observatoriolegislativocele.com/wp-content/uploads/La-regulacion-de-la-libertad-de-expresion-America-Latina.pdf

64 Proyecto de ley N° 179 de 2018 sobre regulación del buen uso y funcionamiento de redes sociales y sitios web, disponible en: https://bit.ly/3H9McLM

65 Disponible en https://web.karisma.org.co/proyecto-de-ley-anti-prostitucion-crea-censura-sobre-temas-sexuales/

los procesos, criterios y prácticas de moderación de contenidos de los PSI y atención de solicitudes. Sin embargo, para el contexto nacional, el 2021 dejó evidencias de cómo la libertad de expresión se puede ver afectada no solo por los bloqueos, sino también por fallas en el acceso y conectividad a internet. Lo que exige que los PSI no solo implementan activamente los principios de neutralidad de la red y las prácticas de debida diligencia a las solicitudes de bloque de contenidos, sino que también garanticen la infraestructura, analicen y reporten los eventos de cortes o caídas de internet[66].

4. Eje sobre seguridad digital

En este eje, se evalúa si las compañías informan las fugas de datos personales y acciones de mitigación en caso de que se presenten, si tienen protocolos de notificación a las autoridades cuando suceden fallas de seguridad que comprometen los datos personales de las personas usuarias de los servicios, así como si las notifican sobre estos sucesos luego de que hayan desplegado las debidas medidas de mitigación. También tomamos nota de los portales web de cada operador y que en efecto usen un protocolo de seguridad https.

Reconocemos que para 2021 pudimos validar que todos los PSI evaluados han implementado el protocolo https en sus sitios web, razón por la que queremos concentrarnos esta vez en los criterios específicos en seguridad digital sobre reporte de fuga de datos personales y acciones de mitigaciones, en el que evaluamos las políticas y programas que respondan a: la notificación sin demora indebida a las autoridades pertinentes, notificación a las personas afectadas y el tipo de medidas que la empresa puede tomar para mitigar los daños.

Mientras que todos los operadores han incluido el certificado de seguridad en sus portales, sólo dos operadores cuentan con políticas públicas para el manejo de fugas de datos. Esta información no ha variado en comparación a los hallazgos de 2020.

66 Disponible en https://web.karisma.org.co/wp-content/uploads/2021/09/Informe-Pistolas-vs-Celulares.pdf

Al igual que lo identificado en 2021, **Movistar y Tigo** son las únicas que cuentan con un protocolo y documentación para realizar acciones de mitigación y bloqueos. **Skynet** advierte en general qué medidas de seguridad despliega pero no cuáles son las de contingencia que aplicaría para posibles brechas de seguridad.

Reconocemos que esta vez **ETB** en su Política de Tratamiento de Datos Personales habla de manejo de incidentes y medidas de seguridad en general, no obstante no describe medidas concretas de mitigación de incidentes.

Movistar advierte en su Centro de Privacidad que notificará a las autoridades ante eventos de fuga, que notificará a las personas suscriptoras de sus servicios y que hará públicas las acciones empleadas para la mitigación.

Tigo expresa en su documento titulado “Requerimiento de datos personales por terceros y bloqueos de contenido” que ante incidentes de seguridad cumplirá con la obligación legal de reportarlo ante la Superintendencia de Industria y Comercio, así como notificará a sus suscriptores de un “mecanismo eficaz (...) y las medidas realizadas por la compañía para disminuir el riesgo”.

Ahora bien, alertamos que si bien hay que avanzar en el reporte de fuga de datos personales y acciones de mitigaciones, nos interesa que los PSI también avancen en transparencia respecto a los mecanismos a través de los cuales se pueden presentar las vulnerabilidades que descubran de los servicios de internet, si revisan y responden a dichos informes de vulnerabilidad.

Recomendaciones

La transparencia en la información es un instrumento clave en la exigencia y la realización de otros derechos. Los proveedores de acceso y servicios de internet en Colombia avanzaron en la anterior evaluación con políticas en la concreción de una mayor transparencia sobre sus actividades comerciales que impactan en la libertad de expresión, privacidad y seguridad digital de las personas usuarias de sus servicios. Sin embargo, para este año, no se evidenció un avance significativo, motivo que nos lleva a reiterar la necesidad de transparencia en temas como la libertad de expresión y las caídas de internet, los problemas de privacidad, vigilancia masiva y seguridad digital, la responsabilidad creciente de los PSI frente a las solicitudes de gobierno.

Tal y como hemos documentado a lo largo de siete ediciones de ¿Dónde están mis datos?, se trata de pasos significativos en la consolidación de sus compromisos con los derechos humanos.

Recomendaciones en el *eje de compromisos políticos* apuntan en concreto a:

- Incentivar a las compañías que aún no adoptan compromisos en materia de género y accesibilidad a que emprendan esfuerzos en este sentido. No solo porque se precisa de una mayor representación del resto de la sociedad en un sector crítico como el de las tecnologías, sino porque las regulaciones y presiones de diferentes grupos de interés exigen cada vez más equidad, inclusión y diversidad, quedando rezagadas las compañías que no incorporan estás prácticas en sus modelos de negocio.

- En materia de transparencia consideramos que los PSI que aun no publican información sobre solicitudes de datos de sus suscriptores, bloqueos de URL e interceptación de las comunicaciones deben hacerlo, no solo por los mandatos legales vigentes que los obligan a ello, sino porque facilitan a su vez el ejercicio de una mayor rendición de cuentas sobre las actividades y obligaciones a cargo del Estado en cada una y respecto de la que éste no provee información activamente.

- Los PSI también deberán considerar los hechos especiales que se presentan cada año para ofrecer información puntual sobre los mismos, la pandemia o eventos especiales de tensión social, pero también situaciones más cotidianas como las elecciones, merecen informes de transparencia especiales.

- En materia de Neutralidad de la red instamos a los PSI a ir más allá de la publicación de sus prácticas de gestión del tráfico, haciendo público y expreso su compromiso por proteger el principio de Neutralidad de la red y aplicándolo a los productos y servicios que ofrecen, evaluando los posibles impactos negativos en derechos humanos.

- Establecer procesos y protocolos más claros de notificación, reporte, origen o causa de las caídas de internet. Esto contribuye a la transparencia en los casos en que no tengan prohibido notificar sobre estos acontecimientos a las personas usuarias, como también presionar a los Estados a no extralimitarse o ser desproporcionados en solicitudes relacionadas a los cortes de internet. Adicionalmente, los PSI deben anticipar que organismos internacionales de derechos humanos ya han establecido recomendaciones sobre este tema en épocas de elecciones.

Recomendaciones en el *eje de intimidad* enfatizan en:

- Empezar una transición del paradigma de notificación y consentimiento automático, a procesos de notificación a las personas suscriptoras de sus servicios para que estén enteradas sobre los eventos de entrega de sus datos personales a otras entidades o personas, especialmente a autoridades públicas.

- Adoptar los avances de las regulaciones y las compañías hacía conceptos de minimización de datos y limitación de la finalidad. Esto proporciona a las personas usuarias derechos positivos sobre sus datos a través de limitaciones directas sobre cómo pueden utilizarse, recopilarse y compartirse. A su vez, se les pide aumentar la claridad y transparencia frente a las categorías de datos personales que recogen los PSI.

- Insistimos nuevamente en que la retención de los datos de las personas usuarias de los servicios de los PSI sea precisa, que en general, de mayor información sobre lo que, en la práctica, significa almacenar y conservar esta información, incluso por un período de tiempo mucho mayor al que prevé la ley colombiana. Se requiere

de una mayor compatibilidad entre las prácticas y las normas que regulan esta materia.

- Incitamos a informar sobre situaciones como el acceso directo, a la infraestructura y datos de las personas usuarias, en sus reportes de transparencia, que permitan exigir una rendición de cuentas por parte del Estado. Al tiempo, es importante que hagan saber a estas personas cuáles son las limitaciones que les impiden efectuar un rol de protección o resguardo de la privacidad de éstos últimos.

- Generar una mayor garantía y confianza mediante buenas prácticas de protección de datos de las personas usuarias mediante análisis de impacto en privacidad. Estas evaluaciones permiten orientar el cómo las PSI pueden mitigar los daños potenciales.

Recomendaciones en el *eje de libertad de expresión*:

- Es preciso transitar al reporte de estadísticas de bloqueo de sitios web y URL más específicas y granulares que respondan a la normas locales y al contexto local. Hay diferentes eventos que se encuentran regulados en Colombia, sumado a la regulación específica para casos como el de los bloqueos por derecho de autor, por lo que, cada año, se necesitan datos de bloqueo más claros desagregados por causal de bloqueo, un período de tiempo que permita comparaciones e incluso la fuente de reporte de dichos contenidos.

- Esta mayor granularidad sobre estadísticas de bloqueo debe contextualizarse en coyunturas nacionales que representen riesgos a la libertad de expresión y el acceso a la información, además de estados de emergencia. Consideramos que es importante aumentar el detalle del procedimiento de atención a estas órdenes, así como las instancias de evaluación y rechazo que pueden insistir en su inaplicación por el impacto que tienen en el ejercicio del derecho a la libertad de expresión de sus suscriptores. Como anunciamos en 2021 esperábamos información sobre bloqueo de sitios web y URL en el paro nacional de 2021, sin embargo no encontramos información suficiente en los reportes de los PSI.

Finalmente, las siguientes son las recomendaciones en el *eje de seguridad digital* :

- Incluir, en las acciones de mitigación, información para ayudar a las personas usuarias a defenderse de los riesgos de ciberseguridad. Los PSI poseen grandes cantidades de datos de las personas usua-

rias, por lo que se espera que sus estrategias también están orientadas a ayudarlas a protegerse contra riesgos de seguridad digital y a comprender la naturaleza de los riesgos a los que pueden enfrentarse; inclusive las mismas PSI. Diferentes acciones y estrategias de comunicación permiten que los esfuerzos en seguridad digital no se queden en un lenguaje técnico y exclusivo de las empresas, sino que las personas también puedan seguir consejos o guías prácticas de mitigación de riesgos.

- Establecer compromisos para notificar en tiempo y forma a las personas usuarias afectadas por brechas de seguridad digital que expongan su información personal y sensible. Este tipo de procedimientos cuando son desplegados de manera activa pueden incluso llegar a fortalecer la imagen y credibilidad de una compañía que decide ser transparente y honesta con sus suscriptores. Adicionalmente, hay que recordar que existe un deber legal consagrado en la Ley de Protección de Datos de notificar a esta entidad este tipo de eventos

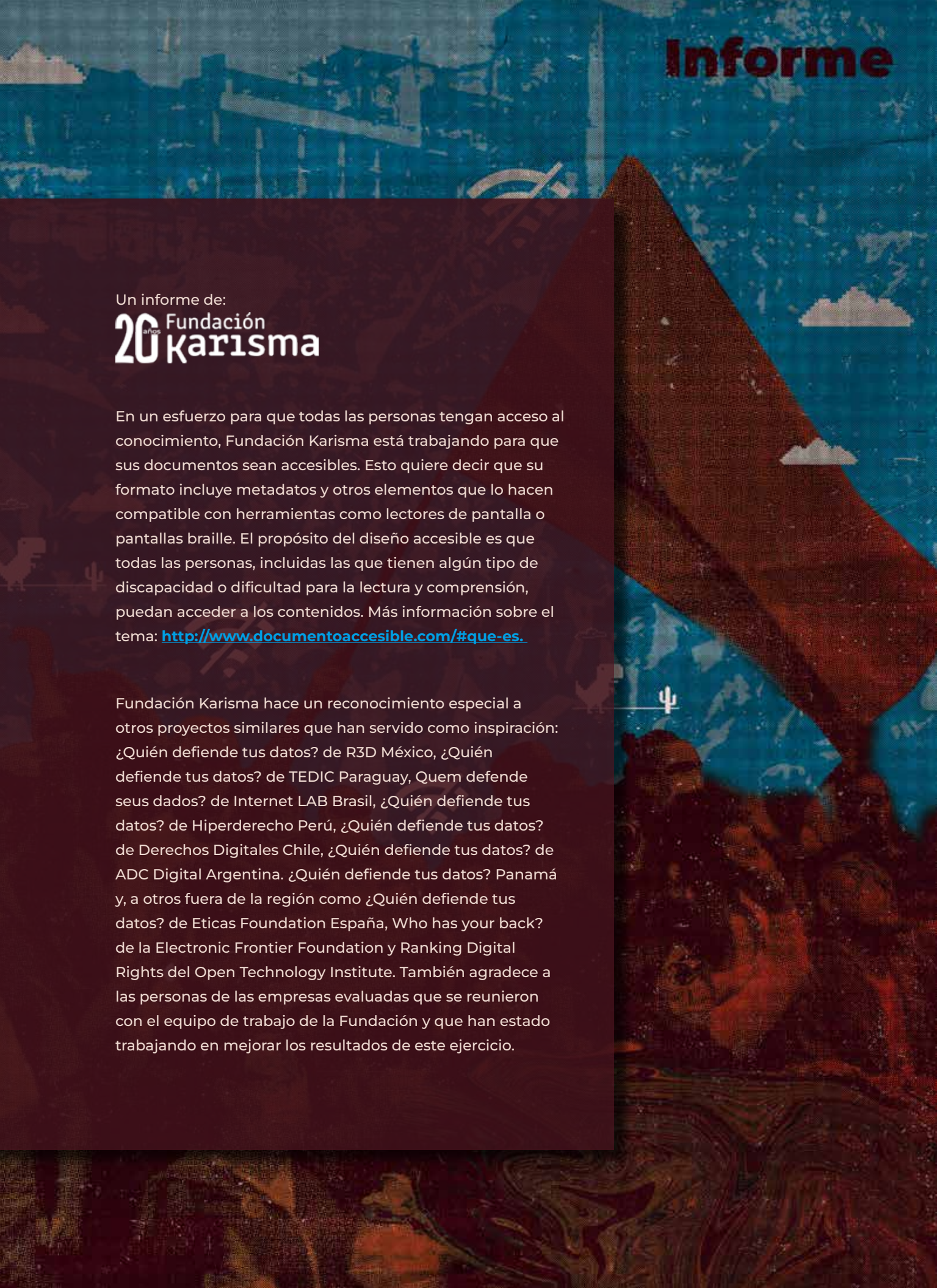
- Analizar cómo informar sobre cómo la empresa aborda las vulnerabilidades de seguridad cuando se descubran. En este tipo de proceso es importante avanzar en mecanismos en los que se puedan presentar vulnerabilidades que descubran de los servicios de internet, los procesos mediante los que se revisan y se responde a dichos eventos.

Nuevamente queremos instar a los proveedores de internet satelital a imitar los progresos de esos otros de mayor tamaño y cobertura, así como a conocer los retos que enfrentan para cumplir estos criterios de transparencia. Su rol como proveedores del acceso a internet en la ruralidad no es de menor impacto o de reducida importancia: también son actores que precisan estar a tono con los compromisos y buenas prácticas en derechos humanos vigentes en el sector de las telecomunicaciones.

Las gráficas

¿Dónde están mis datos?

Los datos de la evaluación de cada empresa se reflejan en las siguientes gráficas:



Informe

Un informe de:

Fundación Karisma 20 años

En un esfuerzo para que todas las personas tengan acceso al conocimiento, Fundación Karisma está trabajando para que sus documentos sean accesibles. Esto quiere decir que su formato incluye metadatos y otros elementos que lo hacen compatible con herramientas como lectores de pantalla o pantallas braille. El propósito del diseño accesible es que todas las personas, incluidas las que tienen algún tipo de discapacidad o dificultad para la lectura y comprensión, puedan acceder a los contenidos. Más información sobre el tema: http://www.documentoaccesible.com/#que-es.

Fundación Karisma hace un reconocimiento especial a otros proyectos similares que han servido como inspiración: ¿Quién defiende tus datos? de R3D México, ¿Quién defiende tus datos? de TEDIC Paraguay, Quem defende seus dados? de Internet LAB Brasil, ¿Quién defiende tus datos? de Hiperderecho Perú, ¿Quién defiende tus datos? de Derechos Digitales Chile, ¿Quién defiende tus datos? de ADC Digital Argentina. ¿Quién defiende tus datos? Panamá y, a otros fuera de la región como ¿Quién defiende tus datos? de Eticas Foundation España, Who has your back? de la Electronic Frontier Foundation y Ranking Digital Rights del Open Technology Institute. También agradece a las personas de las empresas evaluadas que se reunieron con el equipo de trabajo de la Fundación y que han estado trabajando en mejorar los resultados de este ejercicio.