¿QUIÉN DEFIENDE TUS DATOS?

2016

REPORTE DE EVALUACIÓN DE EMPRESAS DE TELECOMUNICACIONES ANTE LAS MEDIDAS DE VIGILANCIA

R3D
Red en Defensa
de los Derechos Digitales

RED EN DEFENSA DE LOS DERECHOS DIGITALES (R3D):

Organización mexicana sin fines de lucro, dedicada a la defensa de los derechos humanos en el entorno digital. Utiliza diversas herramientas legales y de comunicación para hacer investigación de políticas, litigio estratégico, incidencia pública y campañas con el objetivo de promover los derechos digitales en México. En particular, la libertad de expresión, la privacidad, el acceso al conocimiento y la cultura libre.

Este Informe fue realizado gracias al apoyo de:

Agradecimiento especial a:
John Gilmore
Katitza Rodriguez
Kurt Opsahl

La información y opiniones vertidas no reflejan necesariamente los criterios o visiones institucionales de EFF.

Dicembre de 2016

Diseño y formación: Paola Zorrilla Drago
Diseño original: Citlalli Dunne

ÍNDICE

CRITERIOS DE EVALUACIÓN

1 CRITERIOS DE EVALUACIÓN

La evaluación del desempeño de las empresas ha sido construida a partir de los **estándares de derechos humanos y empresas más recientes.** Para ello se han tomado en cuenta diversos instrumentos como los Principios Rectores sobre las Empresas y los Derechos Humanos de Naciones Unidas; la Guía de Implementación de los Principios Rectores para el Sector TIC (Tecnologías de la Información y la Comunicación) elaborada por la Comisión Europea; la Guía de Implementación de la Iniciativa de Internet Global (Global Network Initiative); el reporte "Who has your back?" elaborado por la Electronic Frontier Foundation, entre otros.

Asimismo, **este reporte adopta los estándares de protección de la privacidad** recogidos en el derecho constitucional mexicano, lo cual incluye los tratados internacionales en materia de derechos humanos, así como las decisiones de la Suprema Corte de Justicia de la Nación y de la Corte Interamericana de Derechos Humanos.

Como parte de estos estándares, también se recoge lo expresado por organismos de protección internacionales de derechos humanos como lo es la Resolución 66/167 de la Asamblea General de las Naciones Unidas "El derecho a la privacidad en la era digital", así como documentos e informes elaborados por la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, el Relator Especial de las Naciones Unidas para la Libertad de Opinión y Expresión y la Alta Comisionada para los Derechos Humanos de las Naciones Unidas.

A la luz de estos documentos, la perspectiva del Informe es que **la prestación de servicios de telecomunicaciones puede generar impactos negativos para el ejercicio de los derechos humanos**, especialmente para el derecho a la privacidad, **cuando autoridades llevan a cabo medidas de vigilancia encubierta** a través de esos servicios y, frecuentemente, con la colaboración de las empresas de telecomunicaciones.

Naturalmente, **existen circunstancias en las que la vigilancia de comunicaciones y la interferencia con el derecho a la privacidad** de las y los usuarios de telecomunicaciones **es legítima** desde el punto de vista constitucional y la colaboración de las empresas con las autoridades puede ser requerida por la ley, **incluso, bajo la amenaza de sanciones por la falta de colaboración.**

No obstante, **las empresas deben buscar honrar**, en primer lugar, **su responsabilidad de respetar los derechos humanos internacionalmente reconocidos**, y en caso de que existan exigencias contrapuestas, al menos, ser capaces de demostrar sus esfuerzos por respetar, en la mayor medida posible dadas las circunstancias, los principios de derechos humanos internacionalmente reconocidos.

En el contexto de operación de las empresas de telecomunicaciones, especialmente el relacionado con las medidas de vigilancia estatal, resulta particularmente importante que las empresas que proveen servicios de telecomunicaciones **adopten políticas adecuadas de respeto y protección de los derechos humanos de sus clientes,** en tanto las medidas de vigilancia de comunicaciones y de acceso a datos de usuarios, por un lado, representan una invasión severa en el derecho a la privacidad de las personas, la cual, dado el contexto de debilidad institucional en México, puede representar un grave riesgo a la integridad y la vida de las personas, además de que, **por otro lado, las medidas de vigilancia, por su propia naturaleza, se llevan a cabo sin que la persona afectada tenga conocimiento de ello**, por lo cual resulta indispensable que las empresas actúen con la debida diligencia para impedir ser cómplices de violaciones a derechos humanos.

En atención a este contexto se han desarrollado los siguientes criterios de evaluación, los cuales reflejan las expectativas de cumplimiento de derechos humanos:

1. POLÍTICA DE PRIVACIDAD

La Política de Privacidad es determinante **para la obtención de un consentimiento informado en torno al tratamiento de datos personales.** En particular, este instrumento debe ser visto como una oportunidad para informar de manera clara a los usuarios respecto de cuáles pueden ser sus expectativas y, por el contrario, este instrumento no debe ser visto como un mero formalismo legal.

Al respecto, organismos internacionales de protección de derechos humanos han señalado que **las empresas deben establecer e implementar condiciones de servicio que sean transparentes, claras, accesibles** y apegadas a las normas y principios internacionales en materia de derechos humanos, incluyendo las condiciones en las que pueden generarse interferencias con el derecho a la privacidad de los usuarios[1].

En particular, **respecto de medidas de vigilancia encubierta**, la Política de Privacidad debe establecer de manera clara **qué información es obtenida y conservada respecto de las comunicaciones del usuario,** ya sea el contenido o los metadatos y bajo qué circunstancias sucede. Asimismo, se debe informar respecto de la temporalidad con que los datos son conservados.

Resulta sumamente importante que también se refleje **cuál es la política de actuación de la empresa ante solicitudes de acceso de datos de usuarios por parte de autoridades**, de manera que se establezca claramente bajo qué circunstancias, ante que autoridades y que procedimientos se siguen para analizar y, en su caso, aceptar una solicitud por parte de una autoridad.

[1] CIDH. Relatoría Especial para la Libertad de Expresión. *Libertad de Expresión e Internet.* 31 de diciembre de 2013. OEA/Ser.L/V/II, párr. 112.

2. AUTORIZACIÓN JUDICIAL

Dado los riesgos de abuso que conlleva la utilización de una facultad de vigilancia en donde la persona afectada no tiene conocimiento de ello, **resulta indispensable la participación de un juez, el cual pueda verificar la protección de los intereses de la persona afectada** y el cumplimiento de la ley en cada requerimiento.

Por ello, como principio, **las empresas deben exigir que las autoridades que le solicitan información presenten una autorización judicial.** Lo anterior es exigido además por la Constitución, incluyendo el derecho internacional de los derechos humanos.

Por ejemplo, el artículo 16 constitucional, que reconoce el derecho a la inviolabilidad de las comunicaciones privadas, es claro al exigir la autorización de juez federal, de manera previa a que una autoridad de procuración de justicia o una autoridad judicial federal puede tener acceso al contenido de una comunicación.

Sin embargo, resulta importante señalar que la interpretación de la Suprema Corte de Justicia de la Nación[2] y de la Corte Interamericana de Derechos Humanos[3], han reconocido que **los datos que identifican una comunicación (metadatos) también se encuentran protegidos por el derecho a la inviolabilidad** de las comunicaciones privadas y por tanto, también es necesaria autorización judicial para que una autoridad competente pueda tener acceso.

Es por ello que **las empresas deben exigir la autorización judicial** previa o inmediata cuando les sea solicitado el acceso o la colaboración para obtener el contenido o los metadatos de las comunicaciones de un usuario, pues de lo contrario incumplen sus obligaciones de derechos humanos.

[2] SCJN. 2a Sala. Amparo en Revisión 964/2015.

[3] Corte IDH. Escher y otros vs. Brasil. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 6 de julio de 2009. Serie C No. 200, párr. 114.

3. NOTIFICACIÓN AL USUARIO

Otra de las salvaguardas fundamentales para proteger el derecho a la privacidad de los usuarios es el derecho de notificación al usuario afectado. Es decir, **la notificación a una persona que su privacidad fue interferida mediante una medida de vigilancia encubierta**. Si bien, dicha notificación, podría no poder llevarse a cabo de inmediato en tanto se podría frustrar el éxito de una investigación, **dicha notificación debería llevarse a cabo cuando no esté en riesgo una investigación**, no exista riesgo de fuga, de destrucción de evidencia o el conocimiento no genere un riesgo inminente de peligro a la vida o integridad personal de alguna persona.

Este derecho de notificación a las personas afectadas por medidas de vigilancia han sido reconocidas, por ejemplo, por el Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas:

> Los individuos deben contar con el derecho a ser notificados que han sido sujetos de medidas de vigilancia de sus comunicaciones o que sus comunicaciones han sido accesadas por el Estado. Reconociendo que la notificación previa o concurrente puede poner en riesgo la efectividad de la vigilancia, los individuos deben ser notificados, en cualquier caso, una vez que la vigilancia ha sido completada y se cuenta con la posibilidad de buscar la reparación que proceda respecto del uso de medidas de vigilancia de las comunicaciones[4].

Este derecho de notificación ha sido reconocido, además, por el Tribunal Europeo de Derechos Humanos, el cual determinó en el Caso Ekimdziev vs. Bulgaria que una vez que la vigilancia ha cesado y ha transcurrido el tiempo estrictamente necesario para que el propósito legítimo de la vigilancia no sea puesto en riesgo, la notificación al afectado debe llevarse a cabo sin dilación[5].

La ausencia del reconocimiento del derecho de notificación al afectado, aunado a la ausencia de control judicial o de supervisión independiente de las medidas de vigilancia de comunicaciones, como el

[4] Informe del Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas. 17 de Abril de 2013. A/HRC/23/40.

[5] TEDH. Caso de la Asociación para la Integración Europea y los Derechos Humanos y Ekimdzhiev vs. Bulgaria. Aplicación No. 62540/00. Sentencia de 28 de Junio de 2007.

acceso a datos que identifican las comunicaciones de una persona, **impide al afectado tener conocimiento en algún momento de que el espacio de intimidad que protege el derecho a la privacidad** y a la inviolabilidad de las comunicaciones privadas ha sido interferido, y por tanto, **se impide a la persona afectada el ejercicio del derecho a un recurso efectivo**, conforme a las garantías del debido proceso.

Es por ello que las empresas que prestan servicios de telecomunicaciones deben intentar establecer una política de notificación a los usuarios.

Si bien, el marco normativo mexicano puede resultar adverso a la implementación de esta política de notificación, en tanto se contemplan sanciones por conductas que pueden comprender la divulgación de información sobre una medida de vigilancia, **las empresas deben demostrar su intención real de aplicar esta política,** lo cual incluye el combatir judicialmente los impedimentos legales para notificar a usuarios afectados, al menos, **luego de que haya transcurrido un tiempo razonable para que no se frustre el objeto de la medida de vigilancia**, o al menos llevar a cabo acciones de incidencia legislativa o regulatoria para la implementación de mecanismos legales de notificación.

4. TRANSPARENCIA

La responsabilidad de respetar los derechos humanos **exige que las empresas cuenten con políticas y procesos para saber y hacer saber que respeta los derechos humanos en la práctica**. Lo anterior es reconocido, por ejemplo, en el Principio 21 de los Principios Rectores sobre las Empresas y los Derechos Humanos. Es por ello, que una práctica empresarial cada vez más común es la **emisión de reportes de transparencia.**

En concreto, los reportes de transparencia en el sector de las empresas de tecnologías de la información y la comunicación, sobre todo relacionados con los impactos en el derecho a la privacidad de los usuarios, son cada vez más frecuentes.

Es importante señalar que el reporte de transparencia **debe proveer suficiente información para evaluar el contenido y alcance, en este caso, de las medidas de vigilancia de comunicaciones** por parte de autoridades. Lo anterior implica el revelar información estadística como el número de solicitudes recibidas y cumplidas por tipo de medida, por autoridad y por motivo o fundamento legal esgrimido por la autoridad.

Adicionalmente a lo anterior, los Lineamientos de Colaboración en Materia de Seguridad y Justicia emitidos por el Instituto Federal de Telecomunicaciones (IFT) obligan a las compañías de telecomunicaciones a enviar un **informe semestral sobre el cumplimiento de las solicitudes de colaboración**[6].

[6] ACUERDO mediante el cual el Pleno del Instituto Federal de Telecomunicaciones expide los Lineamientos de Colaboración en Materia de Seguridad y Justicia y modifica el plan técnico fundamental de numeración, publicado el 21 de junio de 1996. Publicado en el Diario Oficial de la Federación el 2 de Diciembre de 2015.

5. COMPROMISO CON LOS DERECHOS HUMANOS

En vista de que, ante las medidas de vigilancia, **los usuarios no tienen conocimiento de la invasión de su privacidad**, la posición de la empresa de telecomunicaciones adquiere una relevancia particular.

En muchas ocasiones, sobre todo cuando no se contempla la intervención explícita de un juez de manera previa a que la medida de vigilancia se lleve a cabo, **la empresa es la única que puede tomar acciones para defender a los usuarios** de ejercicios abusivos de las facultades de vigilancia. Es por ello que la determinación de una empresa de combatir judicialmente una solicitud abusiva en defensa de sus usuarios representa una práctica extremadamente valiosa para los usuarios y para la satisfacción y lealtad de los mismos a la empresa. Lo anterior resulta particularmente importante cuando existen requerimientos legales que entran en conflicto con las responsabilidades empresariales de derechos humanos.

En este sentido, una forma de demostrar el compromiso con dichas responsabilidades es utilizar las herramientas disponibles para **combatir requerimientos legales abusivos** y violatorios de derechos humanos, mitigando así la participación de la empresa en dichas violaciones.

De igual manera, el Principio 16 de los Principios Rectores sobre las Empresas y los Derechos Humanos señala que una de las primeras acciones que debe tomar una empresa para cumplir con su responsabilidad de respetar los derechos humanos es la de **expresar su compromiso** con esta responsabilidad mediante una **declaración política** que, entre otras características, sea aprobada al más alto nivel de empresa.

Asimismo, otra forma de enfrentar requerimientos legales que entran en conflicto con las responsabilidades empresariales de derechos humanos de las empresas es la de llevar a cabo **acciones de incidencia legislativa** o regulatoria en favor de la privacidad de los usuarios.

En particular, resulta importante que las empresas de telecomunicaciones utilicen su capacidad de influencia para demostrar su compromiso con el cumplimiento de sus responsabilidades de derechos humanos rechazando públicamente las medidas de vigilancia masiva y las medidas de vigilancia que no poseen reglas claras ni salvaguardas adecuadas contra el abuso, lo cual, al afectar la privacidad de los usuarios, afecta la operación comercial de las empresas.

Por otro lado, es importante que las empresas **participen en mecanismos sectoriales o multiactor** a través de los cuales puedan afrontar sus responsabilidades de derechos humanos e implementar de mejor manera procesos de debida diligencia en materia de derechos humanos.

6. DERECHO DE ACCESO A TUS DATOS

El artículo 190, fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión obliga a las compañías de telecomunicaciones **a conservar, por un periodo de dos años, datos sobre las comunicaciones de todos los usuarios.** Igualmente, la Ley Federal de Protección de Datos Personales en Posesión de Particulares reconoce el derecho de acceso a los datos personales que una empresa conserve sobre ti.

De esta forma, las personas tenemos derecho a conocer los datos sobre nuestras comunicaciones que son conservados por las compañías que nos prestan servicios como el de telefonía e Internet. **Conocer estos datos puede permitirnos tener mayor conciencia sobre las implicaciones de que la ley obligue** a las personas a conservar de manera masiva e indiscriminada los datos de todas las personas que utilizan servicios de telecomunicaciones e informar de mejor manera el debate en torno a la pertinencia de las obligaciones de conservación de datos.

En particular, dado que el propio artículo 190 de la Ley Federal de Telecomunicaciones y Radiodifusión obliga a las compañías de telecomunicaciones a que el tratamiento de los datos conservados sea llevado a cabo de conformidad con las normas de protección de datos personales, es indispensable que las compañías garanticen el derecho de toda persona a conocer que datos de comunicaciones son recolectados y conservados por la compañía que presta servicios de telecomunicaciones.

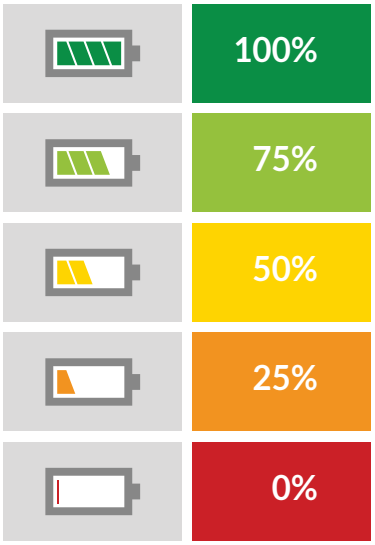
METODOLOGÍA DE EVALUACIÓN

2 METODOLOGÍA DE EVALUACIÓN

La evaluación del desempeño de las empresas evaluadas en el reporte son medidas con base en los criterios de evaluación y representadas mediante baterías de conformidad con la tabla siguiente.

Para la elaboración de este reporte, R3D analizó las políticas, contratos y otra información públicamente disponible sobre cada empresa evaluada. Asimismo, se buscó la colaboración de las empresas evaluadas mediante el ofrecimiento de una entrevista y el envío de un cuestionario con la intención de agregar información adicional al informe[7].

TABLA DE EVALUACIÓN



Las empresas seleccionadas para ser evaluadas ofrecen servicios de telefonía fija, móvil y banda ancha a la mayoría de las y los usuarios de telecomunicaciones en México. Las empresas evaluadas son:

at&t · axtel · izzi · megacable (conectamos tu vida) · movistar · telcel · telmex · totalplay

Con base en los criterios ya desarrollados, la calificación sobre el desempeño de cada empresa se llevó a cabo con base en los siguientes parámetros de evaluación:

[7] A la fecha de publicación del informe, únicamente AT&T, América Móvil y Telefónica Movistar accedieron a entrevistarse con R3D. Se tuvo contacto personal, por correo electrónico, teléfono y mensajes vía redes sociales con representantes de Axtel, Izzi, y Total Play de manera infructuosa. Ninguna empresa envió información adicional o entregó respuestas al cuestionario.

1. POLÍTICA DE PRIVACIDAD

En esta categoría se evalúa si la política de obtención, tratamiento y transmisión de datos personales de usuarios es clara, detallada y accesible para el usuario.

PARÁMETROS

1.1 La compañía tiene una política de privacidad y se encuentra disponible en su página principal de Internet.

En este parámetro se analiza si la empresa posee una política o aviso de privacidad, disponible públicamente en la página principal de Internet de la compañía, sobre el tratamiento de los datos que obtiene al prestar el servicio de telecomunicaciones y no únicamente sobre datos que otorga la o el usuario al contratar el servicio o utilizar el sitio web de la compañía.

1.2 La política de privacidad establece de manera precisa qué información del usuario y sus comunicaciones es obtenida y almacenada.

En este parámetro se evalúa si la política o aviso de privacidad establece de manera precisa y detallada la información sobre la o el usuario y sus comunicaciones que es obtenida y almacenada con motivo de la prestación de servicios de telecomunicaciones.

1.3 La política de privacidad establece la temporalidad con la que los datos del usuario son almacenados.

En este parámetro se examina si la política o aviso de privacidad establece con claridad el tiempo que la compañía conserva la información a que se refiere el punto 1.2.

1.4 La compañía posee una política o documento público en donde se establece el procedimiento a través del cual los datos de los usuarios son transmitidos a una autoridad.

En este parámetro se analiza si la compañía posee una política o documento en el que establezca el procedimiento para la colaboración con autoridades en materia de seguridad y justicia. Para cumplir con este parámetro no es suficiente indicar información de contacto para el envío de solicitudes de colaboración.

1.5 La política o documento público que establece el procedimiento de colaboración con autoridades de seguridad y justicia establece información detallada sobre las tipos de datos que entrega, los tipos de requerimientos legales que atiende y los requisitos que exige la compañía para entregar información de usuarios.

En este parámetro se evalúa si la política o documento público de la compañía a la que se refiere el punto 1.4 detalla información sobre las categorías de datos susceptibles de ser entregadas a autoridades, los tipos de requerimientos legales que atiende, los requisitos que se exigen para entregar información de usuarios y el procedimiento interno que sigue la compañía para evaluar el cumplimiento o rechazo de la solicitud. No se cumple este parámetro si únicamente se menciona la legislación o regulación que rige la colaboración en materia de seguridad y justicia.

1.6 La compañía notifica a los usuarios cuando realiza cambios a su política de privacidad, explica la naturaleza de las modificaciones en dicha notificación y conserva un registro histórico de las distintas versiones.

En este parámetro se evalúa si la compañía notifica a sus usuarios sobre cambios en su política o aviso de privacidad de manera adecuada y suficiente. Para cumplir con este parámetro es necesario que exista dicha notificación, que en la notificación se expliquen los cambios a la misma y que se mantengan accesibles las versiones previas de la política de privacidad de manera que el usuario pueda observar su evolución. No se cumple con este parámetro si la compañía pone en el usuario la carga de visitar periódicamente la página de Internet para conocer los cambios al aviso de privacidad.

Calificación

	Si cumple con todos los parámetros.
	Si cumple con cuatro o cinco parámetros.
	Si cumple con tres de los parámetros.
	Si cumple con dos de los parámetros.
	Si no cumple con al menos dos parámetros.

2. AUTORIZACIÓN JUDICIAL

En esta categoría se evalúa si las compañías exigen el cumplimiento del requisito de presentación de autorización judicial previa para que autoridades accedan al contenido y a los metadatos de comunicaciones de usuarios.

PARÁMETROS

2.1 La compañía exige la existencia de una orden judicial federal previa antes de entregar datos sobre el contenido de comunicaciones a autoridades de seguridad y justicia y ha hecho pública esta política.

En este parámetro se analiza si existe una política o documento público en el que la compañía ha asumido el compromiso público de exigir una autorización judicial previa a la colaboración con instancias de seguridad y justicia para la intervención del contenido de las comunicaciones de los usuarios.

2.2 La compañía exige la existencia de una orden judicial federal previa antes de entregar metadatos de comunicaciones del usuario a autoridades de seguridad y justicia y ha hecho pública esta política.

En este parámetro se analiza si existe una política o documento público en el que la compañía ha asumido el compromiso público de exigir una autorización judicial previa o inmediata para el acceso a metadatos de comunicaciones por parte de autoridades, como lo son los conservados en el registro de comunicaciones que establece el artículo 190, fracción II, de la Ley Federal de Telecomunicaciones y Radiodifusión.

2.3 La compañía ha reportado haber rechazado solicitudes de acceso a datos de usuarios por no cumplir con los requisitos legales.

En este parámetro se analiza si la compañía ha reportado haber rechazado solicitudes de colaboración con autoridades en materia de seguridad y justicia por no cumplir con los requisitos legales. Para el análisis de este parámetro se analiza el reporte de transparencia de la compañía o los informes semestrales que las compañías deben entregar al Instituto Federal de Telecomunicaciones.

Calificación	
	Si cumple con todos los parámetros.
	Si cumple con el parámetro 2.3 y algún otro parámetro.
	Si únicamente cumple con el parámetro 2.3 o si únicamente cumple con los parámetros 2.1 y 2.2.
	Si únicamente cumple con uno de los parámetros 2.1 o 2.2.
	Si no cumple con ningún parámetro.

3. NOTIFICACIÓN AL USUARIO

En esta categoría se evalúa si las compañías notifican a las y los usuarios afectados por solicitudes de obtención de datos personales de parte de autoridades o si han promovido el retiro de obstáculos para llevar a cabo la notificación.

PARÁMETROS

3.1 La compañía notifica al usuario afectado por una solicitud de obtención de datos de manera previa a su otorgamiento o en el primer momento permitido por la ley, o bien, ha controvertido judicialmente impedimentos legales para llevar a cabo este tipo de notificaciones.

En este parámetro se evalúa si la compañía efectúa una notificación al usuario cuando una autoridad solicita el acceso a sus datos personales. La notificación puede llevarse a cabo de manera previa a la entrega de los datos o en un momento posterior. En caso de existir impedimentos legales para llevar a cabo este tipo de notificaciones, se evalúa si la compañía los ha controvertido legalmente.

3.2 La compañía ha promovido públicamente mecanismos de notificación al usuario o usuaria ante el Congreso, el Instituto Federal de Telecomunicaciones u ante otros órganos de decisión.

En caso de que la compañía considere que la ley u otra regulación le impide llevar a cabo la notificación, debe hacer público ese análisis y demostrar que ha intentado controvertir legalmente los impedimentos legales o que ha promovido modificaciones legales o regulatorias para que le sea permitido notificar a las y los usuarios, al menos, en algún momento posterior a la medida de vigilancia en que no se ponga en riesgo la vida o integridad personal de una persona, ni se ponga en riesgo una investigación criminal u otro objetivo legítimo.

Calificación	
	Si cumple con todos los parámetros.
	Si cumple con un parámetro.
	Si no cumple con ningún parámetro.

4. TRANSPARENCIA

En esta categoría se evalúa si las compañías publican un reporte de transparencia que permita a los usuarios conocer el volumen, origen, motivos y alcance de solicitudes de autoridades para acceder a datos de comunicaciones de usuarios y usuarias.

PARÁMETROS

4.1 La compañía ha publicado en el último año un informe de transparencia sobre la colaboración de la empresa con autoridades de seguridad y justicia

En este parámetro se evalúa si la compañía ha publicado un reporte de transparencia respecto de las solicitudes de acceso a datos de usuarios por parte de autoridades de seguridad y justicia.

4.2 El informe de transparencia del parámetro 4.1 se encuentra accesible en la página de Internet de la compañía y provee, al menos, dos de las siguientes categorías:

- Número de solicitudes recibidas y cumplidas por tipo de solicitud.
- Número de solicitudes recibidas y cumplidas por autoridad.
- Número de solicitudes recibidas y cumplidas por motivo de la autoridad.

En este parámetro se analiza si el informe de transparencia respecto de las solicitudes de acceso a datos de la o el usuario por parte de autoridades de seguridad y justicia indica de manera clara y precisa, al menos, dos de las siguientes categorías:

- El número de solicitudes recibidas y cumplidas por tipo de solicitud, es decir, el informe de transparencia debe expresar cuántas solicitudes a recibido para

  1) intervención de comunicaciones privadas;

  2) acceso al registro de comunicaciones;

  3) localización geográfica en tiempo real;

  4) cualquier otra forma de colaboración o entrega de datos a autoridades de seguridad y justicia.

- El número de solicitudes recibidas y cumplidas por tipo de autoridad, es decir, el informe debe expresar el nombre de las instituciones públicas que le han solicitado información.
- El número de solicitudes recibidas y cumplidas por motivo de autoridad, es decir, el informe debe expresar, el motivo y el fundamento legal expresado por la autoridad al realizar las solicitudes.

4.3 La compañía envió al Instituto Federal de Telecomunicaciones el informe semestral correspondiente al primer semestre de 2016 al que se refiere el Lineamiento Décimo Octavo de los Lineamientos de Colaboración en Materia de Seguridad y Justicia.

En este parámetro se evalúa si la compañía ha cumplido con la obligación de enviar un informe semestral al Instituto Federal de Telecomunicaciones sobre la colaboración con autoridades en materia de seguridad y justicia. Para la evaluación de este parámetro se realizó una solicitud de acceso a la información pública al Instituto Federal de Telecomunicaciones para conocer los informes enviados por concesionarios y autorizados de telecomunicaciones respecto del primer semestre de 2016.

Calificación	
	Si cumple con todos los parámetros.
	Si cumple con el parámetro 4.1 y algún otro parámetro.
	Si únicamente cumple con el parámetro 4.1.
	Si únicamente cumple con el parámetro 4.3.
	Si no cumple con ningún parámetro.

5. COMPROMISO EN CONTRA DE VIGILANCIA MASIVA O SIN CONTROLES

En esta categoría se evalúa si las empresas han demostrado tener un compromiso público en contra de la vigilancia masiva o sin controles de sus usuarios. En este sentido, se evalúa si la compañía ha interpuesto recursos legales en contra de solicitudes ilegales o arbitrarias de acceso a datos de usuarios; si ha expresado de manera pública su postura de rechazo a la vigilancia masiva o a la vigilancia sin controles adecuados para impedir vulneraciones a la privacidad de sus usuarios; si posee una política institucional en la que reconoce sus responsabilidad de respeto y protección de los derechos humanos, incluyendo el derecho a la privacidad; si ha llevado acciones de incidencia legislativa en defensa del derecho a la privacidad; y si participa en algún foro o mecanismo para el respeto de derechos humanos en el ámbito de sus responsabilidades empresariales.

PARÁMETROS

5.1 La compañía ha hecho pública la interposición de controversias judiciales ante solicitudes específicas de acceso a datos de usuarios que exceden las facultades legales de la autoridad, que resultan desproporcionadas o que de cualquier otra manera comprometen el derecho a la privacidad de los usuarios o la compañía ha expresado públicamente su rechazo a invasiones desproporcionadas y sin controles a la privacidad de sus usuarios.

En este parámetro se analiza si la compañía ha realizado y hecho pública la interposición de alguna controversia judicial ante una solicitud específica de acceso a datos que no se haya realizado de conformidad con la legislación aplicable o con el parámetro de regularidad constitucional, el cual comprende los estándares de derechos humanos desarrollados en el derecho constitucional e internacional de los derechos humanos.

Alternativamente, se valora si existe algún pronunciamiento público por parte de algún representante de la compañía evaluada en la que exprese rechazo, de manera general o específica, a medidas de vigilancia estatal desproporcionadas o que no contienen los controles adecuados para proteger la privacidad de las y los usuarios.

Se considerará cumplido este parámetro cuando en ningún caso se detecte alguna instancia específica en la que la compañía no haya controvertido judicialmente un solicitud de acceso a datos contraria a la legislación aplicable.

5.2. La compañía ha emitido un posicionamiento institucional público en el que ha reconocido sus responsabilidades de respeto y protección de derechos humanos, incluyendo el derecho a la privacidad.

En este parámetro se analiza si la compañía posee un posicionamiento institucional público en el que haya reconocido sus responsabilidades de respeto y protección de derechos humanos, incluyendo el derecho a la privacidad.

Para este efecto, se analiza si existe algún posicionamiento que cumpla con las características señaladas por el Principio 16 de los Principios Rectores sobre las Empresas y los Derechos Humanos aprobados por el Consejo de Derechos Humanos de la Organización de las Naciones Unidas a través de la resolución 17/4, de 16 de junio de 2011[8].

El posicionamiento político debe ser público y reflejar claramente el compromiso de la empresa de respetar los derechos humanos en el marco de sus actividades empresariales.

5.3 La compañía ha llevado a cabo acciones de incidencia legislativa o ante otros entes regulatorios en defensa del derecho a la privacidad y/o la protección de los datos personales de sus usuarios.

[8] "Compromiso Político: 16. Para asumir su responsabilidad de respetar los derechos humanos, las empresas deben expresar su compromiso con esta responsabilidad mediante una declaración política que: a) Sea aprobada al más alto nivel directivo de la empresa; b) Se base en un asesoramiento especializado interno y/o externo; c) Establezca lo que la empresa espera, en relación con los derechos humanos, de su personal, sus socios y otras partes directamente vinculadas con sus operaciones, productos o servicios; d) Se haga pública y se difunda interna y externamente a todo el personal, los socios y otras partes interesadas; e) Quede reflejada en las políticas y los procedimientos operacionales necesarios para inculcar el compromiso asumido a nivel de toda la empresa."

En este parámetro se evalúa si la compañía ha participado, de manera individual o colectiva, en procesos públicos de incidencia legislativa o ante otros entes regulatorios en defensa del derecho a la privacidad.

Para este efecto, se evalúan las participaciones de representantes de la empresa en consultas públicas, foros de discusión organizados por los órganos de decisión u otros posicionamientos públicos en torno a iniciativas de ley, negociaciones de tratados internacionales o normas que incidan en la privacidad de las y los usuarios.

5.4 La compañía participa en algún mecanismo sectorial o multisectorial para la promoción, respeto y protección de derechos humanos en el ámbito de sus responsabilidades empresariales. (Ejemplos: Global Network Initiative o Telecommunications Industry Dialogue)

En este parámetro se verifica que la compañía participe en algún mecanismo sectorial o multisectorial dedicado a la promoción, respeto y protección de derechos humanos en el ámbito de sus responsabilidades empresariales.

Para la evaluación positiva de este parámetro se requiere la participación en mecanismos como la Iniciativa de Red Global (Global Network Initiative) o el Diálogo de la Industria de Telecomunicaciones (Telecommunications Industry Dialogue).

Calificación	
	Si cumple con todos los parámetros.
	Si cumple con tres parámetros.
	Si cumple con dos parámetros.
	Si cumple con un parámetro.
	Si no cumple con ningún parámetro.

6. GARANTIZA A USUARIOS EL DERECHO DE ACCESO A SUS DATOS DE COMUNICACIONES (SÓLO EMPRESAS DE TELEFONÍA MÓVIL)

En esta categoría se evalúa si las empresas de telefonía móvil garantizan a sus usuarios el derecho de acceso a sus propios datos personales, incluyendo los datos de comunicaciones conservados en el registro de comunicaciones contemplado en el artículo 190, fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión.

PARÁMETROS

6.1 Cuando un usuario lo solicita, la compañía entrega los datos personales solicitados, incluyendo los datos de comunicaciones a los que se refiere el artículo 190, fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión.

Para verificar el cumplimiento de este parámetro se realizaron solicitudes de acceso a los datos de comunicaciones conservados por mandato de la Ley Federal de Telecomunicaciones y Radiodifusión a las empresas de telefonía móvil. Si el resultado de la solicitud es favorable se considera cumplido este parámetro.

6.2 En caso de cumplir con cumplir con el parámetro 6.1, la entrega de los datos solicitados se realiza en un formato electrónico accesible y dentro del tiempo fijado por la ley.

En este parámetro se verifica que los datos sean entregados de manera completa dentro de los plazos establecidos en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Igualmente, se verifica que los datos sean entregados por vía electrónica en un formato accesible y editable como .xls o .csv.

Calificación	
✓	Si cumple con todos los parámetros.
✗	Si no cumple con el parámetro 6.1.
N/A	No aplicable.

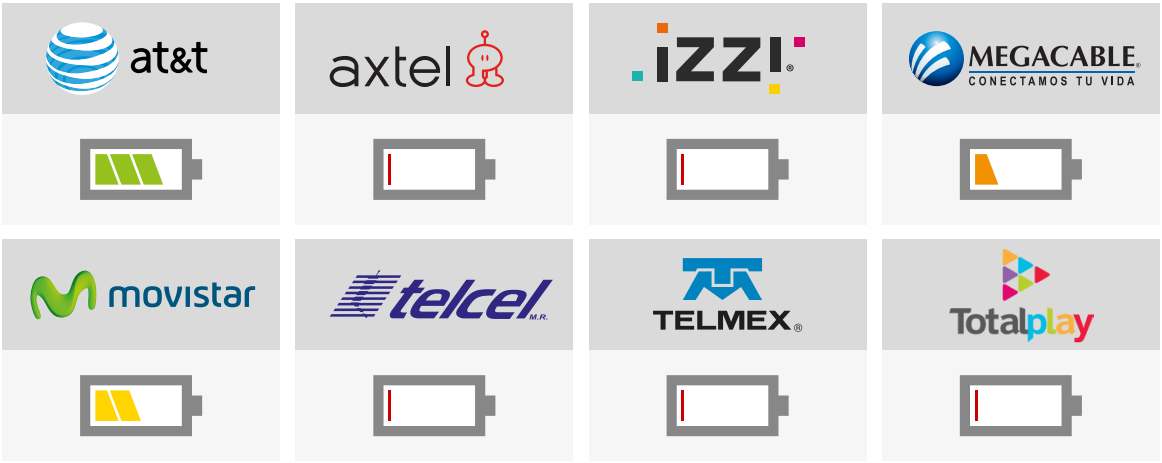
REPORTE DE EVALUACIÓN

3 REPORTE DE EVALUACIÓN

REPORTE GENERAL COMPARATIVO 2016

	PARÁMETROS						
	POLÍTICA DE PRIVACIDAD	AUTORIZACIÓN JUDICIAL	NOTIFICACIÓN AL USUARIO	TRANSPARENCIA	COMPROMISO CON DERECHOS HUMANOS	DERECHO DE ACCESO	TOTAL
at&t						✕	60%
axtel						N/A	5%
izzi						N/A	0%
MEGACABLE CONECTAMOS TU VIDA						N/A	20%
movistar						✕	35%
telcel						✕	10%
TELMEX						N/A	15%
Totalplay						N/A	0%

1. POLÍTICA DE PRIVACIDAD



AT&T[9], Axtel[10], IZZI[11], Megacable[12], Movistar[13], Telcel[14], Telmex[15] y Total Play[16] tienen una política o aviso de privacidad disponible en su página principal de Internet por lo que todas las compañías cumplen con el parámetro 1.1.

Sin embargo, únicamente AT&T y Movistar indican de manera clara qué información se recaba sobre el usuario y sus comunicaciones. El resto de las compañías ni siquiera se refieren explícitamente a los datos de comunicaciones que se recaban mediante la prestación del servicio. Por ello, únicamente AT&T y Movistar cumplen con el parámetro 1.2.

Ninguna compañía indica por cuánto tiempo se conservan los datos personales por lo que ninguna compañía cumple con el parámetro 1.3.

AT&T[17], Megacable[18] y Movistar[19] cuentan con una política sobre el procedimiento para la colaboración con autoridades en materia de seguridad y justicia. Algunas otras

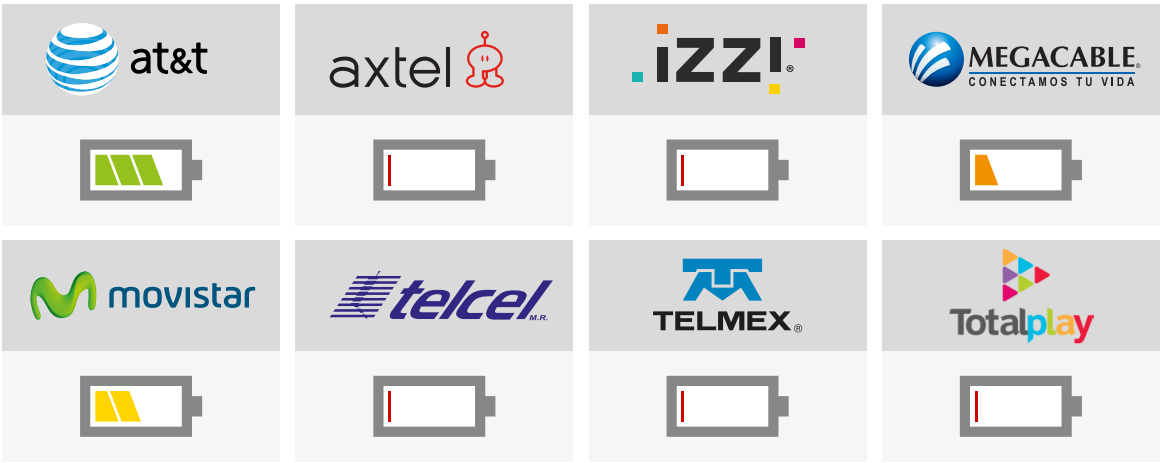
[9] Disponible en: https://www.att.com.mx/legales/aviso-de-privacidad.html
[10] Disponible en: http://axtel.mx/acerca-de-axtel/aviso-de-privacidad
[11] Disponible en: https://www.izzi.mx/legales/aviso-privacidad-izzi
[12] Disponible en: http://www.megacable.com.mx/privacidad.html
[13] Disponible en: http://www.movistar.com.mx/aviso-de-privacidad
[14] Disponible en: http://www.telcel.com/aviso-de-privacidad
[15] Disponible en: http://telmex.com/web/acerca-de-telmex/aviso-de-privacidad
[16] Disponible en: http://www.totalplay.com.mx/pdf/aviso-privacidad.pdf
[17] Disponible en: https://www.att.com.mx/documentos/procedimiento-att.pdf
[18] Disponible en: http://www.megacable.com.mx/pdf/aviso_legal_de_uso_del_portal_02.pdf
[19] Disponible en: http://www.movistar.com.mx/requerimientos-autoridad

como Axtel[20] únicamente informan a las autoridades sobre el medio de contacto para el envío de solicitudes, por ello, únicamente AT&T, Megacable y Movistar cumplen con el parámetro 1.4.

No obstante lo anterior, únicamente AT&T detalla las categorías de datos, los tipos de requerimientos legales y los requisitos que las autoridades deben cumplir para que AT&T entregue datos de usuarios. En este sentido, AT&T es la única compañía que cumple con el parámetro 1.5.

Finalmente, ninguna de las compañías notifica directamente a los usuarios cuando realiza modificaciones al aviso de privacidad sino que se impone la carga al usuario para revisar periódicamente el sitio de Internet. Ninguna empresa mantiene accesibles versiones previas de las políticas en cuestión ni explican en qué han consistido los cambios a lo largo del tiempo. Por ello, ninguna compañía cumple con el parámetro 1.6.

2. AUTORIZACIÓN JUDICIAL



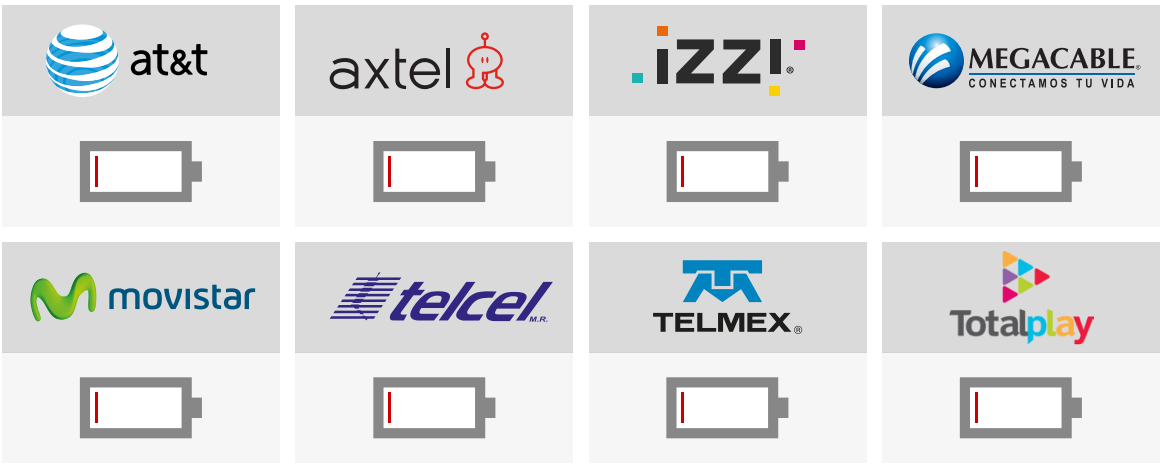
La Constitución es clara al exigir que las autoridades de procuración de justicia y otras autoridades federales designadas por las leyes deben obtener una autorización judicial federal antes de obtener acceso al contenido de las comunicaciones. Sin embargo, únicamente AT&T y Telmex establecen explícitamente este requisito para la colaboración con autoridades de seguridad y justicia que implique la intervención del contenido de comunicaciones privadas. Por ello, únicamente esas dos compañías cumplen con el parámetro 2.1.

[20] Disponible en: http://axtel.mx/acerca-de-axtel/colaboracion-con-la-justicia

Por otro lado, la Segunda Sala de la Suprema Corte de Justicia de la Nación (SCJN), al resolver el juicio de amparo que interpuso R3D en contra de los artículos 189 y 190 de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR), ha confirmado que los "metadatos" de comunicaciones, se encuentran igualmente protegidos por el derecho a la inviolabilidad de las comunicaciones privadas y por tanto, también se requiere una autorización judicial federal para acceder a los mismos. Al respecto, la evaluación no encontró que alguna de las empresas evaluadas hiciera pública su política de exigir la autorización judicial federal cuando le son solicitados metadatos de comunicaciones, por ejemplo, cuando se solicita acceso al registro de comunicaciones contemplado en la Ley Federal de Telecomunicaciones y Radiodifusión. Por ello, ninguna compañía cumple con el parámetro 2.2.

No obstante lo anterior, según los reportes que diversas compañías han entregado al Instituto Federal de Telecomunicaciones,[21] se ha detectado que AT&T, Megacable y Movistar han rechazado solicitudes de acceso a datos de usuarios por no cumplir con los requisitos legales. En el primer semestre de 2016, AT&T rechazó el 46.6% de las 5503 solicitudes de acceso a datos de usuarios, Megacable el 63.55% de las 115 solicitudes que recibió y Movistar rechazó el 7.9% de 4341 solicitudes totales. En contraste, Axtel y Telcel no rechazaron ninguna solicitud. Lo anterior es particularmente preocupante en tanto Telcel fue la compañía que recibió más solicitudes con 27672 en el primer semestre de 2016. En el caso de IZZI, Telmex y Total Play no existe evidencia en tanto no entregaron su informe semestral al IFT y no respondieron a los requerimientos de R3D para la elaboración de este reporte. En vista de lo anterior, únicamente AT&T, Megacable y Movistar cumplen con el parámetro 2.3.

3. NOTIFICACIÓN AL USUARIO



[21] Disponible en: https://drive.google.com/open?id=0B1dUggDCLwIsb0xyVXBXaWVEQIE

No se encontró que alguna empresa evaluada tenga una política pública de notificación a usuarios afectados por medidas de vigilancia. Si bien, pueden existir impedimentos legales para efectuar la notificación de manera previa o simultánea a medida de vigilancia, por ejemplo por poner en riesgo la efectividad de una investigación o comprometer físicamente la integridad de una persona, no se detectó una política de notificación para cuando la medida se haya agotado o haya transcurrido un periodo de tiempo razonable después de la conclusión.

Tampoco se detectó que alguna empresa haya combatido legalmente algún impedimento legal para efectuar la notificación ni que alguna empresa haya promovido el establecimiento de mecanismos de notificación a usuarios ante el Congreso o el Instituto Federal de Telecomunicaciones.

Por lo tanto, por segundo año consecutivo, ninguna compañía cumple con este criterio.

4. TRANSPARENCIA

Únicamente AT&T[22] publicó un informe individual de transparencia respecto de solicitudes gubernamentales de intervención de comunicaciones y de acceso a datos de usuarios y sus comunicaciones, por lo que únicamente esta compañía cumple con el parámetro 4.1.

No obstante lo anterior, el reporte de transparencia de AT&T se encuentra disponible únicamente en inglés y no ofrece suficiente información que permita saber el volumen,

[22] Disponible en: http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/international.html

origen, motivos y alcance de solicitudes, ni el número e identidad de las autoridades autoridades que solicitan a acceder a datos de comunicaciones de usuarios y usuarias por lo que no se cumplen el parámetro 4.2.

Finalmente, según fue reportado por el Instituto Federal de Telecomunicaciones[23], AT&T, AXTEL, Megacable, Telcel y Movistar cumplieron con la obligación de enviar un informe semestral relativo al número de requerimientos de localización geográfica en tiempo real y de registro de datos realizados, según lo señala el Lineamiento Décimo Octavo de los Lineamientos de colaboración en materia de seguridad y justicia emitidos por el IFT. Por lo tanto éstas empresas cumplen con el parámetro 4.3.

5. COMPROMISO CON LOS DERECHOS HUMANOS

Se detectó evidencia de que AT&T interpuso recursos judiciales en contra de solicitudes ilegales o abusivas de acceso a datos de usuarios. En concreto, según reportó el periódico Reforma[24], AT&T interpuso dos juicios de amparo en contra de solicitudes de la Comisión Federal de Competencia (COFECE), la cual no posee facultades legales explícitas para intervenir comunicaciones privadas. Dado que las invasiones a la privacidad de las comunicaciones típicamente suceden sin el conocimiento de la persona afectada, es sumamente valioso que las compañías defiendan a sus usuarios ante solicitudes abusivas o ilegales de parte de autoridades. Por esta razón, se ha considerado que AT&T ha cumplido con el parámetro 5.1.

[23] Disponible en: https://drive.google.com/open?id=0B1dUggDCLwIsb0xyVXBXaWVEQIE

[24] Disponible en: http://www.reforma.com/aplicaciones/articulo/default.aspx?id=706693

Fue detectado que AT&T[25], Movistar[26] y las empresas de América Móvil[27] (Telcel y Telmex) cuentan con un compromiso político público de reconocimiento de sus responsabilidades empresariales en materia de derechos humanos, incluyendo el derecho a la privacidad. Por ello, dichas cuatro empresas cumplieron con el parámetro 5.2.

En el periodo de evaluación del reporte no se detectó que las compañías hayan llevado a cabo acciones de incidencia legislativa o ante otros entes regulatorios en defensa del derecho a la privacidad y/o la protección de los datos personales de sus usuarios y usuarias en México, por lo que ninguna compañía cumplió con el parámetro 5.3.

Únicamente AT&T y Movistar forman parte de mecanismos para afrontar sus responsabilidades en materia de derechos humanos ya que ambas participan en el Diálogo de la Industria de las Telecomunicaciones (Telecommunications Industry Dialogue)[28]. Por tanto únicamente estas empresas cumplen con el parámetro 5.4.

6. DERECHO DE ACCESO A DATOS DE COMUNICACIONES

at&t	axtel	IZZI	MEGACABLE CONECTAMOS TU VIDA
✗	N/A	N/A	N/A
movistar	**telcel**	**TELMEX**	**Totalplay**
✗	✗	N/A	N/A

El artículo 190 de la Ley Federal de Telecomunicaciones y Radiodifusión obliga a las empresas de telecomunicaciones a retener los metadatos de las comunicaciones de todos

[25] Disponible en: https://www.att.com/Common/about_us/downloads/Human_Rights_Communications_Policy.pdf

[26] Disponible en: https://www.telefonica.com/documents/1258915/3538310/principios_actuacion_EN.pdf/90be4c50-55bd-43de-b032-1a159cc17b94

[27] América Móvil Sustainability Report 2015, p. 52. Disponible en: http://www.americamovil.com/sites/default/files/2016-09/AMX-IS-2015-ingles.pdf

[28] Ver: http://www.telecomindustrydialogue.org/about/

sus clientes por un lapso de 24 meses. Estos metadatos incluyen el origen, destino, duración, fecha, hora y ubicación de las comunicaciones, y se ha demostrado que pueden ser utilizados para revelar aspectos sensibles sobre la vida privada de las personas.

Staff de R3D solicitó a AT&T, Movistar y Telcel, el acceso a sus metadatos de comunicaciones conservados por esas empresas, sin embargo, ninguna de ellas accedió a entregar la información.

Después de que R3D interpusiera un procedimiento de protección de derechos ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), se resolvió en todos los casos que los metadatos recabados por las compañías proveedoras de servicios de telecomunicaciones son datos personales, por lo que AT&T, Movistar y Telcel deben entregarlos a los usuarios que se lo soliciten.

Dado que AT&T, Movistar y Telcel no garantizaron el derecho de acceso a datos de usuarios a sus datos de comunicaciones conservados por dichas empresas, obtuvieron una valoración negativa en este parámetro.

DICIEMBRE 2016

R3D

Red en Defensa
de los Derechos Digitales