

# ¿QUIÉN DEFIENDE TUS DATOS?

PROTEGIENDO TUS DATOS DE LA VIGILANCIA ESTATAL

Hiperderecho

Reporte de evaluación de empresas de telecomunicaciones  
ante las medidas de vigilancia estatal

Noviembre 15, 2015

hiperderecho



ELECTRONIC FRONTIER FOUNDATION

## Resumen Ejecutivo

Perú está experimentando una revolución digital. Sus ciudadanos están utilizando cada vez más Internet y los dispositivos electrónicos para ejercer el derecho a la libertad de expresión, organizar movimientos sociales, y obtener información. A medida que más peruanos usan los teléfonos móviles y las computadoras para acceder Internet, cada vez más datos privados son compartidos entre las compañías que proveen estos servicios. Sin embargo, en julio de 2015 el gobierno ha aprovechado este cambio al aprobar una ley que obliga a los Proveedores de Servicios de Internet a retener metadatos de las comunicaciones por un periodo de tiempo y permitir el acceso sin orden judicial a datos de geolocalización en casos de emergencia.

En este contexto, Hiperderecho ha lanzado el reporte “¿Quién Defiende Tus Datos?” en el que evalúa si los ISP peruanos y compañías telefónicas protegen a sus usuarios cuando el gobierno golpea sus puertas exigiendo los datos personales de sus usuarios. Desde sus inicios, este proyecto ha tenido dos objetivos principales: proporcionar a los usuarios con una evaluación clara de qué empresas de telecomunicaciones están adoptando las mejores prácticas para proteger la privacidad; y proporcionar a las empresas con una guía y recomendaciones sobre cómo pueden mejorar sus prácticas de privacidad.

En este informe, Hiperderecho analizó si las compañías publican políticas de privacidad adecuadas y fáciles de entender en sus sitios web oficiales y si las prácticas descritas son suficientes para informar a los usuarios acerca de cómo se tratan los pedidos del gobierno. Son cinco criterios de evaluación y el puntaje otorgado es visible mediante una estrella completa, media estrella o un cuarto de estrella:

- **Política de privacidad:** Para ganar una estrella, la compañía evaluada debe haber publicado una política de privacidad que sea fácil de entender. Se debe informar al usuario acerca de qué datos suyos son recopilados, cuánto tiempo se almacena, y describir directrices y los procedimientos que la compañía tiene instalados cuando una autoridad solicita los datos personales de sus usuarios. El cumplimiento parcial fue recompensado con media estrella.
- **Orden judicial:** Las compañías ganan una estrella en esta categoría si se requiere la orden de un juez antes de entregar las comunicaciones (ya sea el contenido o metadatos). El

cumplimiento con este requerimiento para el contenido de las comunicaciones, pero no para los metadatos, otorga una media estrella.

- **Notificación al usuario:** Para ganar una estrella en esta categoría, las compañías deben comprometerse a informar a sus clientes sobre el pedido de datos por parte del gobierno lo antes posible permitido por la ley. Podrían emitir notificaciones paralelas junto con las notificaciones oficiales emitidas por el gobierno después de que una medida de vigilancia haya ocurrido a través de diferentes métodos de comunicación.
- **Reportes de Transparencia:** Esta categoría busca aquellas compañías que publican reportes de transparencia sobre los pedidos gubernamentales de datos de usuarios. Para ganar una estrella completa, el informe debe proporcionar datos útiles sobre el número de pedidos que se han recibido y cumplido, incluyendo detalles sobre el tipo de pedidos, los organismos gubernamentales que lo solicitaron, y las razones dadas por la autoridad. Cumplimiento parcial es recompensado con una media estrella.
- **Compromiso con la privacidad:** Esta estrella reconoce a aquellas compañías que han desafiado la legislación que permite la vigilancia masiva o la vigilancia que autoriza el acceso del gobierno a los datos sin garantías judiciales, así como aquellos que han tomado públicamente una posición a favor de la privacidad de sus usuarios ante el Congreso u otros organismos regulatorios.

Ninguna de las compañías evaluadas ha obtenido una buena calificación en esta primera edición del informe, y algunas ni siquiera obtuvieron media estrella. Según estos resultados, las compañías de telecomunicaciones en el Perú tienen un largo camino que recorrer para proteger la privacidad de los datos de comunicaciones de sus usuarios. En categorías como “Informes de Transparencia” y “Notificación al usuario,” no existen compañías que se ganaran una estrella. En varios casos, las empresas se limitaron a publicar las políticas de privacidad en las que no incluyeron el tipo de datos que recopilaban o por cuánto tiempo se almacenan los datos.

La reciente aprobación en el Perú de una nueva ley de protección de datos ha obligado a las compañías a divulgar sus prácticas de recolección de datos cada vez que se sumen nuevos usuarios, pero la ley no los obliga a proporcionar una evaluación más completa de los datos que recogen como un subproducto de la utilización del servicio. Por lo tanto, hay poco conocimiento

sobre la forma en que tratan la información que recopilan de los usuarios tales como direcciones IP, registros de tráfico y de geolocalización, entre otros.

En este informe se urge a las compañías a estar del lado de sus clientes mediante la implementación de más y mejores prácticas en la medida permitida por la ley. Sin embargo, una de los principales hallazgos es que ciertas restricciones legales en la legislación nacional peruana pueden evitar que los operadores de telecomunicaciones adopten las mejores prácticas internacionalmente reconocidas para la notificación a usuarios, diseñadas para facultar a los usuarios la posibilidad de defender su propia privacidad. De acuerdo con el Código Procesal Penal o con las reglas del sistema nacional de inteligencia, las compañías de telefonía móvil e internet están obligadas a mantener confidencialidad sobre los pedidos de acceso del gobierno. En consecuencia, las compañías pueden estar impedidas de notificar a sus usuarios por adelantado. Sin embargo, todavía hay mucho más que estas compañías podrían hacer dentro de sus obligaciones legales. Bajo la ley peruana, los tribunales deben notificar a los ciudadanos después de que una medida de vigilancia haya expirado y, cuando esto sucede, las compañías podrían contactar en paralelo a los usuarios mediante correo electrónico o teléfono para informarles sobre la notificación. Esto permitiría que los ciudadanos ejerzan su derecho a oponerse y apelar cualquier medida de vigilancia expedida previamente por los tribunales.

El informe también revela que algunas compañías de alcance regional tienen mejores prácticas en países distintos a Perú. Por ejemplo, la mayoría de las empresas mexicanas, incluyendo Telmex (subsidiaria de América Móvil), tienen una política de privacidad publicada en su sitio web. Sin embargo, el sitio web de Claro en Perú no publica esta información.

Las compañías peruanas aún tienen un largo camino por recorrer en pos de proteger los datos personales de los clientes y ser transparentes acerca de quién tiene acceso a ella. Hiperderecho aguarda publicar este informe anualmente para incentivar a las empresas a mejorar la transparencia y la protección de los datos de usuarios. Al hacer políticas de privacidad accesibles y comprensibles, los peruanos sabrán cómo se utiliza su información personal y cómo es controlada por las compañías de telefonía e internet para que puedan tomar decisiones de consumo más inteligentes.

## Introducción

Cada vez con más frecuencia, los peruanos y peruanas depositamos mayor información sobre nuestras vidas en los teléfonos y computadoras que usamos para comunicarnos. Aunque casi siempre esos aparatos son de nuestra propiedad y uso exclusivo, las redes y servicios con las que interactuamos le pertenecen a empresas privadas nacionales y extranjeras. En este contexto, el resguardo de la privacidad personal ya no solo depende de los propios usuarios sino también de los demás intermediarios a través de cuya infraestructura viaja o se almacena la información personal de los usuarios. Por ende, resulta de mucha relevancia que los usuarios de servicios de telecomunicaciones conozcan en detalle cómo tratan las empresas privadas su información personal y que en nuestro mercado local se convierta al respeto de la privacidad en un factor de competencia más entre empresas.

En Perú, desde hace varios años contamos con normas específicas sobre el resguardo del secreto de las telecomunicaciones y más recientemente sobre protección de datos personales. Aunque estas normas son detalladas en cuanto a los cuidados y medidas de protección que deben de tomar las empresas, se dice muy poco de la forma en la que se debe resguardar esta información de agentes estatales. Las empresas peruanas están obligadas a cumplir con una serie de requisitos al obtener el consentimiento, realizar el tratamiento de datos o almacenar información protegida por el secreto de las telecomunicaciones. Sin embargo, no existen muchas reglas específicas u ordenadas para el tratamiento de las solicitudes de acceso a esta información por parte de jueces, tribunales o agencias de inteligencia. Este panorama se ha complicado en los últimos meses con la aprobación de mecanismos excepcionales de acceso a información personal con los del Decreto Legislativo No. 1182, sobre retención obligatoria de datos, entre otros.

El proyecto “¿Quién defiende tus datos” (en adelante, “QDTD”) busca identificar y sistematizar las prácticas de los proveedores de servicios de acceso a Internet respecto de la privacidad de sus usuarios. Su finalidad es ofrecer un análisis comparativo que permita al público en general conocer qué empresas tienen mejores prácticas respecto de su privacidad y las condiciones en las que se comparten sus datos con terceros. A su vez, los resultados de esta investigación buscan motivar a las empresas a mejorar sus prácticas al respecto para agregarle un elemento diferenciador a su servicios.

Este reporte sigue el modelo creado por la Electronic Frontier Foundation a través de sus reportes *Who Has Your Back? Protecting Your Data From Government Requests*,<sup>1</sup> que se publican anualmente desde hace cinco años, documentando las prácticas de las principales empresas proveedoras de Internet de Estados Unidos en base a sus políticas corporativas públicamente disponibles y destacando sus mejores prácticas. En el 2015, con el apoyo de la propia EFF, varias otras organizaciones latinoamericanas han adaptado la iniciativa en sus propios países y legislación. Es el caso de los reportes *¿Dónde están mis datos?: Buscando la transparencia de los intermediarios de Internet en Colombia*,<sup>2</sup> publicado por la Fundación Karisma de Colombia; y *¿Quién defiende tus datos?: Reporte de evaluación de empresas ante las medidas de vigilancia estatal*,<sup>3</sup> publicado por la Red en Defensa de los Derechos Digitales de México.

## 1. Contexto

### 1.1. Mercado de servicios

El servicio de provisión de acceso a Internet está reconocido en nuestro país como un servicio público de valor añadido de conmutación de datos por paquetes. Para su prestación en el mercado nacional es necesario contar con una concesión otorgada por el Ministerio de Transportes y Comunicaciones. Todas las empresas concesionarias que prestan este servicio están bajo supervisión del Ministerio de Transportes y Comunicaciones y del Organismo Supervisor de la Inversión Privada en Telecomunicaciones (OSIPTEL) en los asuntos de su competencia conforme a la regulación sectorial. Las empresas en este mercado están sujetas a un régimen de libre competencia bajo los principios de servicio con equidad, no discriminación y neutralidad.

La gran mayoría de usuarios del servicio de acceso a Internet se conectan a través de conexiones fijas (xDSL, Cablemódem o Wimax) o conexiones móviles (teléfonos móviles o banda ancha móvil). Conforme a las estadísticas reportadas por OSIPTEL, las principales empresas que prestan el servicio de acceso a Internet en Perú son Movistar (Grupo Telefónica) y Claro

---

<sup>1</sup> Electronic Frontier Foundation. *Who Has Your Back? 2015: Protecting Your Data From Government Requests*. Junio, 2015. URL: <https://www.eff.org/who-has-your-back-government-data-requests-2015>

<sup>2</sup> Fundación Karisma. *¿Dónde están mis datos?: Buscando la transparencia de los intermediarios de Internet en Colombia*. Mayo, 2015. URL: <http://dondeestanimisdatos.info/>

<sup>3</sup> Red en Defensa de los Derechos Digitales. *¿Quién defiende tus datos?: Reporte de evaluación de empresas ante las medidas de vigilancia estatal*. Junio, 2015. URL: <http://www.qdtd.mx/#reporte>

(América Móvil). En el caso del acceso a Internet fijo o domiciliario, a marzo de 2015 hay una clara dominancia de Movistar con un 82% del total de usuarios, seguido de lejos por Claro con 15% y ambos muy por encima del resto de empresas como Star Global Com, Americatel o Gilat to Home que no llegan ni al 1% del total de usuarios. La concentración de mercado es menor en el caso del acceso a Internet a través de líneas móviles, donde a septiembre de 2014 la principal cuota de mercado la tiene Movistar (56%) seguido de Claro (40%), Entel (2.6%), Bitel (0.4%) y Olo (0.2%). En total, las cinco empresas analizadas en este reporte componen más del 95% del mercado de acceso a Internet ofrecido a usuarios finales en Perú.

Aunque no existen estadísticas completas disponibles, el total de usuarios que acceden a Internet a través de redes fijas asciende aproximadamente a 1.717.714 mientras quienes lo hacen a través de redes móviles llegan a los 12.284.229 usuarios. En total, son más de 14 millones de conexiones a Internet que existen en un país con un estimado de 30 millones de personas. Sin embargo, el número de personas que efectivamente cuentan con una conexión a Internet puede variar dado que hay quienes se conectan a Internet a través de más de un dispositivo o línea.

## **1.2. Obligaciones legales en materia de privacidad**

Las empresas concesionarias del servicio de acceso a Internet tienen la obligación de salvaguardar el secreto de las telecomunicaciones y la protección de datos personales. De la misma manera, están obligadas adoptar las medidas y procedimientos razonables para garantizar la inviolabilidad y el secreto de las comunicaciones cursadas a través de tales servicios, así como mantener la confidencialidad de la información personal relativa a sus usuarios que se obtenga en el curso de sus negocios, salvo consentimiento previo, expreso y por escrito de sus usuarios y demás partes involucradas o por mandato judicial.

Esta obligación está desarrollada en una norma especial del Ministerio de Transportes y Comunicaciones que establece medidas destinadas a salvaguardar el derecho a la inviolabilidad y el secreto de las telecomunicaciones y la protección de datos personales. Específicamente, sobre la protección del secreto de las comunicaciones se señala que se atenta contra este derecho cuando deliberadamente una persona que no es quien origina ni es el destinatario de la comunicación, “sustraer, intercepta, interfiere, cambia o altera su texto, desvía su curso, publica, divulga, utiliza,

trata de conocer o facilitar que él mismo u otra persona, conozca la existencia o el contenido de cualquier comunicación, salvo las excepciones previstas en la legislación vigente.”

Adicionalmente, se señala que se atenta contra la protección de la información personal relativa a los abonados o usuarios cuando ésta es entregada a terceros, salvo las excepciones previstas en la legislación vigente.

Para salvaguardar ambos derechos, esta misma norma describe un estándar mínimo de obligaciones y condiciones de seguridad que deben adoptar las empresas que prestan servicios públicos de telecomunicaciones en su calidad de intermediarios del proceso de comunicación. En concreto señala que, además de las obligaciones mínimas que se listan, los operadores de telecomunicaciones estarán obligados a implementar medidas y procedimientos complementarios que resulten razonables para garantizar la inviolabilidad y el secreto de las telecomunicaciones y los datos personales de sus abonados y/o usuarios. Además, cada empresa deberá de presentar anualmente al Ministerio de Transportes y Comunicaciones un informe dando cuenta de las medidas implementadas para salvaguardar el secreto de las telecomunicaciones y la protección de datos personales de los abonados y usuarios de los servicios que preste.

Además de las normas sectoriales, las empresas que prestan el servicio de acceso a Internet también están obligadas a cumplir con la Ley de Protección de Datos Personales y su Reglamento. El artículo 31 de su Reglamento señala que los operadores de los servicios de comunicaciones o telecomunicaciones tienen la responsabilidad de velar por la confidencialidad, seguridad, uso adecuado e integridad de los datos personales que obtengan de sus abonados y usuarios, en el curso de sus operaciones comerciales. A continuación, señala que estos no podrán realizar un tratamiento de los citados datos personales para finalidades distintas a las autorizadas por su titular, salvo orden judicial o mandato legal expreso.

## **2. Metodología**

### **2.1. ¿Qué información hemos analizado?**

Por su propio diseño, este reporte solo ha tomado en cuenta información disponible que las empresas de telecomunicaciones han publicado voluntariamente en su página web. El objetivo de este reporte es analizar las prácticas corporativas que la empresa comunica efectivamente a los



usuarios. Por tanto, no se ha tomado en cuenta cualquier otra práctica que un usuario promedio no pueda estar en capacidad de conocer sin necesidad de consultarlo directamente a la empresa operadora o que no podamos verificar públicamente. De la misma manera, tampoco hemos analizado si es que las empresas de telecomunicaciones cumplen en todos los casos con las promesas o procedimientos que señalan en sus políticas de privacidad dado que ello implicaría analizar la totalidad de casos públicos y privados en donde esto ha sido materia de controversia.

## **2.2. ¿Cómo hemos analizado esta información?**

Esta sección describe cuáles serán los elementos a tomar en cuenta con la finalidad de evaluar a las distintas empresas comprendidas en este reporte. La evaluación final de cada empresa se realizó en torno a cinco (5) factores de competencia que se analizaron y calificaron individualmente en base a información públicamente disponible. Cada factor de competencia responde a la implementación de un conjunto de buenas prácticas respecto de la privacidad de sus usuarios por encima de lo establecido por las normas legales aplicables.

Para determinar los factores de competencia se ha tomado en cuenta el marco legal nacional aplicable al derecho a la privacidad y la protección de datos personales, las normas y decisiones aplicables del Derecho Internacional, y, principalmente, las iniciativas similares a esta implementadas por Electronic Frontier Foundation para Estados Unidos (2015), Fundación Karisma para Colombia (2015) y Red en Defensa de los Derechos Digitales para México (2015).

Sin embargo, este reporte no indaga ni diagnostica el grado de cumplimiento de las empresas de telecomunicaciones respecto de sus obligaciones actuales en materia de respeto del secreto de las telecomunicaciones y protección de datos. Este reporte considera que el simple cumplimiento de las normas nacionales sobre la materia no constituye una garantía suficiente para que el usuario tenga una expectativa razonable de privacidad al usar servicios públicos de telecomunicaciones como telefonía celular o Internet. Por el contrario, todos los criterios analizados constituyen esfuerzos adicionales que las empresas pueden hacer para ir más allá del mero cumplimiento de las normas de la materia. En ese sentido, pueden existir empresas que cumplan minuciosamente con todas sus obligaciones legales y aún así obtengan poco puntaje.

Para obtener el punto completo en cada factor de competencia, será necesario que la empresa cumpla con todos los elementos correspondientes a cada uno de ellos. El puntaje final estará conformado por la suma de la calificación obtenida en cada uno de los factores. Los puntos son gráficamente representados a través del otorgamiento de una estrella completa, media estrella o un cuarto de estrella según el caso.

**A. La empresa se preocupa por comunicar sus Políticas de Privacidad y Protección de Datos a sus usuarios**

- A1. La empresa cuenta con Políticas de Privacidad y Protección de Datos Personales aplicables al servicio de telecomunicaciones que presta (un cuarto de estrella);
- A2. La empresa comunica en lenguaje simple sus Políticas de Privacidad y Protección de Datos Personales (un cuarto de estrella);
- A3. La empresa incluye en sus Políticas de Privacidad y Protección de Datos Personales la información sobre por cuánto tiempo y para qué almacena la información de sus usuarios (un cuarto de estrella);
- A4. La empresa incluye en sus Políticas de Privacidad y Protección de Datos Personales la información sobre bajo qué supuestos y de qué manera puede entregar la información de sus usuarios a una autoridad (un cuarto de estrella).

Este apartado analiza directamente la oportunidad y formato según el cual las empresas de telecomunicaciones comunican a sus usuarios las condiciones aplicables al tratamiento de su información personal. Según la ley peruana, todo aquel que trata datos personales está obligado a informar en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que los datos personales serán tratados; quiénes son o pueden ser sus destinatarios; la transferencia de los datos personales; el tiempo durante el cual se conserven sus datos personales; entre otros.<sup>4</sup> Además, también se tiene en cuenta si es que esta información es

---

<sup>4</sup> **Ley de Protección de Datos Personales, Artículo 18.— Derecho de información del titular de datos personales**  
El titular de datos personales tiene derecho a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados; quiénes son o pueden ser sus destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y, de ser el caso, del encargado del tratamiento de sus datos personales; el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles; la transferencia de los datos personales; las consecuencias de proporcionar sus datos personales y de su

comunicada en términos sencillos o fáciles de entender a los usuarios. Dada el número y complejidad de los documentos legales que un usuario de telecomunicaciones debe suscribir al momento de contratar un servicio, creemos conveniente que la información relevante sobre el tratamiento de datos personales e información protegida por el secreto de las telecomunicaciones sea comunicada de manera sencilla a los usuarios.

Entre la información mínima que creemos que debe de incluirse en estas condiciones hemos verificado dos elementos: el aviso de por cuánto tiempo y para qué almacena la información de sus usuarios y las condiciones en virtud de las cuales se puede compartir esta información con las autoridades nacionales o internacionales.

**B. La empresa exige autorización judicial previa para permitir el acceso al contenido o a los datos relacionados con las comunicaciones de sus usuarios**

- B1. La empresa exige la existencia de una orden judicial expresa y previa antes de entregar datos sobre el contenido de comunicaciones a las autoridades de seguridad y justicia (media estrella);
- B2. La empresa exige la existencia de una orden judicial expresa y previa antes de entregar metadatos almacenados de sus usuarios (media estrella).

Esta sección evalúa si las empresas de telecomunicaciones exigen una autorización judicial previa para permitir entregar copias o permitir el acceso a las comunicaciones de sus usuarios o sus metadatos. Según la Constitución Política del Perú, las comunicaciones, telecomunicaciones o sus instrumentos sólo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado de un juez que lo haya emitido con las garantías previstas en la ley.<sup>5</sup> Sin

---

negativa a hacerlo; el tiempo durante el cual se conserven sus datos personales; y la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello.

Si los datos personales son recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones del presente artículo pueden satisfacerse mediante la publicación de políticas de privacidad, las que deben ser fácilmente accesibles e identificables.

<sup>5</sup> **Constitución Política del Perú, Artículo 2.— Toda persona tiene derecho:**

(...)

10. Al secreto y a la inviolabilidad de sus comunicaciones y documentos privados.

embargo, este criterio evalúa que las empresas incluyan esta garantía dentro de sus propias políticas de privacidad y sean expresas al momento de señalar que las órdenes judiciales deben de ser expresas, motivadas y emitidas por un juez natural conforme a las garantías procesales establecidas en la legislación peruana.

Además, diversas normas legales y jurisprudencia nacional e internacional han señalado que la información relacionada con las comunicaciones de los usuarios o “metadata” también forman parte de la información protegida por el secreto de las telecomunicaciones. Por tanto, este apartado analiza si la empresa considera expresamente la información como la ubicación, frecuencia, ubicación geográfica o tipo de tráfico cursado como parte del secreto de las comunicaciones y, en concordancia con el mandato constitucional, exige una autorización judicial para facilitar este acceso.

**C. La empresa notifica a sus usuarios cuando todo o parte de sus comunicaciones ha sido entregado a un tercero**

C1. La empresa notifica a sus usuarios cuando su información personal o comunicaciones han sido objeto de una solicitud de acceso por parte del gobierno en el primer momento permitido por la ley, a través de notificaciones paralelas a las emitidas por el juez (1).

Este parámetro evalúa si la empresa tienen previsto mecanismos de notificación a los usuarios cuyas comunicaciones han sido objeto de una solicitud gubernamental de intervención o registro. El derecho de las personas a ser notificadas cuando sus comunicaciones han sido objeto de intervención estatal está reconocido en distintos instrumentos internacionales e incluso en la propia legislación peruana. El nuevo Código Procesal Penal señala que una vez ejecutada una medida de intervención judicial y realizadas las investigaciones inmediatas en relación al

---

Las comunicaciones, telecomunicaciones o sus instrumentos sólo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez, con las garantías previstas en la ley. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen.

Los documentos privados obtenidos con violación de este precepto no tienen efecto legal.

Los libros, comprobantes y documentos contables y administrativos están sujetos a inspección o fiscalización de la autoridad competente, de conformidad con la ley. Las acciones que al respecto se tomen no pueden incluir su sustracción o incautación, salvo por orden judicial.

resultado, se deberá de comunicar de la medida al afectado siempre que el objeto de la investigación lo permitiere y en tanto no pusiere en peligro la vida o la integridad corporal de terceras personas.<sup>6</sup> Aunque la obligación legal está inicialmente en cabeza de las autoridades judiciales, hay mucho más que las empresas operadoras podrían hacer en este contexto. Así, pueden llevar un registro de las intervenciones realizadas, promover la notificación a los usuarios luego de vencida la medida o realizar notificaciones en simultáneo con las autoridades a través de correos electrónicos, mensajes de texto o llamadas de manera tal que el usuario pueda hacer valer su derecho de acudir a los tribunales de justicia para solicitar el reexamen de la medida o impugnar las decisiones emitidas. La colaboración de las empresas de telecomunicaciones para lograr que el usuario tome efectivo conocimiento de la notificación de la medida es particularmente relevante dado que la ley sólo otorga tres (3) días hábiles para controvertir la medida. Por el contrario, si consideran que el marco legal vigente no les permite notificar a los usuarios cuyas comunicaciones han sido objeto de intervención, las empresas deben de hacer público ese análisis y demostrar que han intentado desafiar legalmente los impedimentos legales o que ha promovido modificaciones legales o regulatorias.

**D. La empresa publica reportes de transparencia sobre la forma en la que trata los datos personales de sus usuarios**

- D1. La empresa publica reportes de transparencia conteniendo información estadística sobre el número de solicitudes de acceso a información personal o comunicaciones de autoridades nacionales o internacionales recibidas y aceptadas (media estrella);
- D2. La empresa pone a disposición de sus usuarios información estadística sobre la motivación, tipo de datos solicitados, de los pedidos de acceso a datos de autoridades recibidas y aceptadas (media estrella).

Este parámetro busca evaluar si las empresas publican reportes de transparencia y si los mismos son lo suficientemente detallados como para servir de base para determinar la forma y frecuencia

---

<sup>6</sup> **Código Procesal Penal, Artículo 231.— Registro de la intervención de comunicaciones telefónicas o de otras formas de comunicación**

3. Una vez ejecutada la medida de intervención y realizadas las investigaciones inmediatas en relación al resultado de aquélla, se pondrá en conocimiento del afectado todo lo actuado, quien puede instar el reexamen judicial, dentro del plazo de tres días de notificado. La notificación al afectado sólo será posible si el objeto de la investigación lo permitiere y en tanto no pusiere en peligro la vida o la integridad corporal de terceras personas. El secreto de las mismas requerirá resolución judicial motivada y estará sujeta a un plazo que el Juez fijará.

en que se cursan solicitudes gubernamentales de acceso a datos. Los reportes de transparencia son informes publicados por una o más empresas que dan cuenta del número de solicitudes de intervención de las comunicaciones o acceso a registros de las comunicaciones recibidas de las autoridades nacionales. Estos reportes pueden contener información detallada sobre el número de solicitudes recibidas, el origen de las mismas, el tipo de información o acceso solicitado, entre otras.

Sin embargo, estos reportes no señalan casos particulares ni mencionan los usuarios o expedientes involucrados. Su finalidad es proveer un dato estadístico que sirva para medir el volumen de solicitudes de acceso a información privada que el Estado está cursando. Desde hace varios años, la publicación de reportes de transparencia periódicos es una buena práctica que está rápidamente generalizándose entre las principales empresas de tecnología a través de cuyas redes se almacenan o transitan contenidos de los usuarios.

La ley peruana señala que las empresas y sus trabajadores deben de guardar la confidencialidad del caso tanto en el caso de la intervención de las comunicaciones en el marco de un proceso penal como en el marco de un proceso de obtención de información por parte del sistema de inteligencia. Sin embargo, esta obligación se entiende respecto del caso en particular y en principio no prohíbe que las empresas publiquen los números agregados de la cantidad de solicitudes que recibieron, el número de solicitudes que aceptaron o el número de usuarios involucrados en la medida.

**E. La empresa defiende la privacidad de sus usuarios a través de procesos legales y de reforma legislativa o gremios empresariales.**

- E1. La empresa ha controvertido en sede judicial mandatos o pedidos de acceso a información sobre sus usuarios que considera indebidamente formulados o sustentados (media estrella);
- E2. La empresa participa enviando comentarios formales a proyectos de ley y de propuestas de reglamentación en favor de la privacidad de sus usuarios, o ha asumido compromisos públicos con la privacidad de sus usuarios (media estrella).

Esta categoría busca reconocer y premiar a las empresas que han tomado una posición firme en defensa de la privacidad de sus usuarios y la confidencialidad de la información que ellos le han confiado. Así, se evalúa si existen registros públicos sobre si las empresas han iniciado procesos judiciales o procedimientos administrativos para controvertir pedidos de acceso a información personal indebidamente formulados o sustentados. De la misma manera, también se evalúa si la empresa ha expresado, individualmente o a través de un representante, su preocupación con una o más reformas legales que pongan en riesgo la privacidad de sus usuarios o erosionen el régimen vigente de garantías constitucionales al secreto de las telecomunicaciones y la privacidad.

### 3. Resultados de la evaluación

	Política de Privacidad	Autorización judicial	Notificación a usuarios	Reportes de transparencia	Compromiso con la privacidad
BITEL	★	★	★	★	★
CLARO	★	★	★	★	★
ENTEL	★	★	★	★	★
MOVISTAR	★	★	★	★	★
OLO	★	★	★	★	★

### 4. Evaluación por empresas

#### 4.1. Bitel

Parámetro	Resultado	Puntaje
A. Políticas de Privacidad		
A1. La empresa cuenta con Políticas de Privacidad y Protección de Datos	La empresa cuenta con una Política de Privacidad publicada en su página web y aplicable a todos sus usuarios: <a href="http://www.bitel.com.pe/help-">http://www.bitel.com.pe/help-</a>	0.25

Personales aplicables al servicio de telecomunicaciones que presta.	<a href="detail/proteccion-de-datos.html">detail/proteccion-de-datos.html</a>	
A2. La empresa comunica en lenguaje simple sus Políticas de Privacidad y Protección de Datos Personales.	La Política de Protección de Datos Personales sí está expresada en lenguaje simple y puede ser leída por un usuario promedio.	0.25
A3. La empresa incluye en sus Políticas de Privacidad y Protección de Datos Personales la información sobre por cuánto tiempo y para qué almacena la información de sus usuarios.	La Política de Privacidad señala para qué se almacena la información de los usuarios pero no explicita por cuánto tiempo.	0
A4. La empresa incluye en sus Políticas de Privacidad y Protección de Datos Personales la información sobre bajo qué supuestos y de qué manera puede entregar la información de sus usuarios a una autoridad.	La Política de Privacidad señala que que solo se podrá revelar la información de los usuarios por: (i) requerimiento legal; o, (ii) mandato de la autoridad competente.	0.25
<b>B. Autorización judicial</b>		
B1. La empresa exige la existencia de una orden judicial expresa y previa antes de entregar datos sobre el contenido de comunicaciones a las autoridades de seguridad	La empresa señala que la información personal de sus usuarios sólo podrá ser compartida ante: requerimiento legal o de autoridad competente. No se explicita que dicho pedido solo puede provenir de un juez.	0



y justicia.		
B2. La empresa exige la existencia de una orden judicial expresa y previa antes de entregar metadatos almacenados de sus usuarios.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0
C. Notificación a usuarios		
C1. La empresa notifica a sus usuarios cuando su información personal o comunicaciones han sido objeto de una solicitud de acceso por parte del gobierno en el primer momento permitido por la ley.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet	0
D. Transparencia		
D1. La empresa publica reportes de transparencia conteniendo información estadística sobre el número de solicitudes de acceso a información personal o comunicaciones de autoridades nacionales o internacionales recibidas y aceptadas.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet	0
D2. La empresa pone a disposición de sus usuarios	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet	0

información estadística sobre la motivación, tipo de datos solicitados, de los pedidos de acceso a datos de autoridades recibidas y aceptadas.		
E. Compromiso con la privacidad		
E1. La empresa ha controvertido en sede judicial mandatos o pedidos de acceso a información sobre sus usuarios que considera indebidamente formulados o sustentados.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0
E2. La empresa participa enviando comentarios formales a proyectos de ley y de propuestas de reglamentación en favor de la privacidad de sus usuarios, o ha asumido compromisos públicos con la privacidad de sus usuarios.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0

#### 4.2. Claro

Parámetro	Resultado	Puntaje
A. Políticas de Privacidad		
A1. La empresa cuenta con	La empresa no informa o no pone a disposición de	0

<p>Políticas de Privacidad y Protección de Datos Personales aplicables al servicio de telecomunicaciones que presta</p>	<p>sus usuarios esta información a través de Internet. Sin embargo, en los contratos que publica en su página web sí existen disposiciones sobre “entrega de información” que solo alcanzan a la información entregada por el usuario al momento de la suscripción del servicio más la generada como consecuencia del uso del mismo.</p> <p><a href="http://www.claro.com.pe/wps/portal/pe/sc/personas/legal-y-regulatorio">http://www.claro.com.pe/wps/portal/pe/sc/personas/legal-y-regulatorio</a></p>	
<p>A2. La empresa comunica en lenguaje simple sus Políticas de Privacidad y Protección de Datos Personales.</p>	<p>La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.</p>	<p>0</p>
<p>A3. La empresa incluye en sus Políticas de Privacidad y Protección de Datos Personales la información sobre por cuánto tiempo y para qué almacena la información de sus usuarios.</p>	<p>La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.</p>	<p>0</p>
<p>A4. La empresa incluye en sus Políticas de Privacidad y Protección de Datos Personales la información sobre bajo qué supuestos y de qué manera puede entregar la información de sus usuarios a una autoridad.</p>	<p>La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.</p>	<p>0</p>

B. Autorización judicial		
B1. La empresa exige la existencia de una orden judicial expresa y previa antes de entregar datos sobre el contenido de comunicaciones a las autoridades de seguridad y justicia.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet	0
B2. La empresa exige la existencia de una orden judicial expresa y previa antes de entregar metadatos almacenados de sus usuarios.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet	0
C. Notificación a usuarios		
C1. La empresa notifica a sus usuarios cuando su información personal o comunicaciones han sido objeto de una solicitud de acceso por parte del gobierno en el primer momento permitido por la ley.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0
D. Transparencia		
D1. La empresa publica reportes de transparencia conteniendo información estadística sobre el número de solicitudes de acceso a	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet	0

información personal o comunicaciones de autoridades nacionales o internacionales recibidas y aceptadas.		
D2. La empresa pone a disposición de sus usuarios información estadística sobre la motivación, tipo de datos solicitados, de los pedidos de acceso a datos de autoridades recibidas y aceptadas.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0
E. Compromiso con la privacidad		
E1. La empresa ha controvertido en sede judicial mandatos o pedidos de acceso a información sobre sus usuarios que considera indebidamente formulados o sustentados.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0
E2. La empresa participa enviando comentarios formales a proyectos de ley y de propuestas de reglamentación en favor de la privacidad de sus usuarios, o ha asumido compromisos públicos con la privacidad de sus usuarios.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0

### 4.3. Entel

Parámetro	Resultado	Puntaje
A. Políticas de Privacidad		
A1. La empresa cuenta con Políticas de Privacidad y Protección de Datos Personales aplicables al servicio de telecomunicaciones que presta.	La empresa sí publica en su página web un documento de Política de Protección de Datos Personales. Sin embargo, este documento solo alcanza a la información que el usuario entrega al momento de la contratación del servicio y no abarca explícitamente la información que, como parte de la prestación del servicio, la empresa recopila del usuario.  <a href="http://www.entel.pe/wp-content/uploads/2015/10/Politica-ley-de-proteccion-de-datos.pdf">http://www.entel.pe/wp-content/uploads/2015/10/Politica-ley-de-proteccion-de-datos.pdf</a>	0
A2. La empresa comunica en lenguaje simple sus Políticas de Privacidad y Protección de Datos Personales.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0
A3. La empresa incluye en sus Políticas de Privacidad y Protección de Datos Personales la información sobre por cuánto tiempo y para qué almacena la información de sus usuarios.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0
A4. La empresa incluye en sus	La empresa no informa o no pone a disposición de	0

Políticas de Privacidad y Protección de Datos Personales la información sobre bajo qué supuestos y de qué manera puede entregar la información de sus usuarios a una autoridad.	sus usuarios esta información a través de Internet.	
B. Autorización judicial		
B1. La empresa exige la existencia de una orden judicial expresa y previa antes de entregar datos sobre el contenido de comunicaciones a las autoridades de seguridad y justicia.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0
B2. La empresa exige la existencia de una orden judicial expresa y previa antes de entregar metadatos almacenados de sus usuarios.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0
C. Notificación a usuarios		
C1. La empresa notifica a sus usuarios cuando su información personal o comunicaciones han sido objeto de una solicitud de acceso por parte del gobierno en el primer momento permitido por la ley.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0

D. Transparencia		
D1. La empresa publica reportes de transparencia conteniendo información estadística sobre el número de solicitudes de acceso a información personal o comunicaciones de autoridades nacionales o internacionales recibidas y aceptadas.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet	0
D2. La empresa pone a disposición de sus usuarios información estadística sobre la motivación, tipo de datos solicitados, de los pedidos de acceso a datos de autoridades recibidas y aceptadas.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0
E. Compromiso con la privacidad		
E1. La empresa ha controvertido en sede judicial mandatos o pedidos de acceso a información sobre sus usuarios que considera indebidamente formulados o sustentados.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0
E2. La empresa participa enviando comentarios formales a proyectos de ley y	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0



de propuestas de reglamentación en favor de la privacidad de sus usuarios, o ha asumido compromisos públicos con la privacidad de sus usuarios.		
---	--	--

#### 4.4. Movistar

Parámetro	Resultado	Puntaje
A. Políticas de Privacidad		
A1. La empresa cuenta con Políticas de Privacidad y Protección de Datos Personales aplicables al servicio de telecomunicaciones que presta.	Movistar cuenta con una Normativa Interna sobre el derecho al secreto de las telecomunicaciones y la protección de datos personales de los abonados aplicable a todas las empresas de su grupo disponible en Internet <a href="http://www.movistar.com.pe/documents/10182/802001/normativa-sobre-secreto-telecomunicaciones.pdf/d3f54119-77fa-4741-a660-deee2f09b590">http://www.movistar.com.pe/documents/10182/802001/normativa-sobre-secreto-telecomunicaciones.pdf/d3f54119-77fa-4741-a660-deee2f09b590</a>	0.25
A2. La empresa comunica en lenguaje simple sus Políticas de Privacidad y Protección de Datos Personales.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0
A3. La empresa incluye en sus Políticas de Privacidad y Protección de Datos Personales la información	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0

sobre por cuánto tiempo y para qué almacena la información de sus usuarios.		
A4. La empresa incluye en sus Políticas de Privacidad y Protección de Datos Personales la información sobre bajo qué supuestos y de qué manera puede entregar la información de sus usuarios a una autoridad.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0
B. Autorización judicial		
B1. La empresa exige la existencia de una orden judicial expresa y previa antes de entregar datos sobre el contenido de comunicaciones a las autoridades de seguridad y justicia.	La empresa exige que se cuenten con una “orden judicial específica” para otorgar acceso a terceros a la información de sus usuarios.	0.5
B2. La empresa exige la existencia de una orden judicial expresa y previa antes de entregar metadatos almacenados de sus usuarios.	No se distingue si es que el requisito de “orden judicial específica” solo aplica a la información en tiempo real o también a la almacenada o retenida. Tampoco se señala expresamente que esta información abarque los datos relacionados con las comunicaciones o la “metadata”.	0
C. Notificación a usuarios		
C1. La empresa notifica a sus usuarios cuando su	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0

información personal o comunicaciones han sido objeto de una solicitud de acceso por parte del gobierno en el primer momento permitido por la ley.		
D. Transparencia		
D1. La empresa publica reportes de transparencia conteniendo información estadística sobre el número de solicitudes de acceso a información personal o comunicaciones de autoridades nacionales o internacionales recibidas y aceptadas.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0
D2. La empresa pone a disposición de sus usuarios información estadística sobre la motivación, tipo de datos solicitados, de los pedidos de acceso a datos de autoridades recibidas y aceptadas.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0
E. Compromiso con la privacidad		
E1. La empresa ha controvertido en sede judicial mandatos o pedidos de acceso a información sobre sus	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0

usuarios que considera indebidamente formulados o sustentados.		
E2. La empresa participa enviando comentarios formales a proyectos de ley y de propuestas de reglamentación en favor de la privacidad de sus usuarios, o ha asumido compromisos públicos con la privacidad de sus usuarios.	<p>Movistar ha publicado un Manifiesto Digital que incluye a la Privacidad como uno de los pilares de sus operaciones globales y señala la necesidad de que las solicitudes gubernamentales sean más explícitas al pedir información de los usuarios.</p> <p>Además, Movistar forma parte del Diálogo de la Industria de las Telecomunicaciones (Telecommunications Industry Dialogue), una alianza de operadores que han estandarizado sus prácticas a los principios para Empresas y Derechos Humanos de Naciones Unidas.</p> <p><a href="http://www.digitalmanifiesto.telefonica.com/manifiesto/">http://www.digitalmanifiesto.telefonica.com/manifiesto/</a></p>	0.25

#### 4.5. Olo

Parámetro	Resultado	Puntaje
A. Políticas de Privacidad		
A1. La empresa cuenta con Políticas de Privacidad y Protección de Datos Personales aplicables al servicio de telecomunicaciones que presta.	<p>La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet</p> <p><a href="https://olo.com.pe/legal-y-regulatorio">https://olo.com.pe/legal-y-regulatorio</a></p>	0
A2. La empresa comunica en	La empresa no informa o no pone a disposición de	0

lenguaje simple sus Políticas de Privacidad y Protección de Datos Personales.	sus usuarios esta información a través de Internet.	
A3. La empresa incluye en sus Políticas de Privacidad y Protección de Datos Personales la información sobre por cuánto tiempo y para qué almacena la información de sus usuarios.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0
A4. La empresa incluye en sus Políticas de Privacidad y Protección de Datos Personales la información sobre bajo qué supuestos y de qué manera puede entregar la información de sus usuarios a una autoridad.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0
B. Autorización judicial		
B1. La empresa exige la existencia de una orden judicial expresa y previa antes de entregar datos sobre el contenido de comunicaciones a las autoridades de seguridad y justicia.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0
B2. La empresa exige la existencia de una orden judicial expresa y previa antes	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0

de entregar metadatos almacenados de sus usuarios.		
C. Notificación a usuarios		
C1. La empresa notifica a sus usuarios cuando su información personal o comunicaciones han sido objeto de una solicitud de acceso por parte del gobierno en el primer momento permitido por la ley.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0
D. Transparencia		
D1. La empresa publica reportes de transparencia conteniendo información estadística sobre el número de solicitudes de acceso a información personal o comunicaciones de autoridades nacionales o internacionales recibidas y aceptadas.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0
D2. La empresa pone a disposición de sus usuarios información estadística sobre la motivación, tipo de datos solicitados, de los pedidos de acceso a datos de autoridades recibidas y aceptadas.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0

E. Compromiso con la privacidad		
E1. La empresa ha controvertido en sede judicial mandatos o pedidos de acceso a información sobre sus usuarios que considera indebidamente formulados o sustentados.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0
E2. La empresa participa enviando comentarios formales a proyectos de ley y de propuestas de reglamentación en favor de la privacidad de sus usuarios, o ha asumido compromisos públicos con la privacidad de sus usuarios.	La empresa no informa o no pone a disposición de sus usuarios esta información a través de Internet.	0

## 5. Conclusiones

- Todas las empresas evaluadas han obtenido una calificación desaprobatória. Esto significa que existen mucho más que las empresas de telecomunicaciones en Perú pueden hacer para garantizar la privacidad de las comunicaciones de sus usuarios y de sus datos personales. En algunos casos, las empresas se han limitado a publicar un documento de Políticas de Privacidad que, no obstante, no señala la información que se recopila del usuario durante la prestación del servicio ni se precisa el tiempo por el cual quedará almacenada o los supuestos en los que podrá ser entregada a las autoridades. En otros casos, las empresas no han publicado ningún documento que establezca la forma en la que tratarán la información personal de sus usuarios y no han obtenido ninguna estrella en ninguna de las categorías evaluadas.

- La aprobación de un marco legal específico aplicable a la protección de datos personales ha servido para que las empresas se preocupen por listar la información que recopilan de sus usuarios al momento de suscribir el contrato (nombre, dirección, número de documento). Sin embargo, existe muy poca información disponible al público sobre la manera en la que tratan otro tipo de información que recopilan de sus usuarios como direcciones IP, registros de tráfico, registros de geoubicación, entre otros.
- Existen ciertas restricciones legales que impiden que las operadoras adopten mejores prácticas en términos de respeto de la privacidad de sus usuarios. Es el caso de las obligaciones de guardar reserva respecto de las solicitudes de acceso a comunicaciones o entrega de información señaladas en el Código Procesal Penal o en las normas del sistema nacional de inteligencia. Sin embargo, las empresas bien podrían notificar a los usuarios en forma paralela a la notificación oficial emitida por el juez luego de que una medida de vigilancia ha sido llevada a cabo.
- Resulta llamativo que algunas empresas de alcance regional tengan mejores prácticas en otros países que en Perú. Así, por ejemplo, las operaciones colombianas o mexicanas de Claro (América Móvil) sí publican en su página web las Políticas de Privacidad aplicables a los servicios que prestan. Sin embargo, la página web de Claro en Perú no pone a disposición de sus usuarios esta información.