

Privacidad *y seguridad*

En las sociedades democráticas la privacidad es un valor fundacional, reflejada en varios derechos fundamentales, como el de la protección de datos o el derecho a la intimidad. En Telefónica lo tenemos muy presente y ponemos especial empeño en los desarrollos de seguridad para nuestros clientes.



El concepto de privacidad, tal y como lo entendemos en Telefónica, está muy delimitado por el contexto histórico, la cultura, los usos y, desde luego, la innovación tecnológica de un país o región geográfica determinada. En las sociedades democráticas, como la nuestra, la privacidad es un valor fundacional. Los marcos legislativos la han acuñado como el derecho de la persona a que nada ni nadie interfieran sus comunicaciones privadas (derecho al

secreto de las comunicaciones), en la gestión de sus datos personales (derecho a la protección de datos personales), o en la protección de su intimidad personal o familiar (derecho a la intimidad). En este sentido, y desde la expansión de Internet, la 'confidencialidad de la información' y el uso de los datos personales con propósitos comerciales se han convertido en uno de los aspectos más debatidos y controvertidos de la última década.

Nosotros no concebimos la privacidad como un concepto unidimensional y por ello hablamos de 'confianza digital' como un término que abarca los conceptos de privacidad, transparencia y seguridad. Este es un enfoque sostenible en el que los ciudadanos pueden tener el control de sus propios datos personales, conservar su identidad privada y saber que sus datos están seguros.

En definitiva, nuestro compromiso con este principio nos ha llevado a diseñar una cultura basada en mejorar la confianza digital de nuestros consumidores, con unas normas de comportamiento comunes y obligatorias para todas nuestras regiones y entidades, y una serie de posiciones claras y coherentes en relación con nuestras prácticas de privacidad y protección de datos. Los pilares sobre los que se sustenta esta cultura son:

- ⇒ La autorregulación de los derechos y la seguridad de los usuarios, mucho más allá de las leyes locales e internacionales.
- ⇒ La transparencia como motor de la confianza y los atributos claves de Telefónica.
- ⇒ La privacidad como elemento que hace posible la innovación, el bienestar y la prosperidad en el mundo digital.

La aceptación de estos principios globales nos ayudará a establecer un marco global común a partir del cual se podría desarrollar una experiencia digital segura, transparente y privada, una base sólida para el crecimiento sostenible de una economía y sociedad digitalizadas.

PRIVACIDAD

Política y Comité de Privacidad

El objetivo de la Política de Privacidad, aprobada por el Consejo del Grupo Telefónica, es establecer las bases de actuación que deben seguir las empresas del Grupo en la protección de la privacidad de todas aquellas personas que nos confían su información a través del uso de nuestros productos y servicios.

Esta política responde a nuestros [Principios de Actuación](#) y describe qué tipo de información recogen las empresas del Grupo y cómo es tratada para garantizar la privacidad de los usuarios. Adicionalmente, incorpora nuestros compromisos en:

- ⇒ Transparencia y elección en la utilización de información personal.
- ⇒ Derecho de acceso, rectificación, oposición y cancelación de la información personal.
- ⇒ Seguridad e integridad de datos personales.
- ⇒ Privacidad de menores.

Esta Política nos ha permitido mantener una posición única, clara y coherente en privacidad y protección de datos, y aprovechar al máximo las oportunidades que genera el actual entorno digital para Telefónica.

El Comité de Privacidad se creó en 2013 como punto de referencia, tanto interno como externo, para dar soporte a las actuaciones de Telefónica en ese ámbito. Es el órgano que vela por la implantación global de la Política de Privacidad. El Comité de Privacidad es responsabilidad última del Chief Privacy Officer, quien, en el ámbito del Grupo Telefónica, es el encargado de velar por el cumplimiento de la normativa nacional e internacional en materia de protección de datos.

Durante 2014 Telefónica ha seguido trabajando como miembro del Grupo de Diálogo de la Industria –[Telecom Industry Dialogue](#)–, un grupo de nueve operadores y vendedores globales del sector de las telecomunicaciones para implementar de forma conjunta los 10 Principios Rectores para la Privacidad y la Libertad de Expresión firmados y publicados en marzo de 2013. En el Informe de Sostenibilidad de 2013 publicamos por primera vez nuestro avance. Nuestro progreso y las medidas adoptadas durante 2014 se describen en la tabla de la siguiente doble página.

Principios Rectores para la Privacidad y la Libertad de Expresión en Telefónica

Principio rector	Programa de Telefónica
<p>1 Crear y/o mantener políticas pertinentes, bajo la supervisión del Consejo de Administración o equivalente, resaltando el compromiso para prevenir, evaluar y mitigar, en la medida de sus capacidades, los riesgos para la libertad de expresión y la privacidad asociados con el diseño, venta y operación de tecnología y servicios de telecomunicaciones.</p>	<ul style="list-style-type: none"> ■ Nuestros Principios de Actuación revisados en 2010 reconocen el derecho a la privacidad como base de una relación de confianza con nuestros grupos de interés. ■ Asimismo, el Grupo dispone de una Política de Privacidad aprobada por el Consejo en marzo de 2013 que es de obligado cumplimiento en todos los países donde operamos. ■ El Grupo dispone de la figura del Chief Privacy Officer, máximo responsable de la implantación y seguimiento de la Política, que se apoya en los Data Protection Officer locales. ■ En lo que se refiere a la gestión de la seguridad, el Grupo dispone de la Política Corporativa de Seguridad de la Información, además de otras normativas, basada en estándares internacionales y actualizada conforme a las crecientes demandas internacionales en materia de seguridad. Además de realizar formación específica sobre dicha Política, todos nuestros empleados tienen acceso a ella a través de la Intranet del Grupo.
<p>2 Realizar regularmente evaluaciones de impacto en los Derechos Humanos y utilizar procesos de debida diligencia, adecuados a la Compañía, para identificar, mitigar y gestionar riesgos para la libertad de expresión y la privacidad (tanto con relación a tecnologías, productos y servicios, como en países concretos) de conformidad con los Principios Rectores para la aplicación del marco 'Proteger, respetar y remediar' de la ONU.</p>	<ul style="list-style-type: none"> ■ El respeto y el compromiso con los Derechos Humanos es una de las bases de nuestros Principios de Actuación. Por ello, y siguiendo el marco ofrecido por los Principios Rectores sobre Empresas y Derechos Humanos, en 2012 realizamos un <i>assessment</i> –con el apoyo de Business for Social Responsibility– en todas nuestras operaciones para evaluar el impacto global de nuestra actividad. Durante 2014, Telefónica ha seguido integrando las conclusiones de la evaluación de impacto sobre los Derechos Humanos que tuvo lugar a través de sus unidades de negocio en 2012. Esto incluyó una nueva evaluación a nivel global de cómo sus negocios operativos responden a solicitudes gubernamentales de los datos personales de los usuarios o de restricción de contenido, así como las circunstancias y contextos en los que estas peticiones se reciben generalmente. Como parte de este proceso, Telefónica desarrollará en 2015 una guía global de procedimientos ante requerimientos gubernamentales.
<p>3 Crear y/o mantener procesos y procedimientos operativos para evaluar y gestionar las solicitudes gubernamentales que puedan tener un impacto sobre la libertad de expresión y la privacidad.</p>	<ul style="list-style-type: none"> ■ Telefónica dispone de procesos para atender los requerimientos recibidos por autoridades locales/gubernamentales. Estos procesos son responsabilidad de las áreas de Secretaría General y Seguridad de cada una de las empresas del Grupo. Desde el Comité de Privacidad y el Comité de Seguridad se vela por sensibilizar e informar sobre la necesidad de documentar tales procesos.
<p>4 En la medida de lo posible, adoptar estrategias para anticiparse, responder y minimizar el impacto potencial sobre la libertad de expresión y la privacidad en el supuesto de que se reciba una petición o exigencia gubernamental ilegal, o bien se considere que los gobiernos están haciendo un mal uso de los productos o la tecnología para fines ilegítimos.</p>	<ul style="list-style-type: none"> ■ Las figuras del Chief Privacy Officer a nivel global y de los Data Protection Officers dan mayor homogeneidad a los procedimientos y procesos que afectan a la privacidad de nuestros clientes. El Comité de Privacidad articula su misión y funciones a través del Global Chief Privacy Officer y de los Data Privacy Officers/Data Protection Officers (DPOs) de cada empresa del Grupo.
<p>5 Buscar siempre garantizar la seguridad y la libertad de los empleados de la Compañía que puedan estar expuestos a situaciones de riesgo.</p>	<ul style="list-style-type: none"> ■ Salud, seguridad y bienestar en el trabajo son los tres pilares de Telefónica, no solo para garantizar la protección de sus empleados, sino también para tener una influencia directa sobre su satisfacción en el trabajo para la Compañía. En materia de seguridad física, la Dirección Global de Seguridad establece una serie de pautas a seguir adecuadas a los riesgos identificados en cada país, además de cubrir el propio proceso de desplazamiento.

Principio rector

6 Sensibilizar y formar a los empleados involucrados en las políticas y procesos pertinentes.

7 Compartir conocimientos e impresiones, cuando sea relevante y apropiado, con todas las partes interesadas implicadas para comprender mejor el marco legal y la eficacia de estos principios en la práctica, y proporcionar apoyo para su aplicación y desarrollo.

8 Anualmente, y cuando las circunstancias lo hagan necesario, informar externamente sobre los progresos realizados en la aplicación de los principios y, cuando proceda, sobre los principales eventos que se produzcan al respecto.

9 Ayudar en la elaboración de políticas y normativas que promuevan la libertad de expresión y la privacidad, bien de manera individual o en colaboración con otras entidades, buscando mitigar los potenciales impactos negativos derivados de políticas o regulaciones.

10 Examinar, conjuntamente, las opciones para la implementación de los mecanismos adecuados de reclamación, tal como se detalla en el Principio 31 de los Principios Rectores de la ONU para las Empresas y los Derechos Humanos.

Programa de Telefónica

■ El Grupo Telefónica ha diseñado un plan específico para formar y sensibilizar a sus empleados en las políticas y procesos que les competen. Este programa de formación continua se realiza tanto de manera presencial como *online*. Durante 2014, más de 62.250 empleados han sido formados en Protección de Datos y Seguridad de la Información.

■ Consideramos fundamental el diálogo continuo con nuestros grupos de interés para identificar y mitigar los riesgos, así como desarrollar nuevas oportunidades de negocio. Creemos que tanto la transparencia como el compartir conocimientos con dichos grupos es clave para impulsar estos Principios Rectores. Además, Telefónica ha emprendido un proyecto para mapear los grupos de interés internos y externos a nivel corporativo y local en temas de libertad de expresión y privacidad. El resultado de este mapa determinará el nivel y modo de relación con cada uno de ellos, con el fin de mejorar la capacidad de respuesta de Telefónica a las consultas de las partes interesadas. Asimismo, en el seno del Comité de Privacidad, los Data Protection Officers y los responsables de la Corporación ponen en común y discuten los proyectos comerciales, institucionales y regulatorios más relevantes en materia de privacidad, con la idea de asegurar una aproximación consistente en toda la organización. En paralelo, existe un canal de comunicación interno (Global Privacy Center, en Yammer) del que forman parte todas las personas relacionadas o interesadas en la gestión de la privacidad a nivel Grupo y que sirve para compartir experiencias, novedades y estrategias.

■ El presente Informe sintetiza los avances realizados por el Grupo Telefónica en materia de privacidad y libertad de expresión.

■ Estamos convencidos de que la mejor forma de lograr el avance global en el respeto a la libertad de expresión y en la privacidad es a través del diálogo entre gobiernos, industria, sociedad civil (incluidos expertos sobre Derechos Humanos), inversores, organizaciones supranacionales y otras partes interesadas. Evidencia de ello es nuestro [Manifiesto Digital](#), publicado en enero de 2014. El Manifiesto pone de relieve los retos y desafíos a resolver por las políticas públicas para liberar todo el potencial del mundo digital en beneficio de consumidores, empresas y administraciones públicas, a la vez que proporciona diez recomendaciones para mejorar la experiencia de usuario en Internet y promover mayores inversiones en infraestructuras digitales. Asimismo, a nivel interno y con el fin de velar por la adecuada implementación y cumplimiento de la Política de Privacidad, en el seno del Comité Global de Privacidad se desarrollan, consensúan y aprueban normativas, instrucciones y guías relacionadas con los más diversos aspectos de la privacidad (gestión de incidencias, estructuras recomendables, descripción de funciones y actividades, desarrollo de webs y *apps* seguros, etc.). El Comité es el punto de referencia interno y externo, y soporte de las actuaciones en el ámbito de la privacidad.

■ Telefónica está desarrollando los mecanismos de reclamación a nivel corporativo y local apropiados para poder ser implementados en 2015-2016.

SEGURIDAD Y PROTECCIÓN DE DATOS

Para garantizar que los datos de nuestros clientes y de nuestros servicios se mantienen a salvo y seguros, Telefónica dispone de varias normativas que fortalecen la seguridad de la información.



Seguridad de la información

- Política corporativa de seguridad de la información.
- Normativa corporativa de seguridad de la información.
- Reglamento corporativo de controles mínimos de seguridad.
- Reglamento de redes sociales.
- Reglamento corporativo de seguridad de servicios en la nube.
- Reglamento corporativo de seguridad en dispositivos de trabajo.



Protección de datos

- Política de Privacidad del Grupo Telefónica.
- Instrucción sobre la protección de datos de carácter personal del Grupo Telefónica.



Tecnología de la información

- Normativa sobre controles básicos sobre tecnología de la información.

Las empresas del Grupo Telefónica siguen las directrices en materia de seguridad de la información definidas por el Comité Corporativo de Seguridad. El objetivo de este órgano es velar por la mejora continua de la seguridad, garantizando un nivel mínimo homogéneo y acorde con las necesidades de cada negocio. Sus responsabilidades, además, incluyen el establecimiento de políticas, estándares y procedimientos de implementación de usos y buenas prácticas, el seguimiento de la obtención de certificaciones dentro de las compañías del Grupo y una monitorización continua, con reportes al Comité de Seguridad.

Seguridad de los datos

Telefónica tiene un concepto interno de seguridad integral global del Grupo que cubre la seguridad de la información recogiendo un conjunto de medidas preventivas y reactivas sobre la protección de los datos personales y los sistemas tecnológicos, lo cual permite resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad y la integridad de la misma.

Para nuestros clientes la seguridad de la información tiene un efecto significativo respecto a su privacidad, cobrando distintas dimensiones en función de la cultura y el país.

Dentro del Comité Corporativo de Seguridad de Telefónica se realiza un seguimiento específico sobre las certificaciones de seguridad del Grupo cuyo alcance es el desarrollo, la implementación y el mantenimiento del sistema de gestión de certificaciones de la Compañía.

Mapa de certificaciones del Grupo Telefónica



Gestión de servicios de tecnologías de la información.



Gestión de continuidad de negocio.



Gestión de seguridad de la información.



Gestión de la calidad.



Sistema de gestión de seguridad y salud ocupacional.



Estándar de seguridad de datos para la industria de las tarjetas de pago.

Seguridad en los servicios

Las amenazas y ataques, tanto para los usuarios de las redes de comunicación como para las propias redes e infraestructuras críticas de los gobiernos, son cada vez más numerosos y sofisticados. En el propio BackBone de Telefónica se despliegan sistemas como el Escudo DDoS para poder mitigar los ataques de denegación de servicio tanto a infraestructuras propias como a clientes. En cuanto a defensa de *software* malicioso, *phishing* y robo de identidad digital tenemos Smart DNS.



Latch, para Windows Mobile y Firefox OS (FFOS), fue presentado en el MWC 2014.

En 2014, se ha abordado un proceso de transformación basado en la innovación a través de la tecnología. Desde Telefónica, en nuestra apuesta por la ciberseguridad y la inversión en desarrollos propios, hemos lanzado nuevos servicios con nuevas capacidades en materia de seguridad que contribuyen a que los negocios de nuestros clientes estén más protegidos frente a las amenazas en los entornos en los que operan.

⇒ Eleven Paths ha centrado los esfuerzos en el desarrollo de productos innovadores y únicos en el mercado. La prueba de esos esfuerzos han sido varias:

- **Path5**, un nuevo producto de ciberinteligencia para luchar contra las amenazas del mundo móvil. Se trata de un producto de ciberseguridad desarrollado por ElevenPaths que permite y facilita, a los profesionales y expertos en seguridad, la investigación en entornos de aplicaciones móviles mediante su tecnología patentada de *gig data* y motor de correlación. Además, ofrece una solución integral que mejora el análisis y la investigación para responder a cualquier acción fraudulenta en la que haya podido utilizarse algún componente móvil. Path5 permite a los analistas rastrear la actividad de estos componentes móviles creados por desarrolladores y predecir otras actividades similares de estos. También permite fijar alertas que detectan la actividad fraudulenta de estos desarrolladores, lo que convierte a Path 5 en una solución ideal para los equipos de seguridad, legales y de marketing de las empresas, o para analistas de tendencias en aplicaciones móviles.

- **Latch** ha sido lanzado en 2014 para Windows Mobile y Firefox OS (FFOS), el sistema operativo basado en estándares abiertos desarrollado por Mozilla y apoyado desde sus inicios por Telefónica, que comercializa ya terminales con este sistema operativo en España y en varios mercados latinoamericanos. Latch es una aplicación móvil que, de forma muy sencilla, permite a los usuarios crear una capa adicional de seguridad en las diferentes cuentas de servicios *online* que utilizan, ayudándoles a proteger su vida digital. Con este "pestaño" digital ("*latch*", en inglés) los usuarios deciden cuándo "encender y apagar" servicios en Internet, así como sus perfiles en redes sociales, tiendas *online* o banca electrónica, impidiendo su utilización mientras están desconectados. La aplicación envía, además, una alerta en caso de que alguien trate de acceder a los servicios cuando el usuario los tiene "apagados".

⇒ Sinfonier. Ante la necesidad de dar soporte en tiempo real al procesamiento de la información que se recolecta desde diferentes fuentes, Sinfonier pone a disposición de los usuarios una infraestructura gratuita para que puedan crear sus topologías utilizando los módulos disponibles en la comunidad y desarrollar sus propios módulos. Gracias a Sinfonier, podrán recolectar información desde multitud de fuentes, procesarla y enriquecerla de forma dinámica y continua.

Plan de Formación Global en materia de protección de datos

Europa



32.812 empleados
60,8 % total de empleados

Latinoamérica



30.138 empleados
44,2 % total de empleados

Un total de
62.950
empleados han
sido formados en
seguridad de la
información

Plan de continuidad del negocio

Para Telefónica, la continuidad del negocio es un concepto que abarca tanto el plan para la recuperación de desastres (DRP) como el plan para el restablecimiento del negocio.

En base a estos, desarrollamos y mejoramos anualmente los planes logísticos con el fin de poder recuperar y restaurar sus funciones críticas, parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o posible desastre.

Este plan es la respuesta prevista por Telefónica ante aquellas situaciones de riesgo que le pueden afectar de forma crítica. Los análisis de impacto al negocio son revisados anualmente y auditados conforme a la norma ISO 27001 y la Compañía tiene en su camino crítico de certificación la ISO 22301 como objetivo estratégico.

De hecho, en 2012, Telefónica fue el primer operador móvil en Reino Unido en obtener la certificación ISO 22301 para todas sus operaciones.

Protección de datos y auditorías

En Telefónica realizamos las auditorías propias que demanda cada gobierno en cada uno de los países en los que está presente, que suelen hacerse cada dos años. Pero, además, hemos implantado un sistema de auditoría interna anual para comprobar, no solo su cumplimiento, sino la aplicación de las mejores prácticas del mercado en temas de protección de datos. En 2014, hemos continuado realizando revisiones de protección de datos de carácter personal, ejecutando 9 auditorías en entidades colaboradoras de Fundación Telefónica en 5 países de Latinoamérica, una en la región de Centroamérica y 19 auditorías en empresas del Grupo, tanto en Europa como en Latinoamérica.

Para el caso de las auditorías en las empresas del Grupo, los aspectos más importantes que se han revisado han sido: aplicación de las medidas de seguridad en el tratamiento de los datos personales, control de acceso a los mismos, calidad de la información, consentimiento para el tratamiento de los datos y posibilidad de que

los afectados puedan ejercitar sus derechos de acceso, rectificación, cancelación y oposición.

Para el caso de Fundación Telefónica, los aspectos revisados han sido la calidad de la información y el consentimiento para el tratamiento de los datos de carácter personal.

Telefónica, además, dentro de su Plan Anual de Auditoría incluye un plan integral de Auditorías de Ciberseguridad que, entre otras técnicas, incluyen la realización de test de penetración aplicando técnicas de *hacking* ético basadas en los estándares OSSTMM, CVSS y OWASP.

Estas auditorías se realizan una vez al año sobre la totalidad del direccionamiento IP (público y privado) de todas las operadoras del Grupo, así como productos y servicios para determinar y en su caso mejorar su nivel de resiliencia frente a ciberataques.

Durante 2014 se han realizado 18 auditorías de ciberseguridad sobre el conjunto de las redes y sistemas de las operadoras. También se han realizado de forma específica 7 trabajos de este tipo sobre productos y servicios.

Formación y sensibilización

Durante 2014, hemos continuado con el Plan de Formación Global en materia de protección de datos. Un total de 62.950 empleados han sido formados en protección de datos, seguridad de la información y concienciación. Esto supone el 50,9% de los empleados totales del Grupo. El desglose por región es:

⇒ **Telefónica Europa:** 32.812 empleados han recibido formación en materia de privacidad y protección de datos. Esto supone, aproximadamente, el 60,8% de los empleados de Telefónica en la región.

⇒ **Telefónica Latinoamérica:** 30.138 empleados han sido formados, tanto de forma presencial como *online*, en materia de privacidad, protección de datos, seguridad y confidencialidad; esto supone el 44,2% de los empleados en la región.

A nivel corporativo se han realizado diferentes iniciativas de concienciación, entre las que caben destacar:

- ⇒ Concienciación sobre el *phishing*, para sensibilizar a los empleados y conocer el grado de exposición hacia un posible ataque.
- ⇒ Un curso de seguridad de cinco horas para los técnicos que dan soporte a la alta dirección.
- ⇒ Se publicaron y enviaron tutoriales y consejos sobre seguridad a través de correos, la Intranet y Yammer a todos los empleados del Grupo.

Además de la formación interna, también se han impartido talleres de formación y sensibilización en materia de protección de datos, a los que asistieron diferentes organizaciones e instituciones locales:

- ⇒ **Alemania.** Participación regular en las reuniones con el Federal Data Protection Officer y otros organismos federales.
- ⇒ **Colombia.** Telefónica Colombia ha participado a lo largo de 2014 en espacios como expositor y asistente en temas de Ciberseguridad y Protección de Datos (XVI Congreso Nacional e Internacional ANDESCO, Servicios Públicos, TIC y TV, II Congreso Internacional de Protección de Datos, organizado por la Superintendencia de Industria y Comercio, con apoyo de Accountability Foundation).
- ⇒ **Ecuador.** Telefónica Ecuador participó en el Fórum de Intercambio de Experiencia en Seguridad de la Información (FTRESI), un grupo formado por las grandes empresas nacionales para discutir sobre seguridad de la información y cuyo encuentro es trimestral.
- ⇒ **México.** Se adhirió a los Principios de Privacidad Móvil de la GSMA a través de la iniciativa 'Nos Importa México' (*We Care*).
- ⇒ **Uruguay.** Realiza charlas de actualización de nuevas modalidades delictivas en cajeros y vendedores.
- ⇒ **Innovation Security Day.** Durante la jornada, Telefónica presentó los retos de innovación en seguridad TIC a los que nos enfrentamos, derivados de las nuevas tendencias en ciberataques, nuevos mecanismos y herramientas de protección y nuestra oferta de servicios.

Incidentes

Se han reportado nueve incidentes a nivel global en temas de privacidad y protección de datos que fueron resueltos por las áreas de *compliance* del país correspondiente; ocho en Reino Unido y uno en Alemania.

Penalizaciones

En 2014 Telefónica Colombia fue objeto de cinco multas por temas relacionados con protección de datos personales. Tres de ellas no se encuentran en firme pues fueron objeto de recurso por parte de la Empresa. Las dos restantes

fueron confirmadas. El resto de países no ha sido objeto de penalizaciones relacionadas con este tema.

TRANSPARENCIA

La confianza es un valor crítico en una economía caracterizada por la gestión y el análisis de la información. Todos los estudios realizados por Telefónica muestran una creciente inquietud por parte de los usuarios sobre el uso que hacen los servicios digitales y *online* de sus datos y la pérdida de control sobre ellos cuando navegamos por la web.

De hecho, estamos empezando a observar las primeras reacciones de protección frente a estas tendencias. Las descargas de aplicaciones para evitar la publicidad están aumentando considerablemente.

Nuestra receta para mejorar los niveles de confianza es la de la transparencia de las condiciones de uso de Internet. En este sentido, Telefónica I+D ha lanzado el **Data Transparency Lab**, un proyecto de la comunidad digital para identificar el flujo y el uso de los datos personales en la red, explorar nuevas vías para favorecer la transparencia y la responsabilidad en el tratamiento de esta información con la intención de construir un Internet futuro más abierto. A través de esta iniciativa se busca también favorecer la sostenibilidad de la economía web por medio de un uso responsable y transparente de la publicidad, el comercio electrónico y la analítica *online*.

Data Transparency Lab tiene como principales objetivos desarrollar herramientas, abrir bases de datos a los usuarios y apoyar la investigación (por medio de becas, proyectos de I+D, etc.) en esta área. Telefónica I+D es una de las fundadoras de esta nueva institución, junto al MIT Human Dynamics Lab (dirigido por el prestigioso Alex 'Sandy' Pentland), Mozilla, el Open Data Institute (dirigido por Sir Tim Berners Lee) o el Centre for the Digital Economy de la Universidad de Surrey.

Como muestra de la labor que busca desempeñar el Data Transparency Lab, el equipo de Telefónica I+D, conjuntamente con la Universidad Carlos III y la Universidad Politécnica de Cataluña, han desarrollado una herramienta, Sheriff, que identifica cambios en el precio que cada tienda *online* cobra según la dirección IP desde la que se acceda, y con la Universidad de Columbia (Nueva York) para entender qué datos personales son responsables de los anuncios que vemos.

BEST PRACTICE

Telefónica España es líder en facturación, en dispositivos gestionados y proyectos ejecutados, así como en número de empresas e instituciones que en España le confían su seguridad –las principales empresas del país, organismos públicos y Cuerpos y Fuerzas de Seguridad del Estado–.