# 03
# GENERAR CONFIANZA EN LOS DATOS

## Este capítulo:

Examina los datos, su enorme importancia y las innumerables formas en las que estos empoderan a las personas en su vida diaria. Aquí se expone la visión de Telefónica sobre cómo generar confianza: transparencia, seguridad y poder de elección; con el objetivo de que los usuarios puedan tomar el control de su vida digital.

# GENERAR CONFIANZA EN LOS DATOS

## Retos

- Los datos constituyen una parte importante de nuestras vidas. Pueden enriquecer las experiencias de los usuarios y generar nuevas oportunidades, beneficiar a las empresas y facilitar el progreso de la sociedad en general.
- En la actualidad hay falta de confianza sobre el uso de los datos. A menudo, la gente siente que no controla sus datos personales debido a la falta de transparencia y a las opciones existentes.
- El incremento de las amenazas a la seguridad está siendo cada vez más relevante en el mundo digitalizado y conectado, poniendo en peligro tanto a individuos como a negocios.

## Nuestra visión

- Los datos son un recurso muy valioso, por lo que debemos restablecer la confianza en ellos, ayudando a las personas a sentirse cómodas respecto a la utilización de sus datos.
- Necesitamos una nueva ética de datos. Se debe empoderar a las personas para que puedan decidir cómo y cuándo se utilizan sus datos y también para que puedan disfrutar de su valor.
- La transparencia y la variedad de opciones de elección son requisitos necesarios para que la gente pueda controlar su vida digital y generar confianza.
- Los datos abiertos pueden contribuir a resolver múltiples retos sociales y económicos.
- La seguridad y la confidencialidad de los datos deben estar aseguradas más que nunca en un mundo donde todo y todos están conectados. Las nuevas experiencias digitales deberían diseñarse para garantizar al máximo la seguridad de los datos de los usuarios.
- Se requieren nuevas formas de cooperación pública y privada, así como esfuerzos adicionales para mejorar la seguridad de los productos y servicios.
- Los Estados tienen la responsabilidad de garantizar la seguridad de sus ciudadanos, pero también deben respetar sus derechos fundamentales.
- Debe mejorarse la ciberseguridad en toda la cadena de valor de productos y servicios digitales, dado que el eslabón más débil define la seguridad de todo el sistema.



El principal reto para un proceso de digitalización sostenible y una Economía de los Datos será mitigar los riesgos derivados de la utilización de los mismos, al tiempo que se aprovechan sus oportunidades.

Las redes de comunicaciones constituyen los cimientos de Internet y la economía digital dado que transportan cantidades de datos que aumentan de manera exponencial. En un mundo cada vez más digitalizado y conectado, todo lo que hacemos deja una huella en forma de datos: cada viaje, momento compartido, pago enviado, celebración, noticia, reacción, desplazamiento y momento de ocio. Y detrás de cada dato podría haber una historia personal.

Y no se trata únicamente de datos personales: millones de sensores generan cantidades ingentes de datos acerca del clima, la contaminación, los flujos de tráfico, el consumo de energía y otros recursos. El auge de Internet de las Cosas (IoT) hará que el número de objetos conectados con sensores incorporados aumente rápidamente, creando nuevas formas de mejorar nuestro mundo mediante conocimientos basados en datos. Los progresos en IoT, la automatización y la Inteligencia Artificial (IA) están generando oportunidades adicionales para la reconfiguración de los procesos industriales actuales y de las cadenas de valor basadas en datos.

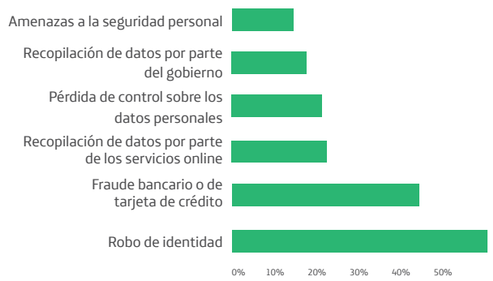
Los datos representan el motor del crecimiento digital y, por lo tanto, la privacidad y la seguridad constituyen los pilares de un futuro digital sostenible y robusto. Consecuentemente, la digitalización debe ir acompañada de una ética de datos renovada y responsable.

## 1. La falta de confianza

Los servicios y soluciones basadas en datos se están desarrollando en un contexto social, económico e institucional determinado, y ello en parte, contribuye a la sensación de incertidumbre y vulnerabilidad que muchas personas sienten.

Cada día más personas están preocupadas por la pérdida de control sobre sus vidas digitales. Los usuarios ya no están seguros de cómo se recogen, almacenan y emplean sus datos personales, ni tampoco quién lo hace ni con qué propósito.

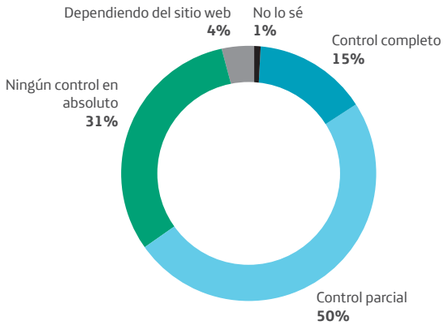
Gráfico 1. Principales preocupaciones relacionadas con la privacidad y seguridad en EE.UU[17]




*Fuente: NTIA*

Gráfico 2. Percepción del control sobre los datos compartidos online en la UE

¿Qué grado de control sientes que tienes sobre la información que compartes online?




*Fuente: Eurobarómetro 2015*

Cuanto menos cómodos se sientan los usuarios con respecto al uso que se hace de sus datos, menor será su predisposición a compartirlos. Esto es un asunto muy relevante para una sociedad con una dependencia creciente de las tecnologías digitales e incluso podría llegar a convertirse en una barrera para la digitalización.

**Afrontar los siguientes asuntos contribuirá a generar confianza en relación a los datos personales:**

- **Transparencia:** los usuarios deberían poder acceder a toda la información que generan.
- **Dar el control a las personas:** las personas deberían tener acceso a herramientas que les permitan aprovechar todos los beneficios de sus datos personales de una forma sencilla y cómoda.
- **Elección:** las personas deberían tener opciones significativas acerca de cómo y con qué propósito se utilizan sus datos.
- **Seguridad de los datos:** los datos de las personas deben mantenerse seguros para poder garantizar la privacidad.

## 2. Los datos como un recurso para el bien común

Los datos permiten nuevas experiencias y servicios y la transformación de sectores completos. Sin acceso a datos, el progreso se detendría. Tenemos acceso a un volumen de información mayor que nunca, así como a métricas que podrían hacer nuestro mundo más eficiente, informado y con una mejor gestión de nuestros recursos.

**Los datos abiertos representan una importante oportunidad para resolver algunos de los retos sociales y económicos que afrontamos en la actualidad, como la reducción del consumo energético y la contaminación, la optimización del tráfico y la mejora de la sanidad.**

Administraciones, empresas y ciudadanos deben colaborar estrechamente para crear un ecosistema que aproveche los datos abiertos. Consideramos que los datos públicos deberían:

- Estar a disposición de todo el mundo, sin restricciones.
- Estar disponibles y ser accesibles online, para que su uso resulte sencillo.
- Estar preparados para ser reutilizados, redistribuidos e incluso transformados.

Los datos enriquecen las vidas de las personas, pero también ayudan a las organizaciones a tomar decisiones más adecuadas y a mejorar la calidad de vida de todos los ciudadanos:

- El transporte podría ser más "inteligente", reduciendo la congestión, mejorando la calidad del aire y sobre todo disminuyendo el número de víctimas de accidentes de tráfico.
- Las infraestructuras urbanas podrían desarrollarse con mejor información sobre las necesidades de los habitantes, haciendo que los servicios públicos fuesen más eficientes y ahorrando recursos que podrían destinarse a otras necesidades.
- Las epidemias y los desastres naturales podrían gestionarse mejor, salvando vidas humanas.
- Podría preverse los movimientos migratorios derivados de las consecuencias del cambio climático para medir su impacto y planificar acciones de acuerdo a los datos.
- Las enfermedades podrían diagnosticarse de manera precoz, mejorando el cuidado de la salud y aumentando la calidad de vida de los pacientes y sus familias.

Los datos pueden enriquecer las vidas de las personas, beneficiar a los negocios y contribuir al progreso de la sociedad en su conjunto. De hecho, el análisis de datos será un elemento crucial para la transformación y el progreso de las sociedades y una herramienta para crear un futuro mejor.



Caso práctico

## *LUCA: DECISIONES BASADAS EN DATOS*

### Transformar los servicios de transporte

Los datos de ubicación de los usuarios combinados con datos procedentes de servicios de transporte público están contribuyendo a determinar el "cuándo", "dónde" y "por qué" de los movimientos masivos, ayudando a mejorar la infraestructura de transporte público en las ciudades. Una mejor planificación y ejecución de los servicios de transporte público podría llegar a ahorrar muchos millones y, aún más importante, reducir drásticamente la cifra de víctimas de accidentes de tráfico.

En las grandes ciudades, la contaminación del aire se está convirtiendo en un problema de salud pública de primera magnitud. Los datos móviles están ayudando a predecir el empeoramiento de las métricas de calidad del aire, permitiendo a las autoridades actuar en consecuencia.

### Transformar los servicios turísticos

Ayudar a todas las partes implicadas (empresas privadas, administraciones públicas, agentes locales, centros tecnológicos y universidades) a establecer sinergias, trabajar juntos y alcanzar un consenso sobre cómo hacer más atractivos los destinos turísticos y, al mismo tiempo, mejorar la calidad de vida de los residentes locales.

### Bancarizar a los no bancarizados

Ofrecer acceso a servicios financieros enriquece las vidas de los clientes que no disponen de cuenta bancaria o no cuentan con el historial bancario necesario para respaldar sus proyectos. Este problema afecta a muchos de nuestros usuarios en Latinoamérica. La calificación crediticia basada en datos móviles es un servicio que ofrecemos a través de LUCA *Scoring*. Podemos ayudar a nuestros clientes a obtener acceso a servicios financieros compartiendo ciertos detalles de su información con terceros, permitiéndoles obtener acceso a servicios financieros.

### Evitar el fraude bancario

A través de servicios en tiempo real, contribuimos a proteger las transacciones de los clientes y evitar el fraude, verificando las identidades de los clientes y confirmando que realmente se encuentran en la misma ubicación donde se está llevando a cabo la transacción.

### *Big Data* para el bien social. Reducir el impacto de los desastres naturales y predecir la expansión de enfermedades

Los datos móviles están siendo utilizados después de desastres naturales, como terremotos y grandes inundaciones, para comprender el impacto de estos eventos sobre las concentraciones y movilidad de la población, así como para guiar las operaciones de socorro. En el caso de las inundaciones, los datos móviles contribuyen a determinar la relación entre el momento e intensidad de las lluvias y la demora antes de su impacto sobre cada área, proporcionando conocimientos vitales para la planificación de evacuaciones y operaciones de socorro de cara al futuro. El valor de los datos relacionados con emergencias aumenta aún más cuando se obtienen en tiempo real.

En este sentido, Telefónica ha anunciado una colaboración con UNICEF a través de su iniciativa Magic Box – una plataforma de *Big Data* para el bien social que recoge datos en tiempo real, combinando y analizando datos agregados y anónimos procedentes de empresas privadas y otros conjuntos de datos del dominio público relacionados con el clima, el Sistema de Información Geográfica de UNICEF (GIS) e información socioeconómica y epidemiológica. Magic Box fue presentando en 2014, cuando se utilizó para responder a la crisis del Ébola en África Occidental y más recientemente durante la proliferación del virus Zika.

La respuesta a emergencias de salud pública y desastres naturales puede optimizarse para aprovechar el valor de los datos en tiempo real, contribuyendo a proteger a los niños y a salvar vidas infantiles en un mundo cada vez más impredecible.

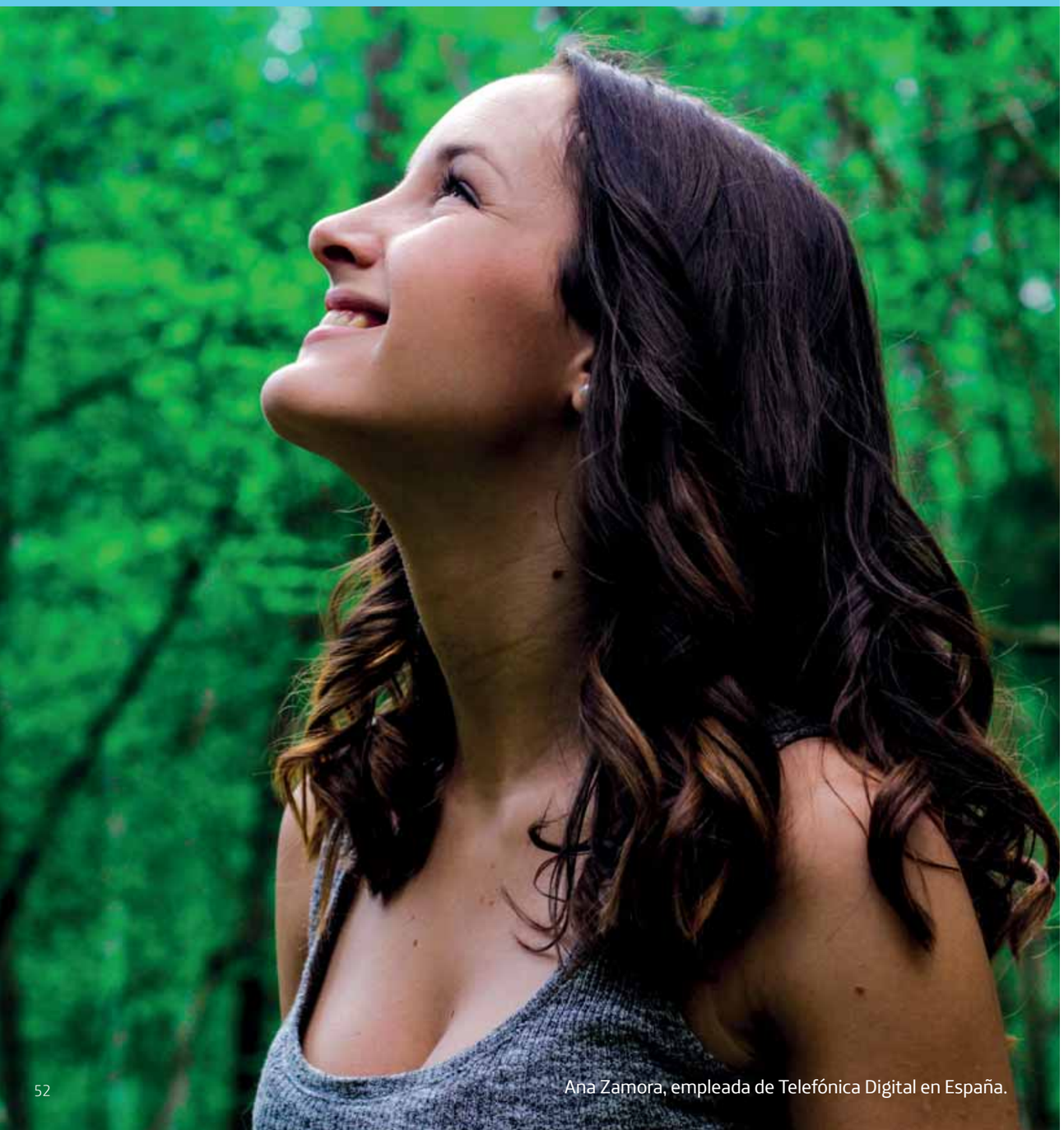
### Medir el cumplimiento de los Objetivos de Desarrollo Sostenible (ODS) de Naciones Unidas

Los datos móviles y otros indicadores relacionados con los servicios de telecomunicaciones constituyen un recurso muy valioso para determinar el progreso de cara a los ODS; un reto clave para la ONU.

Por ejemplo, el uso de mensajes de texto está correlacionado con los niveles de alfabetización entre la población y el volumen de llamadas internacionales realizadas entre dos países revela su nivel de comercio mutuo.

*Es necesario un enfoque basado en las personas que permita a los usuarios controlar la forma en la que se recogen y comparten sus datos personales*

*Giovanni Buttarelli, Supervisor Europeo de Protección de Datos*



Ana Zamora, empleada de Telefónica Digital en España.



# 3. Una nueva ética de datos para generar confianza

Ante el enorme valor para las personas y la sociedad de los servicios impulsados por datos, la necesidad de dotarnos de un código ético para la gestión de los datos que incluya aspectos como la responsabilidad, la transparencia y la capacidad de elección está adquiriendo una importancia cada vez mayor.

Los datos están haciendo posible la economía digital, pero para tener valor, deben utilizarse y no guardarse bajo llave. El potencial y número de oportunidades que tienen aumentan rápidamente cuando se combinan diferentes tipos de datos procedentes de diversas fuentes.

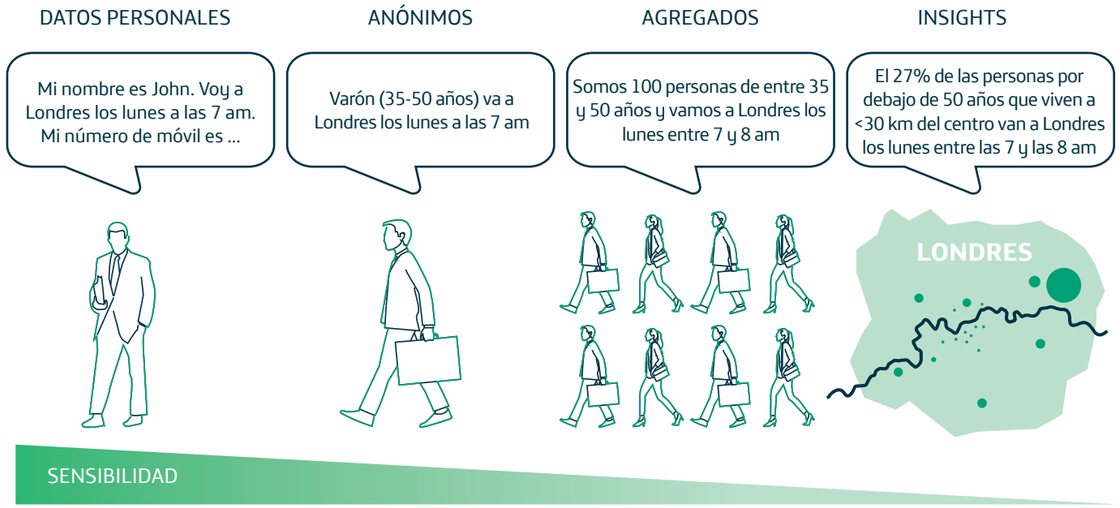
Por ejemplo, los datos relativos a actividades no humanas, como los medioambientales y climáticos, pueden proporcionar conocimientos muy valiosos, especialmente cuando se agregan con otras fuentes de información.

Sobre este punto, es importante recordar las diferencias entre los datos personales y no personales. **Podemos considerar como datos personales cualquier información relacionada con un cliente que enriquezca el conocimiento acerca de su realidad. Por otra parte, los datos no personales se refieren a información que no se encuentra vinculada a ningún usuario concreto.** Por ejemplo, los datos anónimos son datos no personales. Gran parte del valor y los beneficios del empleo de datos pueden atribuirse a la utilización de datos anonimizados y no personales, así como a los conocimientos obtenidos a través de este tipo de datos, respetando así la privacidad de los usuarios (ver caso práctico "LUCA: Decisiones basadas en datos").

Establecer confianza en los datos es un proceso continuo. **Una mayor transparencia debería implicar ser abiertos con los usuarios para que conozcan qué datos se están recabando, cuándo se registran y para qué se emplean.** Los apartados de "términos y condiciones" habitualmente son complejos y nadie los lee y por tanto su existencia no debe asociarse per sé a la idea de transparencia. Para poder alcanzar un nivel significativo de transparencia, las personas deberían contar con acceso a sus datos personales de un modo sencillo y fácil de utilizar.

En este sentido, las tecnologías de *Big Data* e IA también representan una oportunidad para

Gráfico 3: De información personal a insights anónimos

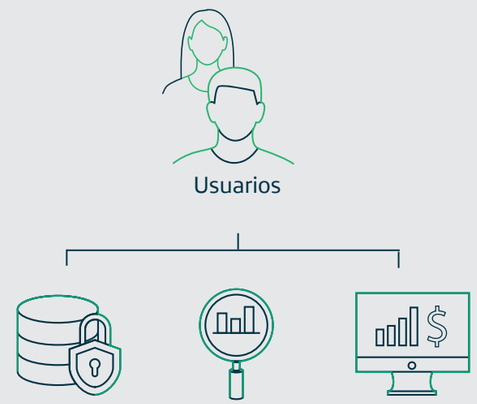


mejorar la transparencia. Las empresas pueden emplear estas tecnologías para establecer una relación personal con cada cliente individual, adaptada a sus necesidades y preferencias. Dicho de otro modo, pueden ofrecer a los consumidores un mejor acceso a su propia información, ayudándoles a comprender sus opciones y proporcionándoles la capacidad de tomar decisiones personales. Este tipo de transparencia está relacionada con las políticas de precios y las condiciones de facturación, las características del servicio técnico, las responsabilidades y, lo más importante, la forma de recabar, almacenar, procesar y emplear los datos personales.

**Los usuarios deberían tener el control sobre sus datos personales, manteniendo la capacidad de decidir cómo se emplean. Esto implica ayudarles a comprender la importancia de sus datos y proporcionarles opciones acerca de su utilización.**

Jessica Rodrigues, Daniel Souto y Marieli Granato, empleados de Telefónica Brasil.

Gráfico 4. Cómo hacemos las cosas:




1. **Los datos deben estar seguros:** la seguridad de los datos y la privacidad de los clientes representan las bases de nuestro negocio y nuestra principal consideración al diseñar nuestros servicios y colaborar con nuestros socios.
2. **Las personas deberían poder decidir cómo se emplean sus datos y mantener el control sobre ellos:** ofrecemos herramientas sencillas para gestionar las opciones para compartir datos, permitiendo el acceso a los datos, ayudando a decidir cómo son utilizados y señalando los riesgos y beneficios asociados.
3. Facilitaremos que nuestros clientes puedan darse de baja de los servicios si cambian de opinión.
4. **Ofreceremos opciones** más allá de los términos y condiciones habituales: "o todo o nada".
5. **Las personas deberían beneficiarse de sus datos:** con su aprobación, utilizaremos los datos de nuestros clientes para ofrecerles servicios sencillos y útiles. Ofreceremos experiencias y servicios personalizados. Innovaremos con terceras partes para ofrecer nuevos servicios mejorados a base de datos y generaremos valor para nuestros clientes: valor para ellos mismos.

La normativa sobre protección de datos asegura que existan unas prácticas equitativas y transparentes en su tratamiento. Sin embargo, la aplicación real de estos conceptos puede ser ineficaz, puesto que la naturaleza global de los flujos de datos genera una situación compleja en su cumplimiento más allá de las fronteras nacionales. Por tanto, se requiere una mejor armonización e implementación internacional respecto a la protección de datos. De hecho, los flujos de datos transfronterizos están siendo objeto de una mayor regulación a escala internacional, regional y nacional para contribuir a proteger la privacidad de los individuos (ver Capítulo 5: Modernizar los Derechos y Políticas).

Un paso más en esta dirección sería **compartir con los consumidores el valor de sus datos.** Este valor podría materializarse mejorando los productos y servicios digitales, haciéndolos mejores y más sencillos de comprender. Este enfoque también incluye buscar formas más eficaces de concienciar al público acerca de la generación y empleo de datos. La transparencia es un prerrequisito para este control, puesto que permite una comprensión de las opciones disponibles. No es posible tener una elección sustantiva sin transparencia.

Los individuos también deben contar con la posibilidad de utilizar sus datos para generar valor para terceras partes. Telefónica está desarrollando una amplia gama de colaboraciones para permitir a nuestros usuarios utilizar sus datos en su propio beneficio.

Por otra parte, la portabilidad de datos también se debe mejorar. Los usuarios deberían poder emplear sus datos para su propio beneficio en diferentes plataformas de su elección. Para que esto sea posible, los consumidores necesitan herramientas que faciliten el acceso a los datos que generan, mediante el uso de servicios digitales y la posibilidad de transportar dichos datos.

En general, una buena práctica para mejorar la privacidad consiste en la aplicación del concepto de "privacidad por diseño", el cual asegura que los riesgos sobre esta materia hayan sido considerados y mitigados durante la fase de diseño de los productos y servicios.

Caso Práctico

## *AURA, EL NUEVO MODELO DE RELACIÓN CON NUESTROS CLIENTES*

# Aura

Telefónica ha desarrollado Aura, un servicio de Inteligencia Artificial diseñado para establecer un nuevo modelo de relación con los clientes, empleando sus datos personales y servicios cognitivos sobre la base de nuestra infraestructura de telecomunicaciones.

Aura busca dotar a nuestros clientes de cuatro súper poderes:

- **Simplificar:** realizar acciones, enviar comandos a la red y utilizar servicios rápidamente, simplemente hablando a la herramienta.
- **Operar algoritmos** sobre las bases de datos de clientes para obtener conocimientos que enriquezcan su experiencia con los servicios de Telefónica.
- **Capacitar:** ofrecer transparencia y control sobre los datos generados al hacer uso de los servicios de Telefónica.
- **Descubrir** lo que los clientes hacen con los datos que generan (propuestas para hacer uso de los datos a cambio de un beneficio/valor, protegiendo su privacidad).

**La propuesta de valor de Aura mejora a lo largo del tiempo; actuará como *trayecto de confianza* para los clientes.** Aura comenzará con unas opciones sencillas para que nuestros clientes puedan interactuar con los actuales servicios de la compañía y más adelante aumentará los beneficios de los usuarios a través de nuevos servicios, permitiéndoles controlar y explotar sus propios datos en el entorno del operador de telecomunicaciones o con terceras partes.

Aura emplea inteligencia cognitiva para comprender las necesidades de los clientes y ayudarles de manera proactiva, transformando la información disponible en conocimientos de gran valor. Estos conocimientos acerca de los usuarios evolucionan a lo largo del tiempo, a medida que los clientes van haciendo uso de los productos y servicios de Telefónica, manteniendo el control sobre el uso que la empresa puede hacer de los datos en manos de los clientes en todo momento.

1. **Aura es una plataforma de inteligencia cognitiva que escucha a los clientes de Telefónica,** aprendiendo de ellos y enriqueciendo su experiencia con los productos y servicios de la compañía.
2. Aura ofrece una **nueva forma para que los clientes puedan establecer una relación con Telefónica, introduciendo capacidades de lenguaje natural:** tecnología adaptada a las personas y no a la inversa.
3. **Aura pondrá el poder de decisión en manos de los usuarios,** proporcionándoles nuevas formas de hacer uso de sus datos, por ejemplo para mejorar y personalizar los servicios de Telefónica, y ayudándoles a descubrir otras maneras de explotar sus datos para su propio beneficio.
4. **Aura permitirá a los clientes decidir** qué datos pueden emplearse en este proceso de generación de conocimientos.
5. Como **plataforma de inteligencia cognitiva,** Aura contará con diversas vías de acceso (canales propios como nuestra app móvil, canales de terceras partes, como Facebook Messenger, e incluso a través de otros asistentes).

El objetivo de Aura es ayudar a los clientes a obtener más valor de los servicios y la tecnología de Telefónica.



# 4. Derechos y seguridad

Las redes y sistemas de información ocupan un papel clave en nuestra sociedad actual. Su fiabilidad y seguridad resultan esenciales para la estabilidad económica y social. Los incidentes de ciberseguridad pueden interrumpir las actividades económicas, generar importantes pérdidas, socavar la confianza de los usuarios y causar un perjuicio considerable a la economía de los Estados.

Se espera que alrededor de 29.000 millones de objetos estén interconectados hacia 2022[18]. A medida que Internet de las Cosas (IoT) vaya creciendo, los coches, aviones, hogares, ciudades e incluso los animales formarán parte de la red, por lo que también se espera que aumenten el número de incidentes que afecten a la privacidad y a la ciberseguridad de los ciudadanos.

Un nivel insuficiente de atención a las ciberamenazas por parte de los sectores público y privado podría perjudicar gravemente la confianza en la seguridad de Internet y poner en riesgo su capacidad para actuar como motor de innovación. La seguridad y los derechos fundamentales están indisolublemente ligados. Las actividades relacionadas con la seguridad nacional, como la vigilancia masiva, deben garantizan el respecto a los derechos humanos, por lo que deberían contar con el apoyo del sector público y organizaciones privadas. **Es preciso mantener un amplio diálogo global, cooperando y utilizando estándares, para poder gestionar la tensión inherente entre la ciberseguridad y los derechos fundamentales.**

Gobiernos[19] y compañías privadas han lanzado diversas iniciativas para promover la presentación de informes anuales de transparencia[20] sobre las peticiones de datos por parte de los gobiernos:

- Un ejemplo es la iniciativa Global Network Initiative (GNI)[21], en el que participan actores de distinta naturaleza.
- Hay otras alternativas de naturaleza gubernamental que cooperan con el sistema de Naciones Unidas y otras vías más académicas como Ranking Digital Rights[22].

Estas iniciativas apoyan la colaboración entre los sectores público y privado de cara a establecer un ecosistema digital más equitativo y sostenible mediante el desarrollo de estándares globales para la presentación de informes de transparencia por parte de las empresas y la responsabilidad de los gobiernos en cuanto a sus actividades de ciberseguridad.

A su vez, mantener seguros los datos de los ciudadanos debería ser el principio que guíe el diseño de las nuevas experiencias digitales. Evitar las filtraciones de datos debe representar una prioridad para todas las empresas. La complejidad de la tecnología, las ciberamenazas y los posibles errores humanos podrían conducir a la pérdida o eliminación de información o permitir que caiga en manos indebidas. La gestión de riesgos es un proceso continuo y un prerrequisito para establecer confianza.

**La cooperación público-privada, junto con el refuerzo de la confianza y el intercambio de información, resultan esenciales para anticipar este tipo de ataques.** Del mismo modo, esta cooperación también resulta esencial durante la gestión de incidentes, para mitigar su impacto e invertir los efectos de estos sucesos.

El cifrado (o encriptación) se ha establecido como una tecnología esencial para garantizar la seguridad de los usuarios y en la actualidad se despliega a gran escala para garantizar la privacidad de los datos. Aunque se trata de una tecnología clave para la seguridad, resulta igualmente importante que los esfuerzos de las autoridades públicas para proteger la seguridad nacional y de los ciudadanos no se vean frustrados. Los responsables políticos y de las agencias de seguridad nacional, como el FBI, argumentan que sus esfuerzos por acceder a información cifrada con autorización judicial fracasan, por lo que demandan una solución urgente a esta cuestión de seguridad pública. Resulta esencial valorar adecuadamente el impacto de la tecnología sobre diferentes derechos así como respetar el principio de proporcionalidad. En última instancia, es necesario definir procesos legales apropiados para conceder a las autoridades acceso a la información, de un modo similar a lo ocurrido en el pasado con la telefonía tradicional.

# 5. Seguridad en productos y servicios

De cara al futuro, el crecimiento de Internet de las Cosas (IoT) permitirá conectar cualquier tipo de dispositivo, y esta mayor dependencia de la tecnología generará nuevas preocupaciones relacionadas con la seguridad que requerirán de un visión más integral y adaptable en esta materia.

La adopción de la tecnología por parte de la sociedad va más rápido que los avances en materia de seguridad, y por ello los riesgos aumentan exponencialmente a pesar de los esfuerzos del sector y la adopción de mejores prácticas.

Además, el nivel de protección de los productos y servicios digitales a menudo se reduce con el tiempo por la obsolescencia de los mismos. Por lo tanto, todos los integrantes de la cadena de valor deben esforzarse por incorporar medidas de seguridad en sus productos, desde las primeras etapas de diseño hasta las últimas (seguridad por diseño). Por otra parte, los fabricantes de productos deben mantener un compromiso firme con la seguridad y responder rápidamente creando parches para resolver las nuevas vulnerabilidades tan pronto como tengan conocimiento de ellas. De modo similar, una política clara de mantenimiento de la seguridad para los dispositivos debería ser un aspecto clave de cualquier relación contractual.

El elevado coste de incorporar seguridad a los productos y la necesidad de acortar el tiempo de lanzamiento no pueden ser excusas para evitar crear productos y servicios seguros. Resulta importante establecer un marco justo para la competencia con el objetivo de mejorar los niveles de ciberseguridad en toda la cadena de valor, como establece la nueva Directiva NIS de la UE sobre redes y sistemas de información. Las actuales asimetrías regulatorias podrían modificarse adoptando el enfoque "mismo servicio, mismas reglas" para todas las empresas, con el objetivo de proteger a los usuarios que accedan a cualquier producto, servicio o dispositivo. El Internet de las Cosas conectará todos los productos imaginables y transformará a todas las empresas en empresas tecnológicas. Por lo tanto, cualquier enfoque de ciberseguridad deberá adoptar una visión holística e intersectorial.

**Resulta importante explorar nuevas formas de ofrecer mayor ciberseguridad:**

- Una autocertificación de ciberseguridad para productos, aplicaciones y servicios basada en las mejores prácticas y recomendaciones de todas las partes involucradas contribuiría a establecer estándares comunes y mejorar la transparencia entre consumidores y negocios.
- Los usuarios deben contar con la posibilidad de actualizar sus productos y servicios digitales para aplicar los últimos estándares de seguridad en un plazo razonable.
- Se requiere concienciar a los consumidores y mejorar sus conocimientos sobre ciberseguridad mediante campañas informativas.

Caso práctico

## *WANNACRY RANSOMWARE*

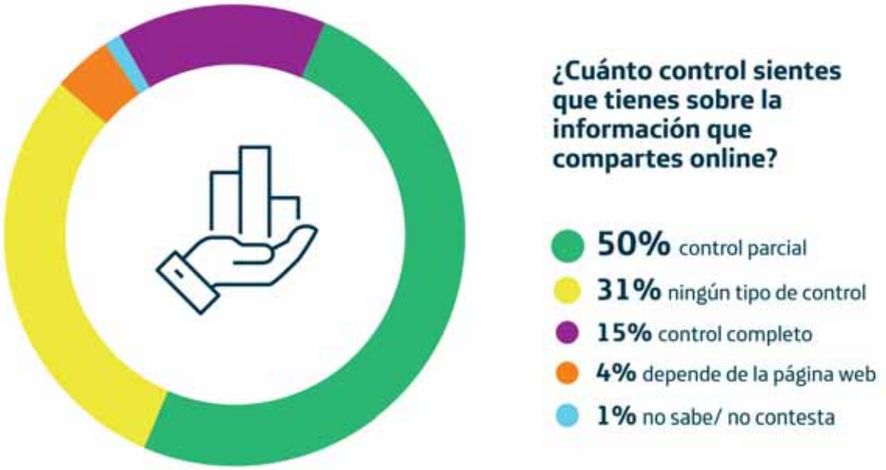
- El 12 de mayo de 2017, 300.000 ordenadores en 150 países fueron bloqueados por un ataque informático que exigía un rescate (*ransomware*) conocido como WannaCry.
- El ataque incapacitó varios hospitales del sistema de salud pública británico e infectó un elevado número de sistemas en múltiples compañías. China y Rusia se vieron particularmente afectadas.
- España fue uno de los primeros países en reconocer que había sufrido el ataque del *ransomware*, debido a la rápida respuesta de Telefónica, confirmando el ataque la misma mañana que sus ordenadores se vieron infectados.
- Desde el principio del incidente, Telefónica contactó con las autoridades para mantenerlas informadas acerca de la situación y colaborar en su resolución, abriendo una investigación y alertando a otras compañías.
- Internamente, se activaron los protocolos de seguridad y ninguno de los servicios de red de los clientes se vieron afectados. El impacto del incidente sobre la red interna fue contenido y la normalidad fue restaurada en un plazo de 48 horas.
- El ejercicio de transparencia de Telefónica ayudó a gobiernos y otras compañías a coordinar sus acciones y mitigar los efectos del *ransomware*.



# Capítulo 3 en un vistazo

## El reto

Los datos son una parte importante de nuestras vidas. Pueden enriquecer las experiencias de los usuarios y generar nuevas oportunidades, beneficiar a las empresas y facilitar el progreso de la sociedad en general. Sin embargo, las personas no siempre sienten que tienen el control de sus datos personales a medida que las amenazas de seguridad aumentan.




*Fuente: Eurobarómetro (2015)*

## Nuestra visión

**01. UNA NUEVA ÉTICA DE DATOS**

Un modelo centrado en las personas debería posibilitar que cada individuo pueda decidir cómo y cuándo se utilizan sus datos.

**02. TRANSPARENCIA Y ELECCIÓN**

Las personas deberían poder acceder a sus datos y a la información que generan, pero también deberían disponer de opciones adecuadas para disfrutar del valor de sus datos.

**03. NUEVAS FORMAS DE COOPERACIÓN PÚBLICA Y PRIVADA**

Se necesitan nuevas formas de cooperación pública y privada así como esfuerzos adicionales para mejorar la seguridad de los productos y servicios.

**04. GARANTIZAR LA SEGURIDAD**

Es fundamental crear unas normas equitativas para mejorar la ciberseguridad en toda la cadena de valor.