25 años de la Agencia Española de Protección de Datos

Acompañando al ciudadano en su transformación digital

25 años de la Agencia Española de Protección de Datos

Acompañando al ciudadano en su transformación digital

Agencia Española de Protección de Datos 2018

Depósito legal: M-38768-2018

Índice

Prólogo

Prólogo 7

Capítulo 1

I. Telecomunicaciones 13
II. Dispositivos 17
III. Redes Sociales 22
IV. Consumo 24
V. Educación 27
VI. Ocio 35
VII. Otros servicios 43
VIII. Medios de comunicación 45
IX. Conclusión 50

Capítulo 2

I. Introducción 52
II. Desarrollo de la comunicación y la información a través de Internet 52
III. Protección de datos personales 60
V. Políticas de privacidad 69
V. Menores y acceso a Internet 71
VI. Futuro y empleo 72
VII. Conclusiones 83

Capítulo 3

I. Introducción 86
II. Los inicios de la Agencia (1993-1994) 90
III. La dimensión constitucional del derecho. Los nuevos retos de la privacidad: las comunicaciones electrónicas (1999-2007) 96
IV. El reglamento de la ley orgánica de protección de datos: del 2008 hasta el 25 de mayo de 2018 106
V. El derecho a la protección de datos en los servicios de internet. Los nuevos desafíos de la privacidad 115
VI. a agencia del futuro 133

The AEPD as a garantor of a fundamental right

I. Introduction 144
II. The Agency's beginnings (1993-1999) 148
III. The constitutional dimension of law. The new challenges of privacy: electronic communications (1999-2007) 153
IV. The regulation of the Organic Law of Data Protection: from 2008 to 25 may 201 162
V. The right to protect data in Internet services. The new challenges of privacy 171
VI The Agency of the future 188


AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS

Prólogo

Es un honor para mí poder prologar un libro que describe los veinticinco años de historia de la Agencia Española de Protección de Datos. Una Agencia que se ha caracterizado por una intensa y diligente actividad en defensa del derecho fundamental a la protección de datos personales y por un acreditado criterio de independencia en el ejercicio de sus competencias.

En reconocimiento a su primer director, Juan José Martín-Casallo, se ha tomado como referencia inicial la fecha de su nombramiento: el 23 de octubre de 1993.

Desde aquel momento hasta el otoño de 2018 han transcurrido veinticinco años de evolución vertiginosa de este derecho fundamental en todos los ámbitos: normativo, institucional, jurisprudencial, de cooperación internacional, de difusión y conocimiento público y, sobre todo, de adaptación a los desarrollos tecnológicos.

Hoy vivimos en una sociedad digital en la que, con gran facilidad y bajo coste, se almacenan, intercambian, analizan, y utilizan para múltiples fines, grandes volúmenes de información sobre la vida de las personas. La actividad en Internet ha conocido un intenso proceso de concentración en el que el modelo de negocio de la mayoría de los prestadores de servicios está basado en la monetización de la información personal de los usuarios.

Este modelo se traduce en la oferta de servicios gratuitos que se financian con una publicidad personalizada cuyo origen se encuentra en un análisis de los hábitos de navegación de los usuarios de Internet para la elaboración de perfiles detallados sobre sus intereses y aficiones.

Esta revolución ha implicado que la Agencia haya pasado de gestionar unas decenas de denuncias referidas, fundamentalmente, a la inclusión indebida en ficheros de morosidad y a la publicidad no deseada por parte de empresas de ámbito nacional, a garantizar la protección de los datos personales respecto de empresas multinacionales cuyos servicios afectan a más de 4.000 millones de usuarios de Internet.

Y, complementariamente, que las iniciales tutelas de los derechos de acceso, cancelación y oposición de los ciudadanos en tratamientos de datos tradicionales hayan evolucionado a su tutela en el entorno de los servicios de búsqueda en Internet o de las redes sociales, configurando nuevos derechos como el conocido “derecho al olvido” en Internet.

Así, la Agencia, tras analizar la compatibilidad de la política de privacidad de Google con la normativa española de protección de datos, declaró que el buscador no incluía información adecuada sobre los datos que se recogían y sobre el destino de su tratamiento, que impedía en consecuencia un consentimiento válido, que se procedía a almacenar y conservar datos por periodos de tiempo indeterminados o injustificados y que se obstaculizaba el ejercicio de los derechos por parte de los ciudadanos. Esta declaración de la Agencia Española de Protección de Datos dio lugar a la modificación de la política de privacidad de la compañía a nivel global.

El mismo ejercicio se realizó cuando una de las redes sociales más preeminentes, Facebook, adquirió la aplicación de mensajería instantánea más utilizada, WhatsApp, e impuso como obligatoria, para poder hacer uso de ésta, la autorización para acceder y

utilizar los datos de sus usuarios para fines distintos de la comunicación entre ellos. La Agencia declaró que el consentimiento prestado no puede considerarse libre y, en consecuencia, resulta inválido.

En cuanto al "derecho al olvido", la Agencia fue la primera autoridad en considerar aplicable la tutela de los derechos de los usuarios de Internet en España a multinacionales establecidas en terceros países.

También ha sido pionera en garantizar la eliminación de los enlaces facilitados por los motores de búsqueda en Internet a partir del nombre de una persona. Se ha conseguido con ello limitar la hiperaccesibilidad temporal y geográfica de los internautas a informaciones personales cuando carecen de relevancia pública y se ha hecho valer el derecho fundamental a la protección de datos.

En definitiva, se ha conseguido, con el refrendo en el año 2014 del Tribunal de Justicia de la Unión Europea, garantizar simultáneamente el respecto al derecho fundamental, a la libertad de información y expresión cuando los datos personales tienen dicha relevancia y a la integridad de las páginas web de los editores a que conducen dichos enlaces.

Todas las personas que hemos ostentado la dirección de la Agencia hemos impulsado un amplio abanico de iniciativas preventivas y orientadoras del conocimiento y cumplimiento de la normativa mediante inspecciones sectoriales preventivas, instrucciones sobre los criterios para su aplicación, canales generalistas y especializados de atención a ciudadanos y responsables e informes preceptivos sobre iniciativas normativas. Este impulso también se ha materializado en el desarrollo de guías, orientaciones y herramientas que faciliten el cumplimiento -en particular, por parte de las pymes- y que permitan limitar riesgos en colectivos de mayor riesgo, como en el caso de los menores.

Iniciativas que han culminado, con la aprobación de un Plan Estratégico cuatrianual que recoge sistematizadamente los objetivos de la Agencia y permite su conocimiento público y su supervisión por terceros.

En una línea constante y sostenida desde sus orígenes, la Agencia ha sido un actor de primera línea en el mundo de la cooperación internacional para promover y garantizar la protección de datos personales en sus distintas vertientes.

Ha participado de forma destacada en la elaboración de dictámenes y opiniones por el denominado "Grupo de Trabajo del artículo 29" de la Unión Europea, en la actividad de supervisión de las agencias y grandes sistemas de información europeos como el SIS, el VIS, Eurodac o Europol. También ha participado en acciones coordinadas con otras autoridades de Estados miembros ante incumplimientos de grandes corporaciones multinacionales como Google o Facebook. Y continúa manteniendo la iniciativa en el Comité Europeo de Protección de Datos, en este avance que supone pasar de la actuación de un grupo meramente consultivo, a un organismo de la Unión Europea con competencias decisorias en la aplicación de la norma.

A lo largo de estos 25 años la Agencia ha contado con la inestimable colaboración del Consejo Consultivo y la cooperación, desde la independencia, de la extinta Agencia de Protección de Datos de la Comunidad de

Madrid, la Autoridad Catalana de Protección de Datos y la Agencia Vasca de Protección de Datos.

Con una mayoría de edad consolidada, la Agencia aborda el reto de promover, facilitar y aplicar un nuevo modelo de cumplimiento normativo basado en la diligencia, la proactividad y el análisis de riesgos para este derecho fundamental, así como un nuevo modelo de supervisión en el que ocupan un lugar destacado, frente a la normativa anterior, las acciones correctivas a imponer a responsables que, pese a una diligencia documentada, hayan podido incurrir en incumplimiento. Y se acompañan de sanciones económicas para incumplimientos importantes u omisión de la diligencia exigible.

Competencias a las que se sumarán las de la norma de transposición de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y el futuro Reglamento de e-privacy.

Confío que todos sigamos andando juntos el camino, no siempre fácil, de hacer compatibles tecnología y privacidad.

Mar España Martí
Directora

1

El imparable avance de la tecnología

La aldea global que preconizaba el más célebre de los teóricos de la comunicación, el canadiense Marshall McLuhan, la aldea global, decíamos, esa interconexión humana mundial a través de los medios electrónicos, hace tiempo que se materializó. Y España, una de las quince potencias mundiales, figura en la vanguardia de esa ola. En consecuencia, las transformaciones sociales ocurridas durante el último cuarto de siglo en nuestro país han venido acompañadas de grandes avances tecnológicos. En términos generales, la sociedad española de hoy tiene más y mejor acceso a nuevas tecnologías de información y comunicación (TIC) que la de principios de los años noventa del siglo pasado. El ciudadano medio de ahora usa diariamente, y cada vez más, herramientas y servicios que antes no hubiese podido imaginar. Sin embargo, no todos los sectores de la sociedad española han gozado de los progresos tecnológicos de igual manera. Las desigualdades sociales, económicas y culturales reseñadas explican el menor acceso a medios técnicos que algunas capas de la población han sufrido, lo que ha derivado en una evidente brecha digital entre la población española.

En este capítulo se realiza un repaso cronológico de los avances en la tecnología y se recopilan los indicadores más representativos del equipamiento y la utilización de las tecnologías de la información y las comunicaciones por parte de los ciudadanos. Asimismo, se describe el uso de las tecnologías digitales en la vida cotidiana y cómo estas herramientas están transformando las actitudes, los hábitos y el entorno de las personas.

Antes de detallar la evolución cronológica de los avances tecnológicos ocurridos en España durante los últimos 25 años es necesaria una breve aclaración conceptual. Por "tecnologías de la información y comunicación" entendemos:

> *"Dispositivos tecnológicos (hardware y software) que permiten editar, producir, almacenar, intercambiar y transmitir datos entre diferentes sistemas de información que cuentan con protocolos comunes. Estas aplicaciones, que integran medios de informática, telecomunicaciones y redes, posibilitan tanto la comunicación y colaboración interpersonal (persona a persona) como la multidireccional (uno a muchos o muchos a muchos). Estas herramientas desempeñan un papel sustantivo en la generación, intercambio, difusión, gestión y acceso al conocimiento. La acelerada innovación e hibridación de estos dispositivos ha incidido en diversos escenarios. Entre ellos destacan: las relaciones sociales, las estructuras organizacionales, los métodos de enseñanza-aprendizaje, las formas de expresión cultural, los modelos de negocios, las políticas públicas nacionales e internacionales y la producción científica (I+D), entre otros. En el contexto de las sociedades del conocimiento, estos medios pueden contribuir al desarrollo educativo, laboral, político, económico, al bienestar social, entre otros ámbitos de la vida diaria" (Juan Cristóbal Cobo Romaní, 2009).*

A lo largo de este texto nos referiremos a las TIC ateniéndonos a esta definición, y pondremos énfasis tanto en los aspectos técnicos y prácticos de las tecnologías referidas como en las consecuencias sociales de las mismas.

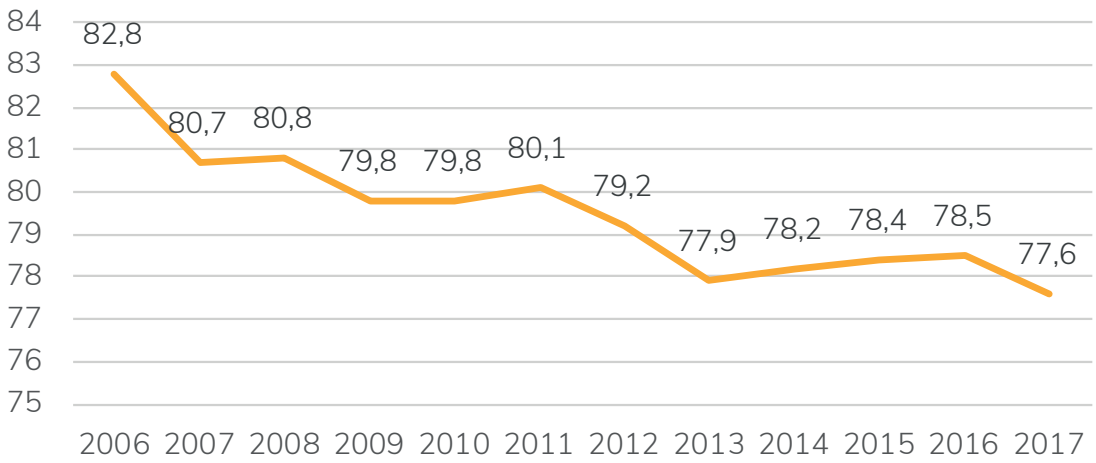
I. Telecomunicaciones

1. Telefonía fija

La telefonía fija –hoy algo perfectamente convencional; en sus orígenes un maravilloso, casi mágico, soporte desarrollado por Alexander Graham Bell– fue la primera TIC, ya que permitió la conexión inmediata entre interlocutores que hasta entonces permanecían incomunicados por la distancia. Hace más de un siglo y cuarto de su llegada a España, con los ensayos pioneros y las primeras conexiones, por parte del Gobierno y de la Corona, y también el ámbito militar. Y pronto se cumplirá un siglo de la fundación en 1924 de la Compañía Telefónica Nacional de España. La escasa demanda inicial, la carencia de recursos de la iniciativa privada, la cambiante legislación y los vaivenes políticos fueron dejando paso a una expansión tan amplia que alcanzó a numerosos hogares españoles. La telefonía fija se mantiene con altos niveles de penetración entre la población, si bien desde mediados de la primera década de este siglo el porcentaje de viviendas que utilizan teléfonos fijos se ha reducido. Mientras que en 2006 casi el 83 por ciento de las viviendas contaban con un aparato telefónico convencional, en la actualidad lo tienen menos del 78 por ciento, según la última Encuesta sobre equipamiento y uso de tecnologías de información y comunicación, efectuada por el Instituto Nacional de Estadística (INE) en 2017.

Gráfico 1
Porcentaje de viviendas con teléfono fijo

Fuente
Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares, 2006-2017. INE

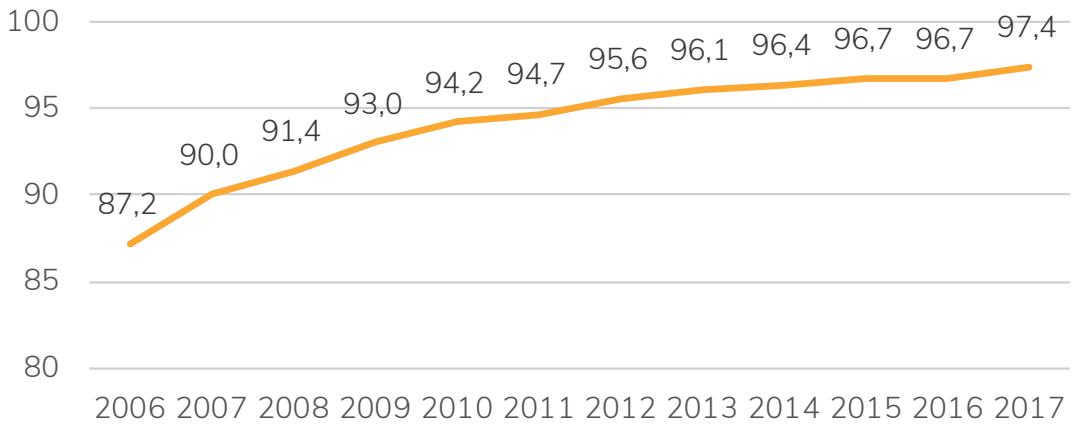


2. Telefonía móvil

La disminución del uso de la telefonía fija se debe a una de las mayores revoluciones que ha experimentado la tecnología, el surgimiento de nuevas soluciones en telecomunicaciones, especialmente la telefonía móvil. Esta tecnología se instala en España en el último cuarto del siglo XX y se masifica de manera comercial a finales de los años 90 y principios de los 2000. Desde entonces, la penetración de telefonía móvil ha aumentado considerablemente: hoy en día casi todos los hogares españoles cuentan con algún dispositivo de este tipo, como se aprecia en el gráfico. Ahora podemos contemplarlo con naturalidad, pero hace no tantos años el fenómeno provocaba vértigo. Pensemos en los hábitos sociales de los años sesenta, setenta y ochenta del siglo anterior. Se hablaba desde el teléfono de casa y para ello se tenía en cuenta un cierto horario. Y para establecer la llamada se operaba no con las teclas actuales, sino de un modo que hoy suena deliciosamente vintage: en aquellos aparatos –que durante muchos años casi siempre estaban fijados en una pared, hasta que se popularizaron los de sobremesa–, había que introducir el dedo índice en uno de los agujeros de una pieza circular troquelada que dejaba al descubierto los números del 1 al 0, inscritos debajo de ella, y tras cada marcación esa pieza circular, metálica o de baquelita, retrocedía acompañada por un peculiar traqueteo. Para las emergencias, estaban las cabinas telefónicas en las calles, los aparatos telefónicos instalados en no pocos bares y en algunos comercios, o los locutorios de las sedes de la Compañía Telefónica o los de las oficinas de Correos y Telégrafos, desde los que solían establecerse las llamadas a otras provincias (“una conferencia, por favor”, era una solicitud habitual en aquella época). Estábamos poco localizables, y aun así, terminábamos por localizarnos, en parte porque por entonces los españoles éramos más caseros que hoy en día: cada etapa tiene sus ritos. La llegada del teléfono

Gráfico 2
Porcentaje de hogares con telefonía móvil

Fuente
Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares. 2006-2017. INE



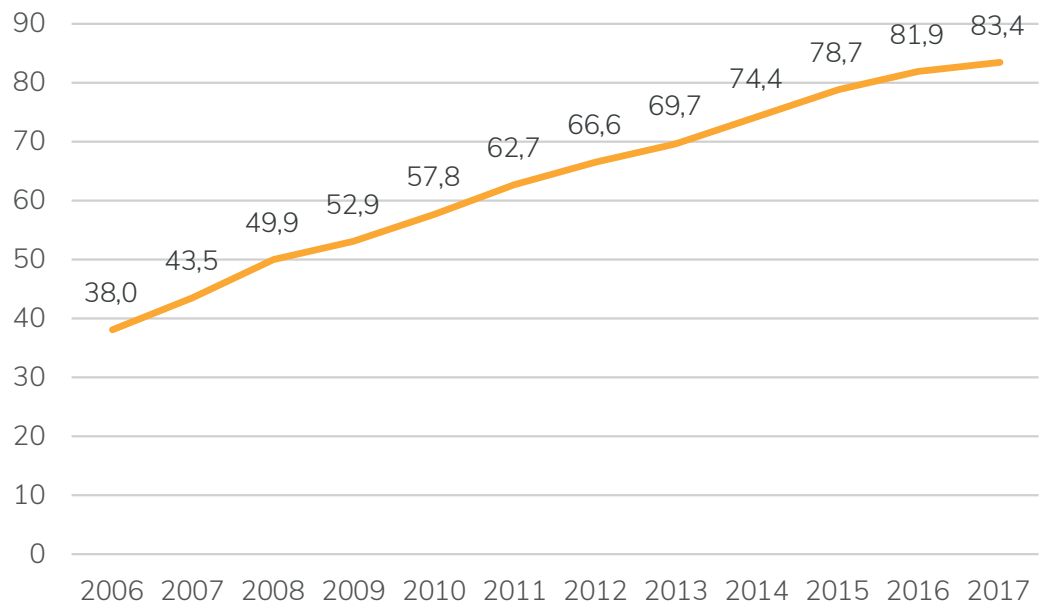
móvil agitó profundamente ese estado de cosas y supuso un vuelco personal, familiar, social y profesional. De pronto, era posible conectar con cualquiera en cualquier lugar. Perfecta y casi diríamos que empírica demostración de la tesis macluhaniana de la aldea global. Pobres y ricos, adultos y niños a partir de los 10-12 años, si no antes, jóvenes y ancianos, todo el mundo lleva aquí su teléfono móvil.

De hecho, en comparación con otros países, España destaca por sus altos niveles de telefonía móvil. Según la agencia We Are Social, en 2018 el 80 por ciento de los españoles tiene un dispositivo de este tipo, una proporción muy por encima del promedio mundial (68%) y de países como o el Reino Unido (75%), China (79%) y Estados Unidos (72%), si bien superada por Corea del Sur (84 por ciento), Hong Kong (83%), Italia (83%), Singapur (82%) y Polonia (81%).

No obstante, entre los segmentos de edad dentro de España todavía se notan importantes diferencias. Según el Barómetro CIS (Estudio 7.715, 2015), el 25 por ciento de los mayores de 65 años no posee un teléfono móvil; para el resto de la población la cifra es de tan solo un 2,2 por ciento. Asimismo, en los municipios menos poblados (hasta 50.000 habitantes) el 9,8 por ciento de los españoles no cuenta con un aparato móvil mientras

Gráfico 3
Porcentaje de viviendas que disponen de acceso a Internet o conexión con banda ancha

Fuente
Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares, 2006-2017. INE



que en los demás la proporción apenas alcanza el 5,6 por ciento.

3. Internet

Además de la telefonía móvil, la otra gran revolución mundial de la década de los noventa fue la llegada y comercialización masiva de Internet. Desde entonces, su incidencia en la población ha aumentado de manera progresiva, y en particular durante la última década: en 2006, menos del 40 por ciento de las viviendas contaban con una conexión a la red mientras que hoy la cifra se ha duplicado holgadamente, superando el 80 por ciento. Una cifra muy expresiva de la velocidad de ese crecimiento en los últimos doce años. Con Internet como instrumento de comunicación ha disminuido notablemente el correo convencional, para ser sustituido por el electrónico, cuyo uso, aun siendo frecuente, se circunscribe sobre todo al ámbito profesional. Porque en el plano individual se imponen rotundamente las modernas aplicaciones: WhatsApp, Telegram, Facebook e Instagram. En cuanto a la utilización de Internet como elemento de consulta, los hechos son palmarios: las enciclopedias han dejado de ocupar espacio en las estanterías domésticas y ahora son una reliquia en librerías de segunda mano, numerosos archivos y bibliotecas están a nuestro alcance con un clic y hasta el Boletín Oficial del Estado ha dejado de editarse en papel y se consulta en la Red.

Gráfico 4
Porcentaje de usuarios de Internet diarios sobre población total de 14 años y más

Fuente
Encuesta general de medios, 1997-2018. INE.

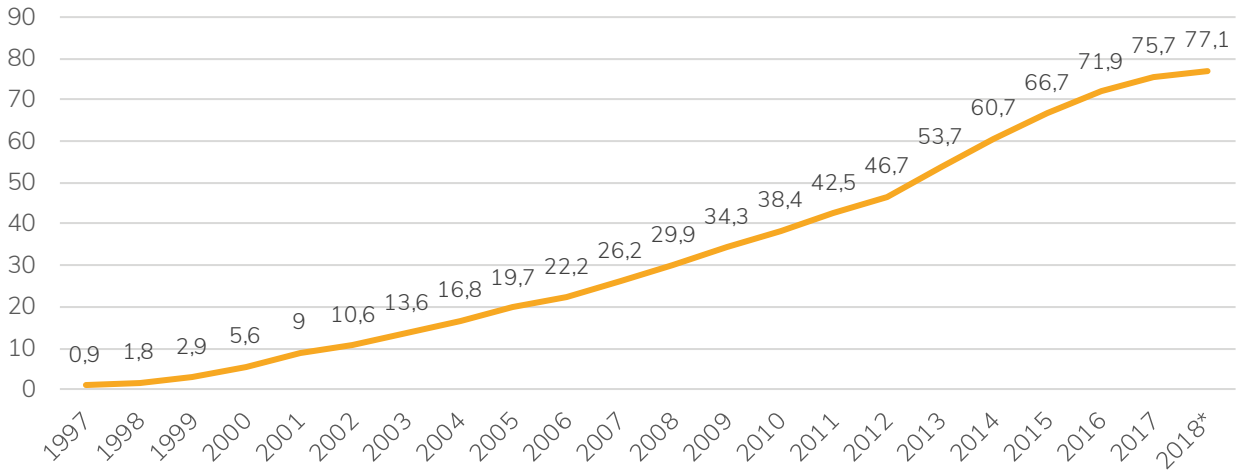
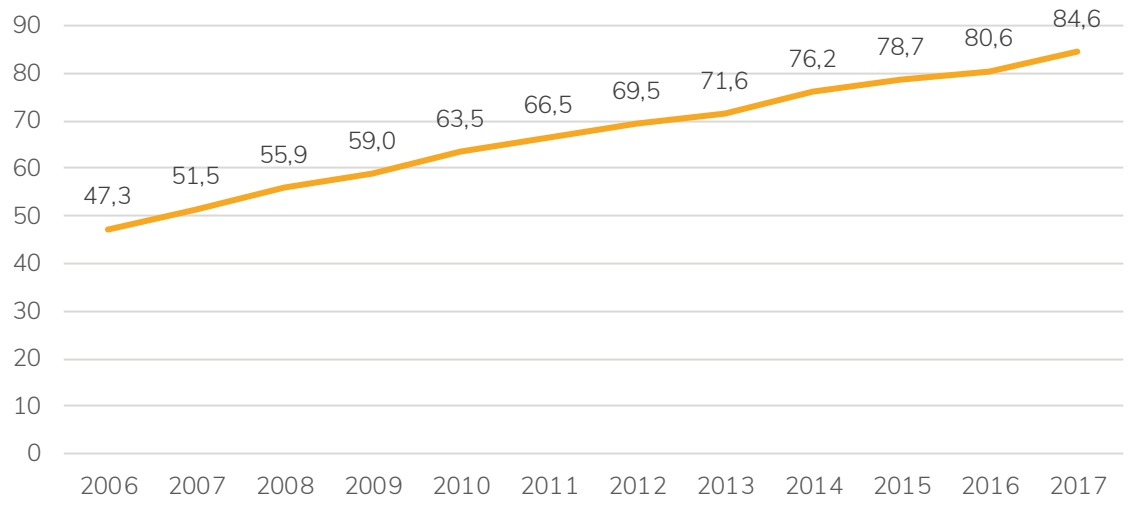


Gráfico 5
Porcentaje de personas de 16 a 74 años que ha utilizado Internet en los últimos tres meses

Fuente
Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares. INE, 2006-2017



Y no solo hay mayor acceso doméstico a Internet, sino que su uso cotidiano ha aumentado de manera exponencial. En tan solo veinte años la proporción de españoles mayores de 14 años que hace uso de Internet diariamente ha subido desde no alcanzar siquiera el 1 por ciento hasta casi el 80 por ciento.

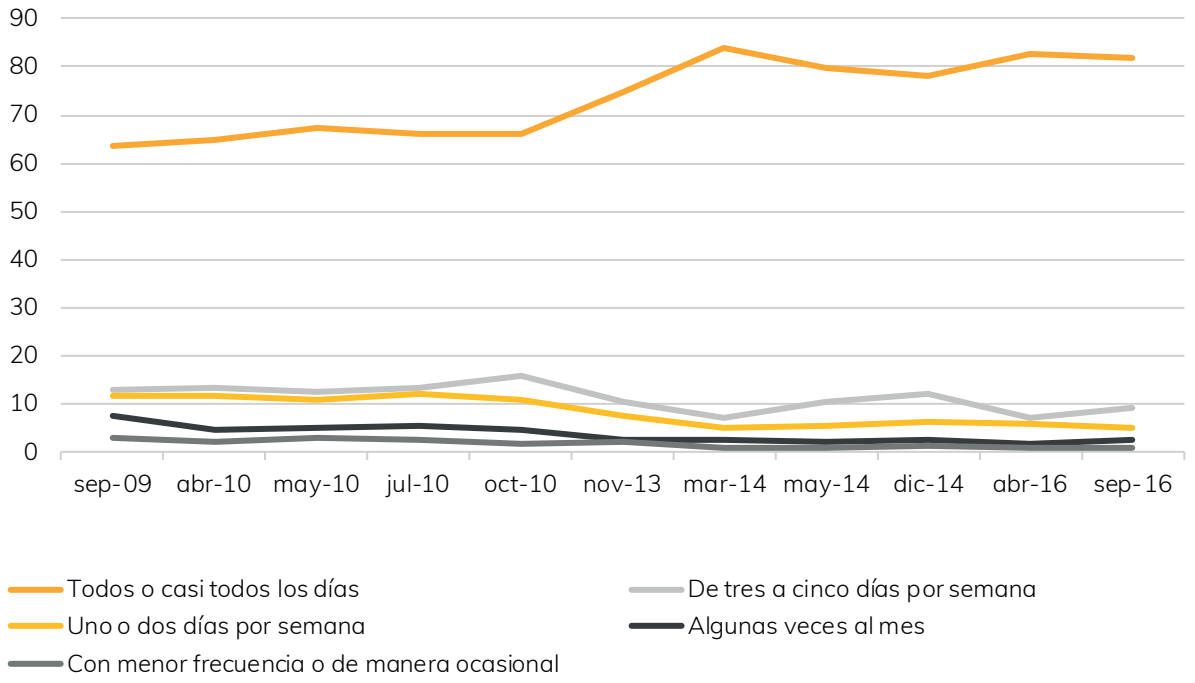
De hecho, al incluir a los internautas menos frecuentes (quienes han usado Internet al menos una vez en los últimos tres meses) la proporción que engloba a casi todas las franjas de edad llega al 85 por ciento. La conclusión más importante es que podemos observar que la gran mayoría de los que navegan por Internet lo hacen de manera diaria.

II. Dispositivos

La irrupción de Internet y de la telefonía móvil supusieron a su vez la entrada en nuestras vidas de nuevos dispositivos, como el ordenador personal, el smartphone, las videoconsolas y las tablets. Y es que la tenencia de este tipo de equipos también ha aumentado considerablemente durante las últimas décadas. Aunque el ordenador personal ya había penetrado de manera apreciable en las casas de los españoles, es la llegada de Internet lo que dispara su utilización, aligera su formato e incrementa sus prestaciones. Qué decir de las videoconsolas, con versiones crecientemente modernas y juegos cada vez más sofisticados. Los

Gráfico 6
Evolución, en porcentaje, de la frecuencia de acceso a Internet en los últimos doce meses (solo quienes lo han utilizado en ese periodo)

Fuente
Barómetros CIS



smartphones son mucho más que un teléfono móvil, al incorporar conexión con Internet: con ellos podemos llevar en el bolsillo la agenda y de alguna manera hasta la oficina, hacer y enviar fotografías, escuchar música, recibir y enviar correos, consultar todo tipo de cosas, reservar billetes y hoteles, grabar imágenes y sonidos, recibir alertas y noticias, comunicarnos con amigos y familiares, efectuar operaciones bancarias... Muchas de estas funciones también las puede cumplir la tablet, el paso que faltaba para nuestra comodidad: un ordenador más reducido que podemos transportar a cualquier lugar por su liviano peso.

1. Ordenadores

Según la Encuesta sobre equipamiento y uso de tecnologías de información y comunicación, el 36 por ciento de las viviendas en España contaban con un ordenador en 2002. En la actualidad, la proporción es de casi el 80 por ciento. Ambas cifras resultan muy

llamativas: si hace doce años ya era apreciable la penetración, que rebasaba un tercio de los hogares, hoy rebasa con mucho las tres cuartas partes, todo un signo de modernidad.

Nuevamente, vemos cómo el aumento en la adquisición de estas tecnologías ha venido acompañado de un incremento en su uso. De hecho, en el año 2017 el 74 por ciento de los españoles ha utilizado el ordenador personal en los últimos tres meses.

Sin embargo, la tenencia y el uso de ordenadores personales no se distribuyen de manera uniforme entre los distintos segmentos de la población española. Otra vez se observan diferencias considerables entre los grupos etarios (aquellos en los que la edad es el rasgo distintivo) y las concentraciones urbanas. Según la Encuesta sobre equipamiento y uso de tecnologías efectuada por el INE para 2017, el 94 por ciento de los españoles entre 16 a 24 años ha usado un ordenador en los últimos tres meses mientras que solo el 36 por ciento de los mayores a 65 años hacen lo propio. Asimismo, si en las concentraciones urbanas mayores de 100.000 habitantes la proporción llega al 79 por ciento, en aquellas con poblaciones menores de 10.000 la cifra es de tan solo del 66 por ciento.

Gráfico 7
Porcentaje de viviendas con algún tipo de ordenador

Fuente
Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares (2006-2017. INE)

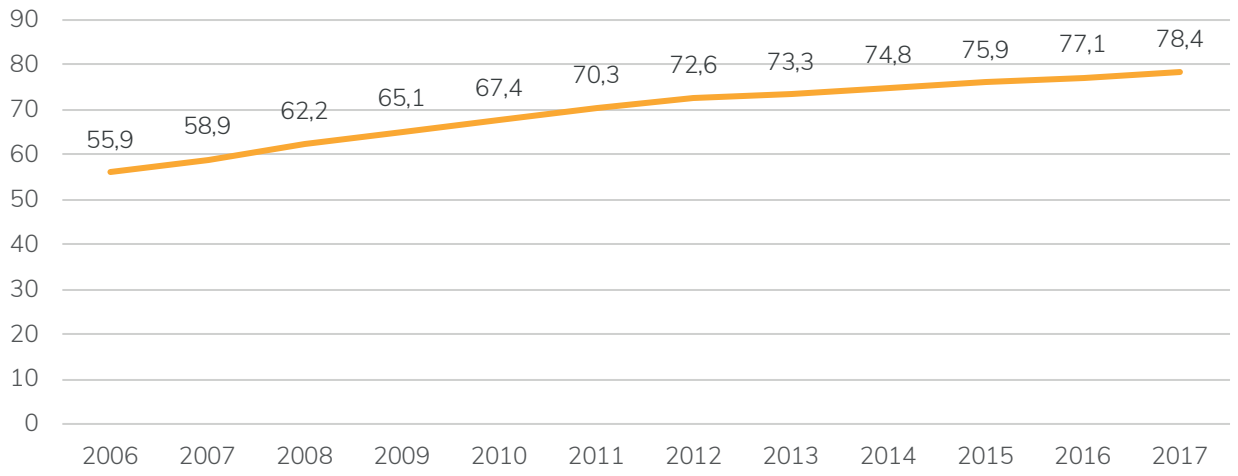
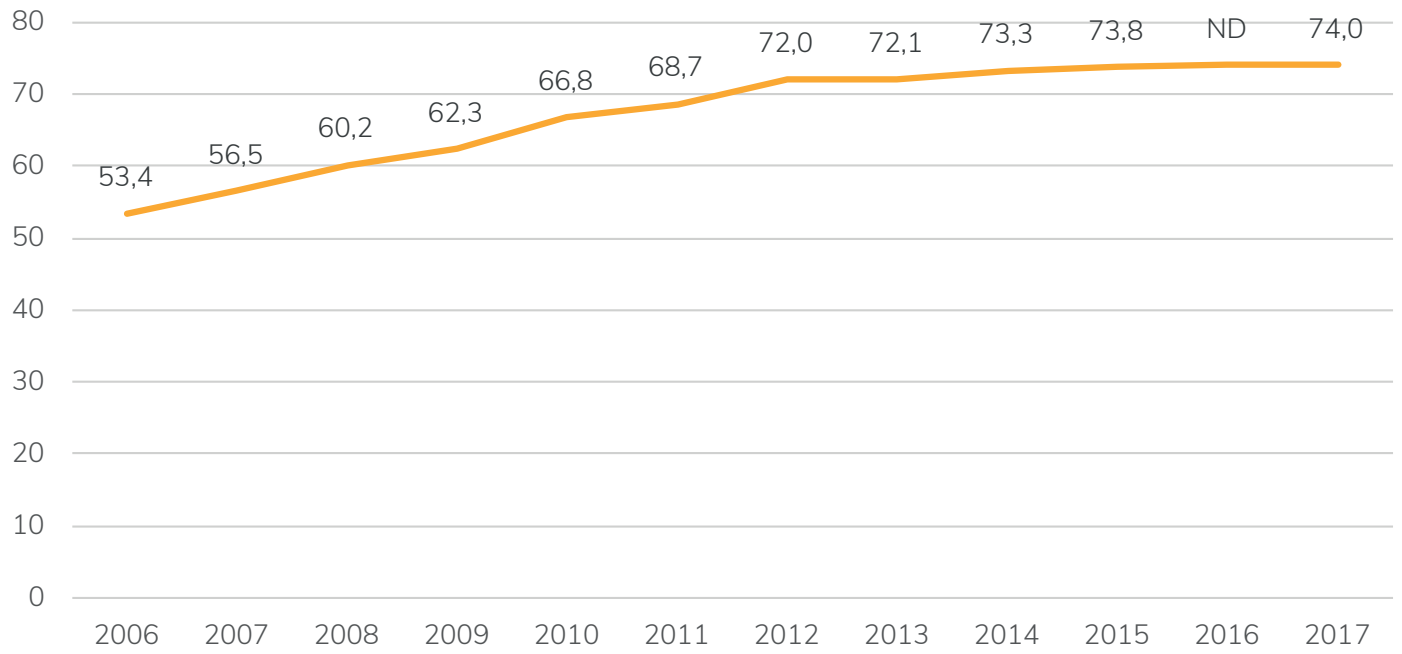


Gráfico 8
Porcentaje de personas de 16 a 74 años que han utilizado el ordenador en los últimos tres meses

Fuente
Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares (2006-2017. INE)



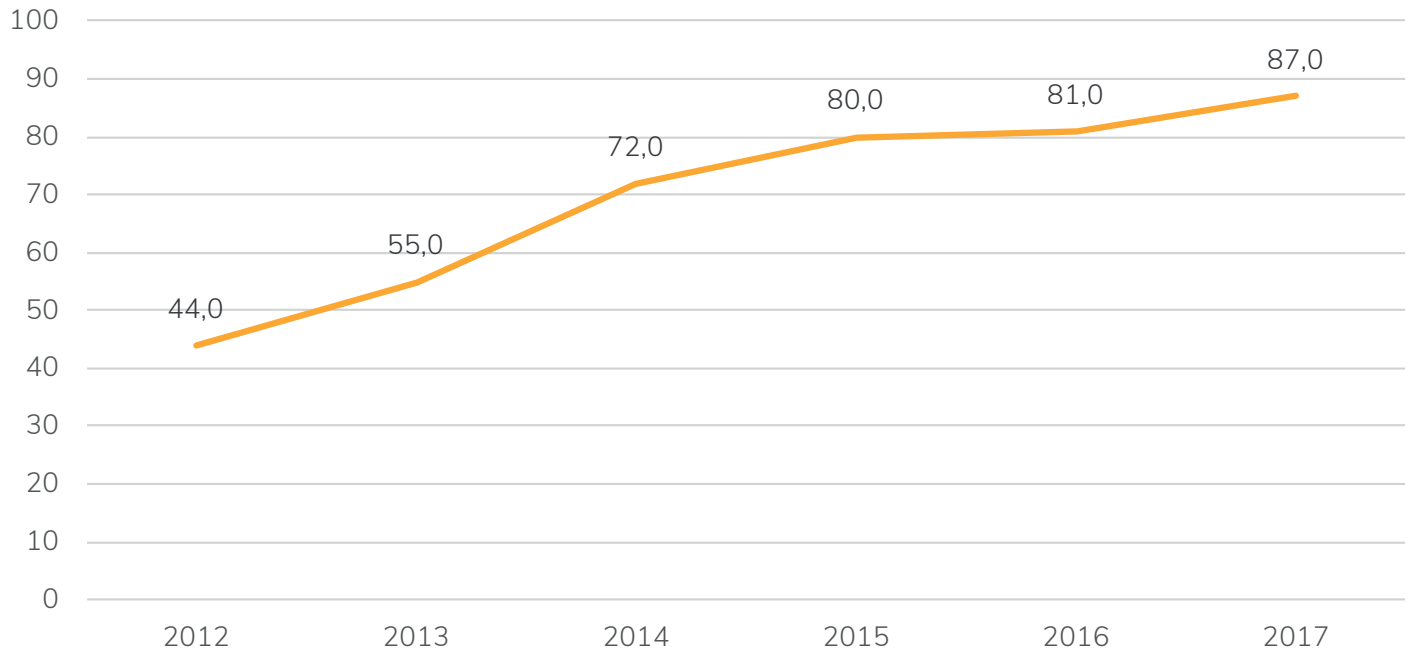
2. Smartphones, tablets y dispositivos inteligentes

Combinando la portabilidad de la telefonía móvil con el poder operativo de los ordenadores, los smartphones se han convertido en otro dispositivo de uso masivo entre los españoles. Estos no solo permiten al usuario realizar llamadas telefónicas, sino también enviar y recibir correos electrónicos, navegar por Internet y hacer uso de una gran variedad de programas (o aplicaciones, "apps") instalados en el sistema operativo del smartphone. Según el Barómetro de Consumidores de Google (2018), el 87 por ciento de la población española usa un smartphone –cifra considerablemente superior a la cantidad de personas que usan un ordenador-. De hecho, la penetración de los smartphones superó a la de los ordenadores en los últimos cinco años.

Más allá de los ordenadores, los smartphones lideran los índices de penetración entre los distintos tipos de dispositivos inteligentes de última generación. Según el Global Mobile Consumer Survey, 2017, de la consultora

Gráfico 9
Evolución del porcentaje que utiliza un smartphone (sobre población total online y offline)

Fuente
Barómetro de Google para España

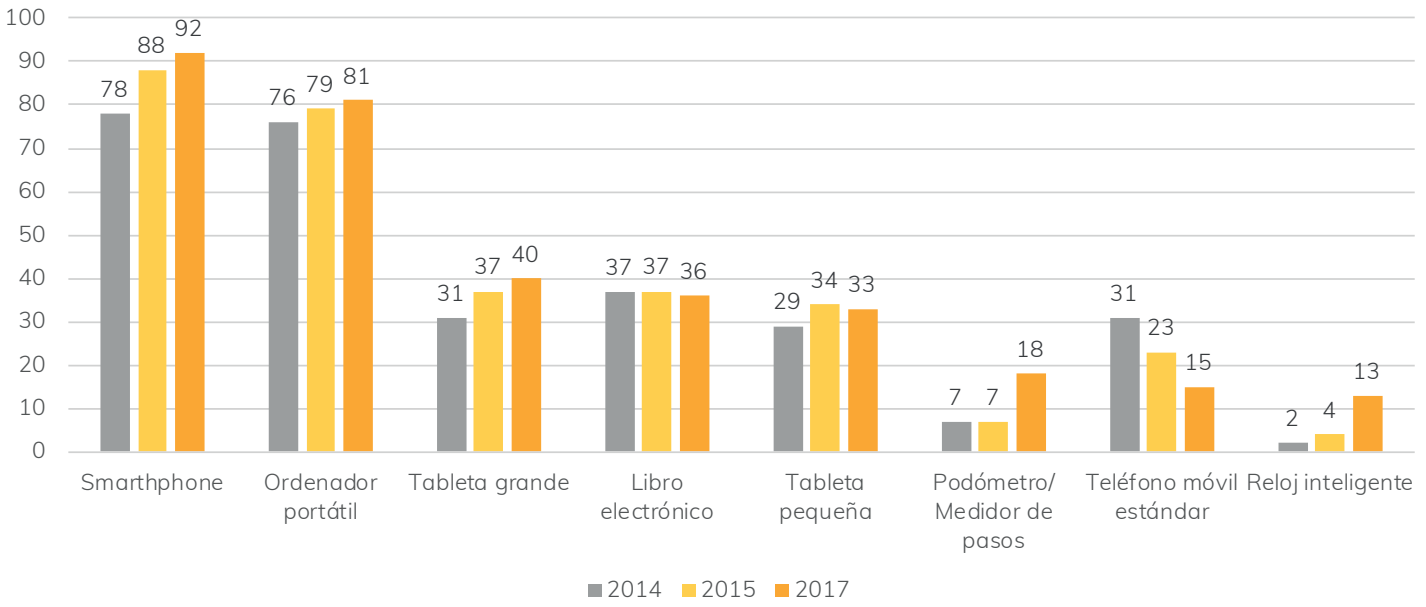


Deloitte, los smartphones y ordenadores portátiles son los más usados entre los españoles, seguidos por las tabletas, libros electrónicos, podómetros, teléfonos móviles convencionales y relojes inteligentes. Cabe destacar que los índices de tenencia de smartphones y ordenadores personales se equiparan a las medias europeas, cuando no las superan.

Al igual que con otros indicadores ya mencionados, la penetración de dispositivos inteligentes no es igual en todos los segmentos de la sociedad. Nuevamente se observan importantes diferencias según grupos de edad; mientras que 43,9 por ciento de los encuestados por el Barómetro del Centro de Investigaciones Sociológicas (CIS) de mayo 2018 aseguran tener una tableta en su vivienda, entre los encuestados mayores a 65 años la cifra desciende al 16,1 por ciento. Con respecto a las smart TV y las consolas de videojuegos, los promedios totales son del 36,3 y del 31,6 por ciento respectivamente, mientras que entre los mayores de 65 años las proporciones apenas alcanzan el 13,6 y el 3 por ciento.

Gráfico 10
Evolución, en porcentajes, de la penetración de dispositivos

Fuente
Deloitte. Global Mobile Consumer Survey, 2017



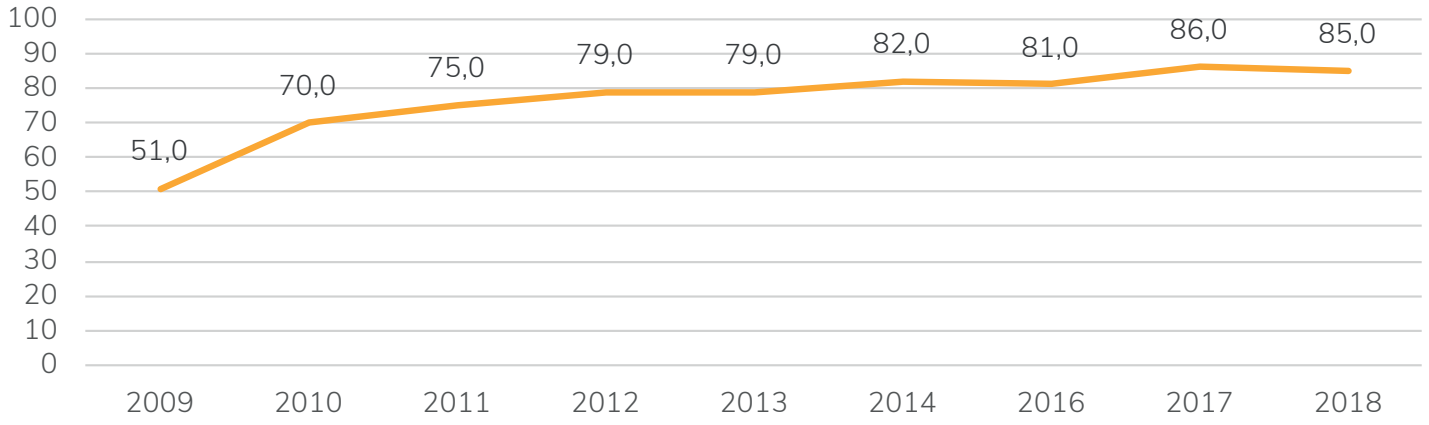
III. Redes sociales

Entre las tendencias más actuales, imperan de forma abrumadora las redes sociales. Generan y difunden opiniones, consignas, modas, noticias, etc. Las redes sociales influyen poderosamente en el ámbito comercial, en la interacción social y, como parecía inexorable, en la praxis política.

Ha aumentado el uso y el acceso a las nuevas redes de telecomunicación y además disponemos en mayor medida de una creciente variedad de dispositivos inteligentes, por lo que resulta interesante observar qué hacemos cuando estamos en línea. Seguramente una de las principales actividades en este mundo hiperconectado de Internet y las TIC es navegar en redes sociales como Facebook, Twitter o Instagram. Estas redes se constituyen en plataformas de Internet que permiten a los usuarios conectarse y comunicarse entre sí facilitando el intercambio de mensajes y contenidos digitales. Puesto que la mayoría de las redes sociales son compatibles con distintos tipos de dispositivos, su uso se ha extendido conforme lo ha hecho el acceso y el uso de las nuevas tecnologías. Igualmente, estas redes han ido aumentado y ampliando sus aplicaciones incluyendo no solo la

Gráfico 11
Evolución, en porcentajes, de la penetración de redes sociales

Fuente
Estudio anual de redes sociales 2018 (IAB)



*Edades 18-55 años hasta 2014, 16-55 en 2016 y 16-65 a partir de 2017

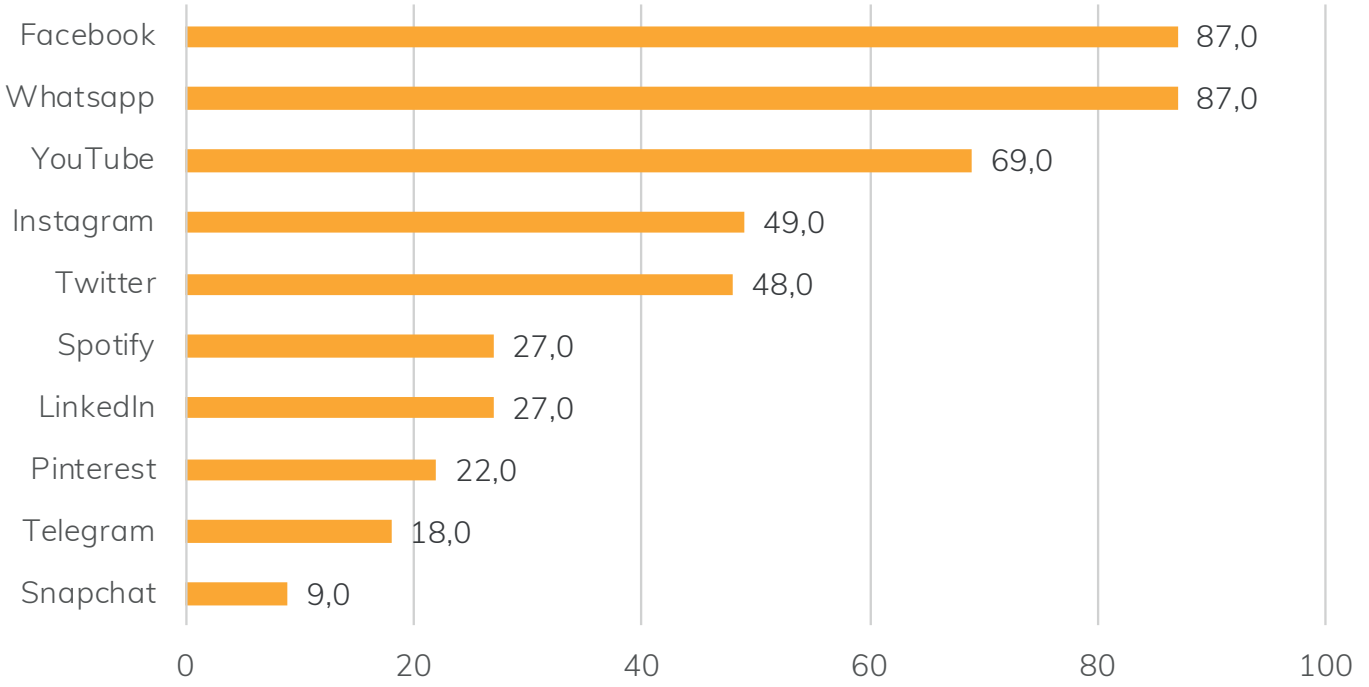
mensajería instantánea y compartiendo contenidos de todo tipo, sino también ofreciendo funciones propias de los medios de comunicación convencionales. Como consecuencia de estos mecanismos de universalización, las redes han aumentado de manera exponencial sus miembros durante los últimos años.

Según el Estudio Anual de Redes Sociales (2018) del Interactive Adverstising Bureau (IAB), la asociación de la publicidad, el marketing y la comunicación digital en España, en la actualidad la penetración de las redes sociales alcanza al 85 por ciento de la población internauta de España. Como referencia, en 2009 la cifra apenas superaba el 50 por ciento.

Entre las distintas redes destacan WhatsApp y Facebook: ambas son usadas por nueve de cada diez usuarios de redes sociales. Le siguen YouTube, Instagram y Twitter. Como promedio, los encuestados declaran dedicarle aproximadamente una hora a cada red social que utilizan y en general utilizan casi cinco redes sociales. De nuevo, son los jóvenes (de 16 a 30 años) los que hacen mayor uso de las redes.

Gráfico 12
Porcentajes de uso de las redes sociales (2018)

Fuente
Estudio anual de redes sociales 2018 (IAB)



IV. Consumo

La revolución tecnológica no solo está afectando a la tenencia y el uso de dispositivos y redes sociales, sino que también está cambiando los hábitos de compra de los españoles. Así, el e-commerce va ganando cada vez más terreno a la compra tradicional. En efecto, para inicios de 2018, el volumen del mercado de compras en línea se estimaba en cerca de 9.000 millones de euros y las cinco empresas de mayor facturación en este campo fueron Amazon, El Corte Inglés, PC Componentes, Media Markt y Mercadona.

En 2017, cuatro de cada diez personas de 16 a 74 años declararon haber comprado a través de Internet en los últimos tres meses. Este porcentaje muestra una tendencia al alza constante desde 2006 (primer año de la serie), y acumula un incremento de 30 puntos en once años.

No obstante, entre los españoles se ven diferencias en la disposición a hacer compras por Internet: los hombres son más propensos que las mujeres, y los jóvenes, mucho más que los mayores. De igual manera, los españoles tienden a comprar por Internet en mayor proporción

Gráfico 13
Horas y minutos diarios del uso de redes sociales (2018)

Fuente
Estudio anual de redes sociales 2018 (IAB)

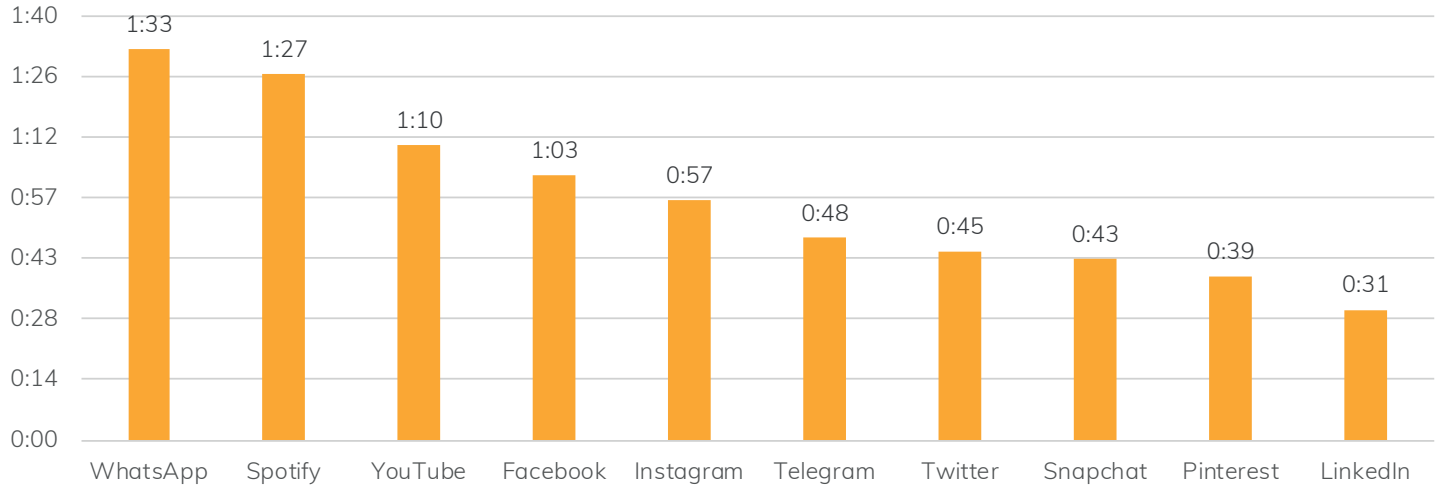


Gráfico 14
Empresas online con mayor facturación en España en 2017

Fuente
ecommerceDB.com

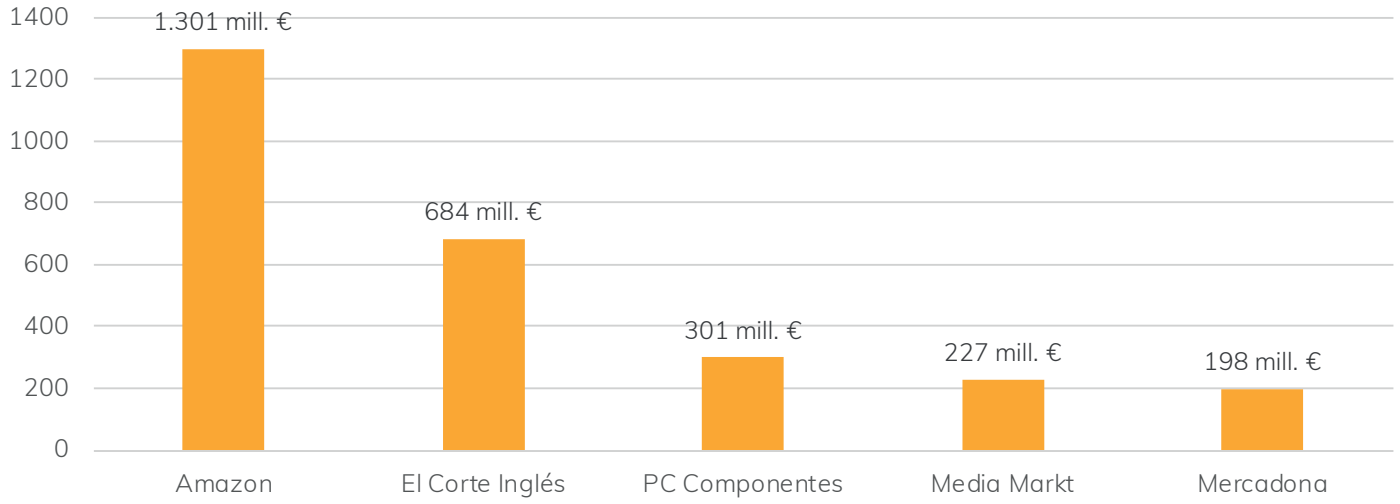
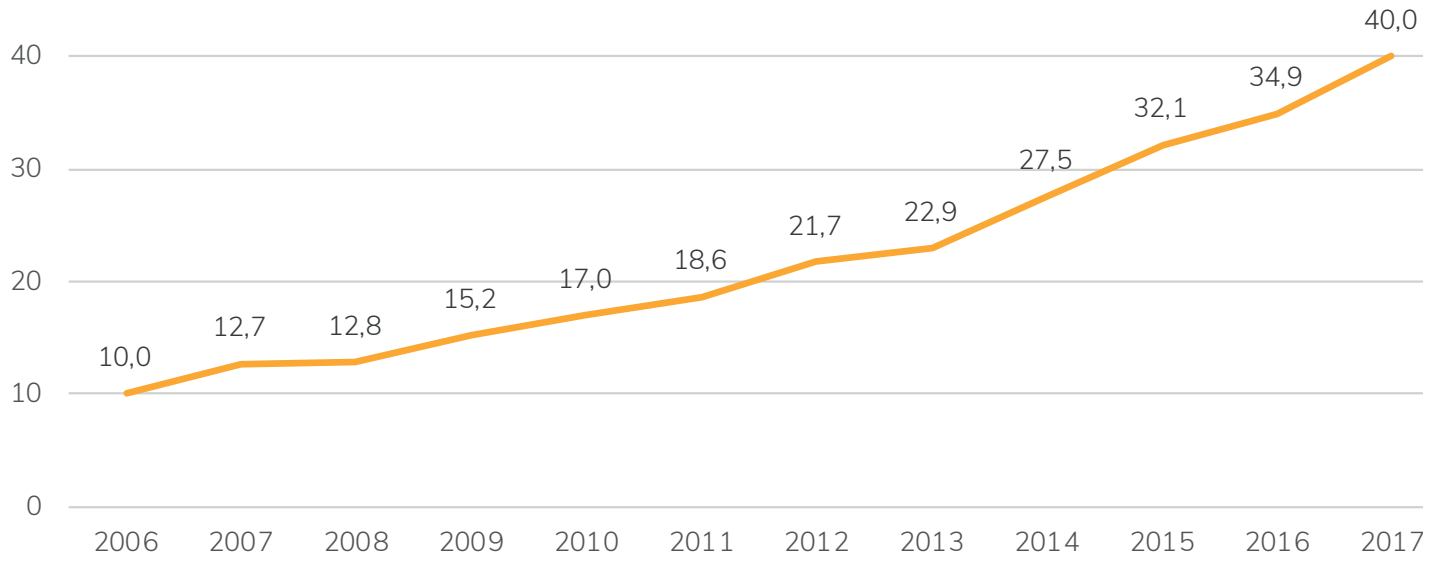


Gráfico 15
Evolución del porcentaje de personas que han comprado a través de Internet en los últimos tres meses

Fuente
Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares (INE. 2006-2017)



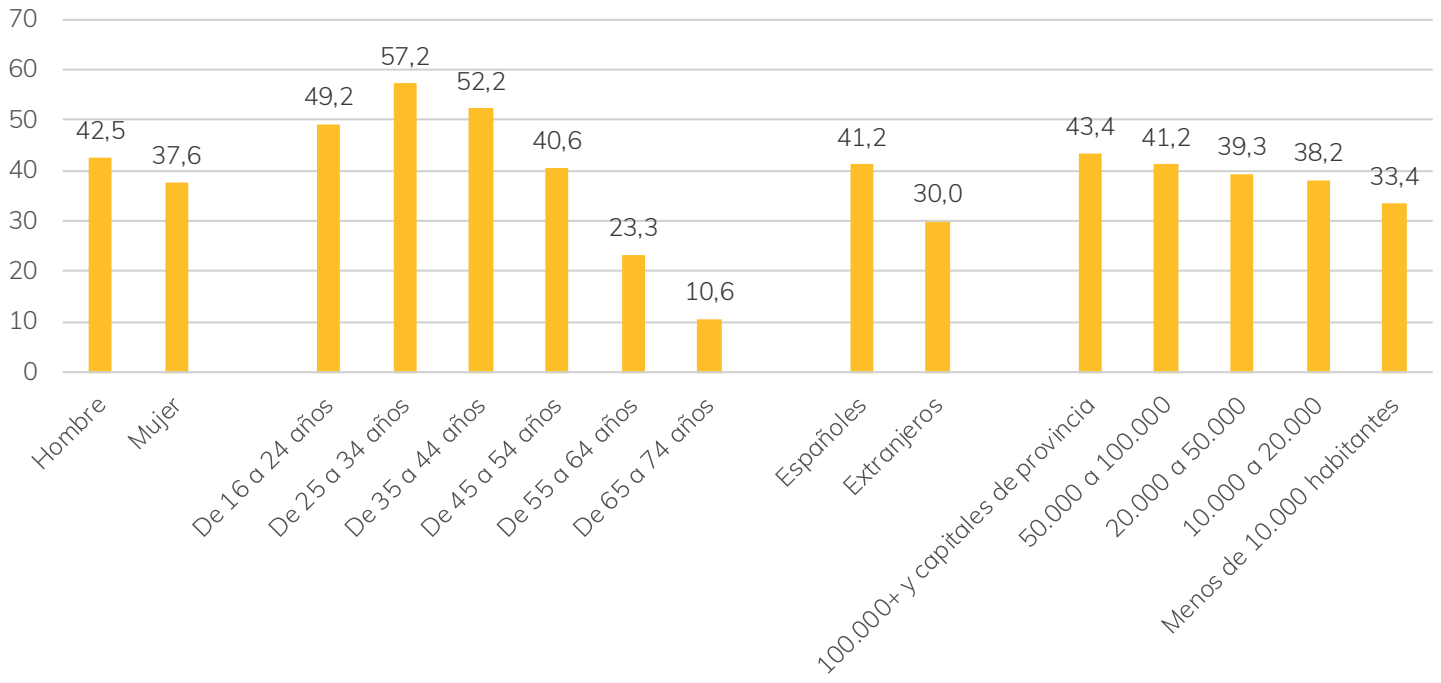
que los extranjeros. Por último, los grandes núcleos urbanos son más propensos que las poblaciones menos habitadas.

Al incluir a los encuestados que han comprado por Internet en los últimos doce meses, los productos o servicios más adquiridos son: alojamiento de vacaciones (54,1 por ciento), material deportivo y ropa (53,5 por ciento), entradas para espectáculos (47,6 por ciento) y otros servicios para viajes (44,7 por ciento). En la cola, quedarían el material formativo online (11,1 por ciento) y los medicamentos (3 por ciento).

Sin embargo, hay ciertos reparos y no todo el mundo está dispuesto a realizar compras por Internet, incluyendo a aquellos que lo usan para otras actividades. Las principales razones para no comprar por Internet alegadas por la población internauta son: la preferencia por comprar personalmente en una tienda (80,5 por ciento), la preocupación por la privacidad o la seguridad en el pago (49,8 por ciento), la falta de habilidades o conocimientos (39,5 por ciento) y la falta de confianza en la recepción o devolución de los productos, en las reclamaciones e indemnizaciones (37,7 por ciento). Las razones menos mencionadas son no disponer de una tarjeta que permita pagar por Internet (18,5 por ciento), considerar que la entrega es problemática (17,7 por ciento), y afirmar que los vendedores extranjeros no atienden pedidos en España (5,3 por ciento).

Gráfico 16
Porcentaje, por características sociodemográficas, de personas entre 16 y 74 años que han comprado por Internet en los últimos tres meses

Fuente
Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares (INE, 2017)



A pesar de que la cantidad de compradores online aumenta con el paso de los años, los españoles adquieren productos y servicios por Internet en menor medida que la mayoría de los demás países de la Unión Europea. Dada la alta penetración de ordenadores y móviles antes mencionada, así como el elevado uso de redes sociales entre los españoles, llama la atención que España se encuentre por debajo de la media con respecto a los demás países europeos. Aparte del peso de la tradición entre nosotros, una explicación razonable de que las compras en tiendas físicas sean tan numerosas en España reside en el clima: salir a la calle con ese objetivo es algo lúdico en sí mismo, no digamos si implica poder hacerlo en compañía de amigos o familiares, una característica también muy nuestra, como país abierto, menos previsible que otros en lo que respecta a sus pautas sociales.

V. Educación

1. La educación a distancia

La revolución tecnológica que ha supuesto el despegue de las tecnologías de la información en España también ha tenido un considerable impacto en la

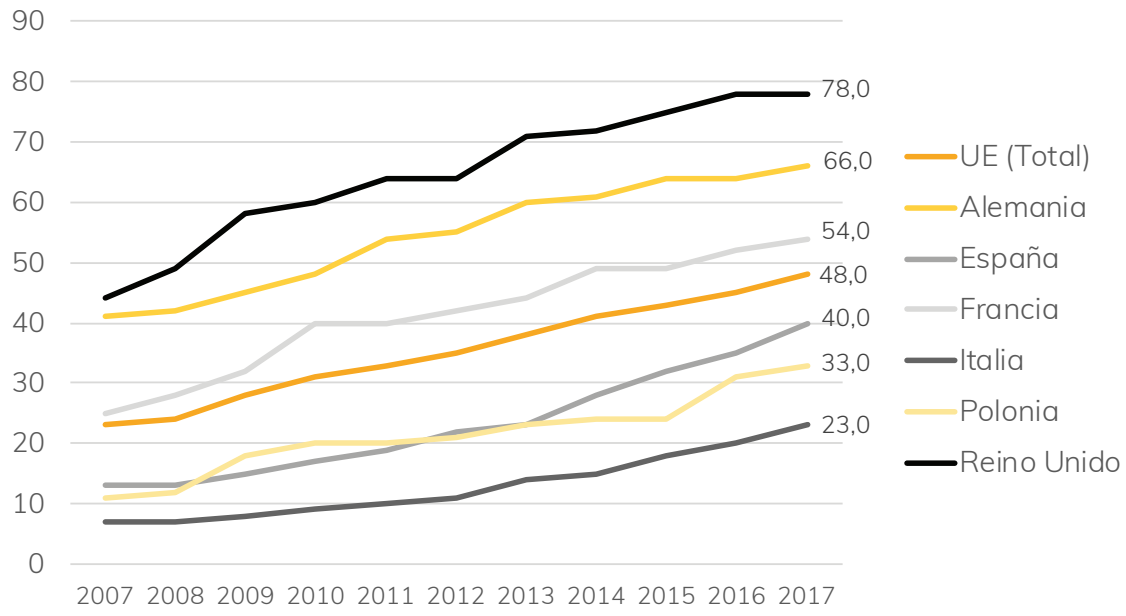
Tabla 1
Uso de comercio electrónico con fines privados o para el hogar en los últimos doce meses por tipo de producto

Fuente
Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares (INE, 2017)

Tipo de compra	% que ha comprado por Internet en el último año
Alojamiento de vacaciones (hotel, apartamento, etc.)	54,1
Material deportivo, ropa	53,5
Entradas para espectáculos (cine, teatros, conciertos...)	47,6
Otros servicios para viajes (billetes de transporte público, alquiler de coches, etc.)	44,7
Bienes para el hogar (de tipo duradero)	36,6
Otros productos o servicios	29,9
Libros, revistas, periódicos (incluye libros electrónicos)	24,5
Equipo informático (ordenadores y accesorios)	21,1
Equipamiento electrónico (p. ej., cámaras fotográficas)	20,3
Productos de alimentación y otros de consumo no duraderos	16,3
Servicios de telecomunicaciones (p. ej., contratos de banda ancha, líneas telefónicas o TV, recarga de tarjetas prepago, etc.)	15,5
Películas, música	13,9
Juegos de ordenador o videoconsolas y sus actualizaciones	13,9
Otro software de ordenador y sus actualizaciones	13,8
Material formativo *online*	11,1
Medicamentos	3,3

Gráfico 17
Porcentaje de personas entre 16 y 74 años que han comprado por Internet en los últimos tres meses, por país de residencia

Fuente
Eurostat

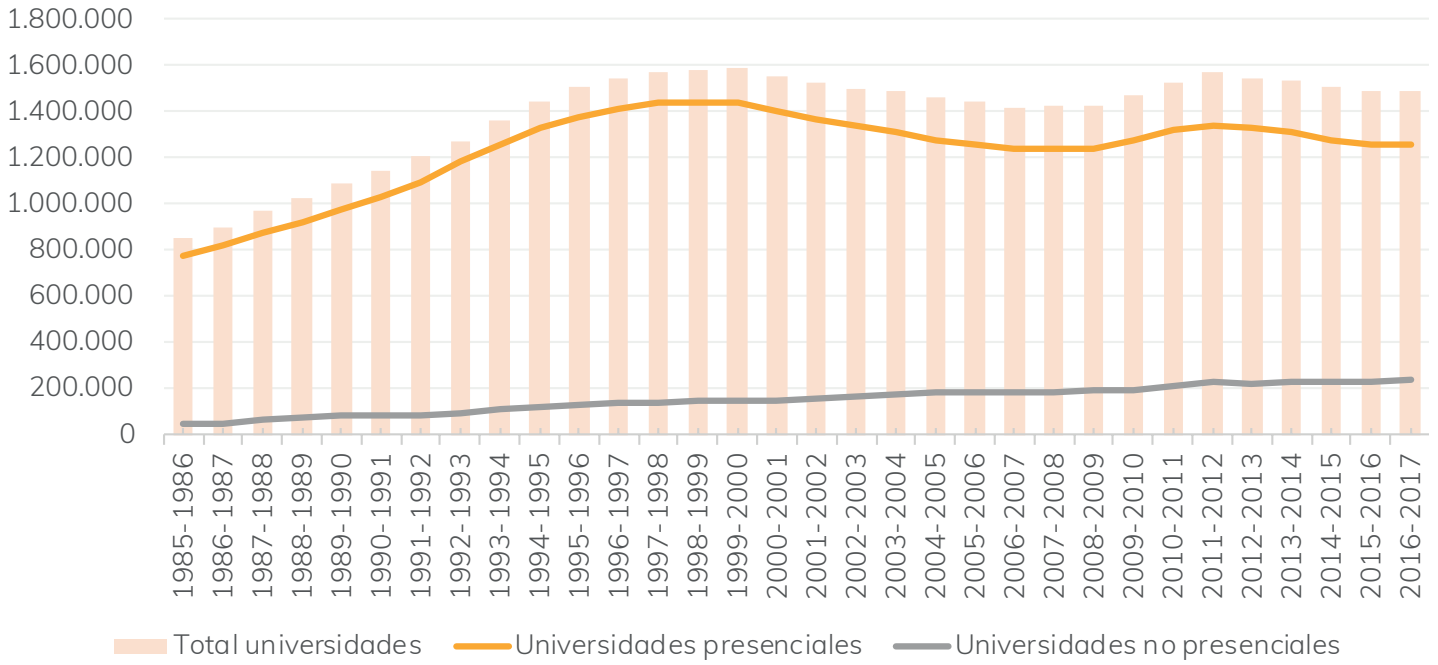


educación, especialmente porque ofrece la posibilidad de poder estudiar cursos académicos sin necesidad de acudir a un centro de enseñanza. Si bien la opción de estudiar a distancia en España ya era posible gracias principalmente a la Universidad Nacional de Educación a Distancia (UNED), la llegada de Internet ha dado un impulso a esta modalidad formativa gracias a la creación de nuevas universidades no presenciales y al crecimiento de la oferta de cursos online en las universidades presenciales, que multiplican de ese modo su oferta.

Desde el curso académico 1993-1994 prácticamente se ha duplicado el porcentaje de alumnos matriculados en universidades de carácter no presencial. En dicho año, el número de estudiantes de las universidades a distancia era de 109.624, un 8 por ciento del total de universitarios. En el curso académico 2016-2017 la cifra de alumnos ascendió a 235.595, lo que representa un 15,8 por ciento de estudiantes universitarios a distancia en España.

Gráfico 18
Evolución del número de estudiantes matriculados en universidades presenciales y no presenciales

Fuente
Subdirección General de Coordinación y Seguimiento Universitario. Sistema Integrado de Información Universitaria (SIIU). Ministerio de Educación, Cultura y Deporte



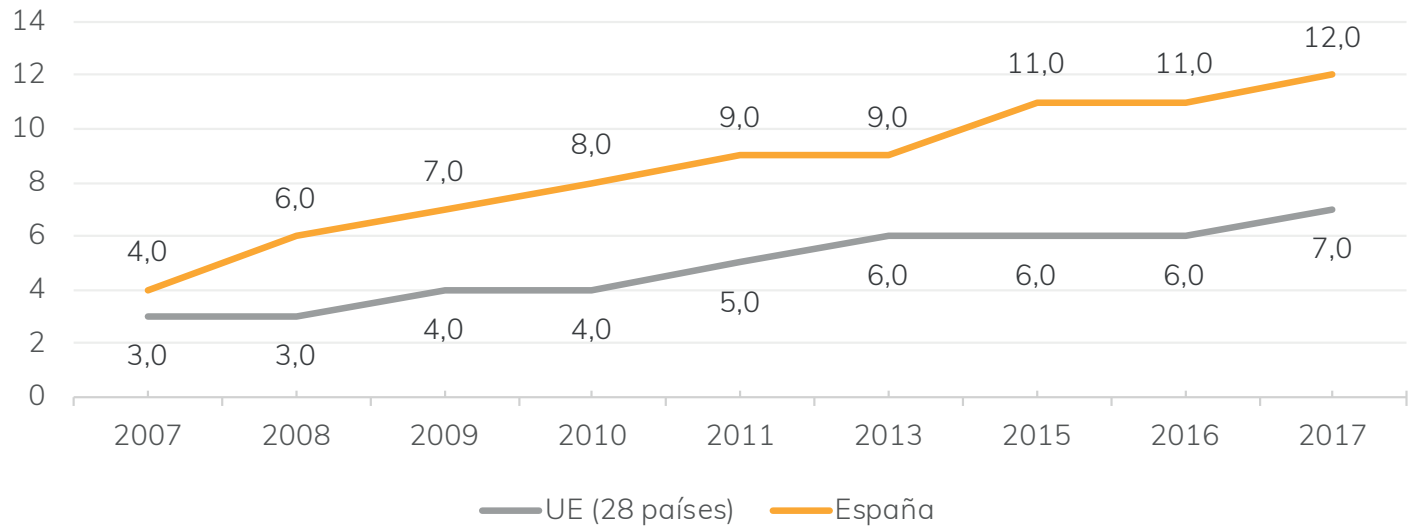
Pero la llegada de las tecnologías de la información no solo ha tenido impacto en el creciente número de estudiantes matriculados en universidades no presenciales: son también muchos los que aprovechan las ventajas y facilidades que les proporciona Internet para obtener formación específica bajo las fórmulas de los cursos online, sin la obligación de estudiar en el sistema universitario.

En este sentido, el porcentaje de personas que usan Internet para realizar cursos online en España ha crecido desde el 4 hasta el 12 por ciento durante los últimos diez años, lo que sitúa a nuestro país cinco puntos por encima de la media de la Unión Europea en este sentido. Los datos también nos muestran que la popularidad de este tipo de cursos ha crecido de forma más acelerada en España que en la Unión Europea en su conjunto, pues en el año 2007 tan solo existía en este capítulo una diferencia de un punto.

Además del uso de Internet para realizar cursos de manera no presencial, esta herramienta también se ha

Gráfico 19
Porcentaje de personas entre 16 y 74 años que usan Internet para realizar cursos online

Fuente
Eurostat



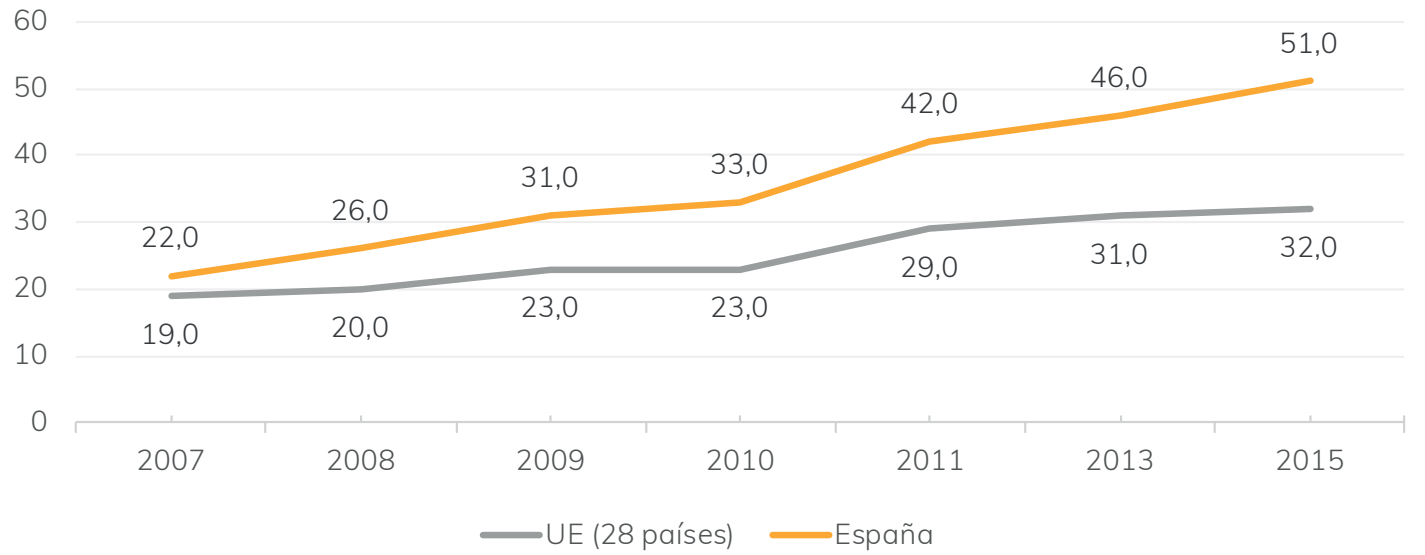
convertido en indispensable para buscar información a la hora inscribirse en algún tipo de oferta formativa, sea esta presencial o no. En este sentido, en el año 2007 un 22 por ciento de los ciudadanos en España usaba Internet para informarse acerca de ofertas de cursos educativos, tres puntos por encima de la media de la UE-28. Unos años después, en 2015, este porcentaje había superado con creces el doble, llegando al 51 por ciento y superando a la media de la Unión Europea en 19 puntos porcentuales.

Más allá de la educación de carácter formal, las tecnologías de la información han influido en la difusión de cursos o tutoriales (neologismo de origen inglés con el que se conocen ciertos cursillos o conjuntos de instrucciones) que no forman parte de un currículo educativo oficial. De hecho, este tipo de formación está mucho más extendida en el entorno digital que la educación reglada. En ese sentido, los datos del Instituto Nacional de Estadística reflejan que más de una cuarta parte de los españoles ha usado, durante los últimos tres meses, material de aprendizaje online (por ejemplo, material de carácter audiovisual o algún software de aprendizaje en línea) que no constituya un curso completo. En contraste, aquellos que han realizado un curso online durante los últimos tres meses representan un 14,8 por ciento de la ciudadanía.

La diferencia entre estas dos cifras es perfectamente comprensible si tenemos en cuenta las potencialidades que ofrece un entorno digital para seleccionar de forma muy precisa aquella información que se desea obtener y aquella que resulta menos prioritaria para el individuo. Un ejemplo muy significativo acerca de la

Gráfico 20
Porcentaje de personas entre 16 y 74 años que usan Internet para buscar información sobre educación o cursos online

Fuente
Eurostat



obtención de conocimiento o habilidades específicas lo encontramos en las plataformas de vídeos online tales como YouTube, donde algunos de sus usuarios (sean particulares u organizaciones) a menudo suben vídeos ofreciendo formación sobre asuntos muy concretos. Según los datos del estudio Mikroscopia, de la firma de investigaciones sociológicas MyWord, un 39,7 por ciento de los usuarios españoles de esta página había accedido a ella en busca de vídeos educativos o de aprendizaje tales como la resolución de algún problema matemático o la pronunciación de palabras en ciertos idiomas. Otro caso relacionado con el aprendizaje específico son los videotutoriales que se pueden encontrar en este tipo de plataformas, entre las que YouTube es la más popular a día de hoy. Del mismo estudio Mikroscopia se desprende que hasta el 56 por ciento de los usuarios de esta plataforma había accedido a ella con el objetivo de buscar tutoriales sobre temas prácticos o manuales específicos. En este tipo de contenido formativo podemos encontrar desde guías sobre cómo usar un programa informático hasta aprender una nueva receta de cocina, lo que da cuenta de la capacidad que tiene Internet para suministrar conocimiento específico sobre cualquier temática.

2. La tecnología de la información en el aula

La transformación digital que ha sufrido España desde mediados de los años noventa también ha afectado a la estructura y al equipamiento del que disponen las instalaciones educativas en nuestro país, donde Internet se ha convertido en un aliado de los centros

Tabla 2
Servicios de Internet usados por motivos particulares en los últimos 3 meses por características demográficas y naturaleza del servicio

Fuente
Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares. INE

Realización de actividades de aprendizaje a través de Internet con fines profesionales o privados	%
Realizar algún curso online	14,8
Utilizar material de aprendizaje online que no sea un curso completo online (p. ej. material audiovisual, software de aprendizaje online, ...)	25,9
Comunicarse con monitores o alumnos utilizando portales o sitios web educativos	16,4
Otras actividades de aprendizaje por Internet	22,5

de enseñanza a la hora de transmitir conocimientos. Así, durante los últimos años hemos podido observar cómo crecía de forma acelerada la presencia de los ordenadores en los centros de estudios. Si en el curso escolar 2002-2003 había, de promedio, un ordenador por cada 13,4 estudiantes, en el curso 2016-2017 encontrábamos un ordenador por cada tres alumnos en los centros de enseñanza no universitaria. Esta evolución se ha producido de forma algo más intensa en los colegios públicos que en los privados: en los primeros el ratio es de 2,8 alumnos por ordenador, y en los segundos, 3,6 alumnos. Un dato muy expresivo sobre el esfuerzo de la Administración en la dotación de medios modernos a los centros de enseñanza.

Además de ver aumentado su equipamiento material, los centros educativos también han experimentado durante los últimos años un crecimiento en su grado de integración en el entorno digital. Por ejemplo, la presencia de la tecnología wifi, que permite establecer conexiones inalámbricas entre dispositivos electrónicos, ha crecido en 18,7 puntos porcentuales en siete años, pasando del 71,8 por ciento del curso académico 2009-2010 al 90,5 por ciento en el curso 2016-2017. Cabe destacar además que la presencia que la tecnología wifi tiene en los centros educativos es parecida en los centros públicos y en los privados.

Otros aspectos del avance de las TIC en el ámbito de la educación pueden apreciarse en el elevado porcentaje (86,5 por ciento) de centros de enseñanza que disponen de una página web propia. Este tipo de páginas suelen usarse para publicar en Internet información referente al funcionamiento del centro o la realización de distintas actividades. Sin embargo, existen centros que no solo usan su página web como portal de información, sino que van más allá y la involucran en el propio proceso formativo, de manera que en la web se puede acceder a contenidos educativos tales como apuntes o ejercicios de prácticas usando un sistema de almacenamiento

Gráfico 21
Número medio de alumnos por ordenador destinado a tareas de enseñanza y aprendizaje (en enseñanzas no universitarias)

Fuente
Estadística de las enseñanzas no universitarias. Subdirección General de Estadística y Estudios del Ministerio de Educación y Formación Profesional

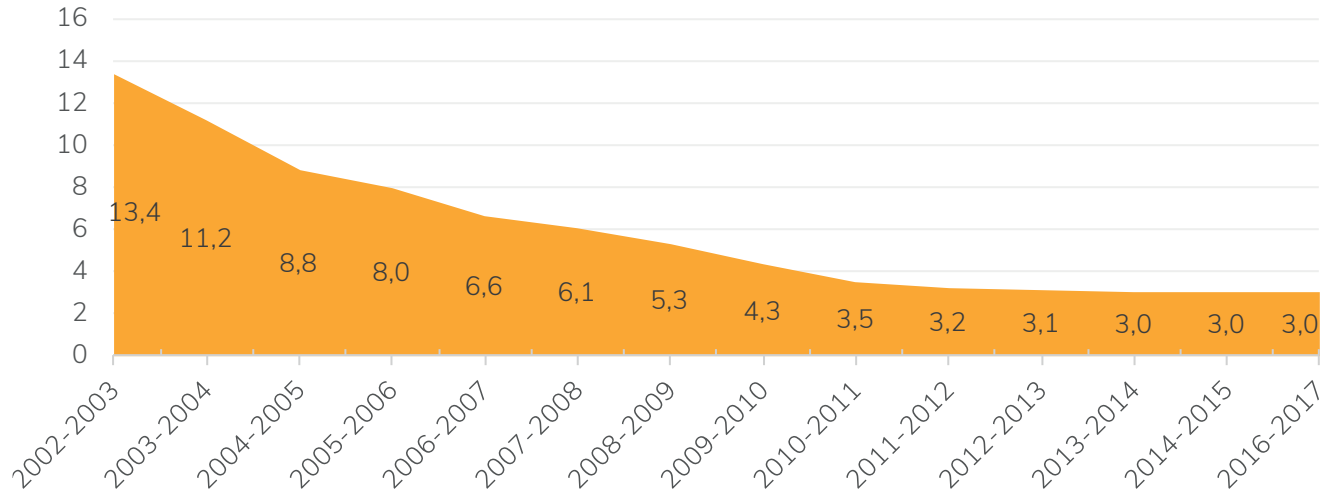
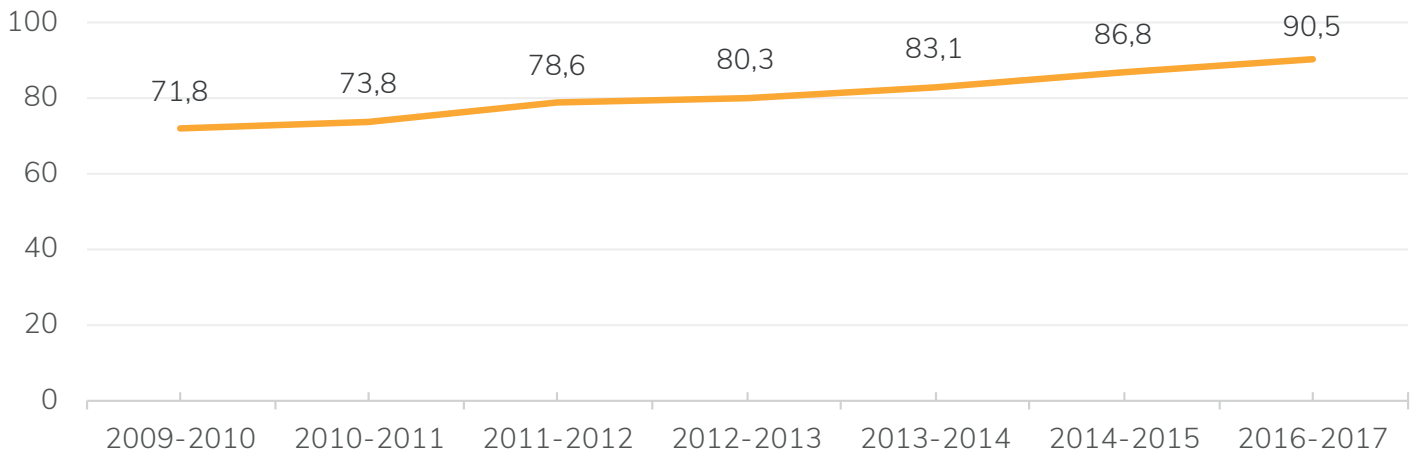


Gráfico 22
Porcentaje de centros con acceso a wifi (en enseñanzas no universitarias)

Fuente
Estadística de las enseñanzas no universitarias. Subdirección General de Estadística y Estudios del Ministerio de Educación y Formación Profesional



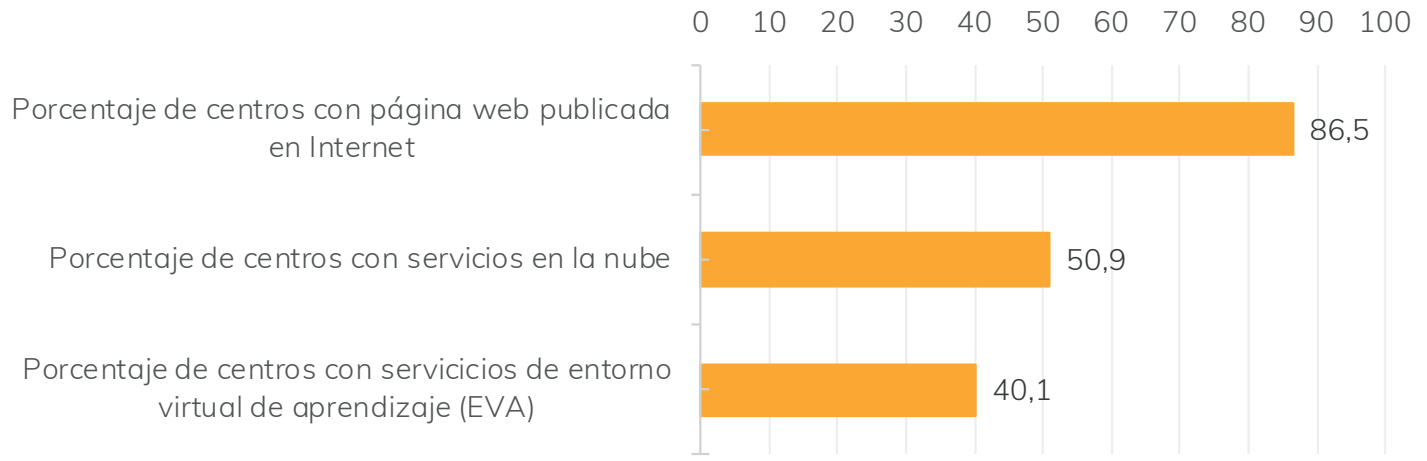
en la nube, tecnología con la que cuentan un 50,9 por ciento de los centros educativos en España. Además, algunos centros también disponen de un servicio de entorno virtual de aprendizaje (EVA), una aplicación informática diseñada para facilitar la interacción entre los participantes del proceso educativo. En los EVA los alumnos pueden comunicarse entre ellos y con los profesores, realizar trabajos en grupo y disponer de información sobre la evolución de determinadas asignaturas, así como acceso a materiales y diversas actividades, un sistema que supone toda una revolución en cuanto a la forma de organizar la enseñanza. Según los datos del INE, el porcentaje de centros de enseñanza no universitaria que disponen de entorno virtual de aprendizaje es del 40,1 por ciento.

VI. Ocio

Como país de clima en general cálido durante muchos meses, sumado al temperamento nacional, España es un país muy inclinado al ocio. Y ese es otro de los aspectos en el que la vida de los españoles se ha transformado radicalmente durante los últimos 25 años. La llegada de las tecnologías de la comunicación ha supuesto para el ciudadano el acceso a diversos contenidos de entretenimiento que anteriormente no estaban disponibles, o bien eran muy difíciles de encontrar y adquirir. Esta mayor capacidad de acceso al ocio ha sido, y continúa siendo, objeto de numerosas polémicas relacionadas con la piratería y el coste que esta ha supuesto para la industria del entretenimiento y de los creadores de contenido. No en balde, la música, el

Gráfico 23
Porcentaje de centros con página web publicada en Internet y con servicios de entorno virtual de aprendizaje (EVA)

Fuente
Estadística de las enseñanzas no universitarias. Subdirección General de Estadística y Estudios del Ministerio de Educación y Formación Profesional



cine, las series de televisión tienen detrás compositores, guionistas, etcétera, que han visto mermados sus ingresos a causa de prácticas que no pocas veces reclaman con pretensión de impunidad "cultura gratis". Una cuestión delicada, y muy peligrosa: sin creadores no habría cultura.

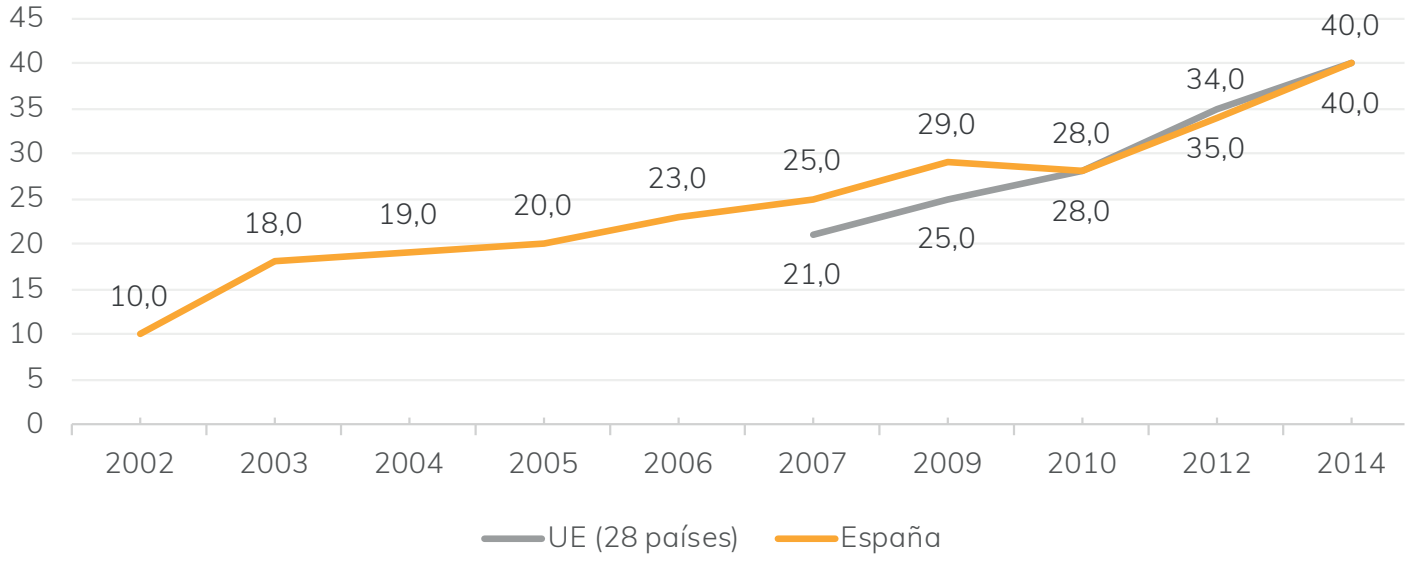
1. Descargas y 'streaming'

El surgimiento de este tipo de debates, tan intensos y de una forma tan repentina, da cuenta del enorme crecimiento que han tenido las descargas de contenidos de entretenimiento en nuestro país. Los datos lo muestran claramente: en el año 2002 un 10 por ciento de los españoles usaba Internet para jugar o descargar juegos, imágenes, películas o música. Tres años después, en 2005, esta cifra se había duplicado, y en 2014 ya eran un 40 por ciento los que realizaban este tipo de acciones en la red de forma habitual.

En el gráfico anterior podemos observar los datos relacionados con el fenómeno de las descargas en España y en la Unión Europea en su conjunto. Ahora bien, cabe preguntarse qué parte de este gran volumen de descargas corresponde a la adquisición de contenido de forma gratuita y qué parte corresponde al contenido de pago. En la siguiente tabla, obtenida del estudio anual Mikroscopia, de MyWord, podemos apreciar que un 48,5 por ciento de las personas entre 18 y 65 años había accedido a Internet para descargar música, películas, series o videojuegos de forma gratuita. En

Gráfico 24
Porcentaje de personas de 16 a 74 años que usan Internet para jugar o descargar juegos, fotografías, películas o música

Fuente
Eurostat



contraste, quienes habían accedido a la red para obtener este mismo tipo de contenido, pero pagando por él, representaban tan solo un 14,7 por ciento. Además, los datos también muestran que un 46,8 por ciento de estas personas había accedido a Internet para consumir contenido en streaming de forma gratuita, es decir, sin necesidad de descargar el contenido a un disco duro físico. Como contrapunto a este dato, encontramos que aquellos que accedieron a Internet para consumir contenidos en streaming pagando por ello eran tan solo un 16 por ciento, lo que representa una diferencia de 30,8 puntos porcentuales.

Sin embargo, a pesar de las grandes diferencias entre el consumo de contenido gratuito y de pago, parece que durante los últimos años existe un estancamiento en el número de personas que descargan o visualizan contenido a través de streaming de forma gratuita. Por el contrario, el consumo de contenidos de pago parece estar sufriendo un repunte en nuestro país. Esta tendencia puede ser debida al incremento que está viviendo en los últimos años el número de abonados a la televisión de pago.

2. Televisión por Internet

El fenómeno de la televisión de pago no es nuevo en España. Está instalado en nuestro país desde principios de los años 90 del siglo anterior, pero durante los últimos tiempos parece estar viviendo una edad dorada, posiblemente gracias a la llegada de nuevas plataformas de televisión por protocolo de Internet

Tabla 3
Usos de Internet (2014-2017)

Fuente
Estudio Mikroscopia, MyWord

Indica, por favor, si en el último año has utilizado habitualmente Internet para realizar las siguientes actividades. Marca todas las respuestas necesarias.	2014 (%)	2015 (%)	2016 (%)	2017 (%)	Diferencia 2014-2017
Descargar música, películas, series o vídeos de forma gratuita	51,9	50,9	51,3	48,5	-3,4
Descargar música, películas, series o vídeos de pago	11,9	13,5	12,3	14,7	2,8
Consumir contenidos (música, películas, series, programas, etc.) en *streaming* (sin descarga) de forma gratuita	-	-	46,1	46,8	(2016) 0,7
Consumir contenidos (música, películas, series, programas, etc.) en *streaming* (sin descarga) de pago	-	-	11,9	16,0	(2016) 4,1

(IPTV) extranjeras, tales como Netflix o HBO, que han despertado el interés del consumidor nacional. Si observamos los datos de número de abonados a la televisión de pago podemos ver como a principios del año 2005 había en España poco más de tres millones de personas suscritas a alguna plataforma de televisión de pago. Seis años después, a comienzos de 2011, se llegaría a un pico de poco más de cinco millones de personas abonadas, que fue descendiendo hacia 3,8 millones de suscriptores a mediados del año 2013. A partir de esta fecha, se produce un gran crecimiento de abonados, gracias principalmente al incremento en las suscripciones a servicios IPTV. Dichos servicios cuentan actualmente con cuatro millones de personas suscritas, lo que representa más de la mitad del total de los abonados (no llegan a siete millones) a servicios de televisión de pago en España.

El incremento en el número de abonados a la televisión de pago sin duda está relacionado con una pujanza en la visualización de contenidos audiovisuales online. Desde hace varios años, la facilidad para consumir estos contenidos está haciendo que cada vez un mayor número de ciudadanos accedan a ellos de

Gráfico 25
Número de abonados de televisión de pago por medio de transmisión

Fuente
Comisión Nacional de los Mercados y la Competencia

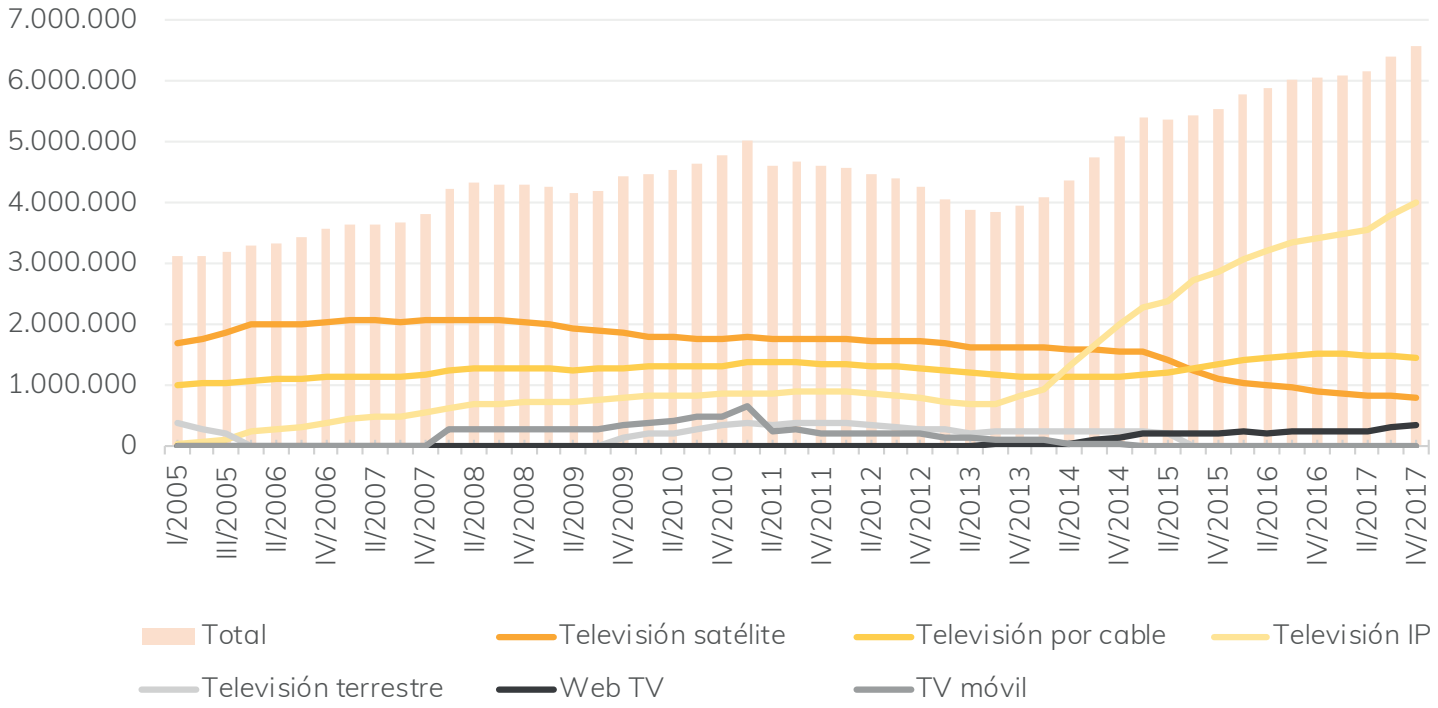
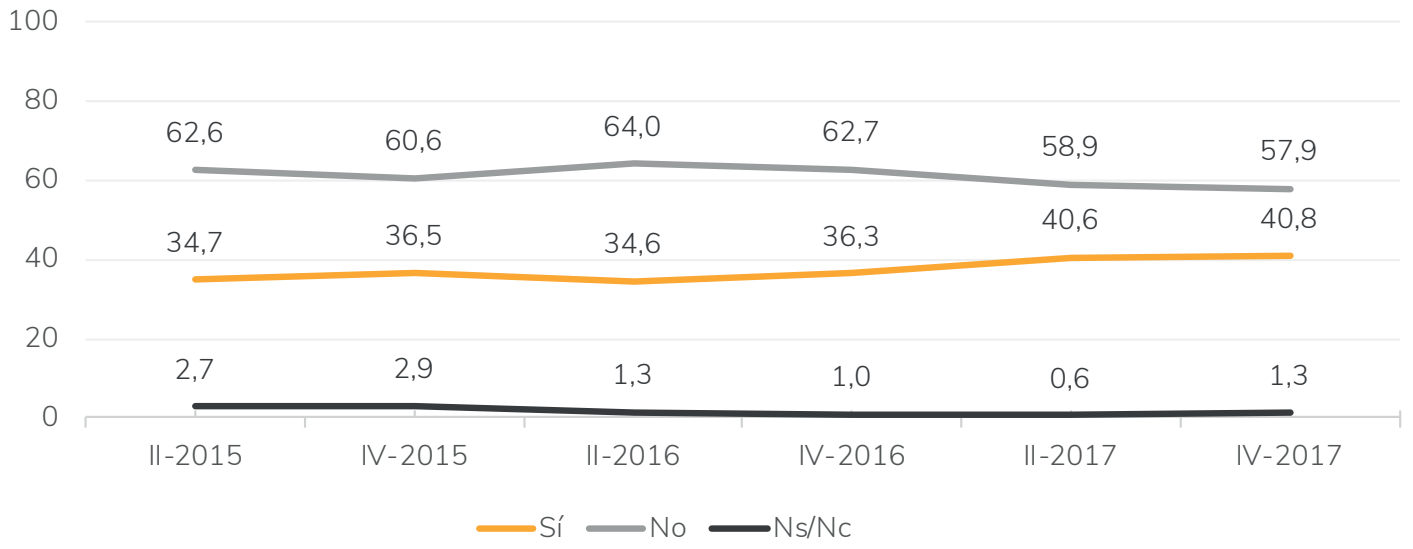


Gráfico 26
Porcentaje de consumo de contenidos audiovisuales online al menos una vez a la semana

Fuente
Comisión Nacional de los Mercados y la Competencia (CNMC)



forma recurrente. Así lo podemos apreciar en el gráfico siguiente: a mediados de 2015, un 34,7 por ciento consumía contenidos audiovisuales de forma online al menos una vez a la semana. Tan solo dos años después, esta cifra llegaba al 40,8 por ciento, lo que supone un incremento de 6,1 puntos porcentuales, un incremento verdaderamente notable.

Tras haber analizado cuánto contenido audiovisual online consumen los ciudadanos españoles, lo siguiente sería preguntarse a qué soporte recurren para ver dichos vídeos. En este punto, se destaca claramente del resto Movistar+. Esta plataforma de contenidos, propiedad del grupo Telefónica, surge de la fusión de Canal+, propiedad del grupo PRISA hasta 2015, con Movistar TV. A mediados del año 2016, Movistar+ estaba presente en un 7,8 por ciento de los hogares españoles con acceso a Internet, y por aquellas fechas ya era la plataforma audiovisual online líder en nuestro país, con una distancia de 6 puntos por delante de su competidora más inmediata, la estadounidense Netflix.

Además, el gran incremento en la popularidad de este tipo de plataformas motivó que Movistar+ pasara, en poco más de un año, a estar presente en un 13,5 por ciento de los hogares de nuestro país, y continuar siendo la plataforma de pago con más suscriptores. Sin embargo, en el mismo intervalo de tiempo, su principal competidor, Netflix, obtuvo un incremento de suscriptores superior, pasando de estar presente en

un 1,8 por ciento de los hogares en 2016 a un 9,1 por ciento a finales de 2017, lo que representa una subida de 7,3 puntos porcentuales.

En tercer lugar de esta clasificación encontramos otra empresa de telefonía, Vodafone, con su plataforma de televisión de pago Vodafone TV Online. Según los datos de la Comisión Nacional de los Mercados y la Competencia, esta plataforma es utilizada por un 5,9 por ciento de los hogares con acceso a Internet para visualizar contenidos online. Tras Vodafone TV, se sitúan Amazon Prime Video, App Orange TV y HBO, con presencia en un 3,5, 2,8 y 2,3 por ciento de los hogares, respectivamente.

3. Videojuegos

El sector de los videojuegos también ha sufrido una transformación muy profunda durante los últimos 25 años. Este cambio ha tenido principalmente su origen en los avances tecnológicos que permitían dotar a las plataformas de videojuegos de una mayor capacidad técnica y en la posibilidad de poder interactuar de modo online con otros jugadores.

Los avances tecnológicos, tanto de hardware como de conectividad, han supuesto una expansión del número de jugadores que usan juegos en red. Según los datos del estudio Mikroscopia, de MyWord, en 2017 un 27,7 por ciento de la población entre 18 y 65 años jugaba a videojuegos online de forma habitual y un 43,1 por ciento de forma ocasional. Con esta cantidad de jugadores, podemos sospechar que se trata de un fenómeno con un impacto considerable en la sociedad española. En este sentido, según los datos de la Asociación Española de Videojuegos, el sector de los videojuegos facturó 1.359 millones de euros en 2017, lo que la convirtió, un año más, en la primera opción de ocio audiovisual en España.

Tabla 4
Uso de plataformas de pago para ver contenidos audiovisuales online (porcentaje de hogares entre los hogares con acceso a Internet)

Fuente
Comisión Nacional de los Mercados y la Competencia (CNMC)

	Movistar+ en dispositivos / Yomvi	Netflix	Rakuten / Wuaki	Vodafone TV online	Amazon Prime Video	App Orange TV	HBO	beIN CONNECT / Total Channel	Filmin	Otras
II-2016	7,8	1,8	1,1	.	.	.	.	0,2	0,1	0,5
IV-2016	7,5	3,4	1,2	.	.	.	.	0,2	0,1	0,6
II-2017	12,6	7,3	0,8	.	1,1	.	2,6	1,2	0,1	0,9
IV-2017	13,5	9,1	1,0	5,9	3,5	2,8	2,3	0,8	.	0,3

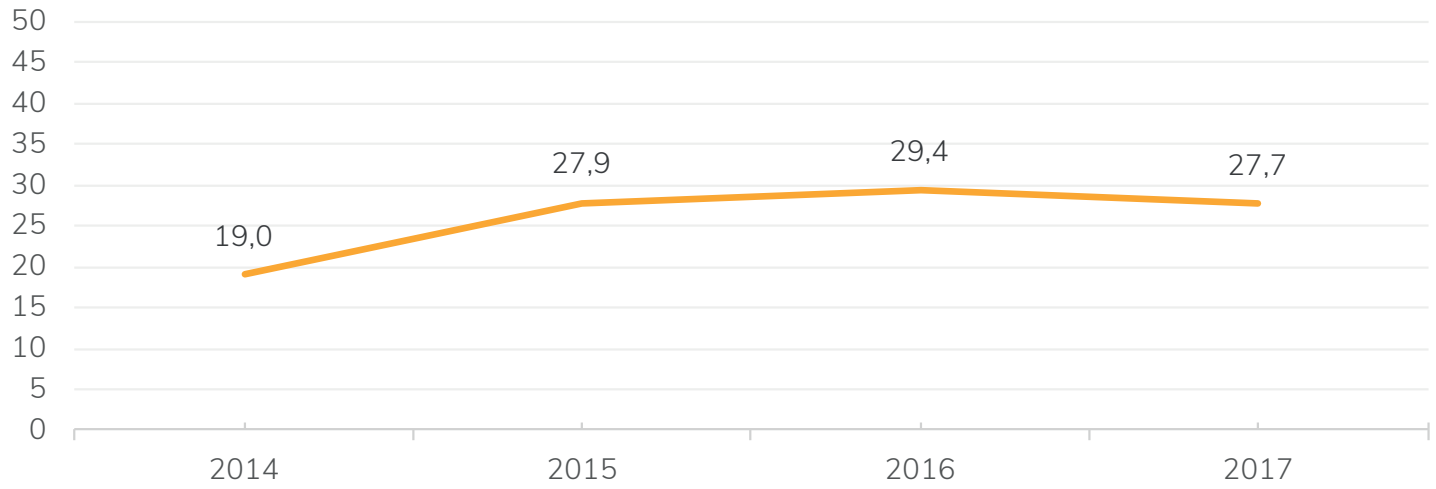
Además de este aumento en el uso de videojuegos, el perfil del jugador también va evolucionando poco a poco. Si allá por los años 90 del siglo anterior se consideraba como un ocio típicamente para el público masculino, hoy en día se está cerrando esta brecha entre ambos sexos. Actualmente, un 56 por ciento de los jugadores son hombres, y un 44 por ciento son mujeres. Sin embargo, si observamos el tiempo medio que se dedica a jugar, los jugadores ocupan un 64 por ciento de las horas de juego totales, mientras que las jugadoras tan solo representan el 36 por ciento del tiempo de juego total. Se impone una reflexión: ¿tiene que ver esa desigual dedicación a los videojuegos con el hecho de que todavía no ha avanzado lo suficiente el reparto de las tareas domésticas entre hombres y mujeres? Y esta otra: quizá las mujeres aprecian más matices y son más variadas en el reparto de su tiempo de ocio.

4. Relaciones sociales y de pareja

La llegada de las tecnologías de la información y comunicación en España también ha afectado a la forma en cómo nos relacionamos entre nosotros, incluso a la hora de establecer relaciones de pareja. Actualmente, y según los datos del estudio Mikroscopia, de MyWord, un 15,1 por ciento de las personas con pareja entre los 18 y los 65 años se ha conocido por Internet. Además, este es un dato bastante consolidado, con un crecimiento de 3,8 puntos porcentuales durante los últimos tres años.

Gráfico 27
Porcentaje de individuos entre 18 y 65 años que juegan habitualmente con la consola, el móvil o el ordenador

Fuente
Estudio Mikroscopia, MyWord



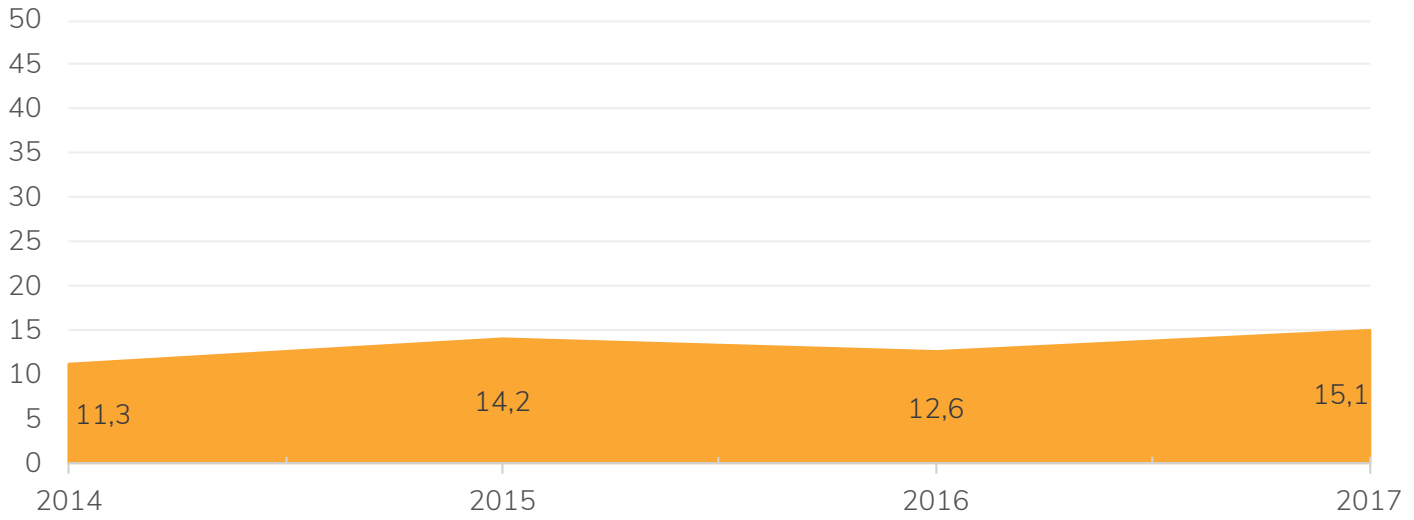
Si bien durante los primeros años del desarrollo de Internet en España ya empezaban a formarse las primeras parejas que se conocieron en la Red, lo cierto es que el número de parejas online ha crecido de forma considerable gracias a los portales web específicos para encontrar pareja, primero, y a la llegada de las dating apps, después. Siguiendo los datos del estudio Mikroscopia en su edición de 2017, observamos que entre las páginas web más populares en nuestro país para este fin estarían Badoo, donde un 3,4 por ciento de los españoles afirma tener cuenta y Meetic, usada por un 1,2 por ciento de la población. Por el lado de las dating apps, podemos encontrar Tinder, utilizada por cerca del 1,3 por ciento de la población española y Grindr, específica para el público homosexual y usada por un 0,7 por ciento de la población. Además, si analizamos estos datos por edad podemos observar cómo entre estas dos modalidades para encontrar pareja online, los portales web tienen un mayor éxito entre las personas que rondan los 30 años de edad, mientras que el público que más recurre a las dating apps son los que están alrededor de la veintena.

5. Hostelería

La buena salud de la que goza en España la hostelería tiene mucho que ver con dos factores: la costumbre y lo benigno del clima gran parte del año. Salir a comer, a cenar, o simplemente a tomar algo es una actividad frecuente, más si tenemos en cuenta la acreditada tradición gastronómica que existe en el país. Como cualquier otro sector, la hostelería ha experimentado cambios derivados de la revolución en las tecnologías de la información. Las novedades, relativamente recientes, se suceden de forma incesante y fundamentalmente tienen que ver con

Gráfico 28
Evolución de las parejas por Internet (sobre el porcentaje de personas con pareja entre 18 y 65 años)

Fuente
Estudio Mikroscopia, MyWord



la forma de relacionarse del cliente con el restaurante y con los pedidos de comida a domicilio.

Respecto a la primera cuestión, la relación del cliente con el restaurante, se ha producido una interesante evolución en lo que se refiere al intervalo de tiempo que media antes de que podamos degustar nuestra comida. Antes, a la hora de elegir un restaurante, teníamos varias alternativas, obvias: ir a uno que ya conocíamos, ir a uno que nos habían recomendado o probar alguno nuevo. Hoy, sin que hayan variado esas posibilidades, podemos ampliar la fórmula para ponerlas en práctica: es posible consultar en Internet la carta del restaurante, su ubicación e, incluso, ver los comentarios que los comensales han realizado sobre él, de forma que tenemos mucha más información a la hora de elegir a qué restaurante podemos ir.

Además, antes de ir al restaurante, era recomendable realizar una reserva, que se podía hacer vía telefónica, pero ello exigía que el restaurante se encontrara abierto en la hora que llamásemos. Hoy existen aplicaciones para poder efectuar reservas de forma automática, sin necesidad de tener en cuenta el horario de apertura del restaurante.

La otra gran transformación que está viviendo el sector actualmente tiene que ver con los pedidos a domicilio. Si en el año 1993 un ciudadano quería pedir comida para consumirla en su casa, debía llamar por teléfono al restaurante en cuestión y, si este ofrecía el servicio de reparto, hacer su pedido. Hoy en día han surgido distintas páginas web y aplicaciones que nos permiten pedir comida a domicilio sin necesidad de realizar una llamada telefónica. Pero, además de esto, algunas de estas aplicaciones cuentan con sus propios repartidores, con lo que no es necesario que el restaurante ofrezca este servicio, porque serán los repartidores de la aplicación los que entregarán la comida a domicilio, lo que amplía el número de restaurantes que pueden ofrecer este servicio. Los repartos se efectúan en todo tipo de vehículos: coches, motos y ese silencioso ejército de ciclistas que transportan a su espalda sabrosos menús en una caja cúbica.

Los datos del sector del encargo de comida a domicilio vía online son espectaculares si tenemos en cuenta su reciente desarrollo. Según la consultora McKinsey & Company, en 2011 las aplicaciones de comida a domicilio online tenían una cuota de mercado del 8 por ciento, mientras que en el año 2016 este porcentaje pasó al 30 por ciento. Según esta misma consultora, se espera que la cuota de mercado de estas empresas pueda llegar al 58 por ciento en el año 2020. En lo que respecta a España, actualmente se calcula que estas aplicaciones generan entre 500 y 600 millones de euros al año, una cantidad muy impactante si tenemos en cuenta su reciente llegada a nuestro país.

VII. Otros servicios

Podemos afirmar que la informatización gobierna el mundo. Gracias a los avances en el manejo y la digitalización de grandes bases de datos, la evolución de las infraestructuras como la red de cajeros automáticos y agencias de atención al público, y la integración de los servicios en plataformas de Internet, las TIC también han cambiado el modo en el que el ciudadano accede a los servicios públicos y financieros.

1. Banca

Durante la última década el número de usuarios que usa Internet para acceder a los servicios bancarios ha

aumentado de manera constante. Hoy en día casi la mitad de los españoles se ha conectado a sus bancos a través de Internet. Nuevamente, se observan diferencias entre las generaciones mayores (de 55 años en adelante) y el resto de la población. Asimismo, los núcleos más habitados recurren a la banca electrónica en mayor proporción que las poblaciones de menor demografía. Con respecto a los demás países de Europa, el uso de la banca online en España es menos común que la media.

Como consecuencia del incremento en la banca online, la cantidad de oficinas ha disminuido considerablemente. Basta una visita a una oficina bancaria para ver grandes cambios respecto a unas décadas atrás: los empleados, ante numerosos, van menguando; cada vez más trámites se efectúan en los cajeros si es que no se habían resuelto en casa gracias al smartphone o el ordenador personal. Hoy en día existe el mismo número de oficinas que en 1982. El camino hacia una nueva realidad bancaria está trazado.

2. Administración pública

La manera en la que el ciudadano se relaciona con la Administración Pública también ha sufrido importantes cambios. Gracias a Internet, una gran cantidad de asuntos y servicios pueden tramitarse sin necesidad de desplazamiento a una oficina pública. Por tanto, la cantidad de personas que recurre a Internet para realizarlos aumenta conforme a la comodidad y facilidad que las nuevas tecnologías suponen.

Gráfico 29
Personas de personas entre 16 y 74 años que usan Internet para acceder a servicios bancarios

Fuente
Eurostat

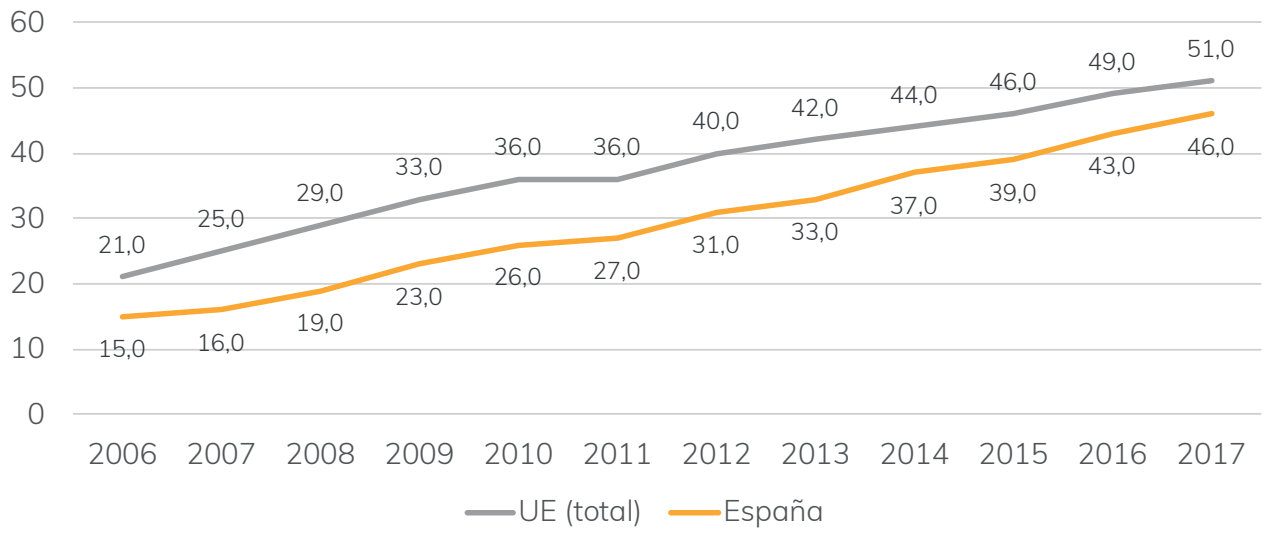
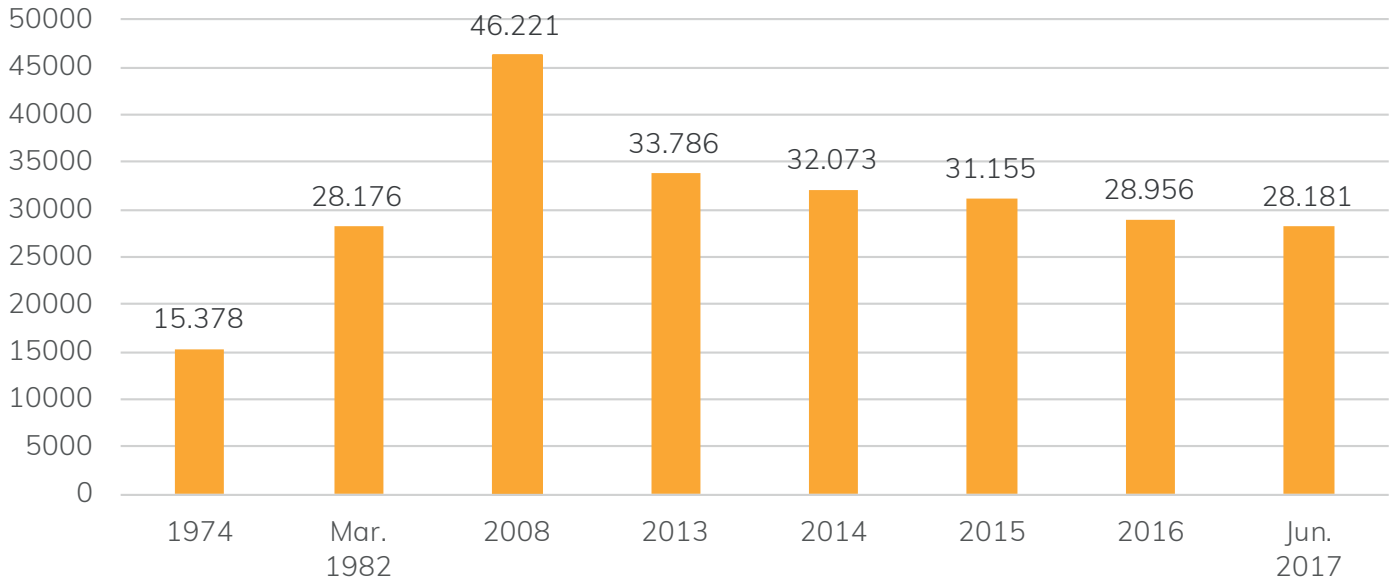


Gráfico 30
Evolución de la red de sucursales. Número de oficinas

Fuente
Banco de España



Según la Encuesta de equipamiento y uso de tecnologías de 2017 (INE), si en 2006 el 48,8 por ciento de la población obtenía información a través de las páginas web de la Administración Pública, hoy en día la cifra alcanza el 54,9 por ciento. Además, la cantidad de personas que ha descargado formularios oficiales ha subido del 28 al 42,8 por ciento en el mismo período de tiempo. Por último, en 2017 el 49 por ciento ha enviado los formularios cumplimentados a través de Internet, mientras que en 2006 tan solo el 14,3 por ciento hacía lo propio.

VIII. Medios de comunicación

Los medios de comunicación de masas no han sido inmunes al avance de las TIC durante los últimos años. Por el contrario, Internet ha multiplicado la oferta de contenidos y portales de acceso a la información. Medios convencionales como la televisión, la radio y la prensa han tenido que adaptar sus estructuras y modelos de negocio para conectar con sus audiencias, ofreciendo nuevas maneras de comunicar sus contenidos. A la vez, las TIC han brindado a nuevos actores y plataformas la capacidad de difusión masiva de contenidos. Entre otras cosas, esto ha significado un cambio drástico en los patrones de producción y consumo de contenidos audiovisuales. En este contexto, las audiencias cambian la manera de acceder a los medios. A continuación, pormenorizamos algunos indicadores de uso y acceso a medios de comunicación.

1. Prensa

Seguramente el medio que más ha sufrido como resultado de la llegada de Internet es la prensa de papel. Con la proliferación de medios de comunicación digitales, la cantidad de individuos que usa Internet para leer noticias ha aumentado considerablemente. Si hace once años menos de un cuarto de la población había visitado un portal de noticias, hoy en día la proporción ha aumentado a dos de cada tres españoles.

De hecho, según la Encuesta de 2017 de la Asociación para la Investigación de Medios de Comunicación (AIMC) a usuarios de Internet, la Red es la forma dominante de acceder a la prensa entre los internautas, mientras que solo un 8 por ciento lo hace exclusivamente en papel.

Nuevamente, según la Encuesta de equipamiento y uso de tecnologías del INE en 2017, se mantienen las diferencias demográficas de rigor: las generaciones más jóvenes son más propensas a usar Internet para leer las noticias, mientras que las mayores lo hacen con menos frecuencia. De igual manera, la población extranjera se conecta en menor medida para acceder a las noticias que la población española.

A pesar de las diferencias entre los segmentos de la población española, la tendencia global es determinante: cada día Internet se sitúa como principal fuente de acceso a los contenidos de noticias. Como consecuencia, la inversión publicitaria en la prensa de papel ha decrecido de manera drástica. De hecho, de continuar esta tendencia, la inversión publicitaria en Internet superará la de papel en los próximos años.

Gráfico 31
Porcentajes de las personas entre 16 y 74 años que han usado Internet para descargar o leer periódicos o revistas de noticias online en los últimos tres meses

Fuente
OCDE

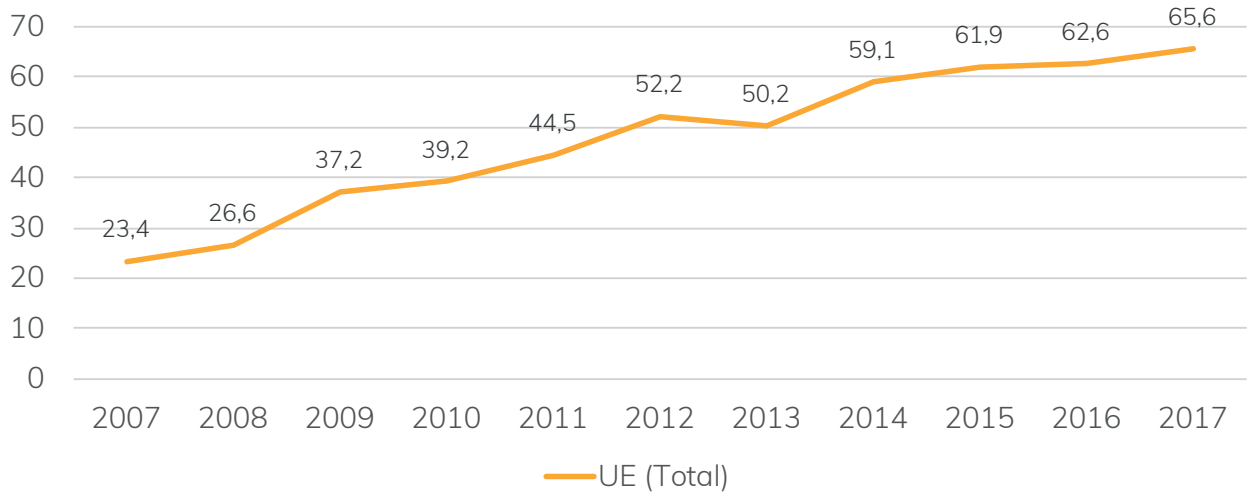
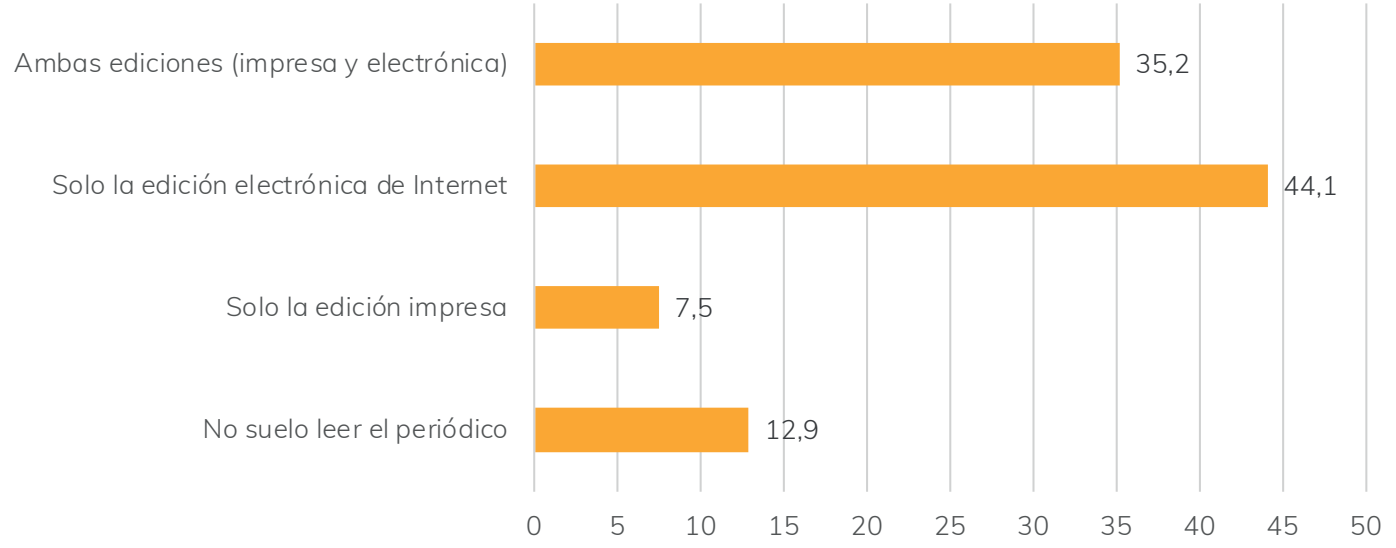


Gráfico 32
Forma habitual de lectura de prensa

Fuente
Encuesta AIMC a usuarios de Internet 2017



Por tanto, podemos pronosticar que los cambios en los patrones de uso de medios de noticia seguirán profundizándose.

2. Radio y televisión

Si la prensa ha sufrido cambios en la manera de ofrecer contenidos a sus audiencias, también la radio ha tenido que adaptarse a la llegada de Internet. Según la Encuesta de 2017 de la AIMC, casi un 60 por ciento de los internautas ha escuchado la radio por Internet en el último año. Otro 27 por ciento responde haber hecho lo mismo, pero no tan recientemente.

De igual manera, la televisión deja de ser vista a través de los equipos convencionales para trasladarse a Internet. En 2017, más de un tercio de la población internauta responde haber visto televisión por Internet, lo que significa un aumento de más de 3 puntos porcentuales con respecto a 2016. Tan solo el 12 por ciento de la población conectada afirma no haber visto nunca televisión por Internet.

No solo se ve más televisión por Internet, sino también a través de una variedad de dispositivos. El ordenador portátil es el dominante, pero el teléfono móvil y la smart TV aumentan su penetración con respecto al año pasado.

Gráfico 33
Inversión publicitaria en prensa de papel y digital (cifras en millones de euros)

Fuente
Índice de inversión publicitaria de Media Hotline y Arce Media

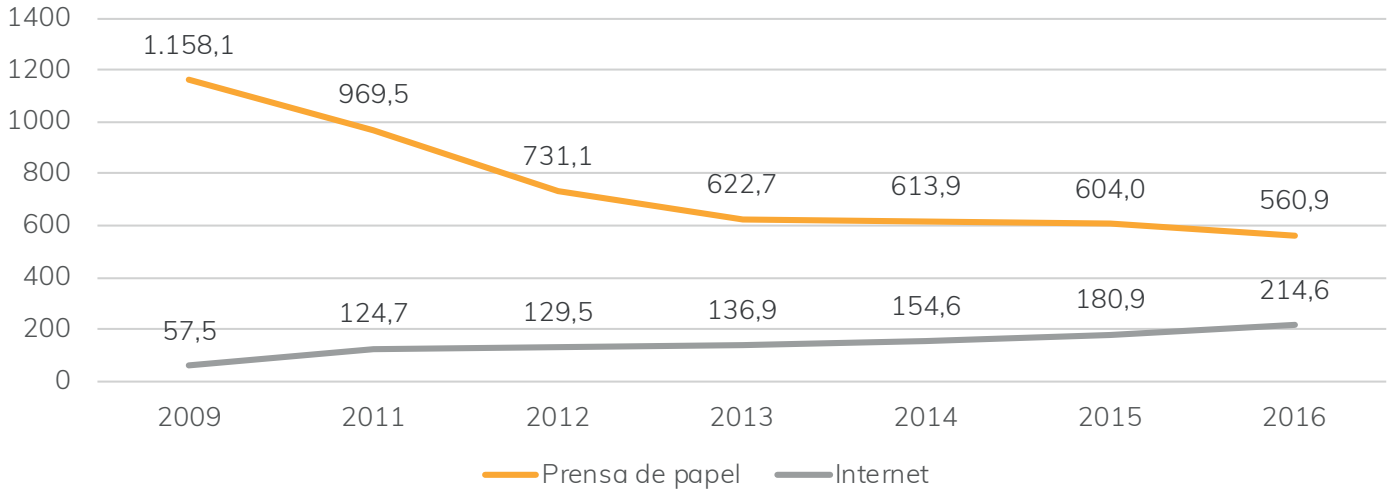


Gráfico 34
Escucha de radio por Internet

Fuente
Encuesta AIMC a usuarios de Internet en 2017

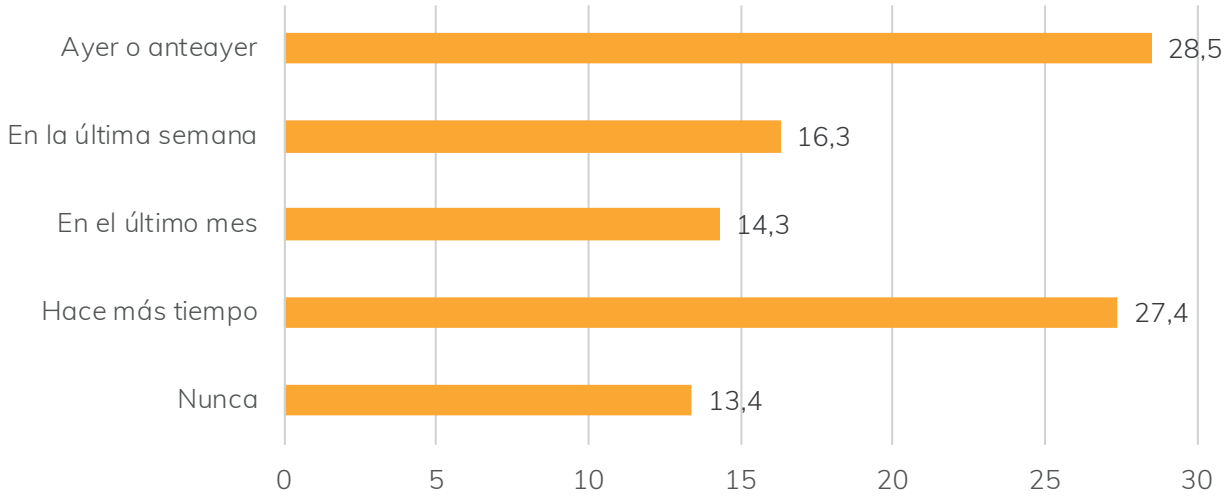


Gráfico 35
Visionado de televisión por Internet

Fuente
Encuesta AIMC a usuarios de Internet en 2017

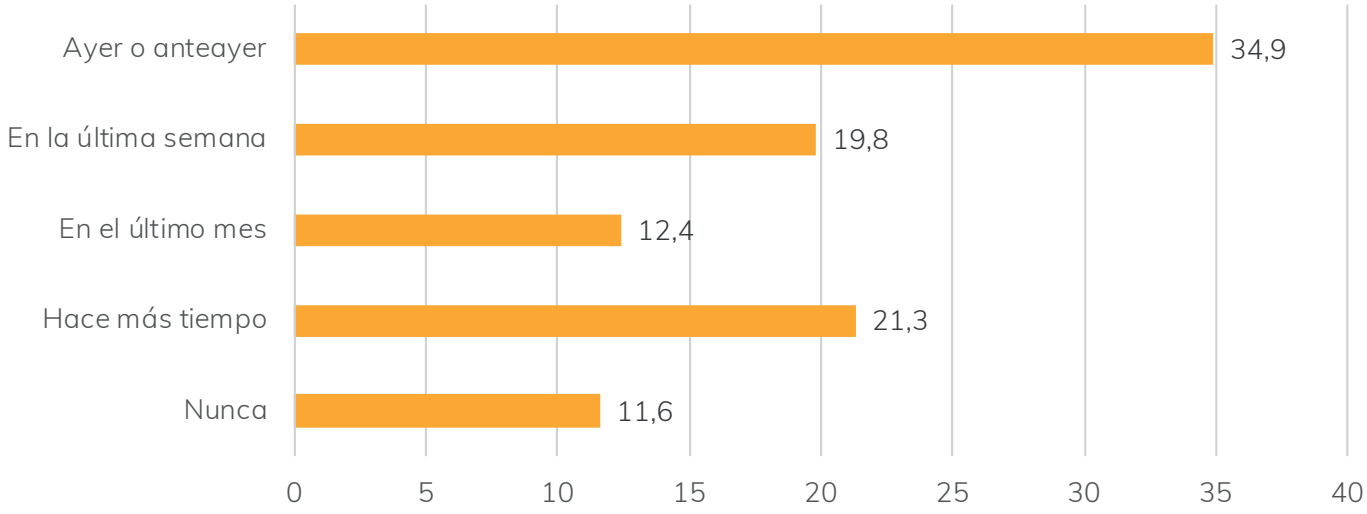
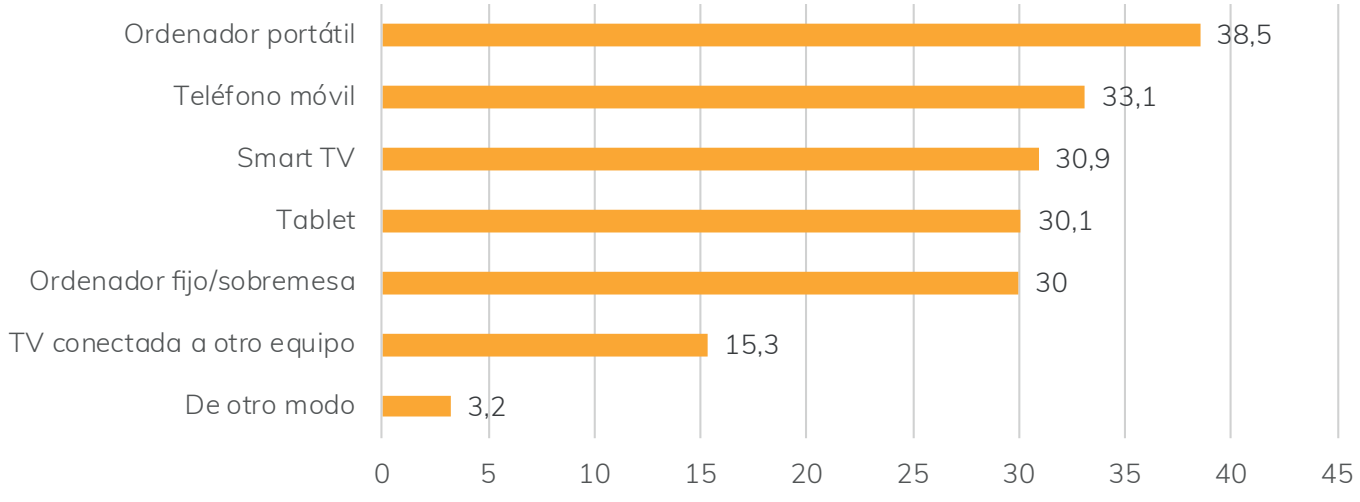


Gráfico 36
Equipos por los que se ha visto televisión por Internet (últimos 30 días)

Fuente
Encuesta AIMC a usuarios de Internet en 2017



IX. Conclusión

Las últimas décadas han aportado cambios importantes en la manera en que el ciudadano común hace uso de las nuevas tecnologías de información y comunicación. Son pocas las áreas del quehacer cotidiano que se escapan de los avances de la tecnología y cada día son más los que hacen uso de nuevos servicios y dispositivos tecnológicos. En gran medida, España sigue tendencias globales y regionales, aunque no todos los segmentos de la población han asumido los cambios de manera uniforme. En ese sentido, resalta la superior penetración tecnológica que registran los núcleos urbanos densamente poblados respecto a las localidades menos habitadas. E igualmente, hay que poner de relieve la masiva incorporación a las nuevas tecnologías de las franjas de edades más jóvenes, que dista de los mayores.

Si el comportamiento y la manera de usar las nuevas tecnologías han cambiado de manera tan drástica durante los últimos 25 años, queda pendiente saber cómo han cambiado las actitudes de los españoles ante los avances de la tecnología. El siguiente capítulo analizará las opiniones de los españoles ante estos avances y, en particular, sus expectativas y preocupaciones en torno a la innovación científica, la protección de los datos y la privacidad, el ciberfraude y los cambios en el mercado laboral, entre otros.

2

Actitudes frente a la transformación tecnológica. Oportunidades y retos

I. Introducción

Como hemos podido constatar en el capítulo anterior, uno de los rasgos distintivos de las últimas décadas es el rápido avance de la tecnología, lo que ha llevado a considerar nuestro tiempo como la era de la revolución científica y tecnológica. Dado el gigantesco desarrollo de la robótica y la ciberfísica, muchos científicos y economistas incluso anuncian la llegada de la cuarta revolución industrial. Lo cierto es que la observación cotidiana revela que el mercado de las telecomunicaciones ya dejó de ser una extensión de tecnología originalmente militar adaptada al consumidor, como los primeros GPS (Global Positioning System), para transformarse en una parte habitual del día a día del ciudadano común. Desde operaciones bancarias, pasando por compras en línea y redes sociales, hasta realidades virtuales destinadas al ocio de niños y adultos, la constante evolución de la tecnología forma parte de nuestra identidad individual y colectiva. Es inconcebible no tener en cuenta este factor: a poco integrado que se esté en el mundo actual, una gran cantidad de asuntos y actividades pasa por interactuar desde un ordenador o un teléfono móvil.

El panorama se vuelve más complejo si consideramos que esta transformación, que crece de modo exponencial, influye de forma diferente en la vida de los miembros de las distintas generaciones que convivimos en este momento histórico. En unos pocos años se han producido cambios trascendentales en las nociones de información, aprendizaje, conocimiento y comunicación. Pero todo ello es mejor absorbido por las franjas de edad más jóvenes. Y todavía encuentra más facilidades para implantarse en los núcleos urbanos más poblados. Pero a estas alturas ya no hay alternativa: los sistemas políticos, económicos y sociales se ven obligados a adaptarse y a transformarse para sobrevivir. Los individuos y las comunidades se ven en la necesidad de reinventar su entorno, sus necesidades, oportunidades, expectativas y herramientas para asegurar su bienestar y su progreso en esta nueva era.

En este capítulo se abordan las actitudes individuales hacia distintos aspectos que forman parte del constante desarrollo tecnológico, haciendo especial énfasis en el asunto de la seguridad de los datos personales y el intercambio de información entre plataformas. También se evalúan las actitudes en lo que se refiere al acceso a Internet para menores de edad, distintas formas de llegar a los contenidos digitales y lo que significa el avance de las TIC para el futuro del mercado laboral.

II. Desarrollo de la comunicación y la información a través de Internet

Según la Real Academia Española (RAE), Internet se define como una "red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación". Entendemos, pues, que diversas redes individuales forman un todo homogéneo que nos conecta como mundo. Y a través de los canales de esta plataforma tecnológica consumimos, producimos, comunicamos y compartimos contenidos digitales.
Como dijimos en el capítulo anterior, existen muchas plataformas y dispositivos desde donde manejamos personalmente los contenidos digitales de nuestra preferencia. Por la naturaleza de la Red, las divisiones entre las áreas laborales, recreativas y sociales en el escenario digital se vuelven cada vez más permeables. Por ello, no resulta extraño compartir en las redes sociales experiencias de trabajo, a través de una conversación

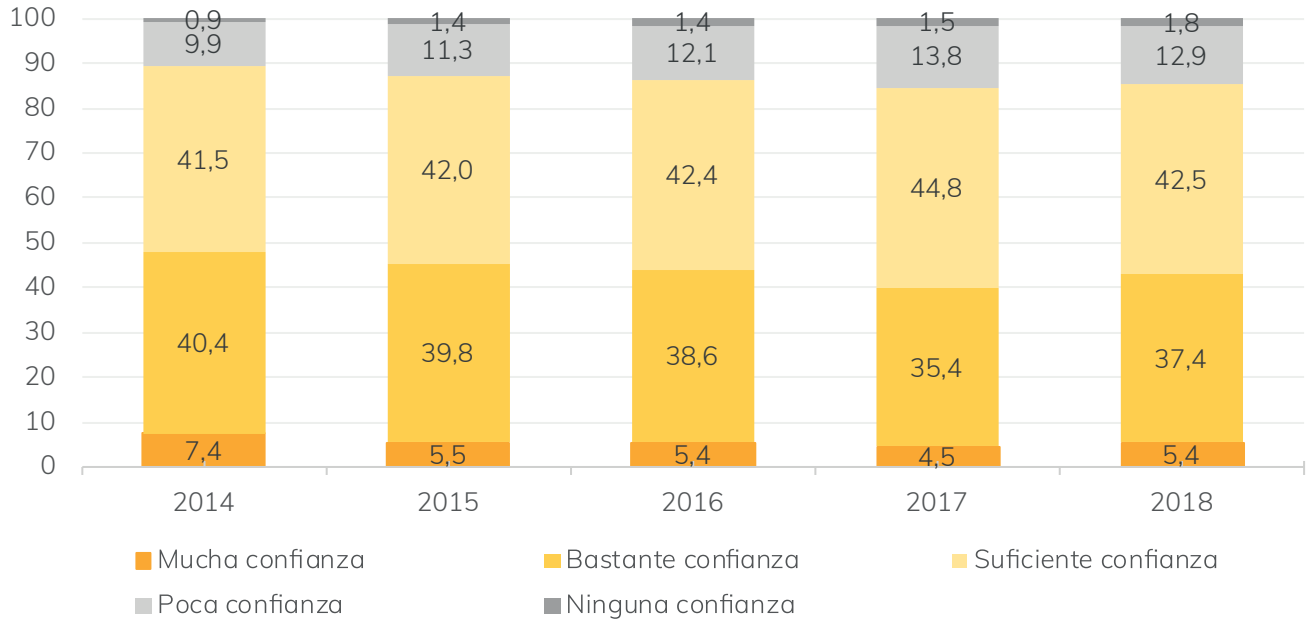
entretenida en la que se intercambian, por ejemplo, fuentes y conocimientos profesionales. Además, los dispositivos son cada vez más eficientes, más rápidos y están mejor conectados. Esto hace que cualquier persona pueda compartir documentos audiovisuales en tiempo real. Ya no somos meros espectadores de lo que predican y presentan los expertos. Ahora participamos y creamos contenidos como actores principales a través de las TIC.

1. Confianza y actitudes hacia el uso de Internet

Con el estado de cosas descrito, se hace necesario un estudio orientativo de la situación: es interesante conocer qué piensan los usuarios de la Red. El Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) publicó en 2017 un estudio en el que se analizan las actitudes hacia Internet y los contenidos digitales. Y los resultados son alentadores, pues durante los últimos años se ha mantenido una tendencia positiva, sostenida, en la que la mayoría de los consumidores sienten mucha, bastante o suficiente confianza en Internet. Solo el 15,3 por ciento de los usuarios manifiestan sentir poca o ninguna confianza hacia la Red.

Gráfico 1
Nivel de confianza en internet (%

Fuente
Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), 2014, 2015, 2016, 2017, 2018



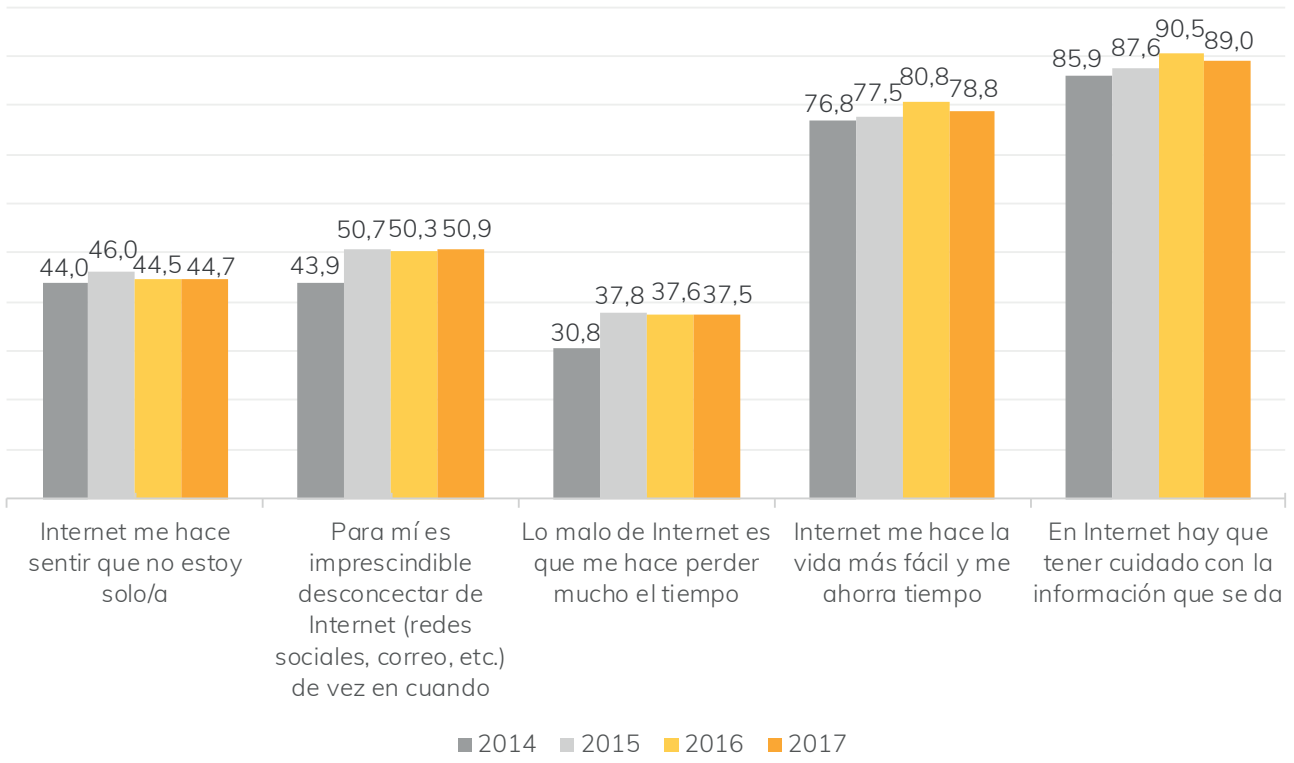
No obstante, el informe plantea que, aparte de la confianza hacia los beneficios del desarrollo de la comunicación y la información a través de Internet, también surgen actitudes críticas y cuestionamientos con respecto a su uso, el acceso a los contenidos digitales y su impacto en distintos ámbitos.

Más de un 75 por ciento de la población siente que Internet les hace la vida más fácil y les ahorra tiempo, aunque una proporción aún mayor, de cerca del 90 por ciento, afirma que hay que ser cuidadoso con la información que se da, asunto en el que profundizaremos más adelante. La percepción sobre el bienestar que proporciona Internet comparándolo con las preocupaciones que derivan de involucrarse demasiado en la Red contiene las dos caras de la misma moneda.

Por ejemplo, la mitad de los españoles expresan que les resulta imprescindible desconectarse de Internet de vez en cuando, mientras que casi la misma proporción de los usuarios manifiestan que estar conectados les hace sentir que no están solos.

Gráfico 2
¿En qué medida te identificas con cada una de las siguientes afirmaciones? (% de personas que responden "mucho" y "bastante")

Fuente
Fuente: Estudio Mikroscopia. MyWord



2. Uso y acceso a contenidos digitales

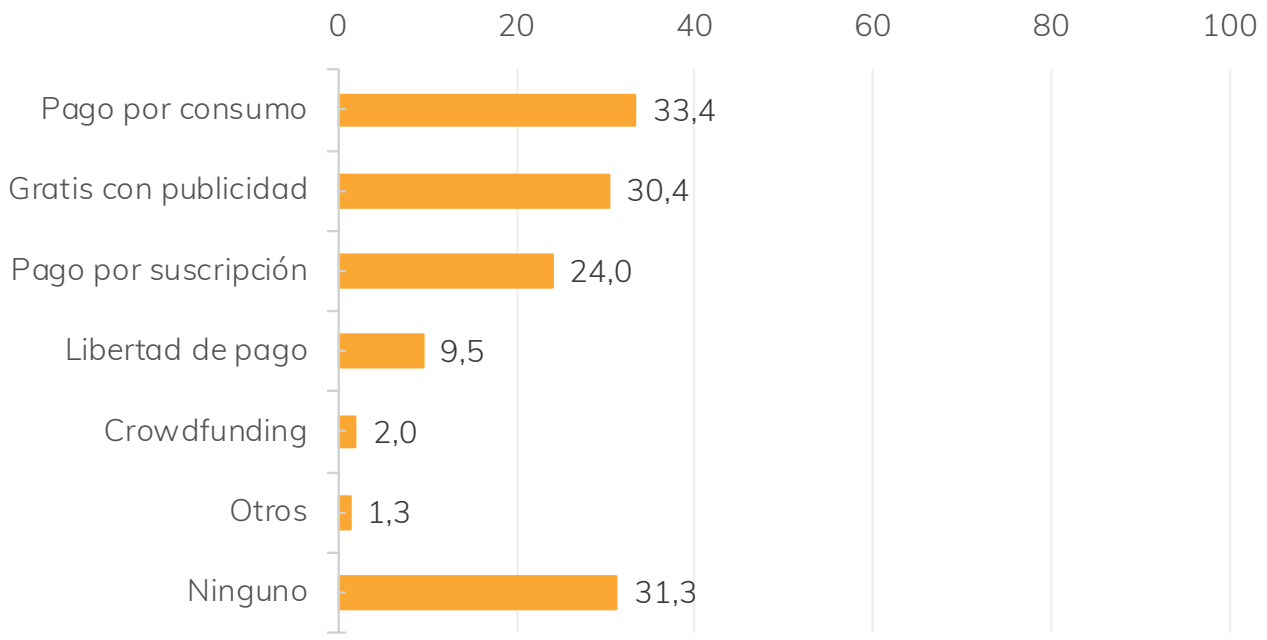
Existen distintas formas de usar y consumir contenidos digitales, un magma de incalculable tamaño ante el hay que tener cierta pericia y algunos conocimientos para manejarlo debidamente. Hay una gran cantidad de información disponible en Internet ("en Internet está todo" es mucho más que un tópico coloquial, es ya una realidad fehaciente), pero varía en formato, calidad y coste. Respecto a este último punto, el perfil del consumidor determinará quiénes están o no dispuestos a pagar por contenidos digitales.

En el caso de España, un 31,3 por ciento de los consumidores no está dispuesto a aceptar ninguna forma de pago, mientras que el 68,7 por ciento está dispuesto a pagar al menos por un tipo de contenido digital.

Los consumidores de contenidos audiovisuales como películas, series, vídeos, documentales, y videojuegos prefieren, en primer lugar, pagar por consumo de unidad (pago por descarga de película, canción, álbum o un videojuego en particular). En segundo lugar, eligen acceder al contenido audiovisual de forma gratuita a cambio de aceptar publicidad. En el caso del consumo de música, la preferencia por consumo gratis con publicidad supera en un 4 por ciento al formato de pago por consumo.

Gráfico 3
Preferencia de pago por contenidos digitales (%)

Fuente
Estudio de uso y actitudes de consumo de contenidos digitales, julio de 2017. Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI)

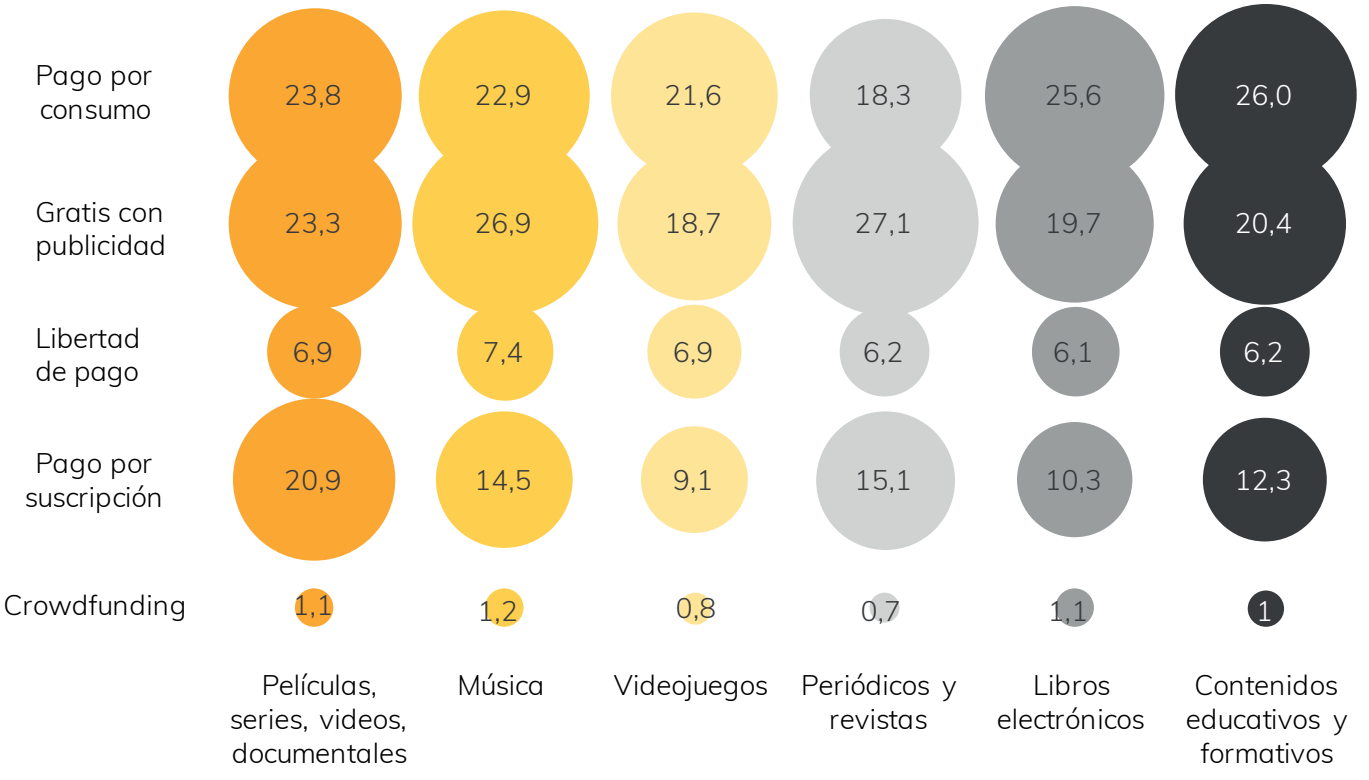


En cuanto al pago por suscripción, el 20 por ciento de los consumidores de contenidos por Internet lo escogerían para acceder a películas, series, vídeos y documentales (a través de plataformas digitales como Netflix o HBO, por ejemplo). La actitud cambia respecto al consumo de música y videojuegos: por los que menos del 15 por ciento de los consumidores estarían dispuestos a pagar una suscripción.

En el caso de contenidos no audiovisuales, como libros electrónicos o contenidos educativos y formativos, uno de cada cuatro españoles paga por su consumo, seguidos de cerca por el grupo que prefiere acceder a ellos gratuitamente, con la contrapartida de que lleven agregada publicidad. La tendencia se invierte en el caso del consumo de periódicos y revistas, con una mayoría que prefiere el formato gratis con publicidad, seguida por quienes eligen pagar por el consumo.

Gráfico 4
Preferencia de pago por tipo de contenido digital (%)

Fuente
Estudio de uso y actitudes de consumo de contenidos digitales, julio de 2017. Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI)



A los contenidos digitales de Internet se puede acceder de muchas maneras. Existen herramientas para personalizar las búsquedas de acuerdo con el perfil de preferencias de las personas, así como buscadores genéricos para quienes eligen buscar la información al momento, sin distinciones. Muchas veces, la destreza del usuario para navegar el Internet define sus actitudes hacia las opciones que se ofrecen para personalizar la experiencia de la red. El estudio sobre consumo de contenidos digitales de la ONTSI ofrece algunos datos sobre distintas actitudes respecto a la forma de acceso a los contenidos.

La mayoría de las personas insiste, varias veces si es necesario, si el contenido que buscan les interesa. Igualmente, para buscar contenido audiovisual o texto optan por escribir el título en la barra de búsqueda del navegador. El 56,5 por ciento de los consumidores, cuando han iniciado su búsqueda, ya saben si quieren acceder al contenido en línea o si prefieren descargarlo. Casi la mitad de los entrevistados reportaron que cuando no encuentran lo que quieren, preguntan a alguien.

Para acceder específicamente a películas o series, el 44,1 por ciento de los usuarios de Internet utilizan YouTube, las páginas de las cadenas de televisión o la propia televisión. Un considerable colectivo, el 27,5 por ciento, sigue temporadas de alguna serie, aunque no esté emitiéndose en ese momento.

A pesar del riesgo de los virus, este no representa un impedimento para la mayoría de las personas. Solo el 18,2 por de los entrevistados afirman que no suelen buscar contenidos en internet por miedo a los virus o a dañar el ordenador. En cuanto a la dificultad, una minoría, el 16,3 por ciento, busca poco contenido porque le resulta difícil encontrar lo que quiere. Asimismo, aunque hay una percepción general de incomodidad con la publicidad online, solo un 5,8 por ciento de los usuarios de Internet indican disponer de bloqueadores (ad-blockers) a la hora de navegar.

Existen diferencias entre grupos de edad en el modo de buscar y acceder a los contenidos digitales. La gran mayoría de los jóvenes de 16 a 24 años utilizan YouTube, las cadenas de televisión o la misma televisión para buscar los contenidos audiovisuales de su preferencia, mientras que solo un tercio de la población mayor de 64 años lo hace. Estos últimos también buscan contenido directamente en la barra del navegador significativamente menos que los más jóvenes. Los resultados muestran una tendencia clara en la que los usuarios más jóvenes tienen una actitud más proactiva hacia las formas de acceso a los contenidos digitales.

3. Riesgos sociales de Internet

Llama la atención cómo, a pesar de la masiva difusión y altos niveles de aceptación de Internet y de las TIC, que crecen de un modo exponencial, casi el 80 por ciento de los consumidores perciben que el uso intensivo de Internet en el móvil “produce cierta actitud antisocial y aislamiento en la gente”. En nivel de preocupación, le sigue la dependencia de la tecnología que puede generarse debido a la disponibilidad de contenidos (71,1 por ciento). Otras inquietudes hacia potenciales perjuicios de la red expuestas por más de la mitad de los usuarios, son la preocupación por la pérdida del valor de libros, música, películas y prensa debido a los formatos más baratos, o gratis, disponibles en Internet. La misma proporción de personas se preocupa porque el fácil y rápido acceso a la información en línea pueda causar pérdida de las capacidades de reflexión de la

Gráfico 5
Actitudes hacia la forma de acceso a los contenidos (%)

Fuente
Estudio de uso y actitudes de consumo de contenidos digitales, julio de 2017. Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI)

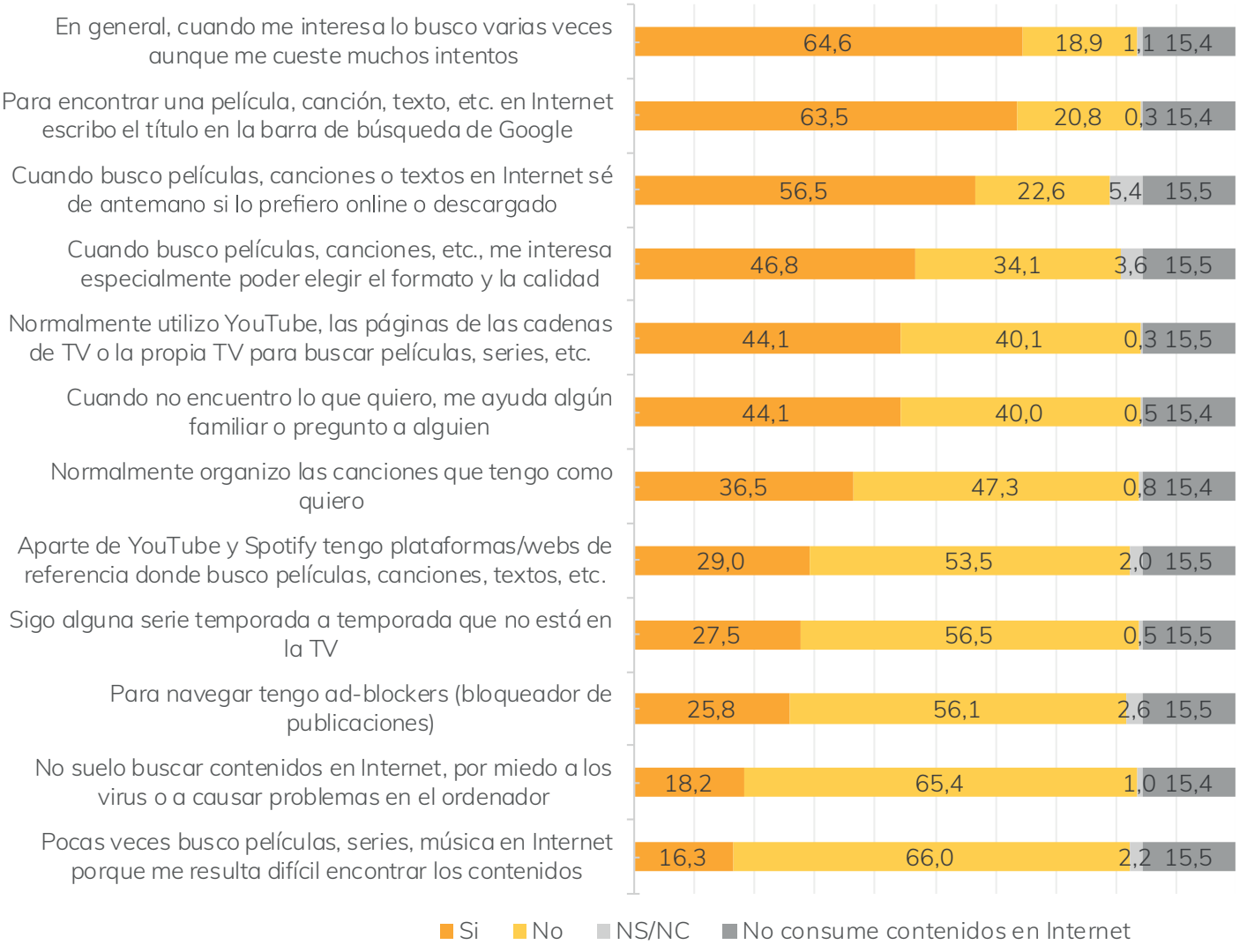
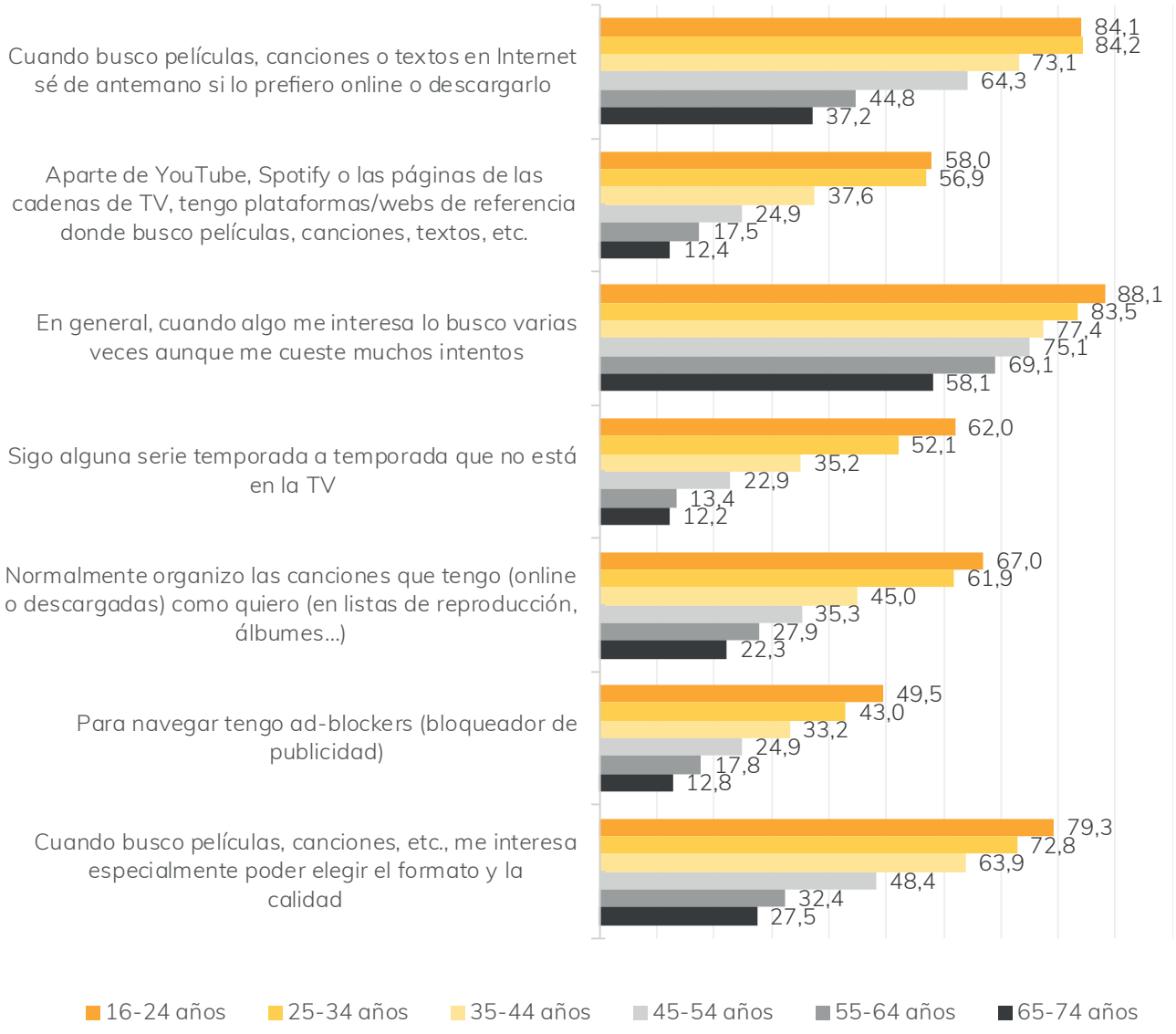


Gráfico 6
Actitudes más proactivas de los usuarios de internet, por edad (% sobre quienes consumen algún contenido en Internet)

Fuente
Estudio de uso y actitudes de consumo de contenidos digitales, julio de 2017. Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI)



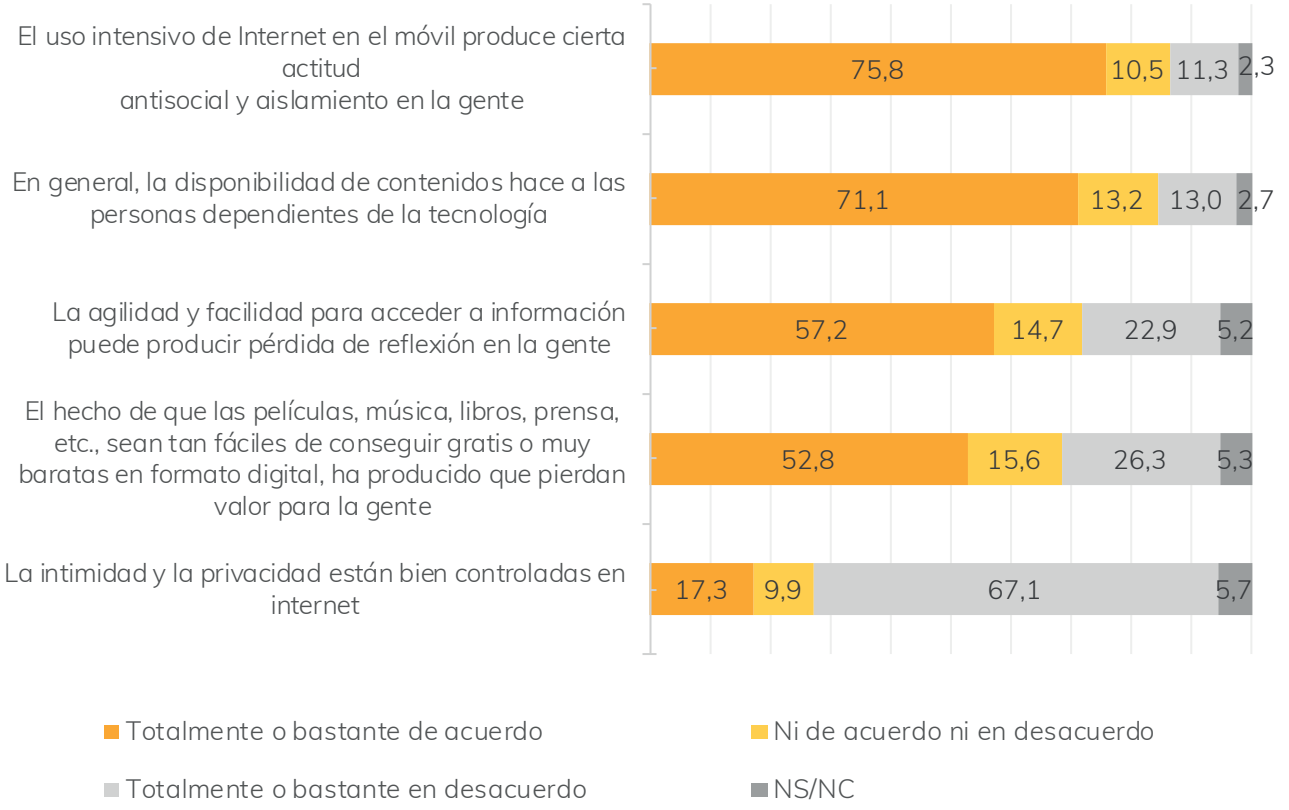
gente. Además, solo un 17,3 por ciento de los españoles consideran que la intimidad y la privacidad están bien controladas en Internet.

III. Protección de datos personales

Para poder utilizar las plataformas tecnológicas en sus diferentes versiones y presentaciones resulta necesario, por lo general, crear un usuario y registrar o permitir el acceso a datos personales. En un escenario donde el diseño y las herramientas tecnológicas están en constante cambio, es importante comprender cuál es la percepción de las personas con respecto al manejo de su información personal y las actitudes que derivan de estas percepciones.

Gráfico 7
Percepción de riesgos sociales de internet (%)

Fuente
Estudio de uso y actitudes de consumo de contenidos digitales, julio de 2017. Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI)



Una de las mayores preocupaciones de la población española con respecto a las nuevas tecnologías es el nivel de protección de los datos personales y la posibilidad de que esta información sea compartida y usada por otros. Según el Barómetro del CIS (2013, 2017, 2018), casi el 80 por ciento de los entrevistados declararon sentirse "muy" o "bastante" preocupados por este tema, tendencia que se ha mantenido constante desde 2013 hasta 2018.

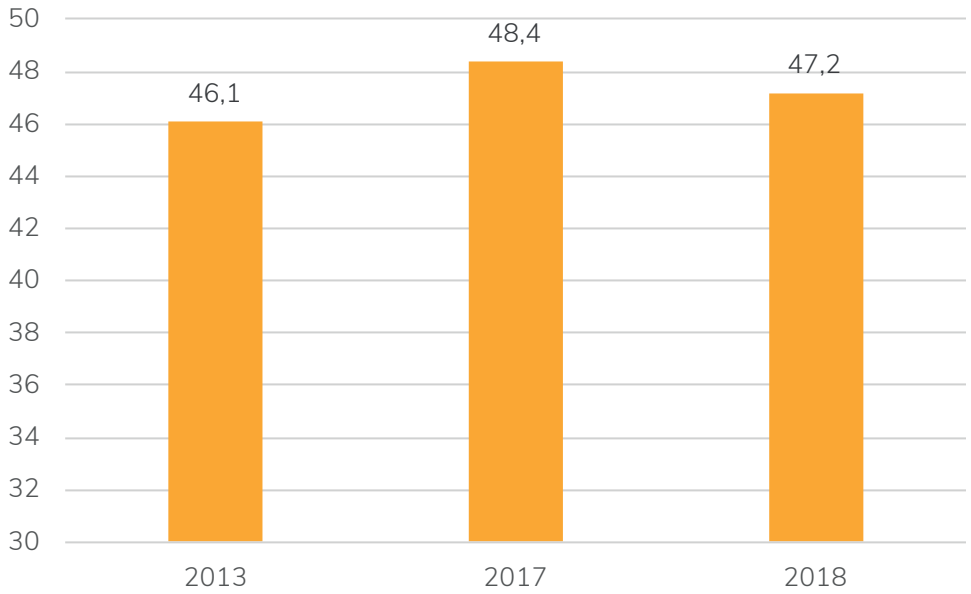
1. Riesgos e información

A pesar de la gran cantidad de información disponible y los múltiples canales de acceso a ésta, la mayoría de los españoles no se sienten bien informados acerca de los riesgos que implica proporcionar datos personales. El Barómetro CIS refleja que menos del 50 por ciento de los entrevistados expresaron sentirse bastante o muy informados sobre estos riesgos, tendencia que se ha mantenido de 2013 a 2018.

Esta percepción de niveles personales de información sobre riesgos se corresponde con la medición del Eurobarómetro. No obstante, la proporción de consultados a nivel europeo que expresan sentirse poco o nada informados es aún mayor que en España y muestra un aumento de seis puntos porcentuales de 2013 a 2017 (58 y 64 por ciento, respectivamente).

Gráfico 8
Me siento 'muy' o 'bastante' informado/a acerca de los riesgos que puede conllevar proporcionar datos personales (%)

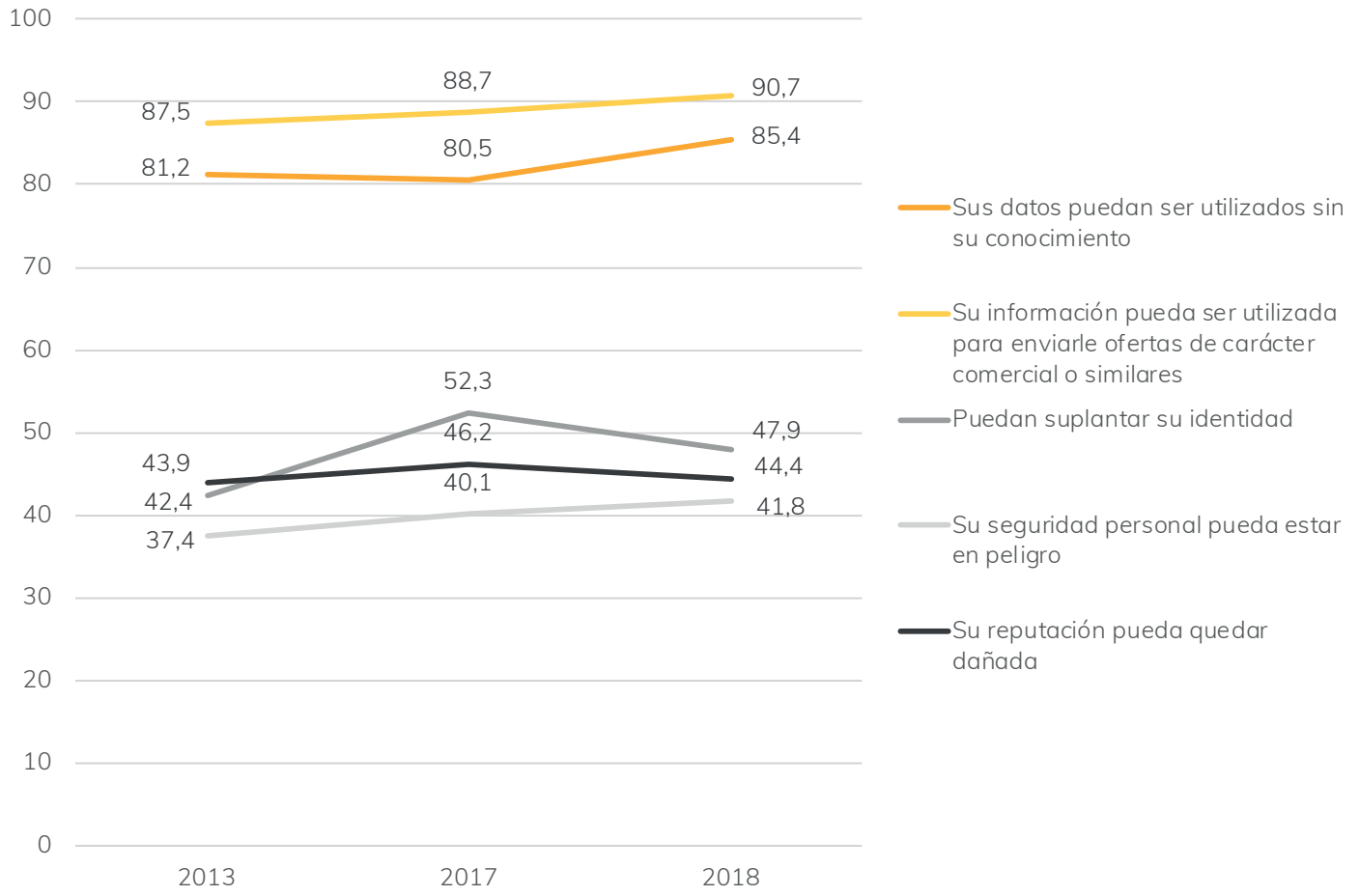
Fuente
Barómetro CIS (2013, 2017, 2018)



Sin embargo, existe un cierto consenso en torno a cuáles son los riesgos respecto a los datos personales que tienen más probabilidad de materializarse. La gran mayoría considera que es muy probable o bastante probable que, cuando se comparten datos personales, estos puedan ser utilizados para enviar ofertas comerciales o similares, percepción que ha aumentado de forma sostenida de 2013 (87,5 por ciento) a 2018 (90,7 por ciento). Le sigue, en segundo lugar, la posibilidad de que los datos proporcionados sean utilizados sin conocimiento de la persona, con una tendencia igualmente ascendente, del 81,2 por ciento en 2013 al 85,4 por ciento en 2018. El riesgo percibido como muy probable o bastante probable, en tercer lugar, es que los datos personales puedan ser

Gráfico 9
Cuando alguien proporciona datos personales, creo que es 'muy' probable o 'bastante' probable que... (%)

Fuente
Barómetro CIS (2013, 2017, 2018)



compartidos con terceros sin el consentimiento de quien los suministró, temor que confiesa el 79,8 por ciento de los encuestados en 2013.

Los riesgos que se perciben como menos inminentes, en comparación con los descritos anteriormente, son: que se pueda suplantar la identidad de la persona, que su seguridad personal pueda estar en peligro y que su reputación se pueda ver afectada negativamente.

2. Percepción de seguridad según la situación

Como se muestra en el gráfico anterior, existe una preocupación generalizada por la privacidad y la seguridad de los datos personales en los dispositivos de las TIC, especialmente por la posibilidad de que sean utilizados para fines comerciales o compartidos sin consentimiento de la persona. Sin embargo, los niveles de preocupación varían dependiendo de las circunstancias y el contexto en que se compartan estos datos.

Por ejemplo, en los últimos nueve años menos del 10 por ciento de los españoles se han sentido muy preocupados o bastante preocupados a la hora de dar datos personales para participar en un concurso. De forma similar, menos del 15 por ciento manifiesta mucha o bastante preocupación por la protección de sus datos al colgar fotos o vídeos de amigos o familiares en internet.

Sin embargo, a pesar del aumento de medidas de seguridad a través de una variedad de mecanismos cada vez más estrictos, como contraseñas personales o claves electrónicas, la preocupación por la protección de datos en otras áreas se mantiene elevada en buena parte de la población, o incluso va en aumento. Por ejemplo, la proporción de la población que se siente muy preocupada o bastante preocupada al efectuar la declaración de la renta por Internet aumentó cuatro puntos porcentuales entre 2009 (44 por ciento) y 2018 (48 por ciento). Asimismo, desde el 2009, casi dos tercios de los españoles, el 61 por ciento, se han sentido muy preocupados o bastante preocupados por la seguridad de sus datos en el momento de pagar en un establecimiento con tarjeta de crédito.

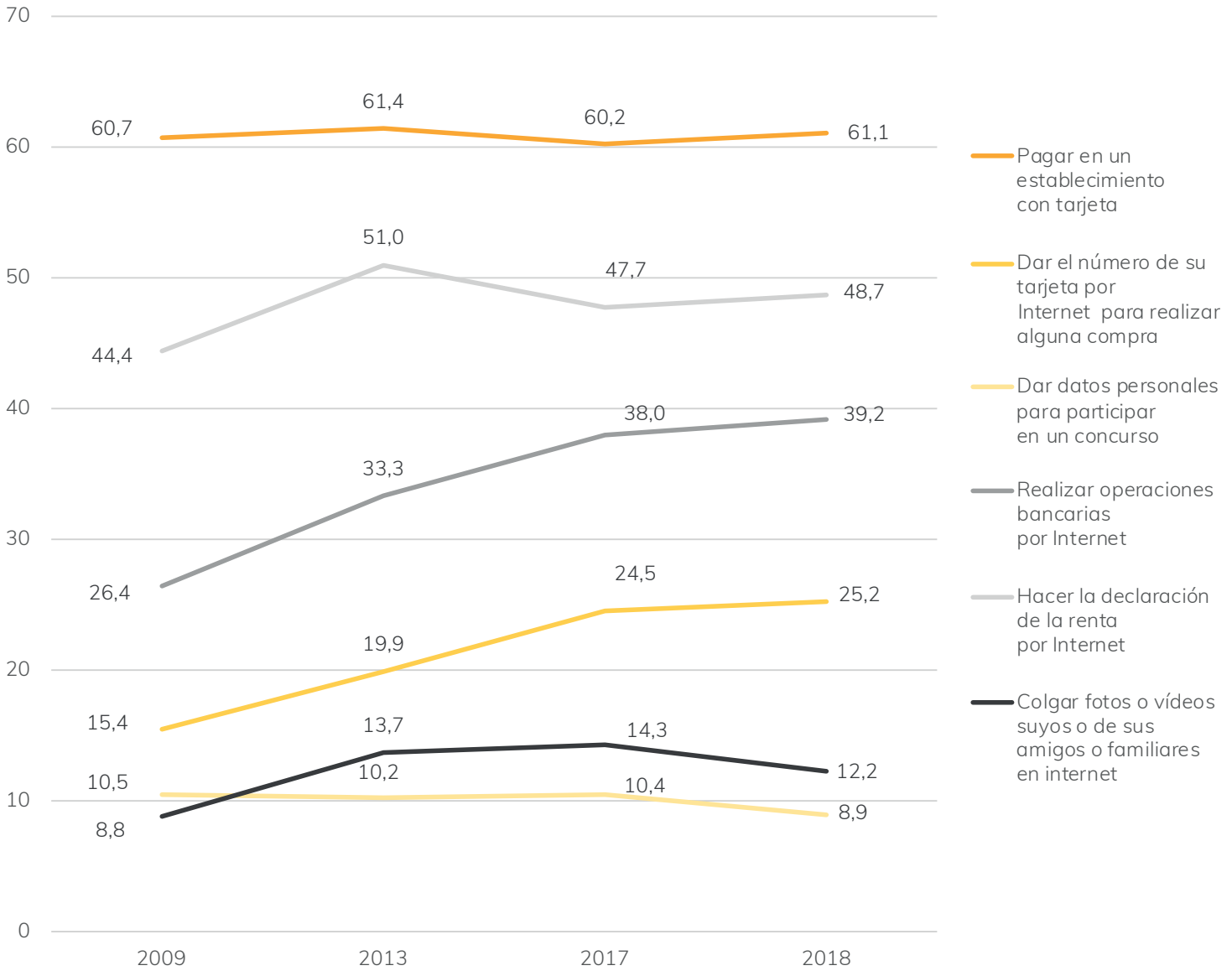
La desconfianza respecto a la seguridad de los datos personales ha aumentado en los últimos años en lo que se refiere a algunas operaciones. En 2018, una de cada cuatro personas afirmaba sentirse muy preocupada o bastante preocupada al facilitar el número de su tarjeta de débito o de crédito para realizar compras por Internet, lo que representa un aumento del 10 por ciento en comparación con 2009. La preocupación a la hora de realizar operaciones bancarias por Internet ha aumentado aún más. En 2009, el 26 por ciento de la población admitió tener mucha o bastante preocupación en ese sentido, un guarismo que aumentó hasta el 39 por ciento en 2018.

3. Variación de actitudes según tipo de datos

Por lo general, las personas mantienen cierto nivel de alerta que se activa en el momento en que se les solicita información de carácter personal. Las tareas cotidianas en la era digital fluyen rápidamente, y por ello muchas veces tenemos que discernir sobre la marcha cuán arriesgado resultaría compartir información personal específica en un determinado contexto o plataforma. En relación con este asunto, el Barómetro del CIS preguntó a sus entrevistados acerca del nivel de dificultad con el que aceptarían compartir diferentes tipos de datos personales.

Gráfico 10
Mucha o suficiente confianza en las siguientes acciones (%)

Fuente
Barómetro CIS (2009, 2013, 2017, 2018)



Los resultados muestran que la información financiera y las huellas dactilares son los datos personales que más del 80 por ciento de las personas no compartirían a menos que fuese imprescindible hacerlo, seguidos por vídeos y fotos personales, relaciones personales e historial médico. La tendencia a proteger estos datos ha aumentado de forma sostenida en los últimos cinco años, particularmente la cautela al decidir compartir información sobre relaciones personales e historial médico, que crecieron un 14 y un 10 por ciento, respectivamente.

El aumento de la renuencia a compartir información sobre relaciones de pareja o amistades llama singularmente la atención, porque coincide con la expansión y diversificación de las redes sociales. Es posible que la percepción de una red social cada vez más grande, hiper e intercomunicada, y la sensación de no estar suficientemente informados sobre riesgos relacionados con la protección de datos personales estén relacionadas con el aumento de la proporción de personas que solo compartirían estos datos si no tuviesen otra opción.

Por otro lado, el estudio muestra que hay algunos datos que la mayoría de las personas sí ofrecería con facilidad. En 2013 y 2017, la nacionalidad es la información que más fácilmente compartirían las personas, seguida por información sobre sus aficiones, gustos y opiniones.

Sin embargo, a pesar de que en los últimos años compartir gustos y opiniones no supone un problema para la mayoría, el grupo que daría fácilmente esta información se ha reducido un 12 por ciento. De nuevo, es posible que las redes sociales jueguen un rol en la disminución de esta actitud. Plataformas como Facebook, Instagram o Twitter se han vuelto herramientas de discusión y debates en donde no se garantiza que la reputación de quien comparta su opinión y sus gustos resulte ilesa.

En el caso de otros datos, como dirección, número de teléfono móvil, nombre y apellidos, historia laboral, sitios web que se visitan y número de identificación, la mayoría de las personas no los daría a menos que fuese imprescindible, o les costaría facilitarlos.

4. Garantías de protección

Las actitudes de las personas hacia la tecnología y los posibles riesgos de compartir datos están también relacionadas con cómo perciben y valoran las garantías de protección que ofrecen los diferentes servicios y plataformas tecnológicas.

La mayoría de los españoles piensa que las garantías de protección de datos más altas las ofrece la Administración Pública (Ministerio de Hacienda, oficinas de la Seguridad Social, servicios sanitarios). En el caso de los bancos, la percepción de los entrevistados es que dan garantías altas (42,5 por ciento) o muy altas (7 por ciento). Le siguen con valoraciones menos positivas los comercios y las compañías de servicios.

Los resultados también muestran que las redes sociales y los buscadores de Internet tienen la valoración más baja en cuanto a garantías de protección de datos. El 72 por ciento de los entrevistados consideran que las garantías de las redes sociales son bajas o muy bajas, seguidas por la evaluación negativa de las garantías de los buscadores de internet (67 por ciento).

Gráfico 11
De los siguientes tipos de datos personales, dígame cuál o cuáles de ellos daría usted fácilmente, le costaría darlos o no los daría, salvo que fuera imprescindible (%)

Fuente
Barómetro CIS (2013, 2017, 2018)

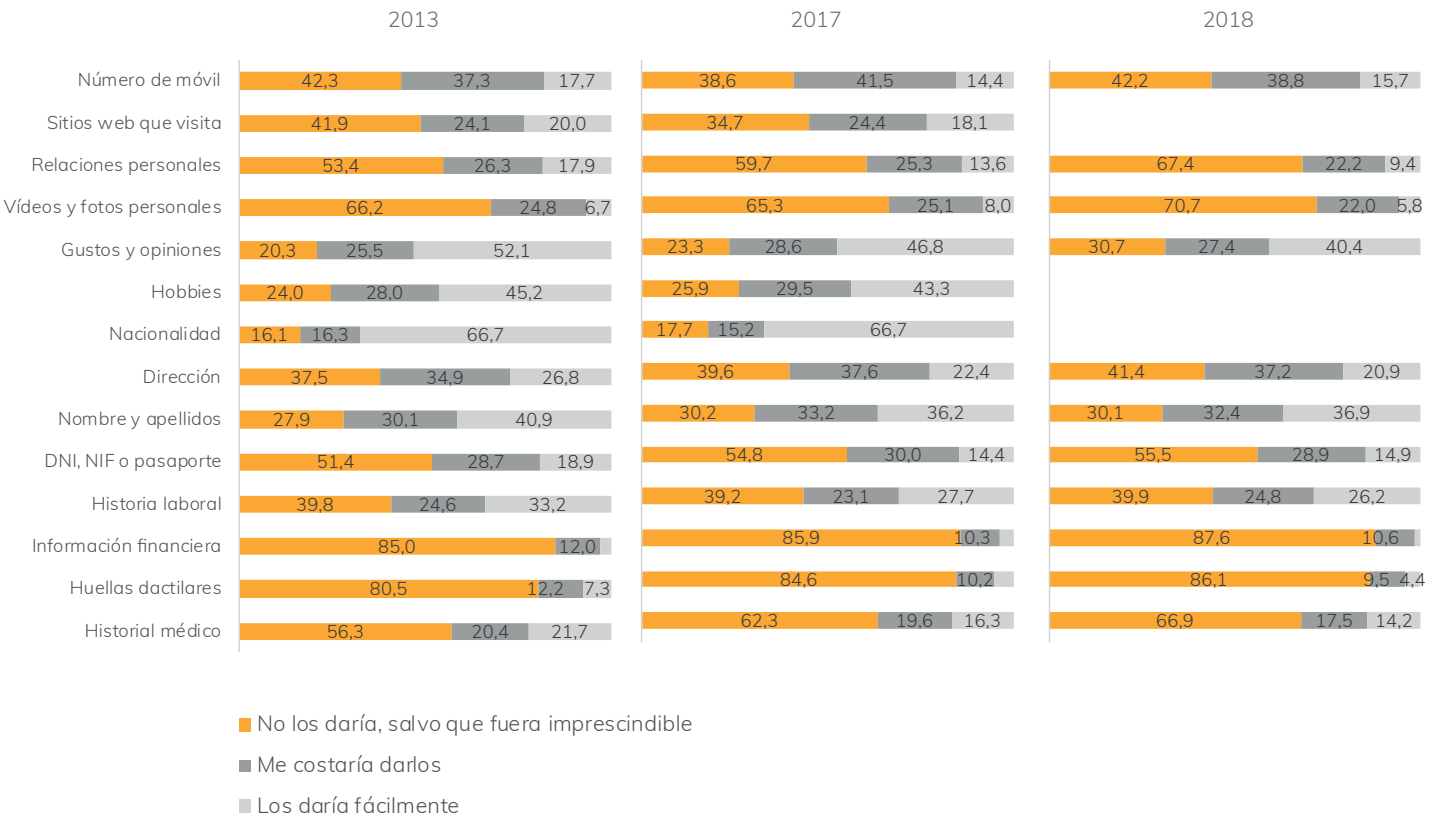
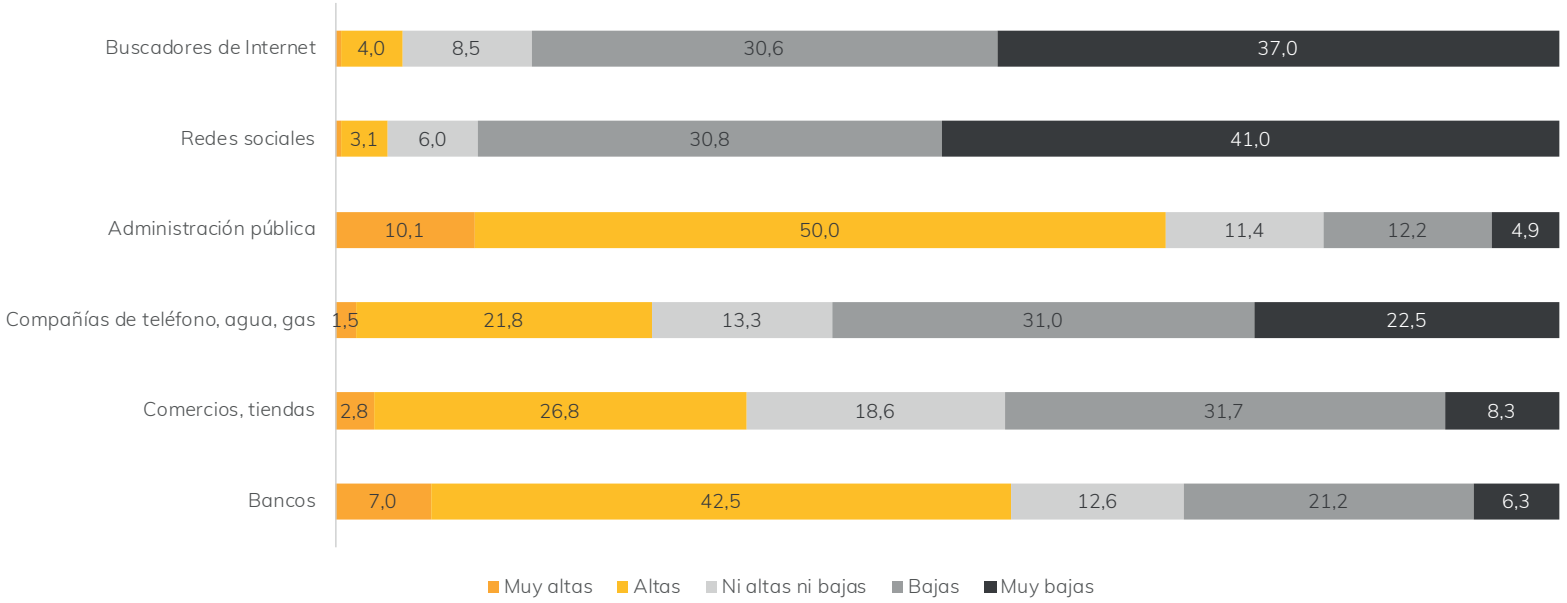


Gráfico 12
Percepción de garantías de protección de datos ofrecidas por plataformas y entidades (%)

Fuente
Barómetro CIS (2018)



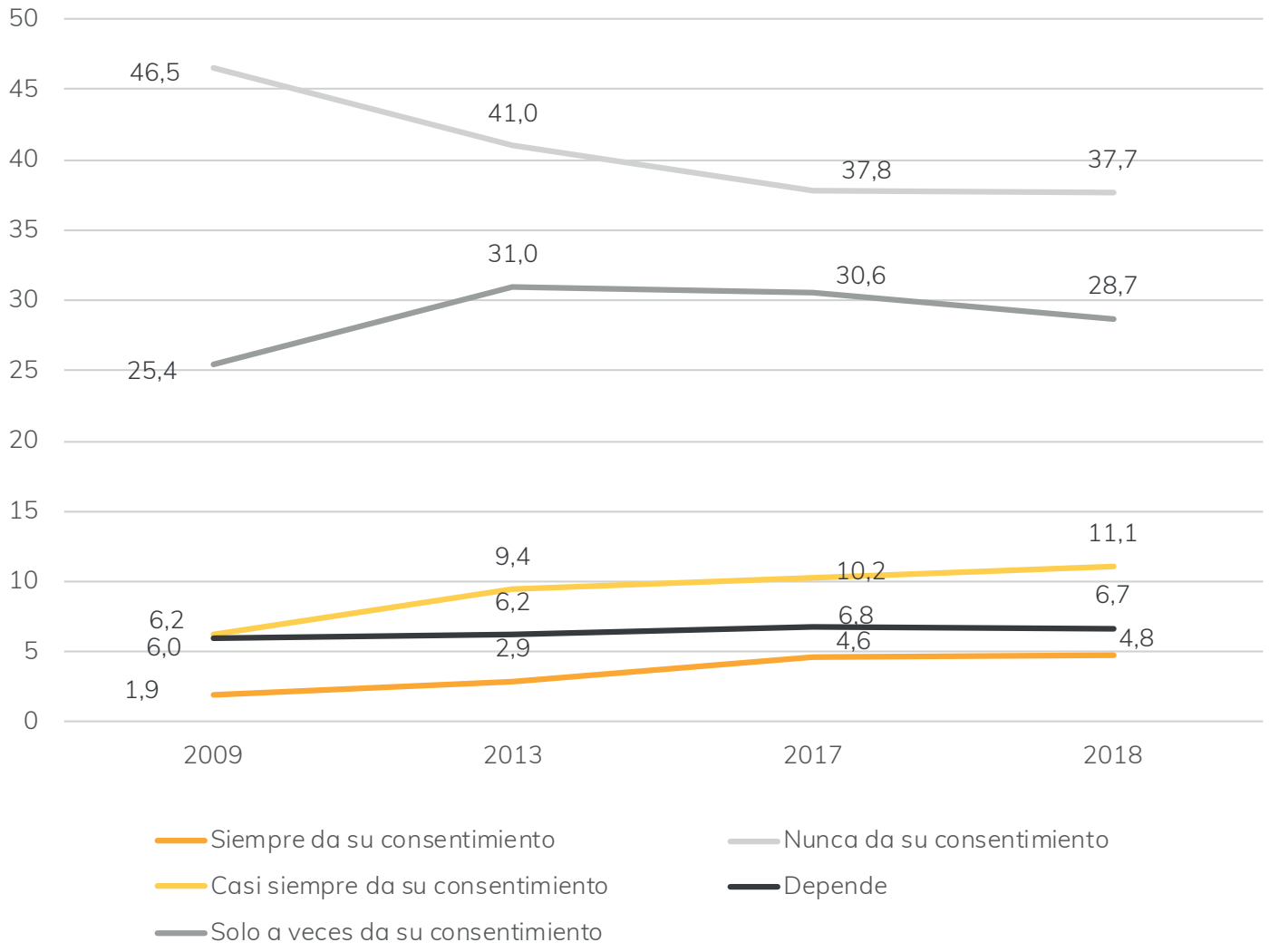
5. Uso de datos personales por otros

Como hemos indicado anteriormente, a más del 80 por ciento de los españoles le preocupa, al compartir sus datos en alguna plataforma digital o entidad, que esta información personal sea usada por otros. Una de las situaciones que resalta como una de las más rechazadas por la población es cuando compañías o instituciones utilizan datos personales para ponerse en contacto con el usuario con fines publicitarios. En 2018, el 70 por ciento de los entrevistados por el estudio del Barómetro del CIS aseguraron haber sido contactados por teléfono o por correo electrónico por entidades a las que no tenían constancia de haber pasado su información personal.

Además, en 2009 casi la mitad de los entrevistados indicó que, al rellenar formularios en los que se les pide autorización para disponer de sus datos personales, nunca dan su consentimiento. La tendencia de esta actitud se ha reducido en algunos puntos porcentuales en los últimos ocho años, pero se ha mantenido en más del 35 por ciento de los usuarios.

Gráfico 13
Actitud hacia consentimiento para uso de datos personales por otros (en porcentaje).

Fuente
Barómetro CIS (2013, 2017, 2018)



IV. Políticas de privacidad

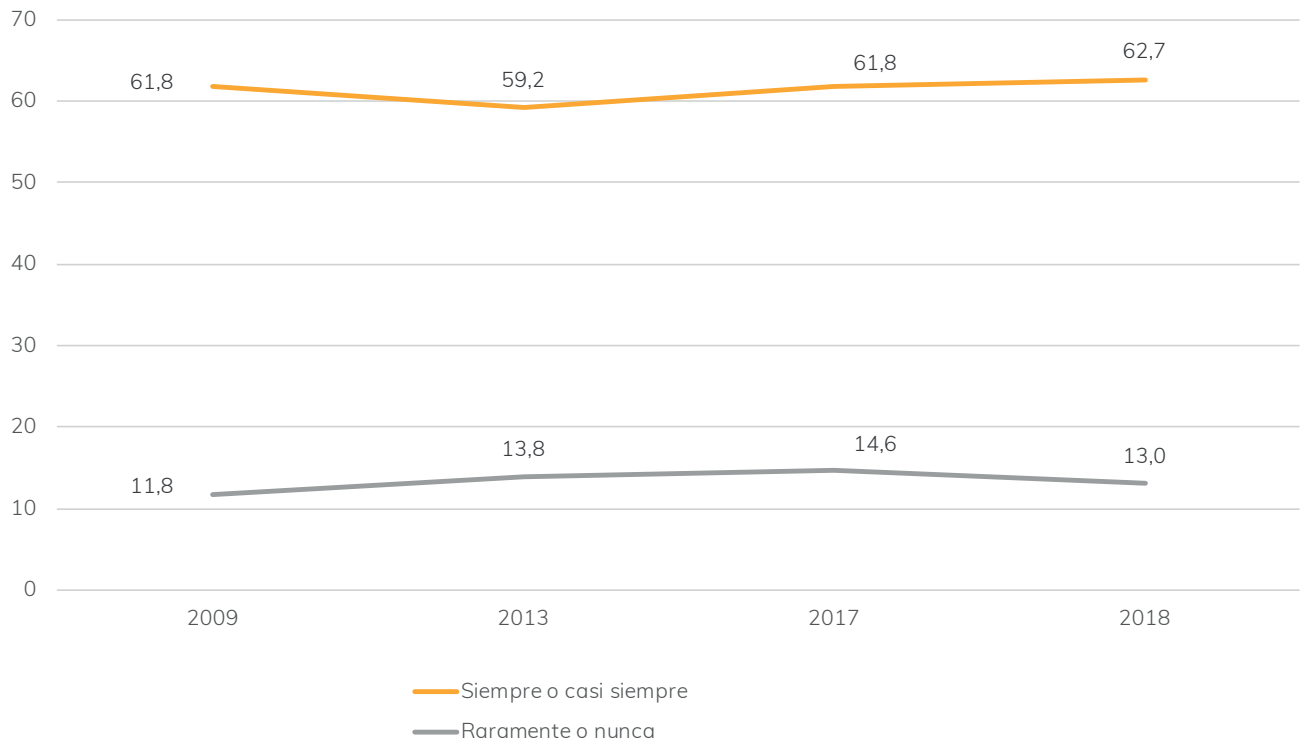
Junto con las preocupaciones en torno a Internet y la digitalización de datos personales, gran parte de la ciudadanía critica las políticas de privacidad que regulan las TIC y demás contenidos plasmados en las redes.

1. Políticas de privacidad de sitios web

Es importante resaltar de entrada que el 60 por ciento de los encuestados por el Barómetro CIS confiesa que "nunca" o "raramente" lee las políticas de privacidad de las páginas que visita, mientras que solo un 4 por ciento lo hace "siempre". Las proporciones se han mantenido constantes en 2009, 2013, 2017 y 2018. Probablemente se deba a que tres de cada cuatro personas que respondieron opinen estar "poco" o "nada de acuerdo" con la afirmación: "Las políticas de privacidad y la información que se ofrece en los sitios de Internet sobre el tratamiento de datos son claras y sencillas de entender".

Gráfico 14
Actitud hacia la lectura de políticas de privacidad de las páginas web (%)

Fuente
Barómetro CIS (2009, 2013, 2017, 2018)



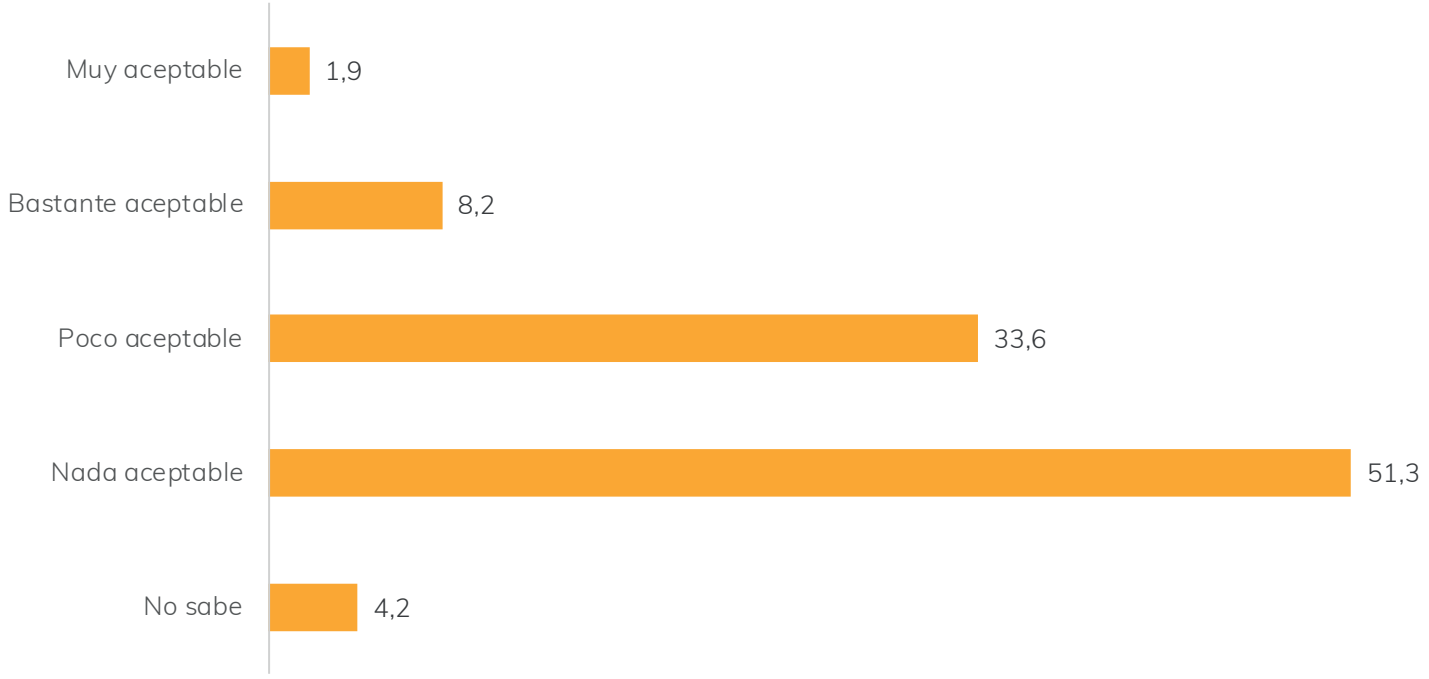
2. Privacidad de sitios web y redes sociales

La gran mayoría de los encuestados no acepta la práctica de algunas páginas de compartir con las redes sociales información sobre los patrones de tráfico del individuo que las visita. No obstante, el 40 por ciento de los encuestados confiesa no usar ninguna herramienta que bloquee el seguimiento que puedan llevar a cabo terceros sobre su comportamiento en Internet. En vez de ello, los internautas se limitan a instalar un programa de antivirus (75 por ciento), filtrar correos electrónicos desconocidos (64 por ciento), no compartir información personal en internet (53 por ciento) o no frecuentar páginas de internet desconocidas (38 por ciento).

Con respecto a las redes sociales, casi un 70 por ciento de los encuestados está "muy" o "bastante de acuerdo" con que es "difícil controlar quién ve la información de mi perfil" mientras que una proporción parecida está "nada" o "poco de acuerdo" con que "las redes sociales cuidan la seguridad de los datos personales". Asimismo, el 95 por ciento cree que las redes sociales no deberían compartir los datos personales con terceros y otro 90 por ciento cree que las políticas de privacidad no deberían cambiarse sin el consentimiento de los usuarios.

Gráfico 15
Práctica de algunas páginas web de compartir su tráfico con redes sociales. Niveles de aceptación (%)

Fuente
Barómetro CIS (2018)



V. Menores y acceso a Internet

El uso de Internet por parte de los menores de edad es también materia de interés –y, por supuesto, de preocupación– para la población española. En este sentido, datos provenientes del Instituto Nacional de Estadística afirman que el porcentaje de personas de entre 10 y 15 años que usan ordenador es del 92,4 por ciento. Además, entre personas de esta misma edad el uso de Internet es del 95,1 por ciento, mientras que la utilización de teléfono móvil alcanza el 69,1 por ciento. Dados estos elevados datos de uso entre menores de edad, es entendible la preocupación por el nivel de acceso que puedan tener a los contenidos digitales, el nivel de supervisión adulta que puedan necesitar y la necesidad de un uso responsable de Internet.

1. Formación en centros educativos

Un pilar fundamental para proteger a los menores del contenido inadecuado de la Red es la formación acerca de un uso sano y eficaz de la herramienta. Pues bien, resulta llamativo que actualmente la mayoría de los españoles evalúen de manera negativa la formación que se imparte a los menores en los centros escolares sobre uso responsable y seguridad en Internet. Así lo reflejan los datos del Barómetro del CIS correspondiente al mes de mayo de 2018. De hecho, menos del 30 por ciento cree que el grado de información recibida es "mucha", "bastante" o "suficiente" mientras que casi un 50 por ciento opina que es "poca" o "ninguna". Otro 22 por ciento de los encuestados por el Barómetro CIS no sabe responder la pregunta, dato que puede indicar no solo falta de conocimiento de los padres sobre el currículo escolar relacionado con las TIC, sino también fallas en los canales de información de los centros educativos.

2. Riesgos más habituales

En cuanto a los riesgos más habituales a los que están expuestos los menores en Internet, en primer lugar, casi el 40 por ciento identifica la "difusión de fotos o vídeos comprometidos", seguido por "dar demasiada información sobre ellos/as" (23 por ciento) y "ser acosado/a u hostigado/a con el fin de obtener concesiones sexuales" (17 por ciento). La tendencia de estas actitudes se mantiene estables a lo largo de los años 2013, 2015, 2016, 2017 y 2018.

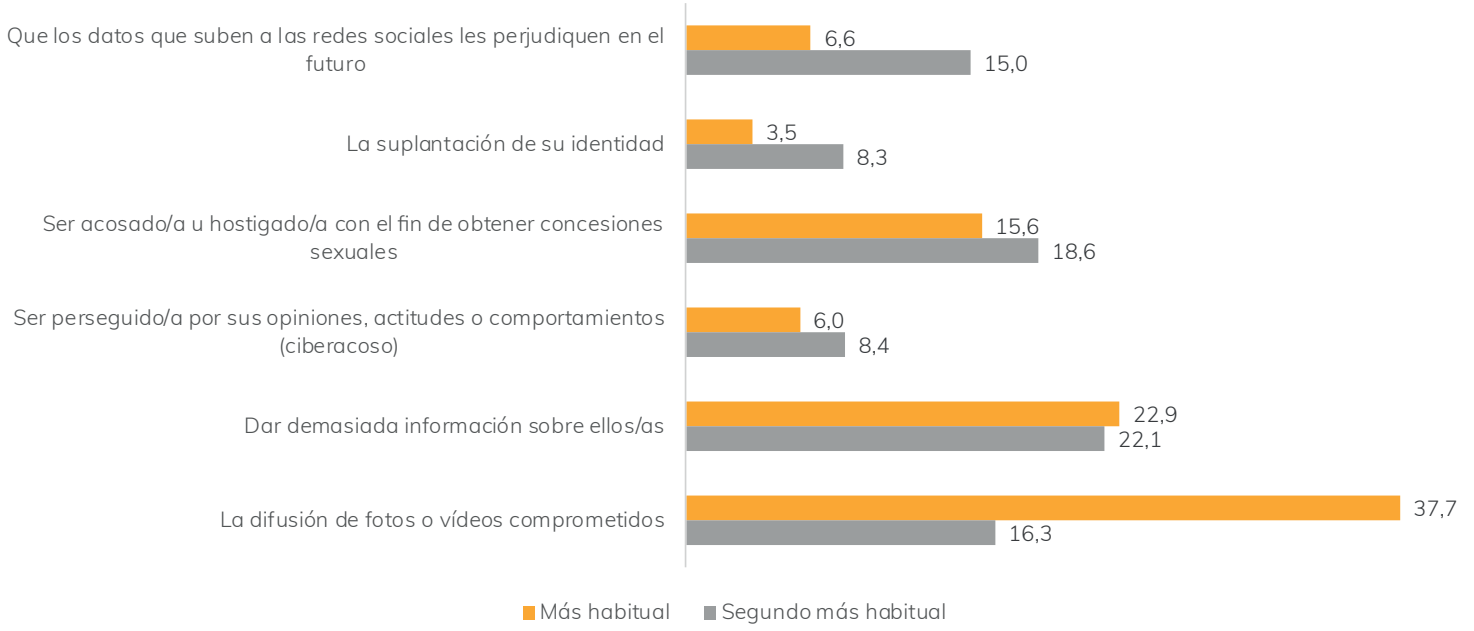
3. Controles, restricciones y responsables

Según los datos de este mismo Barómetro, una parte muy considerable de la población (cerca del 60 por ciento) opina que los menores "deberían tener bastantes restricciones o controles" al usar Internet. Mientras que otro 24 por ciento de la población opina que "deberían tener completamente restringido el acceso". Apenas el 10 por ciento recomienda poco o ningún control. Estas tendencias se han mantenido estables a lo largo de los años 2009, 2013, 2017 y 2018.

Si la gran mayoría opina que el uso de Internet por parte de los menores debería restringirse bastante o por completo, otra gran mayoría de las personas (el 85 por ciento de los encuestados) opina que los principales responsables de establecer estos controles son los padres. En segundo lugar, y con igual nivel de responsabilidad asignada (así opina el 25 por ciento, aproximadamente), le siguen "las escuelas", "los proveedores de servicios de Internet" y el "Gobierno / las autoridades públicas". En otras palabras, proteger a los más jóvenes internautas es una labor compartida, no solo de los padres de los menores, sino también de diversas instancias: educadores, proveedores de servicios y autoridades públicas. El éxito de esta

Gráfico 16
Percepción de los riesgos más habituales a los que están expuestos los menores (%). 2018

Fuente
Barómetro CIS (2018)



colaboración puede desembocar en un escenario en el que el nivel de conciencia de los jóvenes sobre del uso seguro de Internet permita que los controles pasen a un segundo plano.

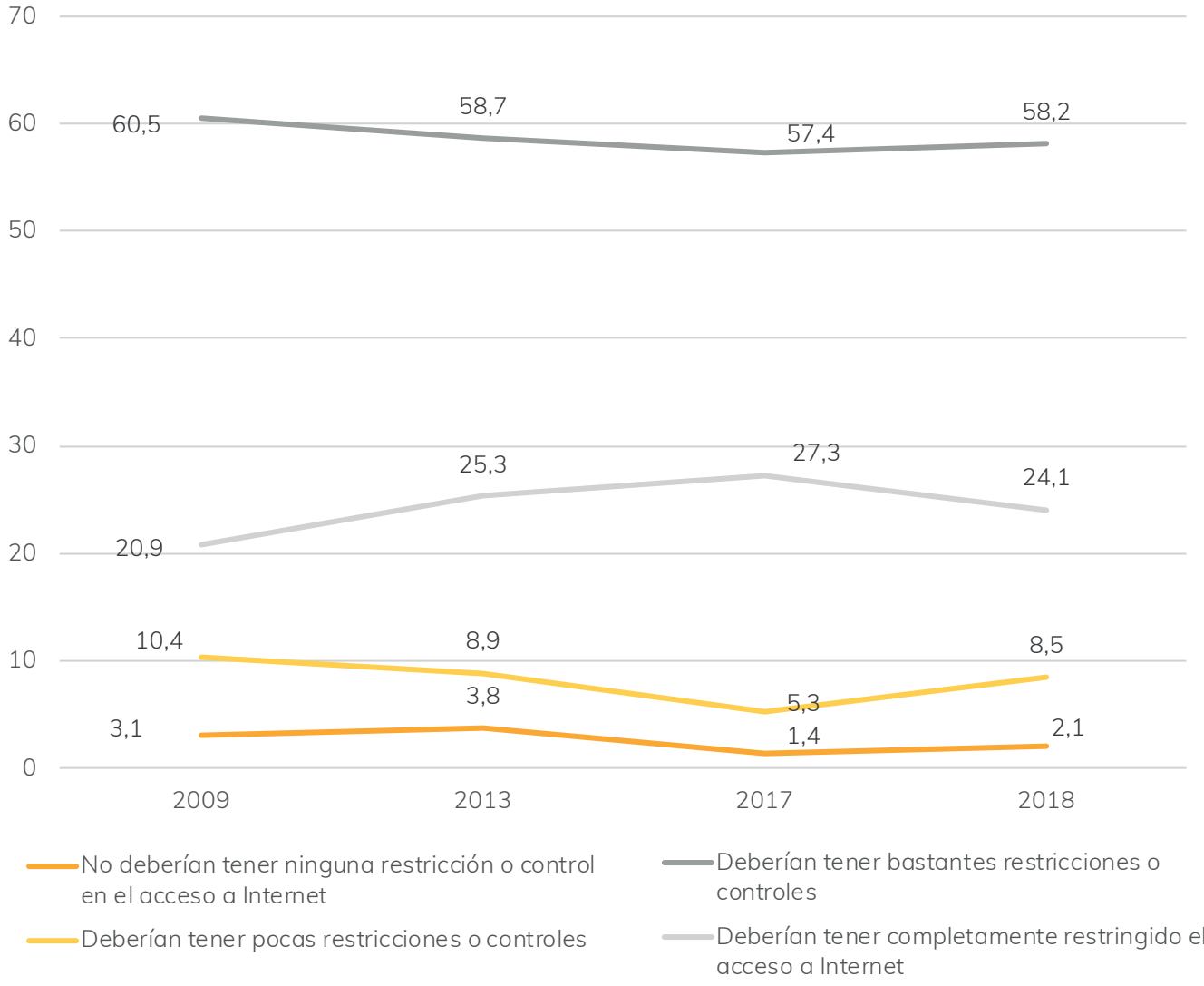
VI. Futuro y empleo

Sin ninguna duda, la revolución de las comunicaciones ha cambiado totalmente el mundo del trabajo de una forma equiparable a la revolución industrial de mediados del siglo XVIII. En aquella época, los telares mecánicos supusieron la expansión de la producción de tela y la creación de nuevos tipos de empleo. Por otro lado, también se produjo una gran destrucción de otro tipo de labores que en aquella época eran muy habituales, especialmente en el ámbito de la artesanía. El mundo empezó entonces a cambiar de la mano de aquellas innovaciones tecnológicas, y ha sufrido en diferentes etapas una acelerada evolución cuyo impacto se manifiesta universalmente de manera muy profunda en la actualidad.

En este apartado del texto realizamos un repaso acerca de los efectos que ha tenido la llegada de las tecnologías

Gráfico 17
Percepción sobre controles o restricciones para el acceso de los menores a Internet (%)

Fuente
Barómetro CIS (2009, 2013, 2017, 2018)



TIC en el mercado laboral español en los últimos años. Además, también observamos las actitudes que los ciudadanos españoles expresan acerca de los efectos que esta revolución tecnológica ha causado hasta ahora, y los que puede causar en un futuro cercano.

1. Los nuevos empleos

Hoy en día, es Internet la herramienta que ha adquirido el papel simbólico en la presente revolución tecnológica, de forma análoga a como lo fue el telar en el siglo XVIII. Gracias a la Red muchos trabajos se han vuelto más eficientes, se han creado nuevos puestos de trabajo impensables hace 25 años y también se han dejado de generar empleos que ya no resultaban tan beneficiosos en el nuevo entorno digital.

En el caso de España, gracias a los datos del Instituto Nacional de Estadística, podemos observar cómo, desde el año 2008, el número de empresas TIC que actualmente operan en nuestro país ha pasado de 43.708 a 66.155. Es decir, se ha producido un incremento del 51,4 por ciento en un período de ocho años. Además, para contextualizar estos datos, cabe destacar que esta etapa coincide con la gran crisis económica mundial, que precisamente desde 2008 sacudió de forma muy intensa a nuestro país. Pero a pesar de la recesión, observamos cómo el número de empresas dedicadas a las tecnologías de la información y las comunicaciones no dejaron de crecer, lo que da una idea de la enorme magnitud del impacto de estas tecnologías en España.

Junto con la proliferación de nuevas empresas del sector TIC, también se ha producido un significativo aumento del número de empleados en empresas de dicho sector. En este indicador sí se puede comprobar con más claridad el efecto de la crisis económica de 2008 en España. Entre ese año y 2013, la cifra de ocupados en el sector TIC descendió en 25.600 personas, pasando de 415.605 empleados a 390.005. Después de ese año, la tendencia se invirtió, y se pasó de destruir empleo a crearlo, de forma que, para el año 2016, el número de trabajadores TIC en nuestro país era de 448.498, el dato más alto hasta la fecha.

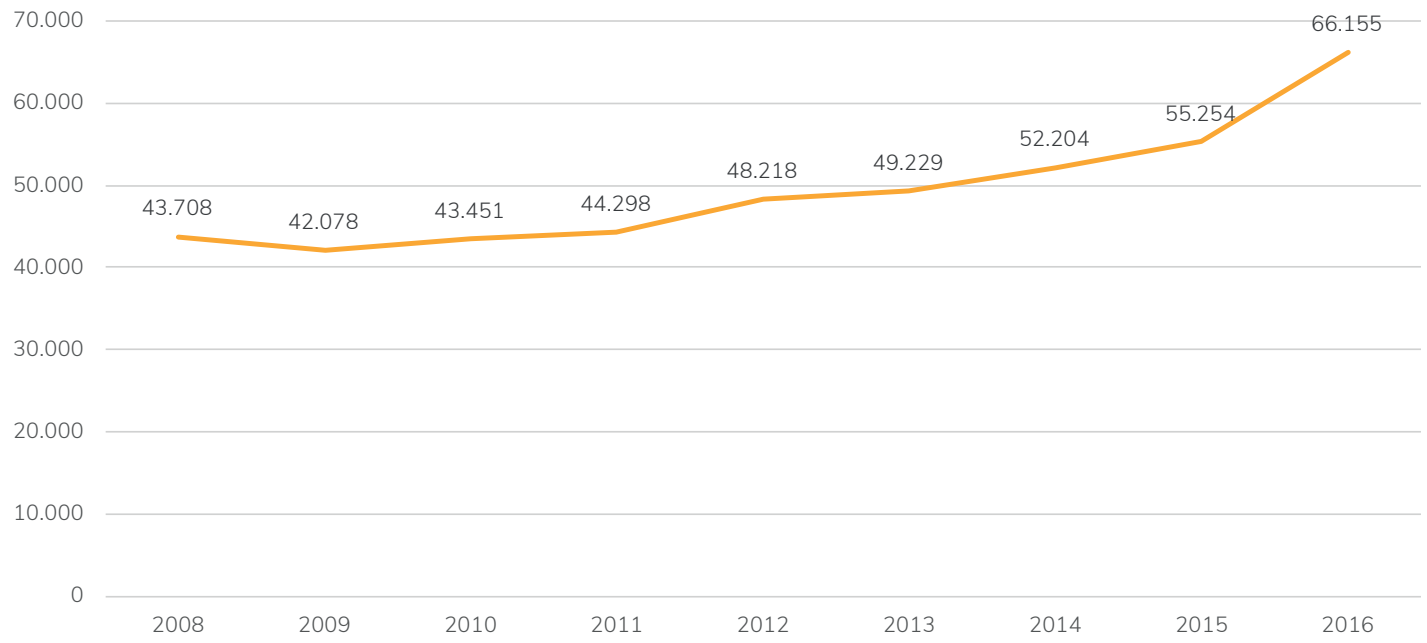
Conviene recalcar la magnitud del fenómeno. La mayoría de estos casi 450.000 empleos corresponden a trabajos que no existían en la España del año 1993, hace ahora 25 años. Valgan como ejemplo de ello los especialistas en posicionamiento web, también conocidos como SEO (acrónimo de *Search Engine Optimization, que se refiere* a la actividad encaminada a la optimización y el aumento de la popularidad de un sitio web) o SEM (sigla de *Search Engine Marketing, que se refiere a la* promoción de un sitio web en los buscadores mediante el uso de anuncios de pago a través de plataformas, por ejemplo Google AdWords). El objetivo de estos profesionales es conseguir la mayor visibilidad de su cliente dentro de la Red. Para ello, es preciso conocer bien el funcionamiento de los algoritmos internos de los motores de búsqueda de los buscadores, como Google. Este tipo de profesional es especialista en integrar palabras clave dentro del espacio web de su cliente, para que así su página web aparezca entre los primeros resultados en los motores de búsqueda.

Este trabajo es actualmente muy demandado por muchas empresas, hasta el punto de que existen compañías integradas por este tipo de profesionales que se dedican a ofrecer asesoramiento SEO a las compañías que las contraten.

Otro empleo relacionado con el sector TIC tiene que ver con el tratamiento de los datos que genera nuestro paso

Gráfico 18
Número de empresas en el sector TIC

Fuente
Estadística Estructural de Empresas: Sector Industrial 2016. Estadística Estructural de Empresas: Sector Servicios 2016. INE. 2017.

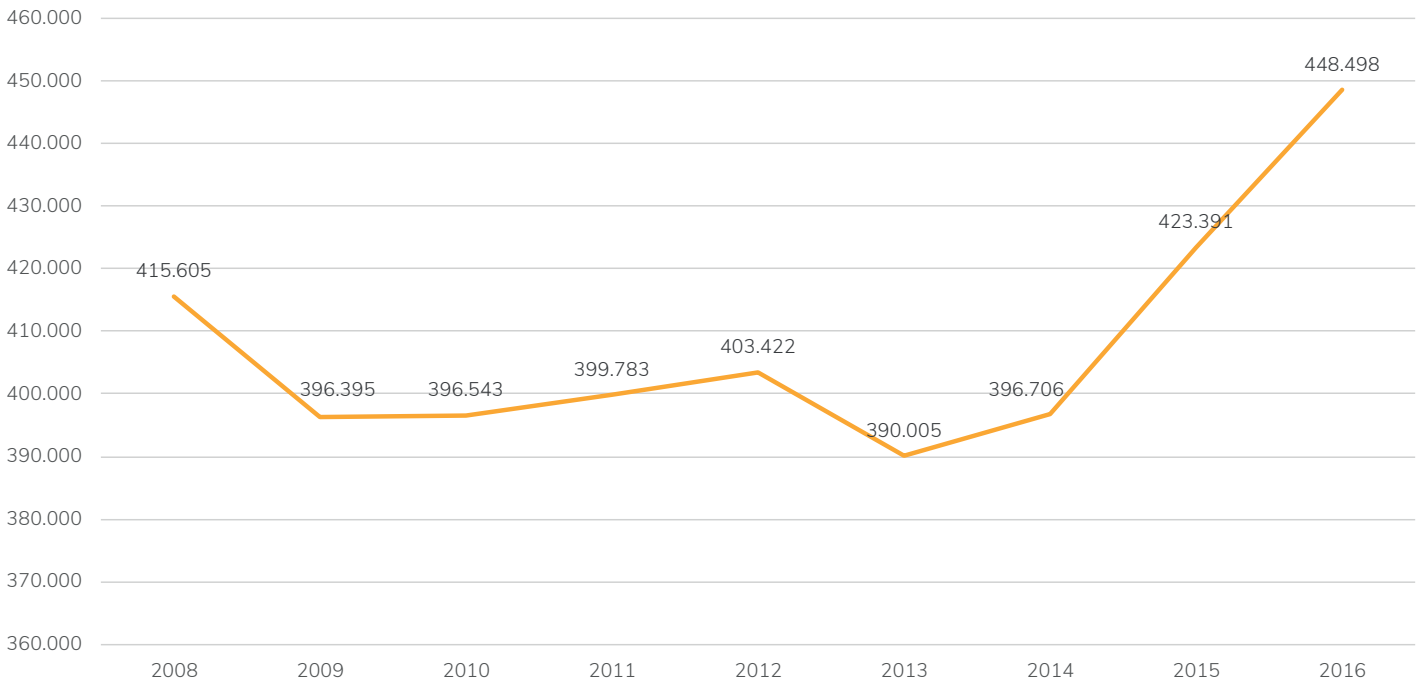


por la red. Este otro trabajo, que tampoco existía hace 25 años, es el de los analistas de big data. Actualmente, al navegar por Internet, se generan miles de datos a partir de información relacionada con nuestra actividad en la red: qué páginas hemos visitado anteriormente, cuánto hemos tardado en apretar un cierto botón, cuánto tiempo hemos pasado leyendo alguna parte de la página.

De sacar partido a todo este volumen de datos se encargan, entre otros, los analistas de big data. Estos profesionales están especializados en la adquisición y la explotación de bases de datos con el objetivo de encontrar tendencias o patrones que puedan ser de utilidad para su empresa. Este tipo de perfiles laborales exigen una formación multidisciplinar, con amplia base en programación informática, estadística

Gráfico 19
Número de ocupados en el sector TIC

Fuente
Estadística Estructural de Empresas: Sector Industrial 2016. Estadística Estructural de Empresas: Sector Servicios 2016. INE. 2017.



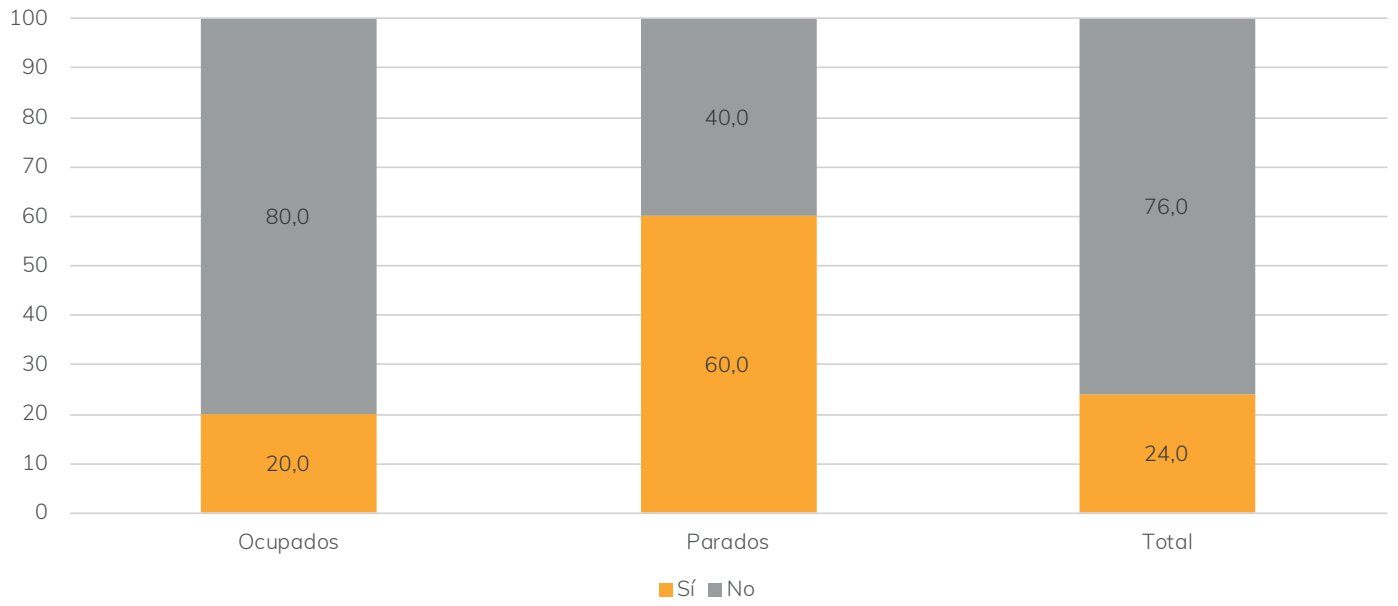
avanzada y conocimiento del mercado. Con este mismo perfil multidisciplinar, hay que hacer referencia a una profesión que empieza a tener un fuerte auge con la plena aplicación del Reglamento Europeo de Protección de Datos a partir del pasado 25 de mayo: el delegado de protección de datos, que está llamado a ser en el ámbito empresarial una figura clave en el nuevo sistema de gestión y protección de los datos personales que articula el Reglamento General de Protección de Datos (RGPD) y, en esa medida, resulta un factor fundamental para facilitar el cumplimiento de la normativa mediante la aplicación de herramientas de rendición de cuentas (tales como facilitar o llevar a cabo evaluaciones de impacto y auditorías de protección de datos), para actuar como intermediario entre las distintas partes (autoridades supervisoras, interesados y unidades de negocio dentro de las organizaciones), y, en definitiva, para garantizar la confianza de los interesados en su relación tanto en las actividades del sector público como del privado.

Pero no todos los empleos relacionados con la revolución de las tecnologías de la información son totalmente nuevos. Existen algunos trabajos tradicionales que se han adaptado a este fenómeno, produciendo nuevos perfiles laborales relacionados con esta actividad. Un ejemplo de este tipo de trabajadores son los expertos jurídicos en medios digitales, también conocidos como abogados TIC. Tienen un profundo conocimiento de la normativa legal referente al sector, por lo que son muy demandados por las empresas tecnológicas para ofrecer asesoramiento legal.

Pero a pesar de las oportunidades de expansión del empleo que ofrecen las tecnologías TIC, no todas las empresas confían en que estas tecnologías permitan crear empleo en sus empresas en el corto plazo. Así se ve reflejado en un informe realizado por el portal de búsqueda de empleo InfoJobs junto con la Escuela Superior de Administración y Dirección de Empresas (ESADE). En él, se pregunta a una muestra de 714 responsables de reclutamiento de distintas empresas si piensan que la automatización y el desarrollo de nuevas tecnologías pueden implicar la creación de puestos de trabajo en su empresa durante los próximos cinco años. Los resultados de esta encuesta nos revelan que un 46 por ciento de los entrevistados pensaban que sí se crearían nuevos puestos de trabajo tecnológicos en sus empresas, mientras que un 54 por ciento opinaba que no sería así.

Gráfico 20
¿Crees que la automatización y el desarrollo de las nuevas tecnologías pueden poner en peligro tu puesto de trabajo?

Fuente
Informe InfoJobs ESADE. Estado del mercado laboral en España



2. La percepción de los españoles sobre los cambios en el empleo debido a las tecnologías TIC

Tras haber hecho un breve repaso de las dos caras de la moneda que supone para el mercado laboral el avance de las tecnologías de la información y la comunicación, cabe preguntarse ahora: ¿cuál de los dos efectos, creación y destrucción de empleo, tendrá una mayor intensidad? Es decir, hasta qué punto piensan los ciudadanos españoles que la destrucción de empleo puede superar a la creación de este en un futuro, o viceversa.

Una buena guía para profundizar en esta cuestión son los datos del informe sobre la 'Percepción social de la innovación en España', realizado por Sigma Dos –empresa de investigación de los mercados y la opinión pública– para la Fundación Cotec –que promueve la innovación como motor de desarrollo económico y social–. En este informe, que se nutre de los datos de una encuesta realizada a 2.400 personas mayores de 18 años residentes en España, se realiza una pregunta

Gráfico 21
El cambio tecnológico (automatización, robotización, etc.) supondrá la desaparición de puestos de trabajo. Pero ¿cree usted que esta pérdida de puestos de trabajo se compensará con la creación de otros nuevos?

Fuente
Informe sobre la Percepción social de la innovación en España. Fundación Cotec. Sigma Dos

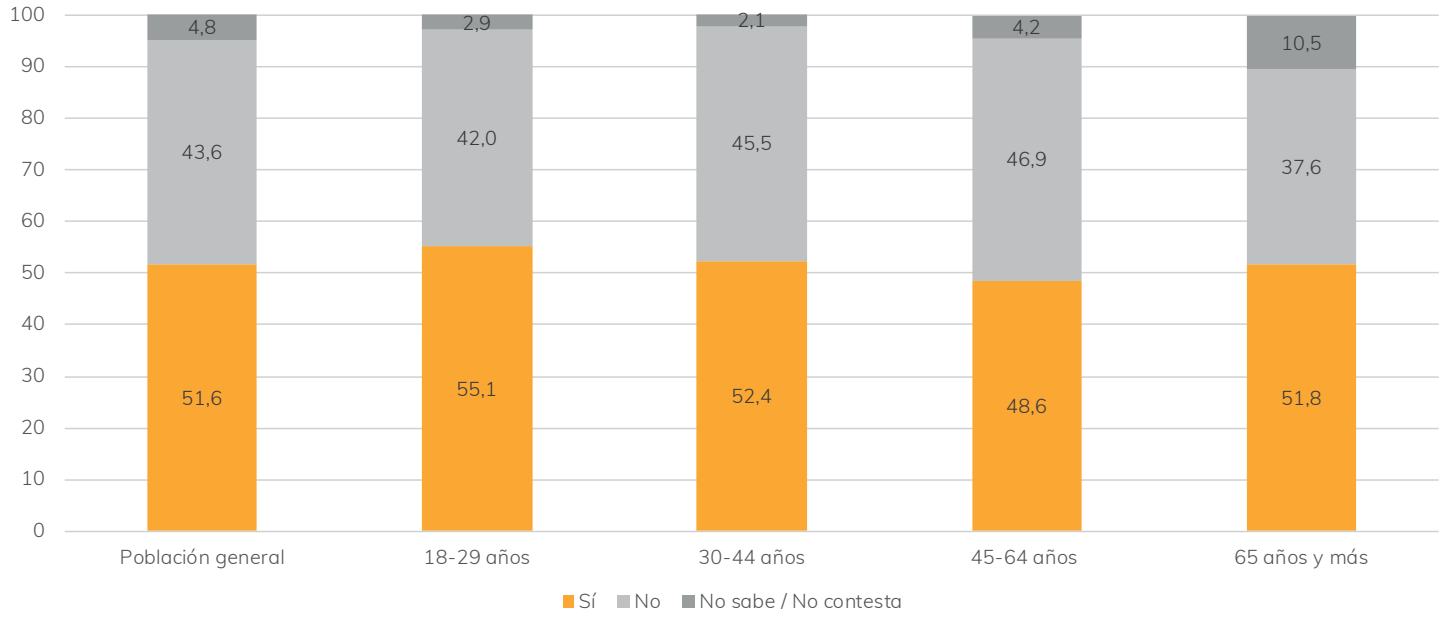
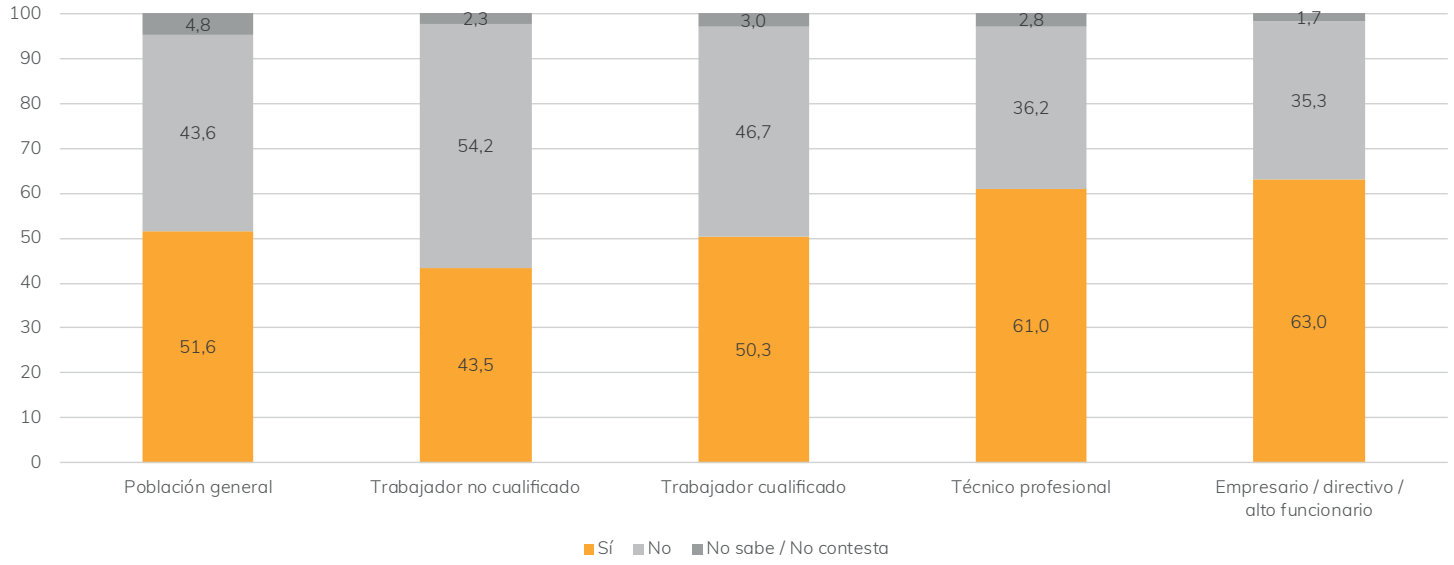


Gráfico 22
El cambio tecnológico (automatización, robotización, etc.) supondrá la desaparición de puestos de trabajo. Pero ¿cree usted que esta pérdida de puestos de trabajo se compensará con la creación de otros nuevos?

Fuente
Informe sobre la Percepción social de la innovación en España. Fundación Cotec. Sigma Dos

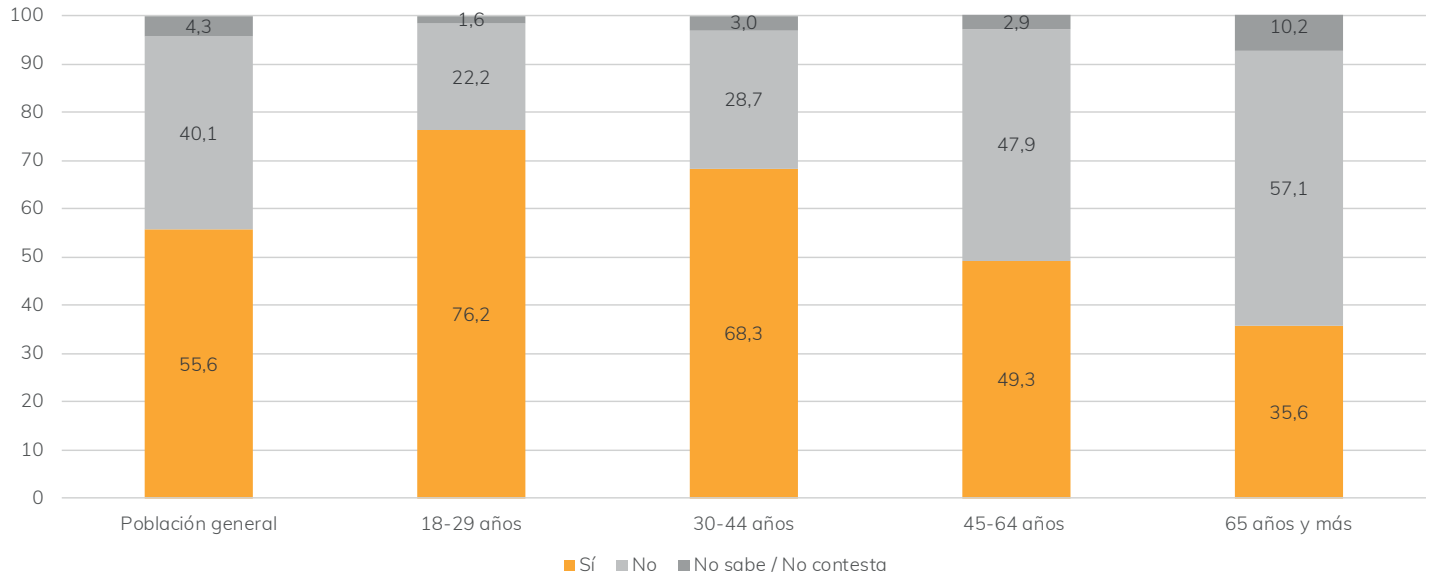


acerca de si se piensa que la pérdida de puestos de trabajo debidos al cambio tecnológico se compensará con la creación de nuevos empleos. Los resultados indican que la sociedad española es ligeramente optimista en este sentido: un 51,6 por ciento pensaba que la pérdida de empleos se compensaría con la creación de otros nuevos, mientras que un 43,6 por ciento pensaba que no sería así. Por rangos de edad, los más optimistas son los ciudadanos más jóvenes: un 55,1 por ciento de las personas entre 18 y 29 años opinaba que la pérdida de empleos se terminaría compensando, mientras que este porcentaje baja al 48,9 por ciento entre las personas de entre 45 y 64 años.

Por otro lado, también resulta interesante analizar estos datos fijándonos en las categorías profesionales de los entrevistados. De esta manera, se puede observar cómo los trabajadores no cualificados son claramente pesimistas acerca de la futura creación de empleos netos derivados de la robotización y la automatización. Entre este grupo, tan solo un 43,5 por ciento pensaba que la destrucción de trabajo se vería compensada con la creación de nuevos puestos, mientras que un 54,2 por ciento opinaba lo contrario. En contraste con este grupo, encontramos al de los empresarios, directivos y altos funcionarios, que son los más optimistas de cara al futuro. Un 63 por ciento de ellos piensa que la

Gráfico 23
¿Se considera capacitado para competir en un mercado laboral automatizado y con fuerte presencia de las tecnologías de la información y la comunicación?

Fuente
Informe sobre la Percepción social de la innovación en España. Fundación Cotec. Sigma Dos

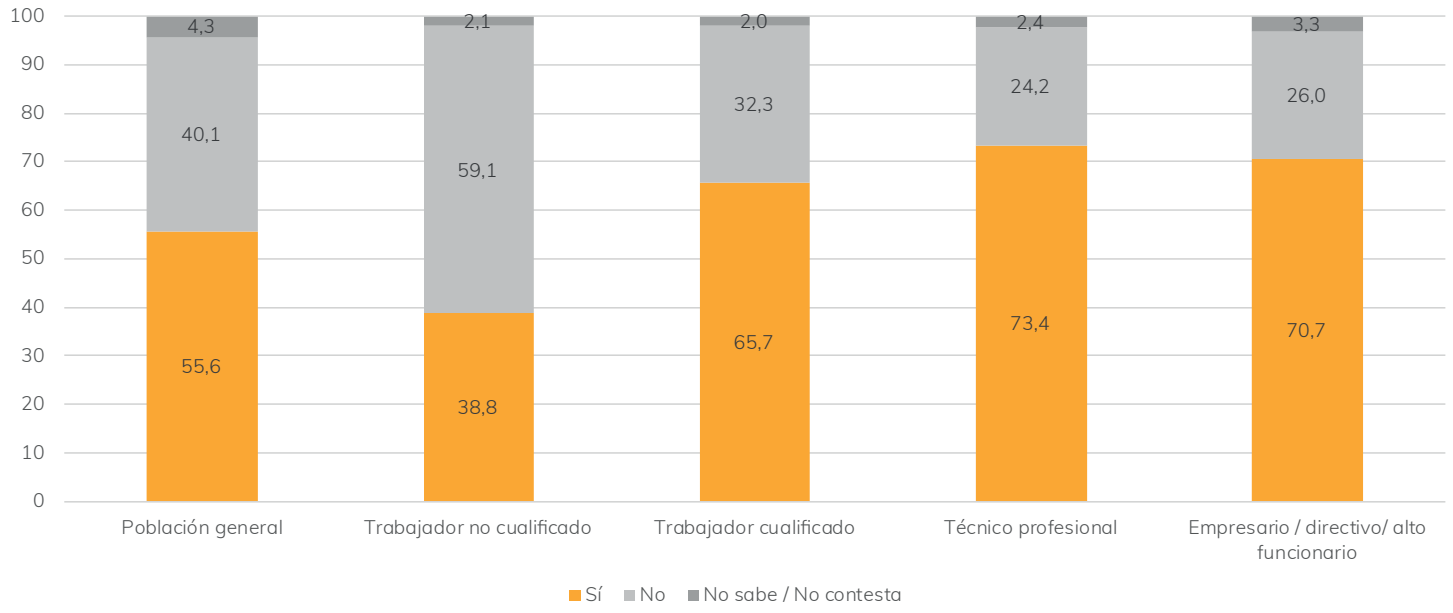


robotización sí tendría un efecto positivo en términos de creación de empleo neto, mientras que tan solo un 35,3 por ciento opinaba que se destruiría más empleo del que se crearía.

Este informe aporta más datos interesantes acerca de las percepciones que tienen los españoles respecto al futuro del mercado laboral. Otra pregunta que se les realizaba a los participantes de la encuesta era si se consideraban capacitados para competir en un mercado laboral automatizado y con fuerte presencia de las tecnologías TIC. Más de un 55 por ciento de entrevistados afirmaba que sí se encontraba capacitado, mientras que un 40,1 por ciento afirmaba que no. Por rangos de edad, eran los jóvenes los que más capacitados se veían para competir en este mercado: más de tres de cada cuatro de ellos afirmaban que así lo creían, mientras que tan solo un 22,2 por ciento pensaba lo contrario. Una conclusión que arroja este informe es que, cuanta más edad, menos confianza se tiene en las propias capacidades. En este sentido, los que se consideran capacitados son una clara mayoría

Gráfico 24
¿Se considera capacitado para competir en un mercado laboral automatizado y con fuerte presencia de las tecnologías de la información y la comunicación?

Fuente
Informe, Percepción social de la innovación en España. Fundación Cotec. Sigma Dos



hasta el rango de edad que incluye a las personas de 44 años, mientras que a partir de entonces y hasta los 64 años, aquellos que se consideran capacitados son prácticamente los mismos que los que no se ven con capacidad. A partir de los 65 años, la percepción de las propias capacidades para competir en un mercado automatizado es claramente menor.

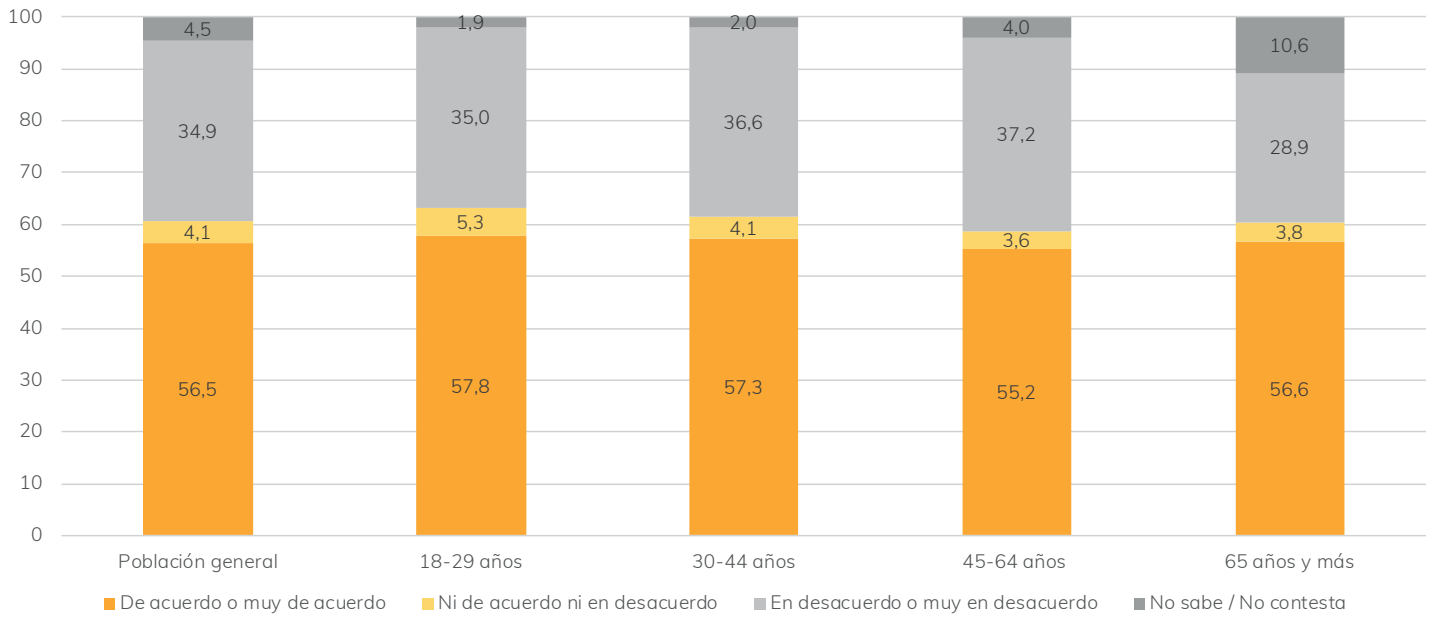
En lo que respecta a las categorías profesionales, cabe destacar que solo un grupo no se considera capacitado para competir en el futuro mercado laboral, los trabajadores no cualificados. De este grupo, tan solo un 38,8 por ciento se consideran con aptitudes suficientes para afrontar los retos de la robotización, un dato que contrasta enormemente con las respuestas de los trabajadores cualificados, los técnicos profesionales y los empresarios, directivos y altos funcionarios, donde la respuesta sí es mucho mayor que la del no.

Finalmente, cabe destacar que el optimismo en el terreno laboral de la sociedad española contrasta con la opinión acerca del efecto de la innovación tecnológica

en la desigualdad social. Mientras que, por lo general, los ciudadanos opinan que el cambio tecnológico brindará más empleos de los que destruirá y, se consideran plenamente capacitados para competir en un mercado laboral automatizado y con presencia de las tecnologías TIC, también opinan que la innovación tecnológica aumenta la desigualdad social. Así se desprende de los datos del estudio citado anteriormente, un 56,5 por ciento de los españoles ve a la tecnología como una de las causas del aumento de la desigualdad, mientras que un 34,9 por ciento no opina de este modo. Respecto a esta cuestión, no parecen existir grandes diferencias entre distintos grupos de edad: esta opinión se sitúa como más mayoritaria entre los jóvenes de 18 a 29 años, y más minoritaria entre los ciudadanos de 45 a 64 años, por lo que entre ambos grupos tan solo existe una diferencia de 2,6 puntos porcentuales.

Gráfico 25
La innovación tecnológica aumenta la desigualdad social

Fuente
Informe, Percepción social de la innovación en España. Fundación Cotec. Sigma Dos



VII. Conclusiones

Si cada época tiene sus retos, uno de los mayores, si no el mayor, al que nos enfrentamos hoy es el ritmo con el que avanza y se reinventa la tecnología de la información y de la comunicación. Pone a prueba la capacidad de adaptación y de respuesta de todas las instancias políticas, sociales y económicas, a las que ya integra e interconecta de manera ineludible. La era de la información es también la era de la velocidad. Todo es importante, todo es urgente, todo es cambiante.

Entretanto, los usuarios de las plataformas digitales redescubrimos nuestra identidad, así como nuevas maneras de converger con otros individuos o grupos de manera simultánea. La facilidad que representa este creciente modo de interactuar no lo exime de peligros, por lo que las autoridades están en el punto de mira del ciudadano, como responsables de garantizar la seguridad frente a riesgos que apenas hemos empezado a comprender.

Queda mucho por descubrir y experimentar, y la percepción de la población nos muestra que se mantienen ciertas formas de cautela, al tiempo que se disfruta y se saca el máximo provecho a las nuevas herramientas digitales y todo el potencial que nace con ellas.

Lo expuesto en este capítulo, cómo afecta a la sociedad un crecimiento tecnológico inevitable, es una realidad compleja pero estimulante. La variedad de cuadros que aparecen en él sirve para definir muchos matices, los que albergan un sinfín de segmentos, tendencias e inquietudes, y supone una radiografía del escenario en el que nos moveremos de aquí en adelante. La revolución tecnológica llegó hace tiempo, pero se acentúa a cada paso y seguirá sorprendiéndonos.

3

La AEPD como garante de un derecho fundamental

I. Introducción

Si alguna palabra puede definir el devenir en España de la sociedad de la información, de las tecnologías de comunicaciones y del tratamiento de datos de carácter personal en los últimos 25 años, esa palabra es ilusión.

En el último cuarto de siglo hemos visto saltos tecnológicos asombrosos y todos ellos estaban guiados en el fondo por la esperanza de hacer un mundo mejor, más libre, más abierto, más justo y con mayores oportunidades para todos.

En ese periodo, muchas han sido las empresas que han surgido y muchas las que han quedado por el camino, muchos desarrollos, muchas expectativas, muchas tecnologías y aparatos, muchas dudas, muchas preocupaciones, muchas incertidumbres, sí, pero todas ellas guiadas por esa ilusión, que algunos pueden tildar de infantil o naíf, pero que hace que la humanidad, nosotros, todos, avancemos.

La Agencia Española de Protección de Datos ha participado de esa ilusión por hacer una España mejor. Una ilusión que ha animado a todos los que han trabajado en ella, guiados por la confianza de los ciudadanos, a compartir las expectativas de los empresarios, investigadores, juristas e ingenieros con los que hemos participado en proyectos de futuro.

El año en el que inició su andadura la Agencia fue un año lleno de acontecimientos relacionados con el tratamiento de la información. En 1994, la página web Hotwired lanzó el primer "banner" publicitario, lo que cambió el marketing para siempre y abrió las puertas a la monetización de los sitios web. Netscape lanzó la primera versión que soportaba cookies. Fue el año en el que se realizó la primera venta online, supuestamente una pizza, y se lanzó el portal NetMarket, el primer mercado seguro en Internet, iniciando nada menos que el comercio electrónico. También fue el año de la primera emisión de radio a través de Internet, abriendo el camino a toda la industria de streaming de audio.

Si volvemos la mirada hacia esa época, vemos una Agencia y una España que nos cuesta reconocer. A todos aquellos que tengan hijos que todavía no hayan salido de la universidad les costará explicarles cómo vivíamos en 1994. Estábamos saliendo de una crisis económica que había reducido el sector tecnológico a niveles de 1987; vivíamos en una sociedad en la que la máquina de escribir todavía dominaba muchos despachos y el único programa que se ejecutaba en la mayoría de los hogares era el de la lavadora.

Internet existía, sí, y había en España unas 20.000 máquinas registradas en el dominio ".es". Fue el momento en el que la primera página web española se asomaba a la red y había poco más de un centenar de empresas conectadas. El acceso a las comunicaciones estaba prácticamente sometido a un régimen de monopolio, con la red telefónica como única conexión y con Infovía estrenándose en 1995, lo que permitía alcanzar Internet desde los hogares. Los modem nos regalaban su música a 56 Kbps, lo que significaba tener que esperar 15 minutos para escuchar una canción de verdad. En todo el mundo sólo había 10.000 páginas de Internet, no los más de 50 billones que hay actualmente y, entre ellas, estaba la primera red social, Classmates, que nacería el año siguiente.

La primera licencia de telefonía digital GSM se otorgó en 1994 a Telefónica y menos del 2% de los españoles tenían un móvil. Un móvil, no un smartphone, aunque

por estas fechas IBM lanza el Simon, una idea, un prototipo exclusivo, que muy poco se parecía a lo que usamos actualmente.

Pero la protección de datos de carácter personal era y es mucho más que pura tecnología. En 1994 la humanidad nos enseñó otra vez su lado oscuro. Ese año, en Ruanda, cientos de miles de personas morían por ser diferentes, porque alguien las había clasificado en hutus y en tutsis, en buenos y malos, porque toda esa información, con nombres y direcciones, estaba en un registro, y toda ella se iba a utilizar para materializar el odio.

Esa tragedia nos trajo ecos del drama que vivió Europa en el siglo XX y que impulsó la Declaración Universal de Derechos Humanos. Nos recordó que el proyecto que se estaba iniciando en la Agencia Española de Protección de Datos tenía como primer objetivo evitar que esas cosas volviesen a suceder, y que teníamos como misión proteger un derecho, un derecho fundamental. Ya en sus grabados, Goya sacudía nuestras conciencias y nos avisaba *"El sueño de la razón produce monstruos"*, o, dicho de otro modo, las ilusiones, si no son compartidas, pueden convertir los sueños en pesadillas.

Y con esa voluntad de compartir ilusiones arrancaba una Agencia con treinta y tres empleados públicos. Comenzaba un viaje lleno de incógnitas, en el que hubo que desarrollar la doctrina y los procedimientos en un mundo a caballo entre lo jurídico y lo técnico. Hubo que desarrollarlo todo desde cero, innovando desde los fundamentos a los procedimientos, pasando por los sistemas de información. En esa primera etapa todo el personal se implicó en un esfuerzo de creación de la conciencia de protección de datos en una sociedad en la que esa idea era completamente nueva. Para conseguir su adecuación, su primer gran impulso fue la campaña para el registro de ficheros o, dicho de otro modo, ayudar a las entidades a realizar un esfuerzo de racionalización y control de los datos que se recogían de los ciudadanos.

Veinticinco años es un largo periodo y para recorrerlo, vamos a fijar algunos hitos. El primero nos despierta en el año 1999 con los llantos de un recién nacido llamado Google. Apple presenta el iBook, un portátil que ya no pesa once kilos, como el Osborne-1, sino tan solo tres. En ese año se multiplican los sitios web por diez, llegando casi a los treinta millones en todo el planeta, surge la tecnología P2P con una primera estrella, Napster. El término Internet de las Cosas, IoT, se acuña en este periodo y las empresas tecnológicas se dan cuenta de la oportunidad de establecer un mecanismo de conexión inalámbrica que fuese compatible entre distintos dispositivos: nace el WiFi.

El panorama en España ya ha cambiado mucho: se acababa de liberar el mercado de operadores de telefonía fija y móvil, y se llegaba hasta un centenar de autorizaciones para nuevos operadores. La primera consecuencia es que el número de móviles se multiplicó por cinco en dos años (¡llegando hasta 25.000 usuarios en el año 2000!). En televisión también se produjo una mayor liberalización y los canales disponibles se triplicaron en tres años. Retevisión ofrece el servicio de acceso a Internet de manera gratuita y se inicia el despegue de los usuarios de la banda ancha con la aprobación de la "Ley ADSL". Esto permitió que la mitad de las empresas españolas tuvieran ese año acceso a Internet, lo que da idea de la automatización de sus procesos.

Para impulsar el comercio electrónico se publicó, entre otros, la Ley de Firma Electrónica, y como no podía

ser de otra forma, recordamos la aprobación de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, LOPD, que ha sido la norma sobre la que se ha desarrollado la protección de los derechos fundamentales en la sociedad de la información en los últimos 20 años... o casi.

Pero, a veces, cuanto más se eleva el espíritu humano, más larga es la sombra que proyecta. En Kosovo miles de personas son asesinadas y millones tienen que huir de sus hogares en los últimos estertores de la desintegración de un país. De nuevo, hay alguien que etiqueta a las personas y utiliza los registros que, creados para la convivencia, alimentan el enfrentamiento. Parece que en Europa seguimos sin aprender.

Por entonces la Agencia Española de Protección de Datos ya está formada por más de sesenta profesionales que afrontan un nuevo marco normativo, más maduro, y se enfrentan a un nuevo modelo de Sociedad de la Información, cuyo centro de gravedad se desplaza desde las grandes bases de datos corporativas al tratamiento realizado por pequeñas empresas cada vez más conectadas a Internet.

Alrededor del año 1999 es cuando la Agencia da un paso hacia adelante e inicia, de forma sistemática, lo que se denominarán los Planes de Inspección de Oficio, es decir, la aproximación a la realidad de los distintos sectores de negocio para, mediante un trabajo conjunto, implementar la protección efectiva de los derechos de los ciudadanos. Esta actividad culminará más tarde con los grandes planes en los sectores hospitalario y educativo. Con la misma ilusión de dar una respuesta más eficiente a las necesidades de los ciudadanos, se implementa el procedimiento de tutela de los derechos fundamentales.

Si tenemos que buscar otro hito significativo antes de llegar a nuestros días este es, sin dudarlo, el año 2007: el año de la presentación del iPhone.

iPhone significa el principio de un nuevo modo de entender la vida, un modelo de comunicación y de interacción social que se copiará y que sigue vigente hasta ahora. En España, actualmente, el 90% de los jóvenes depende de un smartphone para su vida diaria. Tiene sentido que, tan solo unos meses después, surja Whatsapp, y con ello, muera el SMS como forma de comunicación. En ese año culmina la consolidación de los grandes actores del mercado global de la información, sobre todo Google, tras haber adquirido servicios como Android y Youtube. Ya el año anterior nacía Amazon Web Services y el siguiente Google App Engine, lo que materializaba el mercado de la tecnología Cloud o Computación en la Nube, que había iniciado su camino en el año 2000. En paralelo, surge Netflix.

Ese mismo año inicia sus actividades Wikileaks y se empiezan a producir las filtraciones masivas de información. El año anterior se había producido la mayor filtración de datos hasta el momento, 94 millones de tarjetas de crédito quedaron expuestas por un sistema de cifrado ineficiente de la compañía TJX. Anonymous intensifica sus actividades y el escándalo Snowden vendría pocos años después. Todos estos sucesos hacen que los ciudadanos sean más conscientes del peligro de la acumulación masiva de datos en manos de multinacionales y Estados, sobre todo en archivos accesibles desde Internet, y de la fragilidad de la seguridad de la información.

En el año 2007 la mitad de los hogares de España tenía ordenadores e Internet en casa. Existían diez millones de usuarios de redes sociales en nuestro país:

MySpace empieza a agonizar en favor de Facebook, que confirma su ascenso y Twitter se encuentra en su segundo año. Las empresas del sector TIC en España se han duplicado hasta más de 50.000. El 94% de las empresas ya tenía acceso a Internet y, además, con banda ancha. Se extienden de forma masiva nuevas formas intrusivas de tratamiento de datos, en particular los sistemas de videovigilancia, y los ciudadanos dejan de ser sujetos pasivos de los datos y se convierten en elementos activos de la Sociedad de la Información.

A finales de 2007 se publica el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos, aprobado por Real Decreto 1720/2007. En él se establecen los principios para una protección más racional y para una respuesta más ágil por parte de la Agencia. Las reclamaciones de los ciudadanos crecen y pasan de algo menos de dos mil en 2006 a más de siete mil en 2009; más del doble que las acumuladas en los primeros diez años de existencia de la Agencia. También se duplican los procedimientos sancionadores, hasta superar los seiscientos por año y se inician hasta 160 actuaciones de oficio en cuatro años.

Para afrontar estas nuevas necesidades, la Agencia tuvo que reinventarse: duplicó su personal respecto a 1999, implantó nuevos procedimientos, mejoró la respuesta al ciudadano y potenció las actividades de concienciación con la elaboración de guías e informes que interpretan jurídicamente las nuevas tecnologías. Su personal tuvo que adaptarse a estos nuevos desafíos aumentando su productividad y liderando programas internacionales.

Para finalizar, demos un salto hasta el día de hoy. 2018 es un año marcado por la aplicación efectiva del Reglamento General de Protección de Datos de la Unión Europea, pero también por los desafíos que suponen el blockchain, el iHealth, el IoTA, Edge Computing, la realidad inmersiva .... Tal vez nada puede describir mejor el carácter de esta etapa que la siguiente cita:

"Era el mejor de los tiempos y era el peor de los tiempos; la edad de la sabiduría y también de la locura; la época de las creencias y de la incredulidad; la era de la luz y de las tinieblas; la primavera de la esperanza y el invierno de la desesperación. Todo lo poseíamos, pero nada teníamos; íbamos directamente al cielo y nos extraviábamos en el camino opuesto ..."

C. Dickens "Historia en dos ciudades"

Y la Agencia Española de Protección de Datos solo podrá acometer con éxito los nuevos retos de una forma: con ilusión.

Mandatos de los Directores de la AEPD

Juan José Martín-Casallo López (de 1993 a 1998). Nombramiento RD de 22 de octubre de 1993. BOE 23 de octubre de 1993.

Juan Manuel Fernández López (de 1998 a 2002). Nombramiento RD de 27 de marzo de 1998. BOE 31 de marzo de 1998.

José Luis Piñar Mañas. De 2002 a 2007. Nombramiento RD de 8 de noviembre de 2002. BOE 9 de noviembre de 2002.

Artemi Rallo Lombarte. De 2007 a 2011. Nombramiento RD de 23 de febrero de 2007. BOE de 26 de febrero de 2007.

José Luis Rodríguez Álvarez. De 2011 a 2015. Nombramiento RD de 17 de junio de 2011. BOE 18 de junio de 2011.

Mar España Martí. Desde 2015 hasta la actualidad. Nombramiento RD de 24 de julio de 2015. BOE 25 de julio de 2015.

II. Los inicios de la Agencia (1993-1999)

Ya la Constitución de 1978 intuyó la magnitud potencial de las nuevas tecnologías y el desarrollo imparable de los medios de comunicación, al disponer en su artículo 18.4: *"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*.

El Consejo de Europa había previsto en el Convenio 108 de 1981 la existencia de una autoridad independiente que velase por este derecho.

Pero fueron necesarios 14 años para que esa previsión constitucional tuviera un desarrollo normativo. En octubre de 1992 se aprueba por el Congreso de los Diputados la Ley Orgánica 5/1992, de 29 de octubre, de Tratamiento Automatizado de Datos de Carácter Personal, LORTAD, que crea la Agencia de Protección de Datos. Hasta la llegada de esta ley, fue la institución del Defensor del Pueblo la que se encargó de resolver las cuestiones relacionadas con la protección de este derecho fundamental.

La Ley crea también el Consejo Consultivo como órgano colegiado de asesoramiento de la dirección de la Agencia, compuesto por diez miembros nombrados por un período de cuatro años.

España se adelantó así tres años a la configuración internacional de este tipo de instituciones.

En aquellas fechas, no existía apenas el teléfono móvil, el ordenador personal era un artículo de lujo que convivía con las máquinas de escribir, mientras que la televisión estaba expandiéndose.

Se conocía la existencia de Internet, pero no era una herramienta de uso generalizado. Las personas, sobre todo cuando estaban lejos unas de otras, se escribían cartas; a mano las personales y a máquina las de trabajo, que se enviaban por Correos y tardaban varios días en llegar a su destinatario.

Si en los años 70 la televisión era todavía un artículo de lujo, que no podían permitirse todos los hogares, en los 80 se produjo su generalización como electrodoméstico habitual en los hogares. Había una televisión en todos los hogares. Eran aquellas televisiones con forma de caja enorme, con las que había que levantarse para ir a darle al botón de subir el volumen o para cambiar el canal.

Tras los primeros años en los que las emisiones eran en blanco y negro, a finales de los años 80 se extendió la televisión en color. Pero subrayemos: había una televisión, en el salón de las casas. Los canales generalistas eran cuatro: dos emitidos por RTVE y dos cadenas privadas. No había emisión las 24 horas del día, y la interacción social que generaba la televisión eran los comentarios que se suscitaban entre las personas, dentro de la propia casa o al día siguiente en el trabajo o en la calle.

Se veía el telediario de mediodía o el de por la noche, que muchos llamaban "el parte", y las películas eran los clásicos del cine estadounidense. La programación infantil tenía un protagonismo muy marcado; los niños veían *Barrio Sésamo* y *Érase una vez la vida* y todos los fines de semana la primera película después del telediario de las tres era apta para menores.

A mediados de los noventa la programación adulta se encamina hacia nuevos formatos, surgen nuevos tipos de programa, nuevos discursos políticos y sociales en los análisis y las tertulias. Se podía interactuar a distancia con los programas de la tele a través de concursos en los que se participaba por carta.

Esta era la vida cotidiana cuando la Agencia Española de Protección de Datos comenzó su andadura en 1993.

La Agencia se creó como ente público independiente, con presupuesto propio aunque integrado en los Presupuestos Generales del Estado, y con plena autonomía para el desempeño de sus competencias.

El Estatuto de la Agencia fue aprobado por el Real Decreto 428/1993, de 26 de marzo. En él se recogieron sus competencias, su estructura orgánica, las funciones del Director y del Consejo Consultivo, el funcionamiento del Registro General de Protección de Datos, y el régimen económico, patrimonial y de personal.

La Agencia se estructuró en la Inspección de Datos, el Registro General de Protección de Datos, la Secretaría General y una Unidad de Apoyo.

La Inspección de Datos realizaba las funciones de inspección y de instrucción necesarias para el ejercicio de los poderes de investigación y correctivos atribuidos a la Agencia, en el marco de la supervisión permanente del cumplimiento de la normativa por parte de los responsables y encargados de los tratamientos.

El Registro General de Protección de Datos inscribía y daba publicidad a los ficheros públicos y privados, promovía y registraba los códigos de conducta, y tramitaba las autorizaciones de transferencias internacionales de datos.

Por su parte, la Secretaría General tenía encomendada la gestión económica y de personal, daba soporte a las demás unidades y gestionaba los asuntos no atribuidos a otras unidades.

Unos meses después de aprobarse el Estatuto, concretamente el 23 de octubre de 1993, tiene lugar el nombramiento del primer director de la Agencia, D. Juan José Martín-Casallo López.

Es en ese momento cuando se procede a dotar a la Agencia de la necesaria infraestructura y de los correspondientes medios materiales y personales. Pero enseguida se vio la necesidad de contar con un mayor número de efectivos, principalmente personal altamente especializado para el desempeño de las funciones inspectoras e instructoras que la Ley Orgánica le atribuyó, motivo por el cual, en 1994, se amplió la plantilla a 49 puestos de trabajo.

Hasta mayo de ese año, la Agencia ocupó, en régimen de arrendamiento, unas instalaciones cedidas por el Ministerio de Justicia, en concreto, las plantas tercera, cuarta y quinta del edificio del número 41 del Paseo de la Castellana de Madrid.

1. El Registro General de Protección de Datos

En el momento de inicio de su actividad, la prioridad de la Agencia Española de Protección de Datos fue la creación y organización del Registro General de Protección de Datos.

La finalidad fundamental de la creación del Registro y del establecimiento de la obligación de notificar e inscribir los ficheros era facilitar a cualquier ciudadano el acceso de manera gratuita a la información contenida en esas bases de datos. De esta manera, los ciudadanos podían identificar a los titulares de los ficheros en los que se hubieran incluido sus datos personales, y conocer la dirección de contacto de sus responsables, las finalidades para las que se utilizaría la información, el tipo de datos incorporados a los mismos y las cesiones y transferencias internacionales de datos previstas. Y, una vez identificados podían ejercer su derecho de acceso para conocer si estaban incluidos o no en ellos y, en caso afirmativo, qué información se había incorporado.

Así, si una persona descubría que estaba incluida en un fichero de morosidad al acudir a una entidad financiera para solicitar una tarjeta de crédito o financiación para la compra de un vehículo, podía acudir a la Agencia y pedir información de forma gratuita sobre los ficheros de morosidad existentes. Una vez conocidos los titulares de los ficheros, podía ejercer su derecho de acceso ante ellos para obtener información sobre si efectivamente estaba registrado o no. Y, en caso de estarlo, para identificar en cuáles figuraba, qué entidad la había calificado como moroso y comunicado su incorporación al fichero, por qué cuantía de deuda, así como otro dato especialmente relevante como son las evaluaciones y apreciaciones sobre riesgos del afectado que se hubieran realizado en los últimos seis meses, y el nombre y la dirección de aquellos a los que se las hubieran comunicado.

Si el afectado consideraba que esa inclusión era ilícita, bien por no haber tenido relación con el presunto acreedor, o bien aun teniéndola por carecer de deudas pendientes, podía ejercer el derecho de cancelación tanto ante el titular del fichero de morosidad, como ante la entidad que hubiera suministrado la información incluida en el fichero, una entidad financiera por

ejemplo, para que la excluyeran. Y, en caso de que no se atendiera la solicitud de exclusión de los datos del fichero, el particular podía plantear una reclamación ante la Agencia para que se investigara y, en su caso, se sancionara al infractor y se eliminara la información sobre morosidad ilícitamente incluida en el fichero.

A tal fin, se celebraron reuniones, presentaciones y jornadas informativas con numerosas organizaciones públicas y privadas. También mediante información telefónica y postal. Aunque en los inicios el proceso de inscripción se realizaba en gran parte en papel, se desarrolló en cuatro semanas la aplicación informática para la notificación de los ficheros al Registro y se distribuyeron diskettes para la grabación e inscripción de los ficheros por los responsables, a través de la red de estancos de TABACALERA, S.A.

Así, se procedió a la inscripción masiva de ficheros, que supuso que entre junio y julio de 1994 se inscribieran más de 200.000 ficheros de más de 100.000 empresas privadas y la mayor parte de los ficheros de la Administración General del Estado; una cifra que continuó incrementándose hasta alcanzar los 5.094.312 ficheros al cierre del Registro, como consecuencia de la plena aplicación del Reglamento europeo de protección de datos.

2. Las primeras consultas

A medida que mejoraba el conocimiento de los ciudadanos sobre sus derechos, se incrementaban las consultas sobre cómo conocer la identidad de los titulares de ficheros y sobre cómo garantizar su ejercicio.

Desde los inicios, la Agencia Española de Protección de Datos ha tenido encomendada la tarea de proporcionar información a los ciudadanos acerca de sus derechos en relación con el tratamiento de sus datos personales.

Por este motivo, en abril de 1994 comenzó a funcionar el Área de Atención al Ciudadano, que prestaba información telefónica, presencial y contestaba a las consultas por escrito.

Ello, no obstante, en ese primer momento los esfuerzos de la Agencia se concentraron en informar a los responsables de los tratamientos, por lo que el impacto informativo sobre la ciudadanía fue menor, lo que se tradujo en un nivel relativamente bajo de conocimiento de los derechos y posibilidades de ejercicio de éstos que la Ley y la Agencia les ofrecía.

Superado este momento inicial, se produjo un incremento lento pero paulatino del número de consultas ciudadanas.

Si se comparan los datos del inicio del periodo con los del final, se observa una estabilidad en cuanto al número de consultas atendidas a lo largo de estos años. Así, en 1995 se resolvieron casi 10.000 consultas telefónicas, más de 1.500 presenciales y 598 por escrito, mientras que en el año 1999 se contestaron 11.500 consultas telefónicas, 1.150 presenciales y 1.739 por escrito.

En cuanto a las cuestiones objeto de consulta, se distinguen tres temas principales: el ejercicio de los derechos previstos en la Ley, la consulta sobre ficheros concretos y la cesión de datos, perdiendo éste último peso de forma progresiva en favor de otros temas como la información general de la Agencia o la información sobre inscripciones en el Registro.

- En relación con el ejercicio de derechos, se observa una clara tendencia ascendente, pasando esta cuestión de representar el 25% de las consultas en el año 1996 a un 50% en el año 1999. En concreto, los derechos sobre los que más frecuentemente se pregunta son los de acceso y los de cancelación. Lo que significa que, en estos primeros momentos, la principal preocupación de los ciudadanos era la de conocer quién disponía de su información y cómo conseguir suprimirla.

- En cuanto a la consulta sobre ficheros concretos, son los ficheros de solvencia patrimonial los que más preocupan a la ciudadanía, y de manera creciente a lo largo del periodo, pasando de representar un 38% del total en 1996 a un 70% en 1999.

- Las consultas en este periodo se centran en la identidad del responsable y en los derechos de acceso, rectificación y en especial en el derecho de cancelación, dado que al ciudadano lo que le preocupa fundamentalmente es hallar la forma de no figurar en este tipo de ficheros.

- Tras éstos, los siguientes en importancia en cuanto al volumen de consultas son los ficheros con fines de publicidad. La petición más frecuente manifestada ante la Agencia es el deseo de no recibir información comercial no solicitada remitida por empresas con las que el afectado carece de relación previa. Se recomienda el ejercicio del derecho de exclusión de los repertorios de abonados de Telefónica y otras empresas del sector, que tienen el carácter de fuente accesible al público y pueden ser utilizados con fines de publicidad.

- Respecto a las consultas relacionadas con las cesiones de datos, en su mayoría tienen que ver con cesiones entre Administraciones Públicas que, con frecuencia se encuentran previstas por las leyes, o con cesiones de datos procedentes de los censos fiscales de las entidades locales, entre otras.

3. Las primeras denuncias y reclamaciones. Las primeras inspecciones

La Agencia comenzó gestionando un número relativamente pequeño de denuncias, y actualmente recibe miles de reclamaciones todos los años. Algunas de ellas, relativas a tratamientos realizados por grandes empresas, afectan a los más de 4.000 millones de usuarios de Internet. En los apartados siguientes veremos con más detalle cómo la Agencia se ha ido adecuando a la evolución de la sociedad española y a sus demandas.

Los primeros escritos que contenían reclamaciones o denuncias en materia de protección de datos se remontan a finales del año 1993, pero no sería hasta el año siguiente cuando comenzaría la actividad significativa de la Subdirección General de Inspección de Datos.

Mientras que en 1994 se tramitaron 81 reclamaciones, sólo cinco años después ya se habían resuelto 195 procedimientos de tutela, 110 de carácter sancionador y 25 por infracción de las Administraciones Públicas, lo que da idea del aumento tan significativo producido en un período tan corto de tiempo. Coincidiendo con la finalización del plazo de inscripción de ficheros en el Registro General de Protección de Datos es cuando la Agencia comienza a tener una actividad importante en materia de tutela de derechos e instrucción de expedientes sancionadores.

Las denuncias y solicitudes de tutela de ese primer período muestran que las preocupaciones de los ciudadanos giraban en torno a los datos de naturaleza económico-financiera y, entre ellos, especialmente, los relativos a la solvencia, el crédito y la morosidad. El segundo lugar lo ocupan las relativas a la publicidad directa, y después, las referentes a entidades financieras y las que atañen a Administraciones Públicas. Los denunciados mayoritariamente eran entidades o personas radicadas en Madrid, y en segundo lugar, en Barcelona.

Destaca la preocupación del ciudadano por estar incluido en un fichero de morosidad por los importantes efectos que tiene en la vida financiera de las personas, dado que, como consecuencia de esta inclusión, se puede producir una restricción importante en las posibilidades de acceso a cualquier tipo de crédito o padecer restricciones en la contratación de otros servicios básicos como los de telefonía por ser los operadores de los mismos uno de los principales suministradores de información a estos ficheros.

Para minimizar estos efectos, y reforzar las garantías de los ciudadanos, la Agencia elaboró unas Instrucciones relativas a los ficheros de solvencia patrimonial y crédito.

De otra parte, a pesar del número inicialmente reducido de reclamaciones sobre datos sensibles, la Agencia ha tenido un especial interés por el tratamiento de los datos de salud. Así, durante 1995 se realizan las primeras inspecciones de oficio a establecimientos hospitalarios, actuaciones que han continuado a lo largo de los años, especialmente las relacionadas con el acceso a la historia clínica, a las que se aludirá en apartados posteriores.

Si se comparan las cifras del año 1998 con las del ejercicio precedente, se observa que el número de denuncias recibidas disminuyó, debido al descenso en el número de denuncias en los sectores que tradicionalmente han tenido una mayor incidencia en la entrada de reclamaciones: solvencia patrimonial y crédito (218 en 1997 frente a 148 en 1998), entidades financieras (84 frente a 58) y publicidad directa (126 en 1997 frente a 100 en 1998).

Este descenso hay que atribuirlo no sólo a la labor que había venido realizando la Agencia, sino también al progresivo conocimiento de la legislación de protección de datos por las empresas de los sectores mencionados. Esta circunstancia propició que se establecieran procedimientos para garantizar una mejor atención de los derechos de los ciudadanos, especialmente los de acceso, rectificación y cancelación.

Por otro lado, disminuyeron las denuncias que hacían referencia a la utilización de datos procedentes del censo electoral en campañas de publicidad. También se redujo en la misma proporción la constatación por parte de la Agencia de la utilización de dicho fichero para la elaboración de listas de destinatarios de publicidad.

En este período se realizaron diversas inspecciones sectoriales para conocer en profundidad el estado y grado de cumplimiento de la normativa sobre protección de datos personales en determinados sectores de actividad, con el fin último de realizar una política preventiva que garantizase mejor los derechos de los ciudadanos.

En esta línea, en el año 1997 se revisaron los ficheros de varias Policías Locales y en 1998 se revisaron en profundidad los sistemas de información de Telefónica, dentro de un plan más ambicioso que se iría completando con otros operadores de telecomunicaciones.

También se revisaron exhaustivamente los sistemas de las mayores entidades dedicadas a la información sobre solvencia patrimonial y crédito y una muestra de las más grandes compañías aseguradoras españolas.

Asimismo, se revisó la Oficina SIRENE española, órgano de colaboración policial establecido en el marco del Convenio de Schengen y se procedió a la inspección de diversas salas de bingo.

También en 1998 y 1999 se llevaron a cabo los Planes de Inspección a grandes compañías aseguradoras, a la Agencia Estatal de Administración Tributaria, a la Dirección General de Tráfico y al sector de investigación privada. Y, en el ámbito de la salud, a los hospitales psiquiátrico de Foncalent y militar Gómez Ulla, y al Centro Nacional de Epidemiología.

Por último, en 1999, hay que destacar la realización de un plan de inspección de oficio específico en el Sector de las Telecomunicaciones, de modo que las inspecciones ya realizadas al sector respecto del cumplimiento de la LORTAD, se van a ver ampliadas ahora en relación con el cumplimiento de la nueva normativa de protección de la intimidad en el sector de las telecomunicaciones. Así, el art. 50 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, establecía que los operadores que presten servicios de telecomunicaciones al público o exploten redes de telecomunicaciones accesibles al público deberán garantizar, en el ejercicio de su actividad, la protección de los datos de carácter personal, conforme a lo dispuesto en la legislación en materia de protección de datos.

III. La dimensión constitucional del derecho. Los nuevos retos de la privacidad: las comunicaciones electrónicas (1999-2007)

En 1999 nace el euro, pero no sería hasta el año 2002 cuando sustituye oficialmente a la peseta. El empleo de una moneda común facilitaba el intercambio de bienes y servicios, el uso de macrosistemas de información y la elaboración de estadísticas referenciadas a un índice común.

En esta época la tecnología ya había conseguido que las televisiones fuesen mucho más pequeñas y planas, y considerablemente más baratas, por lo que había varias en cada casa.

Proliferaron los programas en los que se requería la participación "en directo" de los espectadores, bien mediante llamada telefónica, bien mediante el envío de SMS, ya fuere para conocer la opinión de los espectadores, ya para votar por la canción favorita o para recaudar dinero para alguna causa solidaria.

También se incrementaron los programas en horario nocturno y de madrugada. Como herramienta interactiva la televisión disponía del teletexto, que permitía buscar la guía de la programación, consultar la previsión meteorológica y hasta algunos horóscopos.

A partir de finales de los noventa se generaliza el uso del teléfono móvil. Unos móviles que servían para llamar, y mandar breves mensajes de texto (SMS). Nada más -y nada menos-. No se podían conectar a Internet, pero a partir de ese momento, se podía estar localizable las 24 horas del día.

Un hecho significativo que merece la pena mencionar en este periodo, es el efecto producido por el Reglamento de Medidas de Seguridad, aprobado por el Real Decreto 994/1999, de 11 de junio, estando ya D. Juan Manuel Fernández López al frente de la Agencia.

El Reglamento preveía una exigencia escalonada de los tres niveles de medidas de seguridad que establece, disponiendo que las medidas de nivel básico, es decir aquellas exigibles a todo fichero de datos, fuesen eficaces con fecha 26 de diciembre de 1999 (luego prorrogado hasta marzo del año siguiente). Ello supuso un notable incremento de actividad en la Agencia a finales de año para responder a las peticiones de los ciudadanos y una repercusión en el aumento de las inscripciones de ficheros en el Registro General de Protección de Datos.

1. La LOPD

En esta etapa, el año 2000 reúne dos acontecimientos de especial transcendencia para la protección de los datos personales: por una parte, la entrada en vigor el 14 de enero de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, la LOPD, que sustituye a la LORTAD y se convierte en el eje del sistema de garantías de este derecho en nuestro país y, por otra, la sentencia del Tribunal Constitucional 292/2000, a la que se aludirá más adelante.

Este pronunciamiento del Tribunal Constitucional coincide en el tiempo con la proclamación de la Carta de Derechos Fundamentales de la Unión Europea, hecha en la Cumbre de Niza el 7 de diciembre del mismo año. El artículo 8 de la citada Carta reconoce expresamente el derecho a la protección de datos personales.

Junto a este reconocimiento, el artículo 8 de la Carta describe, adicionalmente, una referencia a los principios del tratamiento de datos ("se tratarán de modo leal, para fines concretos"), a las bases jurídicas del mismo ("sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley") y a alguno de los derechos que integran su contenido esencial ("Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a su rectificación").

Y, especialmente, añade un elemento estructural del sistema de garantías para la protección de este derecho, de naturaleza institucional, al establecer que "el respeto a estas normas quedará sujeto al control de una autoridad independiente". De este modo, la Carta "constitucionaliza" la independencia de las autoridades de control.

La aprobación de la LOPD fue la consecuencia directa de la trasposición en España de la Directiva europea 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos.

Esta Directiva supuso un importante paso en la regulación de la protección de los datos personales dentro del ámbito de la Unión Europea, no sólo por la articulación de un amplio régimen de garantías para la protección de este derecho, sino también por la asunción de un objetivo esencial en el ámbito europeo como es el de garantizar la libre circulación de datos personales como complemento a la libre circulación de mercancías, personas, servicios y capitales, para el establecimiento y funcionamiento del mercado interior.

Para su consecución, la Directiva trató de alcanzar un sistema armonizado de protección si bien reconociendo a los Estados miembros un margen de maniobra en su derecho nacional.

Con respecto a su antecesora, la nueva Ley Orgánica introdujo importantes cambios en la regulación de la protección de datos, ampliando el objeto de la Ley al incluir en su ámbito de protección todos los ficheros de datos, informatizados o no.

La aplicación de la Ley a los datos personales recogidos en otros soportes y, fundamentalmente en papel, completó la aplicación del régimen de garantías a todos los tratamientos de datos personales en un momento en que los ficheros en papel representaban un importante volumen. Esta ampliación, dirigida a eludir graves riesgos de elusión de la norma, sólo abarcó los ficheros manuales estructurados con criterios específicos relativos a las personas que permitieran acceder fácilmente a los datos personales, excluyendo las carpetas no estructuradas.

Igualmente, el principio de finalidad para el empleo de los datos experimenta un reforzamiento, toda vez que los fines para los que podrán emplearse los datos han de ser no sólo legítimos, como se exigía en la antigua Ley, sino, además, determinados y explícitos., siendo necesario que el afectado conozca en todo caso de forma indubitada las finalidades para las que se procede al tratamiento de los datos.

Esta concreción del principio de finalidad tuvo particular relevancia en algunos tratamientos de datos como los relativos a la publicidad y el marketing, sobre los que se había producido un mayor volumen de reclamaciones por parte de los ciudadanos. Y exigió a las empresas dedicadas a esta actividad la inclusión en sus cláusulas informativas para la obtención del consentimiento de una referencia a los sectores específicos para los que se autorizaba el envío de comunicaciones comerciales (tales como productos financieros, de seguros, de telecomunicaciones...), que permitían a los afectados optar por aquellas que fueran de su interés o rechazarlas en caso contrario.

Adicionalmente, se amplió la información a los ciudadanos y las opciones para evitar la publicidad no deseada en aquellos casos en que la ley permitía realizarla sin el consentimiento de sus destinatarios, por ejemplo, utilizando los datos de fuentes públicas como las guías telefónicas. En estos casos se exigió facilitar en cada comunicación publicitaria, información sobre el origen de los datos, la identidad de quien realizaba la publicidad y los derechos que asisten a los receptores de la misma.

Los derechos de acceso, rectificación y cancelación se completaron con el reconocimiento del derecho de oposición, cuando no fuera necesario el consentimiento del afectado para el tratamiento de los datos, si existieran motivos fundados y legítimos para su concreta situación personal.

2. La Sentencia del Tribunal Constitucional 292/2000

Como segundo acontecimiento a destacar de este período, hay que referirse al pronunciamiento del Tribunal Constitucional a través de la sentencia 292/2000. Su relevancia reside en que el derecho a la protección de los datos personales se configura como un derecho autónomo y distinto del derecho a la intimidad, que tiene por objeto la atribución a la persona de un poder de disposición y control sobre sus datos personales, tanto respecto del sector privado como del sector público.

La sentencia parte de la consideración de que, a diferencia del derecho a la intimidad, que permite garantizar una esfera reservada de la persona, el derecho a la protección de datos atribuye un poder de disposición y control sobre la información personal, inclusive cuando sea accesible a terceros, tanto públicos como privados.

Por otra parte, para el ámbito exclusivo de las cesiones de datos entre Administraciones Públicas, la sentencia restringe su utilización al supuesto en que ejerzan competencias similares. Por tanto, cualquier cesión de datos entre Administraciones Públicas sólo podrá efectuarse si se cumple dicha condición, o está autorizada por una norma con rango formal de ley.

3. Nuevas competencias en el ámbito de las comunicaciones electrónicas. La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI) y la Ley General de Telecomunicaciones (LGT)

En el año 2003 tuvo lugar una importante modificación de la Ley Orgánica de Protección de Datos en cuanto a la transparencia de la actuación de la Agencia: se dispuso la publicación de sus resoluciones, preferentemente a través de medios informáticos o telemáticos, que se materializo a partir del 1 de enero de 2004, a través de la página web de la Agencia.

La publicación de las resoluciones contribuyó además al incremento de la seguridad jurídica al poder conocerse los criterios de aplicación de la norma.

Durante este periodo, el marco regulador de la protección de datos personales se amplió y actualizó a nuevos entornos tecnológicos mediante la aprobación de las leyes 34/2002, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI) y de la Ley 32/2003, General de Telecomunicaciones (LGT). Ambas leyes han sido objeto de modificaciones ulteriores para actualizar las garantías para la protección de datos personales.

Estas normas incorporaron al ordenamiento jurídico interno la Directiva 2002/58/CE relativa al tratamiento de datos personales y la protección de la intimidad en el sector de las comunicaciones electrónicas.

La Directiva tuvo en cuenta la introducción de nuevas tecnologías digitales avanzadas en las redes públicas de comunicación y nuevos servicios de comunicaciones electrónicas, así como la importancia de Internet al

aportar una infraestructura común mundial para la prestación de una amplia gama de servicios. Y, en particular, advertía sobre la necesidad de proteger los derechos y libertades frente a la creciente capacidad de almacenamiento y tratamiento informático de datos relativos a abonados y usuarios de estos servicios.

En consecuencia, la Directiva abordó el reto de armonizar las disposiciones legales de los Estados miembros para actualizar la protección de los datos personales a estos entornos y evitar obstáculos para el mercado interior de las comunicaciones electrónicas, garantizando en todo caso que no se vea obstaculizado el fomento y desarrollo de nuevos servicios y redes de comunicaciones electrónicas.

El elemento común de las dos leyes es su relación con los desarrollos de la actividad publicitaria más allá del tradicional correo postal, bien de forma directa regulando otros canales publicitarios, bien indirectamente abordando el uso de tecnologías imprescindibles para el uso de información personal en el desarrollo de la publicidad "on line".

Así, tras una redacción inicial en el año 2002, en la que se limitaba a establecer garantías sobre las comunicaciones comerciales publicitarias, la LSSI fue objeto de diversas modificaciones que culminaron en una nueva regulación de las comunicaciones comerciales por medios electrónicos que exigía un consentimiento reforzado ya que éstas habían de ser expresamente solicitadas o autorizadas por sus destinatarios (el llamado correo basura o "spam").

No obstante, este régimen reforzado previó una excepción cuando existiera una relación comercial previa con el cliente y la publicidad fuera sobre productos o servicios de la propia empresa similares a los contratados. En estos casos, debía ofrecerse al cliente en cada comunicación comercial la posibilidad de oponerse a seguir recibiéndolas por un procedimiento sencillo y gratuito.

La exigencia de un consentimiento reforzado respecto al de la LOPD se justifica por los cambios tecnológicos que permiten el envío de comunicaciones comerciales masivas por medio de sistemas relativamente sencillos y económicos y por la molestia e incluso los costes que pueden suponer al receptor.

Asimismo, dentro de la evolución normativa de este periodo acabó incorporando una obligación de información a los destinatarios por parte de los prestadores de servicios que emplearan dispositivos de almacenamiento y recuperación de datos en equipos terminales (las más conocidas son las llamadas "cookies"). La importancia del uso de estos dispositivos radica, entre otros aspectos, en que permiten el seguimiento de la navegación de los usuarios de Internet.

En este sentido, los prestadores de servicio están obligados a informar a los destinatarios de una manera clara y completa sobre la utilización y finalidad de la recolecta de dicha información, ofreciéndoles la posibilidad de oponerse al tratamiento de los datos mediante un procedimiento sencillo y gratuito. De este modo facilitan la elaboración de hábitos y perfiles de los usuarios para ofrecerles publicidad personalizada, en un modelo de negocio basado en la oferta de servicios gratuitos en Internet cuyo precio son los datos de los usuarios.

Ahora bien, en la práctica, la garantía basada en el derecho de oposición no resultó efectiva y obligó a una

modificación legal posterior más garantista para el uso de estos dispositivos.

Por otra parte, la Ley General de Telecomunicaciones estableció garantías específicas para el tratamiento de los datos de tráfico y localización y su utilización comercial. Y además reforzó los derechos de los abonados y usuarios de estos servicios para evitar la publicidad no deseada al exigir un consentimiento previo e informado para recibirla a través de llamadas automáticas o de fax y reconociendo el derecho a excluirse de las guías de servicios de comunicaciones electrónicas y de los servicios de información sobre las guías, evitando que la información contenida en éstas pudiera utilizarse para hacer publicidad sin consentimiento de los afectados.

La asunción de nuevas competencias derivadas de la aplicación de ambas leyes tuvo como efecto inmediato para la Agencia un incremento notable de la carga de trabajo para sus empleados. La principal causa de este aumento vino de la mano de las denuncias por spam, que desde entonces han supuesto durante años una de las fuentes más importantes de denuncias en la Agencia. Para ilustrar este dato, baste señalar la evolución producida en las denuncias por infracción de la Ley de Servicios de la Sociedad de la Información, que han pasado de 11 procedimientos sancionadores resueltos, en 2005, a 110 infracciones declaradas en 2017.

4. Incremento de los Recursos Humanos de la Agencia

Todos los cambios vividos por el ordenamiento jurídico español se tradujeron en un crecimiento exponencial de las consultas y de las reclamaciones de los ciudadanos.

Para atender adecuadamente unas y otras la Agencia incrementó su personal, no sólo reforzando el perfil tecnológico de su plantilla, sino también incorporando especialistas en tecnologías de la información y atención al ciudadano.

Los incrementos más significativos de personal se producen en 2003, año en el que se pasó de 68 a 92 personas y en 2008, en el que se pasa de 103 efectivos a 147.

A pesar de que la evolución de denuncias y tutelas ha seguido creciendo cada año en porcentajes significativos, la plantilla de la Agencia ha permanecido prácticamente invariable hasta 2017, pese a las reiteradas peticiones al respecto de los sucesivos Directores, incluso en sede parlamentaria.

Finalmente, en 2017 se autorizó un incremento de plantilla hasta los 180 puestos con los que actualmente cuenta la Agencia.

5. Las consultas

En el año 2000 se incluye en la página web de la Agencia un apartado específico de “preguntas frecuentes” en el que se daba respuesta a los temas más recurrentes en las consultas, a saber: envíos publicitarios, datos de facturación telefónica; datos de las Guías Telefónicas o ficheros de información de solvencia patrimonial y crédito

El catálogo de “preguntas frecuentes” se ha ido ampliando y hoy recoge más de 200 cuestiones.

Además, se fueron incorporando otros recursos, como las recomendaciones de la Agencia a los usuarios de

Internet o los principales dictámenes emitidos por el Gabinete Jurídico.

A partir del año 2001 se observa un crecimiento exponencial de las consultas planteadas, con incrementos anuales de entre el 20% y el 30%: las 19.262 consultas que se atendieron durante el año 2000 convirtieron en 35.251 en 2004. En ese incremento tuvo una influencia decisiva la remodelación integral de la página web de la Agencia practicada en el año 2003, que se convierte en un elemento vertebrador de la normalización del conocimiento del derecho fundamental.

El 15 de octubre de 2004 entró en funcionamiento la línea de atención telefónica inteligente que derivaba al ciudadano discriminadamente al Servicio de Atención al Ciudadano y al resto de Unidades de la Agencia.

La Agencia se autoimpuso el cumplimiento de una serie de compromisos de calidad en la atención al ciudadano: las consultas presenciales, con un tiempo de espera no superior a 20 minutos, las telefónicas, atendidas tan pronto eran conocidos los detalles de la consulta y las escritas, con plazos de contestación no superiores a 30 y 20 días hábiles para las postales y electrónicas, respectivamente.

En cuanto a la evolución cuantitativa de las consultas, ya se ha puesto de manifiesto cómo del año 2000 al año 2004 se incrementaron en un volumen superior al 80%. Pues bien, al final del periodo el número de consultas anuales atendidas alcanzó las 72.652, es decir, de 1999 a 2008 casi se cuadruplicaron.

En este periodo, el mayor incremento anual se produce entre los años 2007 a 2008, sin duda debido a la entrada en vigor del Reglamento de la Ley Orgánica de Protección de Datos. Este incremento se produce singularmente en la atención telefónica, pasándose de 11.500 llamadas en el año 2000 a 58.143 en 2008. La segunda vía más utilizada es la escrita (9.722 consultas en 2008 frente a las 1.739 de 2000) y, en tercer lugar, la presencial (4.785 consultas en 2008 frente a las 1.150 de 2000).

Por lo que se refiere a las cuestiones objeto de consulta, la preocupación fundamental de los ciudadanos se refiere al ejercicio de derechos, que llega a representar, en algunos años, más de la mitad del total de consultas.

En concreto, el derecho que más interés suscita por parte de la ciudadanía es el ejercicio del derecho de cancelación que supuso más de la mitad de las consultas atendidas en 2008. En ello tuvo gran influencia un fenómeno específico referido a la cancelación de datos en los Libros de Bautismo de la Iglesia Católica. Tras el de cancelación, es el ejercicio del derecho de acceso el que centra las preocupaciones de los ciudadanos que, en definitiva, quieren conocer quién y qué datos se utilizan, cómo y dónde ejercer sus derechos y, en mayor medida, evitar que se siga realizando el tratamiento de su información personal.

También se mantienen constantes durante todo el periodo las consultas sobre ficheros concretos, como los de solvencia patrimonial y crédito, el envío masivo de faxes o de llamadas sin intervención humana y la exclusión de guías telefónicas. En estos casos, los ciudadanos se preguntan sobre su aparición en los ficheros de morosos a pesar de estar saldadas las deudas, sobre cómo averiguar si están en los ficheros de morosidad, si puede una empresa cederle a otra los datos personales de sus antiguos clientes para

reclamarles impagos o el procedimiento para no recibir publicidad no deseada por correo.

6. Las denuncias y las inspecciones

El volumen de denuncias que se presentaron en el año 2000 es muy similar al de 1999. En particular, se iniciaron 146 procedimientos sancionadores a entidades del sector privado y 31 al sector público.

No obstante, a lo largo de los años siguientes estas cifras crecerían exponencialmente, de tal modo que en 2007 se resolvieron 399 procedimientos sancionadores y 66 procedimientos de infracción de las Administraciones Públicas. También se resolvieron 37 procedimientos con arreglo a la LSSI y 2 a la LGT.

A lo largo de los primeros años de esta década, con especial incidencia en 2005, se incrementan las actuaciones por fraude en la contratación de productos y servicios, normalmente de telefonía y de acceso a Internet, en muchos casos producido por deficiencias en la gestión de los distribuidores de esos servicios.

En 2007, la mayoría de las inspecciones realizadas afectan a telecomunicaciones y entidades financieras, a las que sigue la videovigilancia, con un incremento superior al 400% en el año 2007 respecto al 2006.

En este período la actividad publicitaria continúa siendo uno de los sectores en los que los ciudadanos plantean un importante volumen de reclamaciones; un sector en el que se produjo un cambio de tendencia en las denuncias como consecuencia de los cambios en el entorno tecnológico. Así descienden las relativas a conductas que hacen uso del canal postal, y se incrementan las referentes al canal electrónico, principalmente a través del correo electrónico o los mensajes SMS, junto con las posibilidades de elaboración de perfiles de los usuarios de Internet.

El envío de correos electrónicos y faxes de carácter comercial sin consentimiento se erige así como uno de los ámbitos en los que se desarrollan más actuaciones de inspección.

Otro de los principales sectores en los que se incrementan las denuncias por parte de los ciudadanos es el de las entidades financieras; y más en concreto en lo relativo a la información sobre solvencia patrimonial y crédito, ya que una parte muy relevante de las reclamaciones, más del 50%, se refieren a la inclusión de datos en un fichero de morosidad, en muchas ocasiones, sin respetar los principios y garantías previstos en la normativa de protección de datos.

El otro gran sector que centra la atención de los ciudadanos es el de las empresas de telecomunicaciones. Y ello, por dos motivos: de un lado, porque estas empresas son fuente de información de los ficheros de morosidad, a los que comunican sus deudores; y de otro lado, por los problemas cada vez más frecuentes que suscita el tratamiento de datos personales en este sector, que incluye no solo los tratamientos más tradicionales relacionados con los directorios de telecomunicaciones, sino también los derivados del propio desarrollo tecnológico, entre los que se encuentran los tratamientos de datos en Internet o en servicios como los SMS.

En este período se produce un considerable crecimiento de las reclamaciones en este sector, que pasan a ocupar en 2004 el primer lugar de las inspecciones (216) y de los procedimientos (62), desbancando así a los relativos

a las entidades financieras. Este incremento está relacionado con los nuevos entornos tecnológicos que describe la Directiva 2002/58/CE, y que se han expuesto anteriormente.

Aproximadamente un 30% de las reclamaciones en el sector de las telecomunicaciones se refieren a la existencia de fraude en la contratación de productos y servicios, normalmente de telefonía y de acceso a Internet.

La principal causa de fraude es la suplantación de identidad de la persona contratante. Esta causa resulta relevante en la contratación telefónica y online de todo tipo de servicios, no sólo de telecomunicaciones, hasta el punto de que, en 2013, los sectores de suministro y comercialización de agua y energía han pasado a ocupar el segundo lugar en cuanto a volumen de sanciones, superando a las entidades financieras.

Por el contrario, se observa una disminución de la actividad sancionadora en los sectores de sanidad, seguros, comunidades de propietarios y administración de fincas, recursos humanos y relaciones laborales, y envío de comunicaciones comerciales por fax.

En lo que respecta a este último aspecto, en este periodo el empleo del fax ya es muy minoritario, y el correo postal ha perdido protagonismo frente al correo electrónico. Así, en el sector de la publicidad el interés de las empresas se centra en los envíos comerciales a través del correo electrónico, bien mediante campañas de mailing masivo, bien mediante correos personalizados. Se vislumbra, por tanto, el perfilado en este sector.

En lo que respecta al ámbito de las administraciones públicas, las inspecciones y declaraciones de infracción se habían reducido en la administración local, mientras que se incrementaron en la Administración General del Estado y en las autonómicas. Entre las infracciones declaradas destacan las relativas a la no inclusión en los boletines de multas o infracciones de la cláusula informativa a la que alude el artículo 5 de la Ley Orgánica de Protección de Datos, a la falta de información en los impresos de datos de entrada de visitantes en los edificios públicos, y al acceso indebido a los datos personales obrantes en un organismo público.

Los grandes debates en el seno de la Agencia en el 2007 versaban acerca de si es posible impedir la utilización indebida de datos personales en Internet, si es inevitable una sociedad videovigilada y una vida laboral controlada con mayor intensidad, si se puede hacer frente a la piratería en Internet respetando los datos personales protegidos y qué garantías pueden lograrse para la privacidad en un mundo globalizado.

Estas inquietudes pueden considerarse los temas precursores de la actividad de la Agencia en el período siguiente, al tiempo que iba encaminándose, junto con las demás autoridades europeas, hacia estándares internacionales de privacidad.

Por último, cabe señalar que se promovieron nuevos planes de inspección sectorial de oficio en los sectores del comercio electrónico y la gestión de tarjetas en grandes superficies comerciales.

7. Las tutelas de derechos

En los primeros años de la década de 2000 se constata un fuerte incremento en las solicitudes de tutela de derechos. Aunque las inquietudes de los ciudadanos siguen siendo básicamente las mismas, sí que se observa

una inversión en la tendencia de años anteriores: el ejercicio del derecho de cancelación supone el 53% de las solicitudes, mientras el ejercicio del derecho de acceso desciende hasta un 42%, lo que pone de manifiesto que la preocupación de los ciudadanos ya no es tanto el acceso o no a los datos, sino conseguir evitar el tratamiento de esos datos.

Las solicitudes de ejercicio del derecho de cancelación hacían referencia principalmente a las siguientes cuestiones: inclusión indebida en ficheros de morosidad y cancelación al término del pago de la deuda, supresión de datos una vez concluida la prestación de servicios contratados con operadores de telecomunicaciones, baja en los ficheros de operadores de telecomunicaciones por cambio de compañía no consentido por el abonado, historial clínico, y cancelación de datos -sobre todo fotografías- en Internet (foros, Youtube).

Los casos más habituales de ejercicio del derecho de acceso versaron sobre las imágenes captadas por cámaras en la vía pública, las valoraciones de solvencia económica realizados por entidades financieras, el historial clínico de familiar fallecido y la historia clínica que se considera que se ha suministrado de manera incompleta.

En cuanto a las solicitudes de ejercicio del derecho de oposición destaca el interés por el tratamiento de datos por empresas de control médico en las bajas laborales y por la recepción de publicidad de una empresa con la que existe un contrato previo.

8. Las Recomendaciones de la Agencia

Al finalizar esta etapa, la Agencia, a partir de la experiencia adquirida en el ejercicio de sus funciones, publicaba una serie de recomendaciones para garantizar la privacidad de los ciudadanos.

- Deberían delimitarse las actividades en las que puede resultar necesario el establecimiento de sistemas de denuncia interna en las empresas por los trabajadores, determinando sus finalidades, los procedimientos de auditoria y los periodos de conservación; garantizando la confidencialidad del denunciante y los derechos de los denunciados.
- El desarrollo de procedimientos que permitan proteger de forma compatible los derechos de autor y el de protección de datos.
- Necesidad de regular la publicación anonimizada de sentencias de órganos jurisdiccionales.
- Las Administraciones Públicas competentes deberían acometer planes de protección de los datos personales de los menores en Internet.
- Impulso de cautelas especiales para evitar el intercambio indeseado de datos personales sensibles en Internet a través de redes P2P. Es preciso que los usuarios se conciencien urgentemente de los riesgos que se derivan de difundir, muchas veces inadvertidamente, informaciones almacenadas en sus equipos informáticos.
- Debe impulsarse la utilización generalizada del apartado que oculta los destinatarios (copia oculta) en el envío de correos electrónicos, como garantía de confidencialidad.
- Promoción de buenas prácticas en garantía de la privacidad en todos los Boletines y Diarios Oficiales. La información publicada suele incluir datos personales y es también captada por los motores de búsqueda en Internet, multiplicando las

posibilidades de acceso y dificultando el ejercicio de los derechos de cancelación y oposición. Esta situación aconseja impulsar los procedimientos que, sin afectar la función propia de los diarios oficiales, limite su captación por los motores de búsqueda en Internet.

- Estrategia Local dirigida a adecuar la instalación de cámaras para control del tráfico, a la normativa de protección de datos personales.
- Promover la autorregulación en los medios de comunicación (escritos y audiovisuales) para garantizar la protección de los datos personales. Con carácter general, cabe proclamar la prevalencia de la libertad de información (art. 20 CE). Si una noticia tiene relevancia pública el afectado tiene el deber de soportarla sin que pueda esgrimir en contra los principios de protección de datos personales. Ahora bien, ello no impide que puedan promoverse practicas más respetuosas con la normativa de protección de datos personales. Un instrumento adecuado para ello es la autorregulación por el propio sector. Otros eventuales conflictos deberán sustanciarse en el marco de la legislación de protección al honor, intimidad y propia imagen.

IV. El reglamento de la Ley Orgánica de Protección de Datos: del 2008 hasta el 25 de mayo de 2018

1. El reglamento de desarrollo de la Ley Orgánica de Protección de Datos

Transcurridos los primeros años de aplicación de la Ley Orgánica, ya bajo la dirección de José Luis Piñar Mañas, se apreció la necesidad de llevar a cabo un desarrollo reglamentario para lograr mayores niveles de seguridad jurídica a la hora de aplicar dicha norma.

El Reglamento vio finalmente la luz recién comenzado el mandato de Artemi Rallo Lombarte mediante la publicación del Real Decreto 1720/2007, de 21 de diciembre.

El reglamento contribuyó decisivamente a objetivar los criterios de aplicación de la Ley Orgánica, de lo que se beneficiaron no sólo las Resoluciones de la propia Agencia, sino, sobre todo, las sentencias de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional y del Tribunal Supremo y dio cumplimiento a la obligación de trasposición de la Directiva 95/46/CE.

Una de las novedades más destacadas del Reglamento, en relación con los llamados ficheros de solvencia, fue que se precisaron los requisitos para la inclusión de los datos y para acceder a la información en estos ficheros.

En los tratamientos de solvencia suelen intervenir cuatro sujetos: el deudor, el acreedor que notifica la deuda, el responsable del tratamiento de solvencia patrimonial, y las entidades que consultan esta información. Para incluir los datos personales de una persona física en un "fichero de morosos", debían cumplirse los siguientes requisitos:

- Que exista una deuda cierta, vencida, exigible y que haya resultado impagada.
- Que no hayan transcurrido seis años desde la fecha en que hubo de procederse al pago de la deuda o del vencimiento de la obligación o de la cuota correspondiente al pago aplazado.

- Que exista requerimiento de pago, advirtiendo de que, si no se paga, se procederá a esta inclusión. Quien notifica la inclusión de la deuda, debe acreditar que efectivamente ha notificado este aviso. Cumplirá con su obligación cuando el destinatario rechace el envío y/o cuando la dirija a la dirección que figure en el contrato.

La AEPD no es competente para dilucidar controversias sobre la existencia de una deuda. No se requiere el consentimiento del titular de los datos para comunicarlos a una empresa de gestión del cobro de deudas. Si una persona desconoce en qué fichero de solvencia está incluida, puede ejercitar el derecho de acceso a sus datos personales ante los ficheros -en la guía editada por la Agencia, accesible a través de su web, figuran enlaces a los ficheros más habituales-. Pagada la deuda, se deben dar de baja los datos personales de esos tratamientos. Si no es así, se puede ejercitar el derecho de cancelación. También se puede ejercitar este derecho de supresión si transcurridos seis años desde el vencimiento de la obligación incumplida, los datos continúan en los tratamientos de morosidad ("ficheros de morosos").

Otra de las novedades relevantes que incorpora el Reglamento respecto de los tratamientos de publicidad, fue la inclusión de los ficheros comunes de exclusión de comunicaciones comerciales. El llamado servicio de "Lista Robinson" fue presentado conjuntamente el 30 de junio de 2009 por la Agencia y la actual Asociación Española de la Economía Digital (ADIGITAL), única entidad que lo gestiona hasta la fecha.

Este servicio permite a quienes se adhieran al mismo gestionar la publicidad no deseada -en particular, a los padres o tutores solicitar que no se traten los datos de los menores para el envío de publicidad-, y posibilita asimismo elegir los canales a través de los que se desea recibir publicidad, incluyendo el postal, el correo electrónico, los mensajes SMS y MMS y el telefónico. En cada uno de estos canales permite seleccionar varias opciones sobre la identidad de la persona, sus domicilios, las direcciones de correo electrónico y los números de teléfono. En la actualidad cuenta con más de 600.000 ciudadanos inscritos.

2. Modificación de la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico y de la Ley General de Telecomunicaciones

En el año 2014 se produjo una modificación parcial de la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico para reforzar las garantías de los ciudadanos frente a la práctica de elaboración de perfiles, en particular, con fines de publicidad "online".

Ante la inoperancia del sistema de derecho de oposición a la utilización de cookies u otros dispositivos similares, la nueva regulación exigió la obtención de un consentimiento inequívoco de los usuarios de Internet, trasponiendo la Directiva 2009/136 UE.

De otro lado, se modificó la Ley General de Telecomunicaciones para obligar a los operadores de telecomunicaciones a notificar a la Agencia las brechas de seguridad en sus sistemas de información y, en su caso, también a los propios interesados si podían sufrir una lesión en sus derechos.

3. Las consultas de los ciudadanos

Durante este periodo, y de forma significativa a partir de 2014, se vuelve a registrar un repunte en el número de consultas sobre la inclusión indebida en ficheros de "morosidad", recogiendo también los supuestos de suplantación en la contratación de servicios básicos como la telefonía o el suministro de agua y energía.

Adicionalmente, los ciudadanos demandan información sobre la obligación de inscripción de ficheros, que ha desaparecido con la entrada en vigor del Reglamento UE el 25 de mayo de 2018, la protección de datos en las comunidades de vecinos, la videovigilancia y sobre cómo interponer denuncias y reclamaciones ante la Agencia.

Tablas 1
Evolución de las consultas ciudadanas sobre derechos (periodo 2008-2017)

Fuente
Elaboración propia

AÑO	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Total consultas*	72.650	97.223	104.826	134.635	111.933	102.064	99.524	85.611	89.658	85.154
Sobre derechos	20.030	30.820	30.200	38.788	11.753	7.883	5.458	5.522	7.226	8.175

Tablas 2
Porcentaje de las consultas ciuadadanas por tipo de derecho

Fuente
Elaboración propia

DERECHOS	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
ACCESO	12,3%	20,62%	23,63%	15,71%	13,1%	22,34%	25%	26,25%	7,92%	31,36%
CANCELACIÓN	53,01%	62,39%	40,64%	50,35%	50,35%	51,57%	55,11%	55,98%	79.9%**	55,72%**
RECTIFICACIÓN	1,23%	2,42%	5,44%	3,57%	1,8%	3,23%	3,75%	2,31%	2,68%	4,16%
OPOSICIÓN	2,82%	8,66%	25,51%	27,85%	30,9%	20,71%	15,03%	13,97%	9,5%	8,73%

** Incluye el denominado "derecho al olvido"

Respecto a las consultas sobre el ejercicio de derechos por parte de los ciudadanos, un 43,34% fueron sobre el derecho de cancelación, y un 12,38% sobre el denominado "derecho al olvido" respecto de los enlaces de servicios de búsqueda en Internet.

Por lo que respecta al resto de derechos, el 31,36% se plantearon sobre el derecho de acceso, un 8,73% sobre el de oposición, y un 4,16% sobre el de rectificación.

En 2016 se reelaboró el catálogo de Preguntas Frecuentes, recogiendo más de 200 preguntas-respuestas agrupadas por temáticas, entre las que ya se incluyeron cuestiones sobre el nuevo Reglamento UE, preparando así su entrada en vigor.

En definitiva, la preocupación de la población española por la privacidad ha crecido notablemente en los últimos años. Así lo pone de manifiesto el Barómetro del CIS de mayo de 2018 en el que el 76% de los encuestados manifiesta que le preocupa mucho o bastante la protección de sus datos personales y su posible uso por terceros.

En un ámbito tan cotidiano como es el del comercio, los encuestados manifiestan que no les ofrece ninguna seguridad dar los datos de su tarjeta bancaria por Internet; aunque curiosamente las entidades financieras parece que van ganando la batalla a la desconfianza porque aunque el 31% de los encuestados señalan que no les ofrece seguridad realizar operaciones bancarias por Internet, ya son un 29% los que dicen que les ofrece bastante seguridad.

Resulta igualmente interesante la identificación de los datos que no daría el encuestado, salvo que fuese imprescindible: la huella dactilar (86,1%), el historial médico (66,9%), y la información financiera (87,6%).

En cuanto a la información sobre gustos y opiniones: un 40,4% los daría fácilmente, a un 27,4% le costaría darlos y un 30,7% no los daría, salvo que fuese imprescindible.

Por lo que respecta a las fotos y vídeos personales, al 22% le costaría darlos, y un 70,7% afirma que no los daría, salvo que fuese imprescindible.

En general, la población no tiene asentada la costumbre de leer las políticas de privacidad de las páginas de Internet: las lee casi siempre el 9,2%, algunas veces el 21,7%, raramente el 29,4% y nunca el 33,3%.

Para concluir esta revisión, resultan reveladoras las siguientes preguntas:

- "En realidad, le importa más acceder a los servicios que le prestan los sitios web que la privacidad de sus datos". Se muestra "muy de acuerdo" un 11,4%, "bastante de acuerdo" el 37,7%, "poco de acuerdo" el 28,7%, y "nada de acuerdo" el 17,8%.

- "¿Se ha arrepentido alguna vez de haber colgado algo (comentario, foto, vídeo) en la red social?". La respuesta fue afirmativa en un 24,5%.

- "¿Ha tenido alguna vez problemas por contenidos que otros/as han colgado en la red social?" Afirmó que sí un 12,2%.

4. Denuncias e inspecciones

En este periodo los expedientes de investigación fueron creciendo hasta el año 2013, en el que comienza una tendencia decreciente.

Tablas 3
Denuncias e inspecciones

Fuente
Elaboración propia

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018[1]
Reclamaciones de tutela	2.159	1.832	1.657	2.230	2.193	1.997	2.099	2.082	2.588	2.654	1.346
Denuncias	3.073	5.310	5.045	7.648	8.594	8.607	10.074	8.489	7.935	7.997	5.311
Reclamaciones RGPD	-	-	-	-	-	-	-	-	-	-	4.407
Total	5.232	7.142	6.702	9.878	10.787	10.604	12.173	10.571	10.523	10.651	11.064

[1] Desde la entrada en vigor del Reglamento General de Protección de Datos, aparece una nueva categoría de clasificación: las reclamaciones RGPD.

Las inspecciones sectoriales de oficio tuvieron un lugar muy destacado en el año 2008, con una fuerte reducción hasta el período 2016 a 2018, en que crecen de nuevo de forma significativa como consecuencia de su inclusión en el Plan Estratégico de la Agencia, como actuaciones de naturaleza preventiva.

Los procedimientos sancionadores al sector privado se han mantenido en cifras constantes durante todo el periodo con una leve reducción a partir de 2016.

Por su parte, los procedimientos declarativos de infracción de las administraciones públicas reflejan una gran estabilidad, salvo unos leves repuntes en los años 2009 y 2010, y una reducción en el período 2011 a 2013.

Los procedimientos relacionados con la aplicación de la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI) y la Ley General de Telecomunicaciones (LGT) durante el período, se recogen en la tabla 4.

Del total de 975 actuaciones en este ámbito correspondientes a todo el período, hay que destacar el aumento de las declaraciones de las infracciones por cookies, que guarda relación con la modificación de la LSSI operada por el Real Decreto-Ley 13/2012, así como en materia de spam, especialmente en las resoluciones sancionadoras durante el período 2012-2016.

Por lo que se refiere a los sectores en los que se realizaron un mayor número de inspecciones y se

Tablas 4

Fuente
Elaboración propia

Tipo Procedimiento	Grupo de Activ-idad	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Pr. Apercibimiento	Cookies (LSSI)							22	28	12		
Pr. Apercibimiento	Spam (LSSI)						3	40	27	19	19	13
Pr. Infracción	Cookies (LSSI)					1		1	2			
Pr. Infracción	Spam (LSSI)	1								1		1
Pr. Sancionador	Cookies (LSSI)						7	17	10	14		1
Pr. Sancionador	LGT (fax y otros)	14	4	1	6	4	2	3	3			
Pr. Sancionador	Spam (LSSI)	49	35	52	31	62	76	81	102	63	39	32
T. Derechos	Cookies (LSSI)									1		
T. Derechos	LGT (fax y otros)					1						
T. Derechos	Spam (LSSI)	2	1			2	4	9	15	8	2	14
TOTAL		66	40	53	37	70	92	173	187	118	60	61

resolvieron más resoluciones sancionadoras durante el período, los relativos a las telecomunicaciones, las entidades financieras, la videovigilancia y los ficheros de morosidad siguen siendo los más destacados, seguidos de los de comunicaciones electrónicas comerciales (spam) y Administración Pública.

Estos datos van en consonancia con la evolución de la situación económica. Si en el año 2007 la Encuesta de Población Activa marcaba una tasa de desempleo del 8,57%, en los años siguientes este resultado se dispararía, con todas las consecuencias que el paro implicaba para los hogares, particularmente el retraso en el pago de los créditos comprometidos o la imposibilidad de afrontarlos.

Otro de los ámbitos que suscitan una mayor preocupación entre los ciudadanos es el de la recepción de comunicaciones publicitarias telefónicas. Por ello, la AEPD realizó de oficio dos inspecciones sectoriales sobre llamadas comerciales y sobre mensajes cortos a telefonía móvil. La Agencia constató deficiencias sobre los mecanismos de que disponen los ciudadanos para oponerse a la recepción de estas comunicaciones y advirtió sobre los riesgos asociados a la contratación de servicios de tarificación adicional.

No se puede dejar de comentar que el año 2008 va asociado a la videovigilancia, que era ya por ese entonces un fenómeno imparable. Los sectores que más ficheros tenían declarados eran el del comercio, seguido del turismo y la hostelería y a continuación, las comunidades de propietarios, desplazando a la cuarta posición los relacionados con la sanidad. En consonancia con lo anterior, se incrementaron notablemente las actuaciones de inspección y sancionadoras en este ámbito.

Resulta llamativo el importante crecimiento de los ficheros de videovigilancia del sector educativo. En este sentido, hay que mencionar el criterio adoptado por la Agencia en relación a la videovigilancia en centros escolares, donde la instalación de cámaras puede servir al interés superior del menor contribuyendo a una mayor seguridad en los patios y en el comedor. Ahora bien, dicho interés no tiene por qué ser absoluto, ya que es fundamental la ponderación de los intereses afectados. Por ello, deberán imponerse estrictas medidas en cuanto al acceso a las imágenes, tanto en el visionado inicial como en los posibles accesos a las grabaciones.

Los criterios de la Agencia en relación con la videovigilancia fueron evolucionando a lo largo de este periodo. En este sentido cabe destacar el cambio en relación con las cámaras simuladas/sin funcionamiento. Así, frente a la práctica de sancionar por incumplimiento de los requerimientos de la Agencia, pasan a archivarse las actuaciones investigadoras en estos casos ante la ausencia de tratamiento real de datos de carácter personal.

A partir de 2008 se iniciaron diversas inspecciones de oficio que traen causa de informaciones publicadas en medios de comunicación, sobre la aparición de documentos con información personal en la vía pública. Cabe destacar, por su especial trascendencia, las inspecciones relativas al hallazgo en la vía pública de documentación judicial y de tarjetas de usuarios de la sanidad pública. No debe olvidarse que la negligencia que supone dejar a disposición de cualquiera informaciones personales que hubieran debido ser destruidas o mantenerse confidenciales y que, en ocasiones, afectan a datos sensibles o especialmente protegidos, como la salud, pone de manifiesto, no ya una ignorancia, sino una verdadera desidia ante los derechos de los ciudadanos.

De otra parte, en el ámbito de la cesión de cartera entre empresas (venta de deuda) en el año 2009 se resolvieron varios expedientes sancionadores que derivaron en la imposición de sanciones que han llegado hasta 420.000 €. Se trataba de casos en que empresas, principalmente adscritas al sector de telecomunicaciones, realizaban la venta de la cartera de deudores a un cesionario que se encargaría de gestionar el recobro de deudas referentes a miles de clientes. Tras la comprobación de que en varios supuestos se estaba realizando la cesión de un deudor o deuda inexistente se adoptaron las decisiones sancionadoras citadas.

La difusión de ficheros con datos personales en redes P2P utilizando las herramientas de trabajo, normalmente con el programa e-mule, fue otra de las principales preocupaciones de la Agencia. Las actuaciones inspectoras incoadas por este tipo de prácticas, que afectan tanto a entidades privadas como a organismos públicos, se refieren a un gimnasio, un sindicato, un club deportivo, un centro de rehabilitación psicosocial, un partido político y un bufete de abogados. Los ficheros difundidos incluían datos sensibles como los de salud.

A lo largo del año 2010 se acometió también un proyecto para elaborar un Informe de cumplimiento de la LOPD en los hospitales, por ser estos centros sanitarios los principales responsables en el tratamiento de datos de salud. Esta iniciativa surgió a consecuencia de la constatación de alarmantes casos de incumplimiento de la Ley vinculados principalmente a la vulneración de los deberes de seguridad y secreto, entre los que pueden citarse la difusión de datos clínicos a través de redes de intercambio de archivos P2P, el abandono de datos de salud en la vía pública, el almacenamiento de información clínica en áreas no restringidas de los centros sanitarios y, por tanto, al alcance de cualquiera, la pérdida de historiales clínicos al proceder a su automatización en formato electrónico o la utilización de datos sanitarios para fines no autorizados o su comunicación indebida a terceros.

Junto a ello se pretendió analizar los sistemas de información a los ciudadanos, los procedimientos para el ejercicio de los derechos ARCO, la inscripción de ficheros y la externalización de servicios.

La evaluación se realizó mediante el envío de un cuestionario a más de 600 centros registrados en el Catálogo Nacional de Hospitales, que fue atendido por el 92% de los centros. En términos generales el grado de cumplimiento era mayor en los centros de titularidad privada que en los de titularidad pública. En materia de seguridad el Informe pone de manifiesto que existía una importante diferencia entre el cumplimiento formal de las medidas de seguridad y su implantación efectiva. Así, aunque la inmensa mayoría disponía de un documento de seguridad, se constataban deficiencias en la aplicación de las medidas. También se concluyó que existía una falta de diligencia a la hora de conocer quién accede a las historias clínicas, si quienes lo hacen utilizan o no los datos para el fin que justificó su acceso -fundamentalmente la asistencia sanitaria a los pacientes-, así como una ausencia de controles sobre la eficacia de las medidas de seguridad.

Con el transcurso del tiempo las entidades del sector sanitario han ido avanzando en la digitalización de sus procesos. En el sistema español la competencia de gestión de la asistencia sanitaria pública se encuentra descentralizada en los Servicios de Salud de las Comunidades Autónomas. Éstas desde mediados de los noventa comenzaron a implantar la tramitación electrónica en determinados procesos, como la gestión de los partes de incapacidad y paulatinamente se fueron explorando otros sistemas de información, como es el caso de la historia clínica electrónica, de los sistemas de información de laboratorios (LIS) o la receta electrónica. Ese esfuerzo realizado a partir de principios del siglo XXI se centró en la interoperabilidad de los distintos sistemas empleados por los servicios autonómicos de salud en base a estándares comunes. Actualmente casi todas las Comunidades Autónomas tienen los sistemas de Historia Clínica Electrónica del Sistema Nacional de Salud (HCE) en fase de implantación, y los sistemas de receta electrónica están muy avanzados.

El interés de la Agencia por el tratamiento de datos en el ámbito hospitalario tuvo su continuación en la realización en 2017 de un nuevo Plan de Inspección de Oficio. El Plan está centrado en la auditoría de los aspectos en los que se detectaron carencias en los planes de inspección de 1995 y 2010 y, en concreto, en las medidas de seguridad implementadas. Para ello, se auditaron hospitales que, partiendo de una situación de historia clínica en papel, la han transferido a formato electrónico; hospitales que conservan todavía la historia

clínica en papel y que están inmersos en procesos de automatización, y hospitales que cuentan con historia clínica electrónica desde su creación. Entre los servicios hospitalarios inspeccionados se encuentran: Admisión, Urgencias, Consultas Externas, Anatomía Patológica, Unidad de Cuidados Intensivos, Laboratorio de Análisis Clínicos, Farmacia Hospitalaria, Departamento de Informática, Atención al Paciente, Servicios Sociales y Biobanco.

Entre las principales conclusiones del análisis se ha constatado, en líneas generales, una tendencia favorable a la progresiva asunción no sólo de la normativa, sino de los principios y la cultura de protección de datos. El informe pone de manifiesto que los errores detectados en el tratamiento de los datos no constituyen comportamientos generales, lo que supone una mejoría en comparación con las situaciones anteriores.

Entre los aspectos que se pueden y deben mejorar hay que destacar los relacionados con la información ofrecida a los pacientes o el refuerzo de las medidas de seguridad.

La publicación de este Plan de inspección está acompañada de un decálogo básico que recoge los puntos más relevantes de la normativa de protección de datos orientados al personal sanitario y administrativo de los centros, con el objetivo final de elevar el nivel de cumplimiento y generar confianza en las actuaciones de las instituciones sanitarias tanto en el ámbito asistencial como en el de la investigación.

Junto a las actuaciones de oficio, en el sector sanitario se produjo un incremento de las denuncias debidas a los accesos injustificados a las historias clínicas de los denunciantes, declarándose infracciones al centro sanitario por incumplimiento de las medidas de seguridad y al autor de los accesos por desvío de finalidad.

Por último, con el fin de destacar los casos más significativos del ejercicio de las funciones reactivas de la Agencia, se relacionan las sanciones más cuantiosas en la historia de la Agencia (tabla 5).

5. Tutelas de derechos

Las cifras de tramitación de las tutelas de derechos han mantenido una tendencia creciente que se acentúa entre los años 2012 y 2017.

Entre ellas, el olvido en Internet se convierte en una demanda creciente en la Agencia a partir de 2010. El incremento del ejercicio de los derechos de cancelación y oposición ante los responsables de motores de búsqueda acreditan la intensidad de esta demanda, ascendiendo a casi un centenar las resoluciones dictadas sobre la tutela de estos derechos. El 87% afectan al motor de búsqueda de Google y el resto a otros, como Yahoo!, Lycos, Altavista, Bing y Terra. El 75,5% de las resoluciones estimaron las reclamaciones de los ciudadanos.

Al respecto, el año 2014 viene marcado en el ámbito de la protección de datos por la sentencia del Tribunal de Justicia de la Unión Europea en el caso de la Agencia frente a Google que se describirá posteriormente en el apartado V, sobre el derecho a la protección de datos en servicios en Internet.

Tablas 5
Relación las sanciones más cuantiosas en la historia de la Agencia

Fuente
Elaboración propia

Expediente	Sancionado	Fecha resolución	Importe sanción
PS/00082/2017	FACEBOOK, INC.	21/08/2017	1.200.000,00
PS/00095/2000	Zeppelin Televisión, S.A.	29/12/2000	1.081.821,79
PS/00345/2013	GOOGLE INC	18/12/2013	900.000,00
PS/00433/2017	J.V.L.F.G.	08/03/2018	800.000,00
PS/00169/2006	INVERTRED, S.L.	28/03/2007	602.214,12
PS/00146/2011	J.V.L.F.G.	21/09/2011	600.000,00
PS/00146/2011	SABERLOTODO INTERNET S.L.	21/09/2011	600.000,00
PS/00348/2005	COMERCIAL REDES SISTELCOM, S.A.	12/09/2006	450.000,00
PS/00006/2006	DATASUN 2, S.L.	19/07/2006	540.000,00
PS/00166/2008	INFORMACION EUROPEA ON-LINE, S.L.	19/06/2008	450.000,00
PS/00251/2005	Comercial Redes Sistelcom, S.A.	27/04/2006	450.000,00

V. El derecho a la protección de datos en los servicios de internet. Los nuevos desafíos de la privacidad

Estamos inmersos en una sociedad digital, o sociedad de la información, caracterizada por la existencia de más información sobre las personas, sobre más aspectos de su vida, que puede ser almacenada, intercambiada y procesada para una enorme variedad de fines con gran facilidad y con relativamente bajos costes.

Ese es el escenario en el que actualmente tiene que desenvolverse el derecho fundamental a la protección de datos personales. Ingentes cantidades de información que son constantemente generadas y compartidas por todos los ciudadanos en un contexto altamente tecnificado.

Algunos datos, a pesar de que se mueven en escalas que resulta difícil visualizar, pueden ayudar a tener una idea aproximada de las dimensiones de este fenómeno.

Se ha publicado recientemente un estudio según el cual el tráfico global sobre Internet se multiplicará por tres entre 2016 y 2021, alcanzando 3,3 Zettabytes anuales en 2021.

En España, ese tráfico alcanzará los 37 exabytes anuales en 2021, desde los desde los 12 registrados en 2016.

Como esas cifras seguramente se nos escapan a todos, valga decir que equivaldrían a que todas las películas producidas en el mundo en toda la historia crucen las redes IP españolas cada dos horas.

En España habrá 36,3 millones de usuarios de Internet en 2021 (el 79% de la población), desde los 33,5 millones contabilizados en 2016 (73% de la población).

Y también en España habrá 345 millones de dispositivos conectados en 2021 (7 conexiones por habitante), desde los 196 millones contabilizados en 2016.

Al mismo tiempo, poco se puede decir sobre el avance tecnológico que no seamos todos capaces de percibir en nuestro día a día.

El desarrollo de Internet está en la base de este avance. Todos los servicios de la Sociedad de la Información se apoyan en la red y, al tiempo, han contribuido a su crecimiento y a la universalización de su utilización.

Un factor a destacar es que la presencia de Internet se hace patente no solo en los servicios que se prestan íntegra y directamente "on line", sino también en la cada vez más frecuente integración de actividades "off-line" con versiones o utilidades en línea. O dicho de otro modo es creciente la penetración de la dimensión "on line" en el que tendemos a definir como "mundo real", pese a que ambos lo son.

Esto es muy evidente en sectores como el financiero o comercial, donde grandes superficies o bancos aúnan la oferta en establecimientos físicos con alternativas en la red que están cobrando cada vez mayor protagonismo.

Quizá es menos obvio, pero igualmente real, en multitud de otras actividades. El más sencillo modelo de teléfono inteligente tiene una capacidad de procesamiento de información superior a la de los grandes ordenadores que hace algunos años que estaban solo al alcance de las empresas. Y además permite hacer llamadas telefónicas.

El futuro inmediato se anuncia también cargado de novedades en este terreno.

Conceptos como "big data", "Internet de las cosas", "inteligencia artificial", "blockchain" y las tecnologías asociadas a ellos y que los hacen posibles, van a tener, están teniendo ya, un impacto enorme en el ámbito de los datos personales.

Porque con independencia del lugar que ocupemos por nuestra actividad profesional, empresarial o política, todos desempeñamos durante buena parte de nuestras vidas el papel de ciudadanos titulares de esos datos. Y nos veremos afectados por el uso que se haga de ellos.

Estos efectos pueden analizarse desde diferentes perspectivas, y una de ellas es la de la protección de

los derechos de las personas en la utilización de esos datos.

Las modernas tecnologías y su empleo de la información personal han mejorado nuestra vida, y sin duda lo harán aún más en los próximos años. Son un factor determinante para el cambio y la innovación.

El acceso a la información y a la formación del que disfrutamos actualmente no tiene parangón con el que se nos ofrecía en un pasado no demasiado lejano.

Una información que es, además, más plural y variada. Ya no hay un número limitado de actores en los procesos de comunicación. Es una comunicación abierta y multidireccional.

Internet, y el uso de nuestros datos, nos ofrecen mayores posibilidades de relación personal y una enorme diversidad de formas de gestionar nuestro ocio.

No se puede de ninguna manera ignorar su impacto en la actividad económica. Nuevos negocios, nuevos modelos de negocio, una forma diferente de gestionar las relaciones de las empresas con sus clientes son el resultado de la irrupción de las nuevas tecnologías en el entorno empresarial.

Las tecnologías son un factor fundamental de generación de riqueza en el marco de la economía digital.

Y es necesario aludir también a sus efectos en el terreno de las políticas públicas, incluidas las relacionadas con la seguridad. Las tecnologías y el análisis de la información contribuyen de manera significativa a una mejor identificación de las necesidades de los ciudadanos y a una mejor prestación de los servicios que demandan.

Igual que lo hacen en la lucha contra la delincuencia, especialmente en sus manifestaciones más graves, tanto en la dimensión preventiva como en la de persecución y enjuiciamiento de los responsables.

Es crucial su papel en el desarrollo de la investigación científica en todos los campos, pero en particular en el de la salud. Gracias a estos avances y a la capacidad que ofrecen de procesar grandes cantidades de información se están pudiendo identificar las causas, y también las respuestas, de enfermedades que hasta ahora se resistían al estudio por métodos tradicionales.

Pero si las posibilidades y ventajas son grandes, también lo son los riesgos que se plantean para los ciudadanos.

Algunos de estos riesgos tienen que ver simplemente con una cuestión de cantidad y de estadística. Cuantos más datos hay circulando sobre más aspectos de las vidas de las personas, más probabilidades hay de que algo vaya mal y de que ese problema tenga consecuencias graves para los afectados.

Pero otros riesgos están asociados, sobre todo, a usos no previstos, injustos o ilegales de esa información.

Desgraciadamente es de la máxima actualidad el uso aparentemente ilegal de datos obtenidos a través de una aplicación distribuida en la red social Facebook, que en principio tenía finalidades investigación científica, con el objeto de manipular procesos electorales.

Estaríamos ante un ejemplo perfecto de uso ilegal e interesado de unos datos proporcionados de buena fe y con el convencimiento de que se usarían en el marco de una investigación científica. No sólo resultarían afectados el derecho a la intimidad y a la protección de

datos de las personas afectadas, sino que estaríamos ante un ataque directo a los propios cimientos del sistema democrático.

Y todo ello a partir de un uso no autorizado de unas informaciones; un uso sobre el que sus titulares no tenían ningún conocimiento.

Podrían citarse numerosos casos de características similares.

Muchos de ellos obedecen a razones que tienen que ver con el modo en que se ha configurado y ha evolucionado la economía en el entorno digital.

Se trata de un sector que ha conocido un intenso proceso de concentración en poco más de una década. Con un grupo reducido de actores en posiciones dominantes que almacenan cantidades ingentes de información.

Al mismo tiempo, el modelo de negocio de muchos, si no de la mayoría, de prestadores de servicios de la sociedad de la información está basado en la monetización de la información personal de sus usuarios.

En principio, esos datos se comercializan con fines de publicidad comercial. Pero también podría hacerse con otro tipo de finalidades. Por ejemplo, con destino a empresas que quieren conocer los perfiles de sus potenciales clientes para determinar los precios a los que van a ofrecerles sus productos o servicios.

Pronto se cumplirán cinco años de las revelaciones de Eduard Snowden que pusieron en evidencia cómo, con unos muy legítimos fines de lucha contra el terrorismo y otras formas graves de delincuencia organizada, los servicios de inteligencia estadounidenses habían desarrollado proyectos para acceder a los datos de ciudadanos manejados por las grandes compañías de Internet.

Entre estos datos se encontraban los de ciudadanos en la Unión Europea que habrían sido transferidos a Estados Unidos en el marco del conocido como Esquema de Puerto Seguro. Un instrumento que fue declarado ilegal por el Tribunal de Justicia de la Unión Europea, precisamente como consecuencia de la falta de límites y garantías en ese acceso de los servicios de información.

Las posibilidades que las tecnologías ofrecen para la recogida y tratamiento de la información personal se nos presentan así como prácticamente ilimitadas.

Muchas personas afirman que están dispuestas a ofrecer sus datos personales a cambio de servicios. Pero, al mismo tiempo, esas mismas personas nos dicen que desconfían de los servicios digitales y que quieren recuperar el control, o tener un mayor control, sobre la información que les proporcionan.

Uno de los principales obstáculos para el desarrollo de la economía digital es la falta de confianza de los ciudadanos. El conjunto de los retos mencionados necesita respuestas. Respuestas que permitan garantizar los derechos de los ciudadanos europeos en un mundo de servicios globalizados que en muchas ocasiones se prestan desde fuera de la Unión Europea.

Precisamente para afrontar con garantías todos estos retos y generar la confianza necesaria entre los distintos actores implicados, la Agencia puso en marcha en 2016 la Unidad de Evaluación y Estudios Tecnológicos (UEET), como unidad especializada para analizar

las implicaciones de los nuevos desarrollos, realizar estudios prospectivos y evaluar los productos y servicios que están en el mercado; todo ello en colaboración con la universidad, con grupos de investigación tecnológica, con la industria y con las administraciones públicas competentes en el fomento de las TIC.

- **El derecho al olvido en Internet: una necesidad de nuestro tiempo**

Los motores de búsqueda se han convertido en herramienta esencial en la vida diaria de todos los usuarios de Internet. Sin ellos, sería enormemente difícil acceder a la información existente en la red. Pero, al mismo tiempo, su potencial resulta cada vez más problemático, por cuanto permiten localizar instantáneamente, salvando cualquier barrera de tiempo y espacio, información de todo tipo relativa a una persona. Las capacidades de recuperación y agregación de los motores de búsqueda pueden ocasionar considerables perjuicios a los individuos, tanto en su vida personal como en sus relaciones sociales.

Una de las cuestiones más importantes del debate actual sobre la privacidad en la red es el relacionado con lo que se ha dado en llamar el "derecho al olvido".

Las resoluciones de la Agencia Española de Protección de Datos en materia de tutela de derechos, y muy singularmente del derecho de cancelación, venían siendo atendidas puntualmente por los responsables de las diferentes páginas Web, pero no ocurría lo mismo cuando la resolución tenía como destinatario a Google: el mayor prestador del servicio de búsqueda impugnaba sistemáticamente las resoluciones de la Agencia ante la jurisdicción contencioso-administrativa.

La Audiencia Nacional decidió el 27 de febrero de 2012 y antes de resolver los recursos interpuestos por Google, plantear una cuestión prejudicial ante el Tribunal de Justicia de la Unión Europea. Pretendía recabar la interpretación del Tribunal europeo sobre varios apartados de la Directiva 95/46/CE que resultaban relevantes para la resolución de los más de 200 recursos pendientes ante la Audiencia; en concreto, determinadas cuestiones relevantes sobre la ley aplicable, la responsabilidad de los buscadores y los titulares de los sitios web, las competencias de las autoridades de protección de datos y la posibilidad de evitar la indexación de la información personal.

El 13 de mayo de 2014, siendo Director de la Agencia D. José Luis Rodríguez Álvarez, el Tribunal de Justicia de la Unión Europea emitió su sentencia en el asunto C131/12 (Google Spain, S. L., Google Inc. vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González), resolviendo la citada cuestión prejudicial planteada en 2012 por la Audiencia Nacional.

La Sentencia asumió totalmente la tesis que venía defendiendo la Agencia Española de Protección de Datos, y sus pronunciamientos provocaron el cambio de la política de privacidad de Google, convirtiendo a la Agencia en un referente a nivel mundial entre las Autoridades de control.

En esencia, la Sentencia estableció que el derecho europeo, y más concretamente la legislación española, son aplicables a Google y lo justifica en que la empresa cuenta con un establecimiento en territorio europeo.

De otra parte, la Sentencia consideró que las operaciones técnicas que realizan los motores de búsqueda para encontrar la información en Internet se integran en la

definición de "tratamiento" que ofrece la Directiva, y que los propios motores de búsqueda son los responsables de ese tratamiento porque deciden sobre los medios y sobre sus fines.

El Tribunal europeo destacó asimismo que la actividad de los buscadores tiene un impacto significativo sobre los derechos fundamentales del respeto a la vida privada y de protección de los datos personales, ya que en las búsquedas que se realizan en Internet a partir del nombre de una persona, se puede obtener una visión completa y estructurada de toda la información existente sobre ella y ello permitiría la elaboración de perfiles más o menos detallados. Para la Sentencia, son la difusión y accesibilidad universales que ofrecen los motores de búsqueda las que pueden dar lugar a lesiones sobre los derechos de las personas de una forma mucho más intensa y grave que la publicación original de la información.

El Tribunal de Justicia no asume la tesis según la cual la actividad del buscador estaría, como tal, legitimada por el ejercicio de la libertad de expresión. Para el Tribunal, el interés legítimo que el buscador puede aducir para desarrollar los tratamientos que realiza es meramente económico y no basta para justificar la grave injerencia sobre los derechos individuales que conlleva.

Con carácter general, los derechos de la persona afectada prevalecerían también sobre ese interés en localizar una información mediante búsquedas nominativas, pero en cada caso específico ese equilibrio dependerá de la ponderación entre la naturaleza de la información de que se trate, de su carácter sensible para la vida privada de la persona afectada y del interés del público en disponer de la información. Es importante destacar que el Tribunal señala expresamente que no es necesario que se cause un perjuicio para ejercer el derecho frente al buscador.

En mayo de 2015 la Agencia tras las oportunas actuaciones de inspección declaró ilícita la práctica de Google por la cual, a través del servicio Webmaster Tools, comunicaba a los responsables de las diferentes páginas web qué información de sus sitios web estaba siendo eliminada de los resultados de búsqueda. De esta forma, los editores de esas páginas web, simplemente volviendo a editar la información o con un pequeño cambio en la URL, recuperaban la información eliminada, que volvía a aparecer inmediatamente en las búsquedas a través de Google.

- **El servicio Street View**

En octubre de 2010, tras una exhaustiva investigación previa, la Agencia inició un procedimiento sancionador a Google Inc. y Google Spain por la captación y almacenamiento de datos de localización de redes inalámbricas abiertas (redes Wi-Fi) y de datos de tráfico transferidos a través de ellas por los vehículos utilizados para obtener imágenes para el servicio Street View.

La existencia de un procedimiento judicial penal abierto obligó a la Agencia a suspender la tramitación de su procedimiento sancionador. En 2017, una vez se tuvo conocimiento de la firmeza del Auto que acordó el sobreseimiento y archivo de las actuaciones en vía penal, la Agencia reanudó el procedimiento administrativo.

Se comprobó que Google recogía información de las WiFi abiertas de los usuarios, sin que los afectados tuviesen conocimiento de que dicha recogida de datos se estaba llevando a cabo y sin su consentimiento. No

se constató que Google tratase datos especialmente protegidos a través de estos sistemas.

En octubre de 2017 la Agencia dictó resolución declarando la existencia de una infracción grave e imponiendo a Google una sanción de 300.000 euros. En cuanto a que los datos se recogiesen de redes WiFi abiertas, la resolución especifica que "el hecho de que los titulares de redes WiFi no aseguren el cifrado de estas redes, en perjuicio de la seguridad de sus datos, no autoriza en modo alguno la recogida de la información llevada a cabo ni ningún uso posterior de la misma".

- **La política de privacidad de Google**

La Agencia inició un procedimiento para analizar la compatibilidad de la política de privacidad y de las condiciones de uso de los servicios de Google con la normativa española de protección de datos. En el marco de esta investigación, se constató que Google recoge y trata ilegítimamente información personal, tanto de los usuarios autenticados (dados de alta en sus servicios) como de los que no, e incluso de quienes son meros "usuarios pasivos" que no han solicitado sus servicios pero que acceden a páginas que incluyen elementos gestionados por la compañía sin explicitarlo.

Las actuaciones de inspección permitieron comprobar que Google recopila información personal a través de casi un centenar de servicios y productos que ofrece en España, sin proporcionar en muchos casos una información adecuada sobre qué datos se recogen, para qué fines se utilizan y sin obtener un consentimiento válido de sus titulares.

Así, por ejemplo, no se informa con claridad a los usuarios de Gmail de que se realiza un filtrado del contenido del correo y de los ficheros anexos para insertar publicidad. Cuando se informa, se utiliza una terminología imprecisa, con expresiones genéricas y poco claras que impiden a los usuarios conocer el significado real de lo que se plantea.

La falta de información adecuada sobre las finalidades específicas que justifican el tratamiento de los datos impide que pueda considerarse que existe un consentimiento específico e informado y, en consecuencia, válido.

Por otra parte, Google combina la información personal obtenida a través de los diversos servicios o productos para utilizarla con múltiples finalidades que no se determinan con claridad, y vulnera con ello la prohibición de utilizar los datos para fines distintos de aquellos para los que han sido recabados.

En contra de lo exigido por la legislación española, Google almacena y conserva datos personales por periodos de tiempo indeterminados o injustificados. La conservación de los datos por tiempo indefinido, más allá de las exigencias que se derivan de las finalidades pretendidas en el momento de la recogida, constituye un tratamiento ilícito.

Finalmente, la Agencia concluyó que Google obstaculiza -y en algunos casos impide- el ejercicio de los derechos de acceso, rectificación, cancelación y oposición. El procedimiento que los ciudadanos deben seguir para ejercer sus derechos o gestionar su propia información personal les obliga a recorrer un sinfín de páginas dispersas en varios enlaces que no están disponibles para todos los tipos de usuarios y, en ocasiones, con denominaciones que no siempre hacen referencia a su objeto.

La AEPD declaró la existencia de tres infracciones de la LOPD e impuso a Google una sanción de 300.000 euros por cada una de ellas, requiriéndole para que cumpliera con la ley sin dilación.

Como consecuencia de esta actuación de la Agencia, cambió la política de privacidad de Google a nivel mundial, introduciendo modificaciones significativas en materia de información, consentimiento y ejercicio de derechos.

• La información en la nube o "cloud computing"

La prestación de servicios de "cloud computing" en sus distintas tipologías de nube (pública, privada, híbrida, etc.) y de modalidades de servicios (infraestructura como servicio, plataforma como servicio y software como servicio) ha venido a modificar las relaciones tradicionales entre los clientes -responsables del tratamiento de los datos- y los encargados del tratamiento -prestadores de servicios de "cloud computing"-.

El cambio de paradigma en esas relaciones determinó que la Agencia iniciara un proceso de análisis sobre sus implicaciones y sobre las modulaciones necesarias en la aplicación de la normativa de protección de datos para garantizar los derechos de los ciudadanos.

Este análisis concluyó con la elaboración de una guía sobre cloud computing, cuyos aspectos más destacados son los siguientes:

- La legislación aplicable en materia de protección de datos es la del cliente que trata datos en España.
- El proveedor de servicios de *cloud computing* es un encargado de tratamiento, aunque sea una gran compañía multinacional. El cliente que contrata con el proveedor de servicios sigue siendo responsable del tratamiento de los datos y debe actuar diligentemente en la elección de prestador de servicios de cloud. El proveedor de servicios por su parte debe ser diligente a la hora de facilitar garantías para la protección de datos. En esa diligencia juega un importante papel la transparencia que permita obtener información sobre esas garantías y, en particular, sobre las existentes en la subcontratación de servicios y en las transferencias internacionales de datos.
- El cliente debe informarse sobre si las medidas de seguridad son adecuadas para el tratamiento de los datos y obtener garantías para auditarlas, aunque sea a través de un tercero fiable e independiente.
- El cliente debe obtener garantías para que, al término de contrato, pueda recuperar los datos personales, o bien trasladarlos a un nuevo proveedor de estos servicios.

• La crisis del Sistema de Puerto Seguro

El 6 de octubre de 2015 se produjo la crisis del sistema que servía de base para las transferencias internacionales de datos desde Europa a Estados Unidos. Ese día se publicó el fallo del Tribunal de Justicia de la Unión Europea que invalidaba la Decisión de la Comisión Europea 2000/520/CE, conocida como Decisión de Puerto Seguro, que regulaba la transferencia de datos desde la Unión Europea a aquellas entidades establecidas en Estados Unidos y acogidas al sistema de "Puerto Seguro".

La decisión del Tribunal fue consecuencia de una reclamación de Maximiliam Schrems, de nacionalidad austríaca y usuario de Facebook, en la que pedía que Facebook Irlanda no transfiriera los datos a Facebook Inc., su matriz con sede en Estados Unidos.

El reclamante alegaba que el derecho y las prácticas en vigor estadounidenses no garantizaban una protección suficiente de los datos personales conservados en su territorio contra las actividades de vigilancia practicadas por sus autoridades públicas. El Sr. Schrems hacía referencia en ese sentido a las revelaciones de Edward Snowden sobre las actividades de los servicios de información de Estados Unidos, en particular las de la National Security Agency (NSA).

Entre las motivaciones de la Sentencia se encuentra la revelación de la existencia en Estados Unidos de varios programas de vigilancia para la recogida y el tratamiento de información a gran escala de datos personales.

Se constató que, como consecuencia, por ejemplo, de la contratación de servicios de Internet, las autoridades norteamericanas tenían acceso a datos personales de residentes europeos y que esos datos eran utilizados para finalidades diferentes e incompatibles con aquellas que justificaron las transferencias. Se acreditó además que los interesados no podían ejercitar ninguna acción legal para acceder a sus datos personales y que les estaba igualmente vetada su rectificación o supresión.

El pronunciamiento afectó a empresas de Internet, como Google, Facebook, Microsoft, Apple o Yahoo, que cuentan con centenares de millones de clientes en Europa y transfieren los datos personales de esos clientes para su tratamiento desde Europa a Estados Unidos.

También influyeron en el fallo las revelaciones del Sr. Snowden sobre las actividades de la National Security Agency (NSA) que, al amparo de motivaciones de seguridad nacional, interés público o cumplimiento de la ley norteamericana, podían conocer los datos de europeos que habían sido transferidos a Estados Unidos, sin ninguna regla para limitar las posibles injerencias en los derechos de éstos.

La supervisión de las acciones de los servicios de información se realiza a través de un procedimiento secreto y no contradictorio. Una vez transferidos los datos personales a Estados Unidos, la NSA y otros organismos federales, como el Federal Bureau of Investigation (FBI), pueden acceder a ellos en el contexto de la vigilancia y de las interceptaciones indiferenciadas que ejecutan a gran escala.

Todas estas razones y alguna otra motivaron la declaración de invalidez del sistema de Puerto Seguro. Por lo que entre dicha fecha (6 de octubre de 2015) y la del 12 de julio de 2016, en que se aprobó por la Comisión de la Decisión del "Escudo de la Privacidad" en sustitución de la anulada, la Agencia Española desplegó toda una serie de acciones destinadas a paliar la ausencia de garantías para los interesados cuyos datos habían sido y eran objeto de transferencias a entidades de Estados Unidos adheridas al sistema de Puerto Seguro.

• Los riesgos de la geolocalización

La proliferación de dispositivos móviles inteligentes ha supuesto la aparición de multitud de servicios que permiten localizar a sus titulares. Éstos utilizan sus móviles para conocer la previsión meteorológica, encontrar una calle, localizar a amigos o buscar un determinado servicio en un lugar específico.

La tecnología utilizada por estos terminales móviles, vinculados estrechamente a las personas, permite a los proveedores de servicios de geolocalización, mediante la captación de señales de estaciones de base y de puntos de acceso Wi-Fi, disponer de detalles de hábitos y pautas de comportamiento del propietario del móvil, y, por ende, establecer perfiles exhaustivos de estos usuarios.

La Agencia participó en el análisis de este fenómeno realizado por el Grupo de Trabajo del artículo 29 del Comité Europeo de Protección de Datos, que concluyó en el Dictamen sobre los servicios de geolocalización que se aprobó en mayo de 2011 (WP 185).

En este mismo terreno, varios medios de comunicación publicaron que Google recopilaba información sobre la ubicación de los terminales móviles con sistema operativo Android, independientemente de que el usuario lo hubiera autorizado en los ajustes del sistema, e incluso aunque se encontrase desactivado el sistema de geolocalización del terminal.

La Agencia concluyó tras la correspondiente investigación que Google solo utiliza la información transmitida por estos terminales para establecer conexiones, pero no se registra en los servidores de la entidad, ni se usa para rastrear la ubicación de los usuarios.

- **Los avances en el reconocimiento facial**

En los últimos años ha habido un rápido incremento en la disponibilidad y precisión de la tecnología de reconocimiento facial. Esta tecnología ha sido integrada en servicios online y dispositivos móviles que permiten a los usuarios capturar imágenes y vincularlas en tiempo real a una amplia variedad de servicios online. Como resultado, los usuarios pueden tomar fotografías con su teléfono móvil, etiquetar a personas, que pueden o no estar registrados en el servicio, y compartir las imágenes con otros usuarios.

La popularización de estos servicios, su implantación en redes sociales o en servicios de reconocimiento facial y etiquetado de fotografías como “Find my Face” de Google, conlleva una serie de desafíos para la privacidad. Entre ellos, el tratamiento de imágenes digitales de personas que no utilizan el servicio y no han dado su consentimiento para ello, la utilización de las imágenes para otras finalidades distintas para las que fueron tomadas, o la posibilidad de buscar personas mediante la introducción de su imagen en un buscador obteniendo como resultado imágenes coincidentes o el perfil de la persona en redes sociales.

- **La recopilación de datos por las redes sociales (Facebook)**

En septiembre de 2017 la Agencia concluyó las actuaciones iniciadas para analizar si los tratamientos de datos que realiza la red social Facebook se adecúan a la normativa de protección de datos.

En el marco de la investigación realizada, la Agencia constató que Facebook recababa datos sobre ideología, sexo, creencias religiosas, gustos personales o navegación sin informar de forma clara acerca del uso y finalidad que le iba a dar a los mismos. En concreto, se verificó que la red social trataba datos especialmente protegidos con fines de publicidad, entre otros, sin obtener el consentimiento expreso de los usuarios como exige la normativa de protección de datos.

La investigación también permitió comprobar que Facebook no informaba a los usuarios de forma exhaustiva y clara sobre los datos que iba a recoger y los tratamientos que pretendía realizar con ellos, sino que se limitaba a dar algunos ejemplos. En particular, la red social recogía datos derivados de la interacción que llevan a cabo los usuarios en la plataforma y en sitios de terceros sin que éstos puedan percibir claramente la información que Facebook recoge sobre ellos ni con qué finalidad la va a utilizar.

La Agencia también confirmó que los usuarios no eran informados de que se iba a tratar su información mediante el uso de cookies -algunas de uso específicamente publicitario y otras de uso declarado secreto por la compañía- cuando navegan por páginas que no son de Facebook y que contienen el botón 'Me gusta'.

Esta situación también se producía cuando los usuarios no eran miembros de la red social pero habían visitado alguna vez alguna de sus páginas, y cuando algún usuario registrado en Facebook navegaba por páginas de terceros, incluso sin iniciar sesión en Facebook. En estos casos, la plataforma añadía la información recogida en dichas páginas a la información asociada a su cuenta en la red social.

Por todo ello, la Agencia consideró que la información facilitada por Facebook a los usuarios no se ajustaba a la normativa de protección de datos. Igualmente se constató que la política de privacidad de Facebook contenía expresiones genéricas y poco claras, y obligaba a acceder a multitud de enlaces distintos para conocerla.

La red social hacía referencia de forma muy imprecisa al uso que daba a los datos que recogía, de forma que un usuario de Facebook con un conocimiento medio de tecnología no llega a ser consciente de la recogida de datos, ni de su almacenamiento y posterior tratamiento, ni de para qué van a ser utilizados.

En relación con la conservación de datos, cuando un usuario de la red social ha eliminado su cuenta y solicita el borrado de la información, Facebook capta y trata información durante más de 17 meses, por lo que los datos no son cancelados en su totalidad, ni cuando han dejado de ser útiles para el propósito para el que se recogieron, ni cuando el usuario solicita explícitamente su eliminación.

La Agencia impuso a Facebook una sanción de 1.200.000 euros.

• Caso Facebook Messenger

En mayo de 2016 una usuaria de Facebook denunció ante la Agencia que las cuentas de Facebook disponen de un servicio de mensajería integrado, denominado Chat, que le permite conocer a un usuario de Facebook cuándo otros usuarios están conectados o cuándo ha sido su última conexión, y que el usuario no tiene la capacidad de impedir que otro pueda monitorizar su actividad.

La Agencia inició actuaciones de inspección, que siguen su curso a fecha de cierre de este libro, en las que se ha podido comprobar el funcionamiento de este servicio:

- Cuando un 'amigo' del usuario tiene una sesión iniciada en Facebook y el servicio de Chat activado, en la cuenta del usuario y asociado al nombre del 'amigo' aparece una señal, un indicador verde, que revela que el 'amigo' tiene sesión abierta en

ese momento. En el caso que el 'amigo' no esté conectado, no aparece el indicador verde, pero sí un valor numérico, que revela hace cuántos minutos tuvo la sesión abierta en por última vez.

- En la página principal de la política de privacidad de Facebook no existe información explícita y completa sobre la revelación de la información de conexión y su posterior utilización o revelación a terceros o una referencia a cómo administrar el registro de tiempos de conexión, entre otras.

• Los cambios en la política de privacidad y los términos de servicio de Whatsapp tras la compra por Facebook

Cuando Facebook adquirió el servicio de mensajería Whatsapp en octubre de 2016, la Agencia Española de Protección de Datos decidió abrir actuaciones de oficio para determinar el modelo general de tratamiento, la extensión de los datos transferidos, el ámbito de procesamiento y la base jurídica de la comunicación de datos en los que están implicadas tanto la empresa Whatsapp como Facebook.

Facebook impuso como obligatoria la aceptación de nuevas condiciones para poder hacer uso de la aplicación de mensajería que le permitían utilizar los datos personales para finalidades que no tienen relación con las establecidas en la recogida de datos original, sin una información adecuada y sin posibilidad de oponerse a ello. Al exigir que los usuarios presten su consentimiento en estos términos y, teniendo en cuenta la implantación social de la aplicación de mensajería, el consentimiento prestado no puede considerarse libre y, por tanto, válido.

Durante las actuaciones de la Agencia ambas entidades admitieron que comparten información de los usuarios de la aplicación Whatsapp. En concreto, Whatsapp confirmó que "actualmente" comparte con Facebook información de todos los usuarios de Whatsapp, sean o no usuarios de Facebook, y que esa información se transmite en tiempo real.

En concreto, ambas entidades detallaron que comparten el identificador de la cuenta de usuario de WhatsApp, incluyendo un identificador común incluido en las aplicaciones de Facebook y WhatsApp; información sobre el dispositivo, el prefijo y código de la red móvil del país, información de la plataforma, y de la versión de la aplicación que permiten un seguimiento de la aceptación de la actualización de las aplicaciones y las opciones de control; el "estado de última conexión" del usuario, esto es, información sobre la última vez en que el usuario utilizó el servicio y la fecha en que el usuario se dio de alta en su cuenta de WhatsApp.

Por otro lado, se constató que las cesiones o comunicaciones de datos personales entre Whatsapp y Facebook que no guardan relación con las finalidades que determinaron su recogida, se realizan sin ofrecer a los usuarios opción alguna para mostrar su negativa a las mismas, por cuanto Whatsapp únicamente habilitó mecanismos para aceptar la cesión de información con la finalidad de "mejorar mi experiencia con los productos y publicidad en Facebook" y únicamente en el caso de usuarios existentes. Por tanto, el consentimiento que se presta con la aceptación de la Política de Privacidad y Términos de Servicio no puede considerarse libre, y ello impide que el consentimiento prestado pueda considerarse válido.

Cabe añadir que la información sobre los posibles destinatarios de los datos, sobre las finalidades para las que se le ceden o la utilización que harán de los mismos los cesionarios se ofrece de forma poco clara, con expresiones imprecisas e inconcretas que no permiten deducir, sin duda o equivocación, la finalidad para la cual van a ser cedidos los datos.

Por todo ello, en septiembre de 2017 la Agencia inició un procedimiento sancionador a Whatsapp, y a Facebook, que concluyó en la imposición de una sanción económica de 300.000 euros a cada una de las entidades.

- **El Plan Estratégico de la Agencia Española de Protección de Datos**

La Agencia se dotó en noviembre de 2015 de un Plan Estratégico que guiara sus actuaciones en el periodo 2015-2019, estructurado en cinco ejes: prevención, innovación, transparencia y participación, cercanía a los responsables y a los profesionales de la privacidad y agilidad y eficiencia.

El Plan Estratégico responde no sólo a la necesaria puesta al día tras veinticinco años de funcionamiento, sino también, y sobre todo, a la exigencia de dotar a la Agencia de una base sólida para afrontar el esfuerzo adicional de adaptación al Reglamento europeo, tanto del ordenamiento jurídico español, como de la propia estructura y procedimientos de actuación de la Agencia.

Así lo entendieron los principales destinatarios del Plan Estratégico que realizaron casi cuatrocientas aportaciones con ocasión del proceso de consulta pública que tuvo lugar para la elaboración del Plan.

El Plan Estratégico se plasmaba en 113 iniciativas, que se han visto incrementadas sucesivamente hasta las 145 existentes en la actualidad.

Así, por una parte, la Agencia ha desplegado una intensa actividad de información y divulgación de la cultura de la privacidad dirigida a los ciudadanos, con el objetivo de que conozcan cuáles son sus derechos y sepan cómo hacerlos valer.

Con esta finalidad, se han elaborado varias guías: privacidad y seguridad; derechos del ciudadano; centros docentes; compra segura en Internet, protección de datos y prevención de delitos, administradores de fincas, pacientes y usuarios de la sanidad o videovigilancia.

También se han creado *microsites* en la web de la Agencia para temas específicos; en concreto, sobre reclamaciones en materia de telecomunicaciones o sobre publicidad no deseada.

La Agencia sigue empeñada en que la protección de datos sea una temática que se aborde en los medios de comunicación tradicionales. Así, ha puesto en marcha una campaña específica para informar sobre las implicaciones derivadas de la entrada en vigor del nuevo Reglamento UE; campaña que consiguió la declaración de 'campaña de servicio público' y, por tanto, su difusión gratuita en los canales de A3media, Mediaset, TVE1 y Radio5.

También ha sido muy significativa la labor en el terreno digital: la nueva página web de la Agencia, en la que se aloja el Blog que contiene análisis relevantes sobre privacidad; la mejora y actualización de las 'preguntas frecuentes', el nuevo diseño del canal de atención al ciudadano y, por último, la intensa presencia de la Agencia en la red Twitter; un terreno, el de las redes sociales, en el que la Agencia se propone seguir avanzando.

Una parte importante de la política de prevención de la Agencia se despliega como consecuencia de las conclusiones que se extraen en los llamados Planes Sectoriales de Inspección. En estos últimos años se ha trabajado de forma específica en hospitales públicos; servicios de *cloud computing* en el sector educativo; contratación a distancia; entidades financieras, y sector sociosanitario

La Agencia ha querido focalizar su trabajo de prevención en tres sectores: el tecnológico, la publicidad y los menores de edad.

En septiembre de 2017 la Agencia Española de Protección de Datos y la Asociación para la Autorregulación de la Comunicación Comercial (Autocontrol) firmaron un Protocolo de actuación, para la implantación de un nuevo sistema de mediación voluntaria en el que participan Movistar, Orange/Jazztel, Simyo, Yoigo/Masmóvil/Pepephone/Happy/Llamaya, Vodafone y Ono.

De acuerdo con este procedimiento, los ciudadanos que hayan presentado una reclamación en materia de suplantación de identidad o recepción de publicidad no deseada ante estas compañías y no hayan obtenido una respuesta satisfactoria pueden recurrir a la mediación de Autocontrol.

Recibida la reclamación, Autocontrol comprobará que cumple con los requisitos establecidos y, de ser así, iniciará el proceso de mediación para promover que las partes alcancen un acuerdo que solucione la controversia.

Este sistema de mediación es perfectamente compatible e independiente de las reclamaciones que los ciudadanos pueden seguir planteando ante la Agencia.

La Agencia ha trabajado también de forma especial en el ámbito de la publicidad con el objetivo de ampliar los derechos de los ciudadanos frente a la publicidad no deseada. Se ha reforzado el servicio de exclusión publicitaria conocido como «Lista Robinson», gestionado y prestado por ADIGITAL, y que ya cuenta con más de 600.000 ciudadanos inscritos.

En concreto, se han incrementado las posibilidades de los ciudadanos para oponerse a la publicidad no deseada, mediante una mayor selección de sus preferencias. Así un ciudadano puede ahora decidir que no quiere publicidad en el correo electrónico, pero sí en

su móvil, o que quiere que le manden publicidad sobre viajes o electrónica, pero no de otros asuntos).

La protección de los derechos y libertades de los menores en lo que afecta al tratamiento de sus datos personales constituye una de las constantes preocupaciones de la Agencia; una preocupación que se ha visto incrementada con el auge de los servicios de Internet, en particular de las redes sociales.

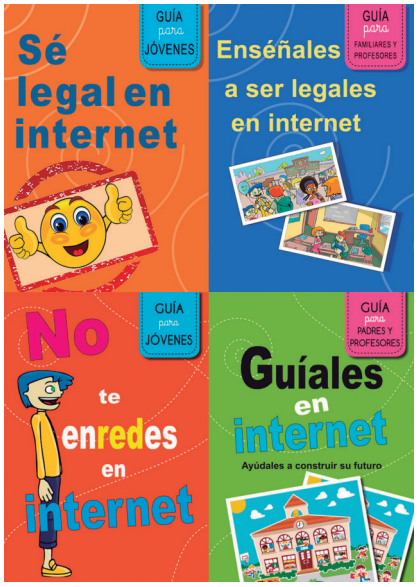
La Agencia elaboró en 2007 el "Plan de Protección de los datos personales de los menores en Internet" y, en 2008, la guía "Navega seguro" sobre los derechos de los niños y los deberes de los padres.

La Agencia hacía suya la preocupación de la sociedad ante los riesgos del uso de Internet reflejada en el barómetro del CIS de septiembre de 2009, en el que más del 80% de los ciudadanos consideraban que la preocupación es mayor aún respecto de los menores.

Desde entonces la Agencia dirige sus actuaciones en este ámbito a la formación, concienciación y sensibilización de menores, padres y, del sistema educativo que cuenta con más de 8 millones de alumnos.

Las distintas autoridades de protección de datos, las agencias vasca, catalana, de la Comunidad de Madrid y española, colaboraron en la elaboración de un recurso formativo sobre protección de datos y privacidad en relación con los menores. Además, la Agencia instó a Facebook a establecer en 14 años la edad de entrada en la red social en España, cuando en sus términos y condiciones de uso está establecida en 13 años conforme a la normativa norteamericana.

En 2013, se creó el portal "Tú decides en Internet" (www.tudecidesenInternet.es), con contenidos destinados a educar y sensibilizar a la población más joven de la importancia de la privacidad y del valor que tienen los datos de carácter personal para su salvaguarda.



En 2015, se renovó el portal no sólo desde el punto de vista de la imagen, sino también incorporando nuevos materiales y recursos (nuevas guías, vídeos, canales de ayuda, concursos infantiles, talleres...), que lleva recibidas más de 335.000 visitas hasta el cierre de este libro.

Además se ha trabajado en este terreno de la protección de los menores en el mundo online con diferentes agentes públicos (Ministerios de Educación, de Justicia, de Sanidad y Servicios Sociales, de Interior, Fiscalía de menores, Red.es, INCIBE, INJUVE, la CNMC) y también privados (Fundación ANAR, el Observatorio

de Contenidos Audiovisuales, Pantallas Amigas, o Telefónica, Orange, Google, RTVE, Mediaset o Atresmedia).

Para fomentar la difusión y conocimiento de la protección de datos y la importancia que tiene para la formación y el desarrollo de los menores se han llevado a cabo, además de jornadas, sesiones o talleres informativos y divulgativos, campañas de divulgación a través de la televisión. Se ha obtenido la colaboración del canal Clan de TVE y del grupo Mediaset para la difusión de aquellos consejos fundamentales para disfrutar de una navegación sin riesgos por Internet.

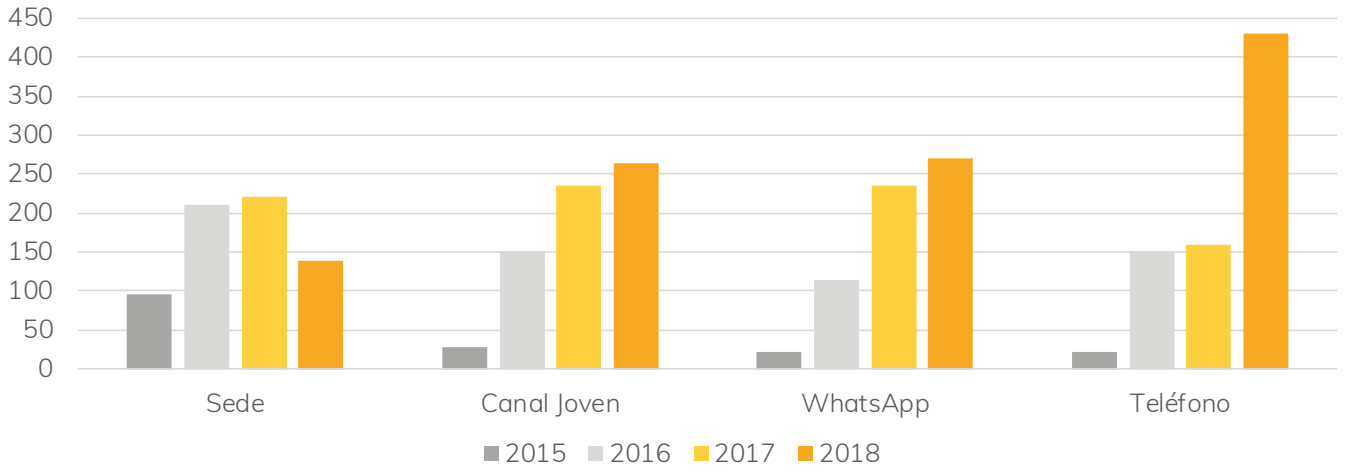
En 2015 la Agencia Española de Protección de Datos estableció un canal de atención específico para informar y asesorar a familias, profesores, monitores y a los propios menores sobre cuestiones de privacidad.

Este canal cuenta con una dirección de correo electrónico (canaljoven@agpd,es), un teléfono de atención personal (901 233 144) y un sistema de WhatsApp (616 172 204).

Las consultas más frecuentes tienen que ver con las imágenes de los menores. En concreto, versan sobre controversias entre padres divorciados por la publicación de imágenes de sus hijos en redes sociales; utilización de imágenes de menores de 14 años en redes sociales, fundamentalmente en Facebook e Instagram, sin el consentimiento de sus padres o tutores legales; publicación en abierto en Internet de imágenes de

Gráfico 1
Evolución consultas Menores

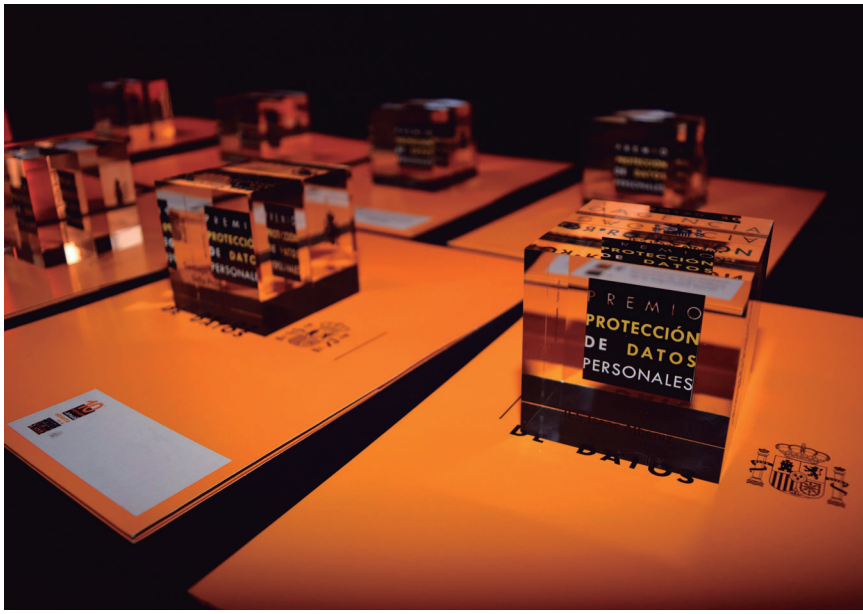
Fuente
Elaboración propia



menores que se han obtenido en grupos de WhatsApp, o en cuentas de redes sociales; tratamiento de datos de menores por parte de los centros educativos y las AMPAS, fundamentalmente la publicación de imágenes tanto en web propias como en redes sociales o utilización de plataformas educativas por parte de los centros educativos.

El déficit de formación y concienciación de los menores en el uso responsable de la información personal en Internet es la razón por la que la Agencia, al igual que otras instituciones, ha insistido en la inclusión de la formación sobre protección de datos personales, privacidad e Internet en los planes de estudio y en los currículos académicos. Objetivo que finalmente se ha visto cumplido en la Ley Orgánica de Protección de Datos Personales y Garantías de los Derechos Digitales, cuyo artículo 83.1 establece que el sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente, con el respeto y la garantía de la intimidad personal y familiar y la protección de los datos personales. Igualmente, se garantiza que el profesorado reciba las competencias digitales y la formación necesaria para su enseñanza.

A esa constante tarea de concienciación sobre los peligros que acechan a nuestra privacidad, responde también la convocatoria anual de los Premios de la Agencia de Protección de Datos en sus diversas modalidades: comunicación, buenas prácticas educativas en Internet, buenas prácticas en la adaptación al Reglamento UE y premio de investigación en protección de datos personales «Emilio Aced».



Asimismo, la Agencia se ha propuesto acompañar a personas, entidades y administraciones en el camino del cumplimiento de la normativa de protección de datos. Para lograr que ese camino sea fácil de recorrer, se han elaborado herramientas o guías que pretenden facilitar ese cumplimiento:

- «FACILITA_RGPD», herramienta gratuita para la autoevaluación de riesgos para pymes con tratamientos de muy bajo riesgo; e infografía con orientaciones sobre los pasos a seguir para realizar la adaptación al Reglamento UE por aquellas empresas que no pueden hacerlo con la herramienta FACILITA_RGPD.

- «Guía del Reglamento General de Protección de Datos para responsables de tratamiento», con la información y explicaciones necesarias para preparar y adoptar las medidas correspondientes para cumplir con las previsiones del Reglamento UE.

- «Directrices para la elaboración de contratos entre responsables y encargados de tratamiento», para identificar los puntos clave a tener presentes en el momento de establecer la relación entre el responsable del tratamiento y el encargado del tratamiento, así como las cuestiones que afectan de forma directa a la gestión de la relación entre ambos.

- «Guía para el cumplimiento del deber de informar», para orientar sobre las mejores prácticas para informar a los interesados, en virtud del principio de transparencia, acerca de las circunstancias y condiciones del tratamiento de datos a efectuar, así como de los derechos que les asisten.

- «Orientaciones y garantías en los procedimientos de anonimización de datos personales», para garantizar la protección de datos personales en el desarrollo de estudios e investigaciones de interés social, científico y económico, e impulsar su desarrollo y divulgación.

- «Guía práctica de análisis de riesgos», hoja de ruta enfocada a la gestión de los riesgos potenciales asociados al tratamiento de datos desde su diseño, mediante el establecimiento de medidas de seguridad y control para garantizar los derechos y libertades de las personas.

- «Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al Reglamento UE»

- «Listado de cumplimiento normativo para facilitar la adaptación al Reglamento UE»

- «Guía de brechas de seguridad», dirigida a responsables de tratamientos de datos personales, con el objetivo de facilitar la interpretación del Reglamento UE en lo relativo a la obligación de notificar a la autoridad competente y, en su caso, a los afectados de modo que la notificación a la autoridad competente se haga por el canal adecuado, contenga información útil y precisa a efectos estadísticos y de seguimiento, y se adecúe a las nuevas exigencias del Reglamento.

- Adaptación de la Herramienta de evaluación de riesgos para Administraciones Públicas (PILAR) a los requerimientos del Reglamento.

- Documentos «El impacto del RGPD en la actividad de las Administraciones Públicas», y «El Delegado de Protección de Datos en las Administraciones Públicas».

- Guía sobre tratamientos de datos en el ámbito de las Administraciones Locales.

Se han desarrollado igualmente distintas iniciativas con las organizaciones empresariales más representativas en el ámbito de las PYMES y autónomos (CEPYME, ATA, UPTA...). En particular, hay que destacar el Protocolo suscrito entre la AEPD, CEOE y CEPYME para fomentar la difusión del RGPD y de aquellas herramientas, guías y publicaciones realizadas por la Agencia y que puedan ayudar a las pymes en el cumplimiento de sus obligaciones. Esta colaboración se ha concretado en un intenso programa de actos públicos desarrollado por la AEPD en todas las Comunidades Autónomas para la difusión entre los asociados de CEPYME de dichos recursos, en especial de la herramienta FACILITA_RGPD.

La adaptación a las nuevas exigencias del Reglamento UE es especialmente costosa para autónomos y pymes, nuestro tejido empresarial mayoritario. Por ello, la Agencia, más allá de la herramienta FACILITA viene desarrollando numerosas jornadas de formación y de difusión de las guías y herramientas elaboradas por la Agencia con las organizaciones empresariales más representativas CEOE, CEPYME, ATA, UPTA, ...).

Por otro lado, en los primeros meses de vigencia del Reglamento UE se ha prestado una especial atención a la figura del Delegado de Protección de Datos, figura obligada para las administraciones públicas y para un buen número de empresas y entidades.

Así, con el objetivo de garantizar una referencia de calidad en el mercado, la Agencia puso en marcha en julio de 2017 en colaboración con la Entidad Nacional de Acreditación (ENAC), un esquema de certificación de Delegados de Protección de Datos, convirtiéndose con ello en la primera autoridad europea que elabora un marco de referencia para esta figura.

En nuestro ordenamiento jurídico esta certificación no es la única vía para ser Delegado, pero desde la Agencia se ha considerado necesario ofrecer una referencia sobre los contenidos y elementos con los que debe contar cualquier mecanismo que pretenda certificar la cualificación y capacidad profesional de un Delegado de Protección de Datos.

También se ha realizado un importante esfuerzo de formación de los Delegados de Protección de Datos de las administraciones públicas, en colaboración con el INAP, los institutos de formación de empleados públicos de todas las Comunidades Autónomas, la Federación Española de Municipios y Provincias y el Colegio Oficial de Secretarios, Interventores y Tesoreros de la Administración Local.

Adicionalmente, se ha desarrollado un plan de formación con el INAP para funcionarios de las tres administraciones públicas, del que forma parte un curso on line que contará en 2018 con 9 ediciones; al que se suma un programa específico -online y presencial- de formación especializada para Delegados de Protección de Datos de las tres Administraciones.

Otra línea de trabajo la representan los distintos colegios profesionales. La Agencia ha suscrito un Protocolo con la Unión Profesional, entidad que reúne a los Consejos Generales y Superiores y Colegios profesionales de ámbito nacional, con más de un millón y medio de profesionales, para difundir entre sus organizaciones todas las herramientas, guías y materiales elaborados por la Agencia para ayudar al cumplimiento de las obligaciones derivadas del Reglamento UE.

Finalmente, la Agencia puso en marcha en 2017 un canal específico («INFORMA RGPD») para atender las consultas de responsables, encargados y delegados de protección de datos, que ha recibido ya más de tres mil consultas.

VI. La agencia del futuro

El Reglamento General de Protección de Datos. Principales novedades. Nuevos derechos

El 25 de mayo de 2016 se aprobó el nuevo Reglamento General de Protección de Datos, norma con la que la Unión Europea pretende dar respuesta a los retos que plantean el uso generalizado de las tecnologías de la información y las comunicaciones.

El Reglamento puede considerarse una evolución de la Directiva95/46/CE, a la que sustituye, y de la que recoge, reforzándolos, los principios básicos de la protección de datos y los derechos de los interesados.

Sin embargo, desde el punto de vista de los procedimientos y mecanismos de protección, el Reglamento contiene importantes novedades.

La primera de ellas es que el Reglamento es una norma que se aplica directamente en los Estados Miembros, sin necesidad de normas de trasposición. Estos podrán, eso sí, normas de desarrollo en los casos en que el Reglamento les habilite para ello. Así ha ocurrido en España con la Ley Orgánica de Protección de Datos Personales, cuya tramitación parlamentaria concluirá en el mes de noviembre de 2018.

Desde el punto de vista de los ciudadanos, esta norma, que uniformiza el derecho europeo de protección de datos, garantiza un nivel similar de protección en toda la Unión. Es, además, el único caso de un derecho fundamental regulado mediante un Reglamento UE.

Otra de las novedades destacadas es que sus preceptos resultan de aplicación a los tratamientos que afecten a los ciudadanos que residan en la Unión Europea, con independencia de que el responsable o encargado del tratamiento de esos datos esté establecido o no en la Unión. En los casos en que no exista establecimiento en la Unión, el Reglamento será de aplicación siempre que esos tratamientos estén relacionados con la oferta de bienes y servicios a ciudadanos en la Unión o con actividades de control de su comportamiento también cuando se encuentren en la Unión.

Igualmente, se refuerza el control que los ciudadanos tienen de sus datos personales. Así, se establece una mejor regulación del consentimiento, que deberá prestarse de forma inequívoca mediante declaraciones o acciones afirmativas claras, o de la información que ahora es un derecho vinculado al principio de transparencia, y se reconocen nuevos derechos como los de limitación de los tratamientos o la portabilidad.

El Reglamento menciona también el "derecho al olvido". Sin embargo, ha renunciado a configurarlo como un derecho autónomo, siguiendo la línea del Tribunal de Justicia de la Unión Europea en la Sentencia sobre el caso Google Spain, donde señaló que este derecho es una adaptación a la actividad de los motores de búsqueda de derechos clásicos como el de cancelación y el de oposición.

El Reglamento también incluye una novedad en el caso del derecho de oposición, disponiendo que corresponderá al responsable demostrar que sus intereses prevalecen sobre los derechos, libertades e intereses del interesado en relación con sus circunstancias específicas.

Respecto de las obligaciones de los responsables y encargados del tratamiento, el Reglamento apuesta por un nuevo modelo de cumplimiento, que pasa a pivotar sobre una conducta proactiva de responsables y encargados desde la perspectiva de los riesgos que el tratamiento de datos puede suponer para los derechos y las libertades de los interesados.

Este nuevo enfoque supone un giro sustancial en el modo en que ha de entenderse el cumplimiento de la normativa de protección de datos. En el sistema hasta ahora vigente el foco de los reguladores y de las entidades reguladas se ha puesto en los resultados. Los datos se tratan intentando cumplir con la legislación para evitar posibles infracciones. La supervisión de los reguladores comienza como regla general cuando esa infracción se ha producido.

El Reglamento, por el contrario, sitúa las obligaciones de los sujetos obligados y también la acción de los supervisores en el terreno de las medidas proactivas, preventivas, que deben adoptarse para garantizar que responsables y encargados están en condiciones de cumplir con sus disposiciones.

Este enfoque preventivo se une al de riesgo para determinar cuál ha de ser la actuación de las organizaciones. La confluencia de ambos supone que las organizaciones deben documentar y estar en condiciones de demostrar que han analizado los riesgos de los tratamientos de datos que realizan y han aplicado las medidas adecuadas para eliminarlos o paliarlos hasta niveles aceptables.

Entre estas medidas se cuentan las de protección de datos desde el diseño y por defecto, el mantenimiento de un registro de tratamientos, la necesidad de aplicar medidas de seguridad adecuadas al riesgo derivado de los tratamientos, la realización de evaluaciones de impacto sobre la protección de datos de los tratamientos que a priori parezcan entrañar un alto riesgo para los derechos y libertades de los interesados y la también obligatoria implantación de un delegado de protección de datos en todas las organizaciones públicas y en las privadas que lleven a cabo determinados tratamientos.

Otra de las novedades más relevantes del Reglamento UE, que marca una clara diferencia con la Directiva, es la relativa al nuevo modelo de supervisión, que pasa de concentrarse en verificar si se ha producido una infracción, o si se aplican correctamente las medidas tasadas que la legislación prevé, a tener que valorar, junto con responsables y encargados, los procesos de análisis de riesgos y las decisiones sobre la aplicación de las medidas que los minimicen.

Es, además, un sistema más flexible, en la medida en que abre el abanico de posibilidades de las autoridades supervisoras a un conjunto amplio de

medidas correctivas (advertencia, apercibimiento, etc.) cuya aplicación habrá de valorarse atendiendo al caso concreto, incluso antes de imponer sanciones económicas.

Todo ello no excluye que la norma prevea sanciones económicas muy importantes, que pueden llegar hasta los 20 millones de euros o de una cuantía equivalente el 4% del volumen de negocio total anual global de la empresa en el ejercicio financiero anterior. Sanciones que pueden tener una eficacia disuasoria y cuya aplicación dependerá del nivel de diligencia adoptado para el cumplimiento del Reglamento y de circunstancias diversas relacionadas con su incidencia en los derechos y libertades de los ciudadanos.

Es, al mismo tiempo, un modelo de supervisión que podría calificarse de cooperativo, ya que las autoridades estarán obligadas a cooperar no solo en el establecimiento de los criterios para su interpretación, sino en su aplicación al caso concreto cuando varias autoridades puedan verse afectadas como consecuencia de un determinado tratamiento. Esta obligación de cooperación se regula en los complejos procedimientos de cooperación y coherencia. En este procedimiento juega un papel especialmente relevante al Comité Europeo de Protección de Datos y, en última instancia, al Tribunal de Justicia de la Unión Europea.

Este marco legal se tiene aún que completar con otras dos importantes normas europeas pendientes de transposición o de aprobación: la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, pendiente de transposición y el Reglamento E-privacy, aún en tramitación, que pretende actualizar la todavía vigente Directiva 2002/58/CE para aplicar los principios y exigencia del Reglamento General de Protección de Datos al ámbito de las comunicaciones electrónicas.

El efecto combinado de todas estas medidas debe repercutir finalmente en un cambio en la cultura de protección de datos de las organizaciones y en una mejor protección de los derechos de los ciudadanos.

La Ley Orgánica de Protección de Datos

La recientemente aprobada Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales pretende cumplir cinco objetivos básicos: adaptar el derecho español al modelo establecido por el Reglamento, introducir novedades y mejoras desarrollando algunas de las materias contenidos en el mismo, reforzar los derechos de los ciudadanos, clarificar conceptos y dotar de seguridad jurídica a aquellos que tratan datos.

Destacan en primer lugar los aspectos relacionados con los derechos de los ciudadanos.

El texto legal facilita, con carácter general del ejercicio de los derechos al exigir, en particular, que los medios para su ejercicio sean fácilmente accesibles para los afectados.

Se reconoce el derecho de acceso y, en su caso, de rectificación o supresión por parte de las personas vinculadas a los fallecidos por razones familiares o de hecho y a sus herederos, superando la omisión de

la anterior Ley que generó situaciones conflictivas, especialmente en internet, al no poder ser tutelados por la Agencia. Derechos que podrán ejercitarse salvo que el fallecido lo hubiera prohibido.

La Ley ha introducido una importante novedad, que afecta incluso al título de la norma, relacionado con los que denomina derechos digitales, regulados en su título X. En dicho título, se pueden distinguir dos grandes bloques de derechos en función de si su tutela es o no competencia de la Agencia.

De ellos, la competencia de la Agencia Española de Protección de Datos se circunscribe a los regulados en los artículos 89 a 94 de la Ley Orgánica.

Respecto de ellos cabe destacar que la Ley actualiza las garantías del derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo, así como el derecho a la intimidad en el uso de dispositivos digitales puestos a su disposición, tanto para los trabajadores como para los empleados públicos, complementando este derecho con la regulación del derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral. Derechos en el ámbito laboral que pueden ser reforzados a través de los convenios colectivos.

En el entorno de internet y los servicios de redes sociales u otros equivalentes de la sociedad de la información, la norma ha sistematizado los criterios de la Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo, de 2014 en el caso de la Agencia contra Google respecto al derecho al olvido en las búsquedas en internet, con objeto de facilitar su aplicación e incrementar la seguridad jurídica.

Complementariamente, la ley orgánica regula el derecho al olvido en servicios de redes sociales y en servicios de la sociedad de la información equivalentes, limitándose a permitir la supresión de los datos personales cuando han sido facilitados por el propio interesado; supresión que en muchos casos podrá realizar él mismo sin solicitarlo del responsable. Y, también, cuando hubiesen sido facilitados por terceros aplicando los mismos principios recogidos en la citada sentencia.

En todo caso, se exceptúa la supresión cuando hubieran sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.

La finalidad de esta disposición es igualmente facilitar la comprensión de los operadores y garantizar la seguridad jurídica.

Mención especial merece la regulación respecto de los menores en la que destacan, aún no siendo en algunos casos competencia de la Agencia, los siguientes aspectos.

Se fija en 14 años la edad a partir de la cual pueden prestar autónomamente su consentimiento.

Se regula expresamente el derecho a la supresión, por su mera solicitud, de los datos facilitados a las redes sociales u otros servicios de la sociedad de la información equivalentes por el propio menor o por terceros durante su minoría de edad.

Se refuerzan, de manera particularmente destacada, las obligaciones del sistema educativo para garantizar la plena inserción del alumnado en la sociedad digital y en el aprendizaje de un uso de los medios digitales que sea seguro y adecuado para garantizar su privacidad,

incluyendo una formación específica en los currículums académicos y exigiendo que el profesorado reciba una formación adecuada en esta materia.

A tal efecto, el Gobierno deberá remitir en el plazo de un año desde la entrada en vigor de la Ley, un proyecto de ley dirigido específicamente a garantizar estos derechos y, las administraciones educativas tendrán el mismo plazo para la inclusión de dicha formación en los currículums.

Finalmente, se contemplan medidas para la protección de los datos en internet, indicando que los padres, madres o representantes legales procuren que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales. Y, previendo la intervención del Ministerio Fiscal cuando la utilización o difusión de imágenes o datos personales de menores en redes sociales o servicios de la sociedad de la información puedan implicar una intromisión ilegítima en sus derechos.

Como novedades y mejoras, cabe citar la regulación de los sistemas de información crediticia, conocidos como ficheros de morosidad, en los que se reduce de 6 a 5 años el periodo máximo de inclusión de las deudas y se exige una cuantía mínima de 50 euros para la incorporación de las deudas a dichos ficheros. De este modo se limitan los efectos adversos, que pueden generar situaciones de discriminación, especialmente en el acceso a servicios financieros o de telecomunicaciones, en casos de inclusión ilícita o de inclusión por cuantías ínfimas que pueden ser solo de céntimos.

El texto legal actualiza también la regulación de la Lista Robinson, como fichero de exclusión publicitaria en el que pueden registrarse voluntariamente quienes deseen evitar la publicidad no deseada a través de los canales postal, telefónico y electrónico.

Se modifica la ley de competencia desleal regulando como prácticas agresivas las que tratan de suplantar la identidad de la Agencia o sus funciones y las relacionadas con el asesoramiento conocido como "adaptación al Reglamento con coste 0" a fin de limitar asesoramientos a las empresas de ínfima calidad.

Así mismo se facilitan los medios para que las empresas puedan acreditar diligencia ante posibles casos de responsabilidad penal, regulando los sistemas de denuncias internas, permitiendo incluso las anónimas.

Una de las principales novedades es la regulación del tratamiento de datos en el ámbito de la investigación en salud, flexibilizando las finalidades para las que se puede utilizar la información sanitaria, el acceso a la misma y su reutilización, con garantías adecuadas. De este modo se da respuesta a las inquietudes que esta nueva regulación había suscitado en el ámbito científico.

Con el fin de promover la seguridad jurídica, el nuevo texto legal exige una norma con rango formal de ley en los casos en que la legitimación del tratamiento se base en el interés público o en el ejercicio de poderes públicos; facilita el tratamiento de datos de contacto de personas jurídicas, empresarios individuales y profesionales liberales; así como los tratamientos de datos en operaciones societarias, con fundamento en una presunción de interés legítimo prevalente de los responsables del tratamiento.

Adicionalmente, actualiza la regulación de los tratamientos con fines de videovigilancia.

Y, respecto de la novedosa e importante figura del delegado de protección de datos, detalla ejemplificativamente los supuestos en los que es obligatoria su designación. Y, aclara que no será responsable de los incumplimientos en el tratamiento de los datos; responsabilidad que recaerá en la entidad en que presten sus servicios.

Por otra parte, la ley orgánica clarifica algunos conceptos como la presunción de exactitud en el tratamiento de los datos en determinados casos y, sobre todo, señalando que el consentimiento debe manifestarse a través de una clara afirmación afirmativa, excluyendo el consentimiento tácito y que, no podrá supeditarse la ejecución de un contrato a que el afectado consienta el tratamiento de datos que no guarden relación con el mismo, por entenderse que no sería un consentimiento libre.

Por último, resultan de interés algunos aspectos relevantes relacionados con las Administraciones Públicas.

Como medida de transparencia, la norma exige que dichas administraciones hagan públicos los registros de actividades de tratamiento, que sustituyen a la publicidad de las antiguas disposiciones de creación de los ficheros. De este modo los ciudadanos pueden conocer quiénes tratan sus datos, con qué finalidades y la base jurídica que lo legitima. Así mismo actualiza la relación entre el derecho a la protección de datos y los de transparencia y acceso a la información pública.

En el caso de anuncios y publicaciones de actos administrativos a través de los diarios oficiales, limita el número de datos identificativos del DNI y otros documentos oficiales que pueden publicarse, prohibiendo la publicación del nombre y apellidos de manera conjunta con el número completo de dichos documentos. De este modo previene riesgos para víctimas de violencia de género y reduce las posibilidades de suplantación de la personalidad.

En cuanto al derecho de los interesados de no aportar documentos que se encuentran en poder de la administración, salvo que exista oposición expresa del interesado o la ley requiera su consentimiento expreso, la norma legitima este tratamiento de datos en el cumplimiento de una misión de interés público, y en particular el ejercicio de poderes públicos, sin necesidad de que los interesados presten un consentimiento expreso ni tácito, prohibido expresamente por el Reglamento Europeo.

El texto legal regula las medidas de seguridad en el sector público, a través del Esquema Nacional de Seguridad, que ha sido adaptado al Reglamento Europeo y habilita la notificación de incidentes de seguridad a los equipos de respuesta a emergencias informáticas (CERT) o a incidentes de seguridad informática (CSIRT).

Así mismo, la Ley refuerza las competencias de las Administraciones Públicas permitiendo la verificación de los datos personales que obren en su poder, para comprobar su exactitud cuando se formulen solicitudes de los interesados por cualquier medio.

En materia de infracciones y sanciones de las Administraciones Públicas, la Ley ha optado por no imponer sanciones económicas en caso de incumplimiento, limitándose a ordenar un apercibimiento para que se adapten medidas correctoras. Si bien, se prevé la posibilidad de exigir responsabilidades disciplinarias a los empleados públicos que las hubieren

cometido o una amonestación pública a los directivos cuya conducta hubiera dado lugar a la infracción, pese a haber recibido información sobre el posible incumplimiento de la norma. Resoluciones que en todo caso se publicarán en Diarios Oficiales.

En el ámbito institucional, la Ley contempla como autoridad de control a la Agencia Española de Protección de Datos modificando su composición al prever una Presidencia y un Adjunto con carácter auxiliar definiendo sus competencias y funciones.

Se modifica el procedimiento de designación en el que el Gobierno preselecciona a los candidatos y los remite al Congreso de los Diputados con un informe motivado. El Congreso debe ratificarlos por medio de mayorías cualificadas siendo ulteriormente nombrados por el Gobierno.

Se modifica el mandato de los miembros de la Agencia ampliándolos a cinco años renovables por una sola vez, así como las causas de su cese.

La Ley amplía la composición del Consejo Consultivo permitiendo la incorporación de representantes de nuevos sectores relacionados con la protección de datos personales.

Así mismo se establecen los procedimientos de cooperación con las Autoridades Autonómicas de Protección de Datos en el ámbito interno y en el de Comité Europeo de Protección de Datos.

La norma recoge los sistemas de resolución extrajudicial de conflictos y las especialidades de los procedimientos administrativos contempladas en el Real Decreto ley 5/2018, de 27 de julio, incluidos los que permiten la cooperación y coherencia con el Comité Europeo de Protección de Datos.

Y finalmente establece el régimen de prescripción de infracciones y sanciones relacionándolo con una descripción ejemplificativa de las previstas en el Reglamento Europeo de Protección de Datos.

La Agencia del futuro

La Agencia de los próximos años debe estar en condiciones de afrontar con decisión y eficacia los grandes desafíos, actuales y futuros, a los que se enfrenta la privacidad.

El cumplimiento de este objetivo pasa por alinear su actividad y su modo de funcionamiento a los presupuestos fundamentales que marca el Reglamento General de Protección de datos, haciendo primar la diligencia y la proactividad y aplicando un nuevo modelo de supervisión con instrumentos preventivos, correctivos y, en su caso disuasorios ante los incumplimientos de los responsables.

Sin olvidar la atribución a las autoridades de protección de datos de facultades de investigación comunes a todas ellas que permitan realizar eficazmente sus funciones y, en su caso, imponer sanciones económicas disuasorias para asegurar que la ley se respete.

La Agencia Española está llevando a cabo un importante esfuerzo de adaptación de toda la organización para dar respuesta a estos desafíos.

Junto a los requerimientos que específicamente debe cumplir la Agencia como sujeto obligado (creación del registro de tratamientos de actividades; análisis

previo de riesgos; evaluación de impacto; adaptación de formularios en brechas de seguridad, cláusulas informativas, contratos de encargado; nuevos modelos de códigos de conducta.....), se han previsto en su Plan Estratégico un amplio grupo de iniciativas orientadas a la formación interna, al rediseño de los procedimientos de gestión y en definitiva, a la adecuación de la organización al nuevo marco normativo.

Ello, sin duda, va a suponer un reto de envergadura para esta Agencia, pero al mismo tiempo una magnífica oportunidad para llevar a cabo la necesaria "puesta al día" tras más de veinticinco años de funcionamiento en un período que ha experimentado cambios tan profundos.

3

The AEPD as a garantor of a fundamental right

I. Introduction

If any single word can define the future of the information society, communication technologies and the processing of personal data in Spain over the last 25 years, that word is dream.

In the last quarter of a century we have seen amazing technological leaps and all were guided deep down by the hope of making a better, freer, more open, more just world, and with greater opportunities for all.

In that period, many companies have emerged and many others have gone by the way. There have been a plethora of developments, expectations, technologies and devices, and a lot of doubts, concerns, and uncertainties, as well, but all have been guided by that dream, which some may call childish or naive; but which makes humanity, all of us, advance.

The Spanish Agency for Data Protection has participated in the aspiration to make Spain better. It is a dream that has enthused all who have worked on it, guided by the trust of citizens, to boost the hopes and expectations of entrepreneurs, researchers, lawyers and engineers, with whom we have shared the journey.

The year in which the Agency started was a year full of events related to the processing of information. In 1994, the website Hotwired launched the first advertising 'banner', which changed marketing forever and opened the doors to the monetization of websites. Netscape released its first version of an Internet browser, which supported cookies. It was the year in which the first online sale was made, supposedly a pizza, and the NetMarket portal was launched, which was the first secure market on the Internet, initiating nothing less than electronic commerce. It was also the year of the first Internet radio broadcast, opening the way to the entire audio streaming industry.

If we look back at that time, we see an Agency and a Spain that we cannot recognize. All those who have children who have not yet left university will have a hard time explaining how we lived in 1994. We were emerging from an economic crisis that had reduced the technological sector to 1987 levels; we lived in a society in which the typewriter still dominated many offices and the only program that was executed in most homes was the washing machine.

It is true that the Internet was in existence at that time, and there were some 20,000 machines registered with the '.es' domain in Spain. It was also the moment in which the first Spanish web page appeared on the network and there were little more than one hundred companies connected. Access to communications practically operated within a monopoly, with the telephone network as the only connection and with Infovía debuting in 1995, which allowed people to use the Internet from home. Modems provided music at 56 Kbps, which meant having to wait 15 minutes to listen to an actual song. Throughout the world there were only 10,000 Internet pages, not the more than 50 billion that exist today, and among them was the first social network, Classmates, which came into being at around that time.

The first GSM digital telephone license was granted in 1994 to Telefónica and less than 2% of Spaniards had a mobile. This was a mobile phone; not a smartphone - although by this time IBM was launching the Simon, an idea, an exclusive prototype, that bore very little resemblance to what we currently use.

However the subject of personal data protection was, and is, much more than being about pure technology. In 1994, humanity showed us its dark side again. That year, in Rwanda, hundreds of thousands of people died because they were different; because someone had classified them into Hutus and Tutsis, into good and bad; because all that information, with names and addresses, was in a registry; and all of it was going to be employed to materialize hatred.

That tragedy brought us echoes of the drama that Europe experienced in the 20th century and that led to the Universal Declaration of Human Rights. It reminded us that the project that was being started at the Spanish Agency for Data Protection had as its primary objective to prevent these things from happening again, and that we had as a mission to protect a right, a fundamental right. Already in his etchings, Goya had shaken our consciences and warned us that "The dream of reason produces monsters"; or, put another way, that dreams, if they are not underpinned by shared values, can turn into nightmares.

It was with that desire to share a dream that an Agency began, with thirty-three public employees. It was a journey full of unknowns, in which doctrine and procedures had to be developed in a world that existed between the legal and the technical. Everything had to be developed from scratch, innovating from the basics to the procedures, through information systems. In that first stage the whole staff team was involved in an effort to create awareness of data protection in a society in which that idea was completely new. In the development of its models and methods, its first great motivation was to campaign for the registration of files or, in other words, to encourage entities to strive to rationalize and control the data collected from citizens.

Twenty-five years is a long time and to go through it, we are going to fix some milestones. The first wakes us up in 1999 with the cries of a newborn named Google. In that same year Apple also presents its iBook, a laptop that no longer weighs eleven kilos, like the Osborne-1, but only three. In 1999 the number of websites multiply by ten, reaching almost thirty million worldwide, and P2P technology arrives with its first star, Napster. The term Internet of Things, IoT, is coined in this period and technology companies take the opportunity to establish a wireless connection mechanism that is compatible between different devices: WiFi is born.

The outlook in Spain had already changed considerably: the market for fixed and mobile telephone operators had just been liberated, and up to a hundred authorizations for new operators were conceded. The first consequence was that the number of mobile phones multiplied by five in two years (reaching up to 25,000 users in the year 2000!). There was also greater liberalization of the television market, and consequently the number of available channels tripled in three years. Retevisión offered Internet access service for free and the take-off of broadband users began with the approval of the 'ADSL Law'. This allowed half of the Spanish companies to have access to the Internet that year, which gives an idea of the speed of automation of their processes.

To promote electronic commerce the Electronic Signature Law was approved, among others. In particular, we recall the passing of Organic Law 15/1999 for the Protection of Personal Data, LOPD, which has been the regulation upon which the protection of fundamental rights in the information society has been developed over the last 20 years ... or almost.

But, sometimes, the more the human spirit rises, the longer the shadow it casts. In Kosovo, thousands of people were killed and millions had to flee their homes in the last throes of the disintegration of a country. Again, a group of people were labelled and there were others who used records that, created for coexistence, fuelled confrontation. It seems that Europe does not learn.

At that time the Spanish Agency for Data Protection comprised over sixty professionals who faced a new normative framework, which was more mature, and had a new model for an Information Society, whose center of gravity rotated around the big corporate databases and processing carried out by small companies, which were increasingly connected to the Internet.

Around 1999 the Agency took a step forward and systematically began to implement Occupational Inspection Plans and promote cooperation within the business sector, which through joint work, sought to effectively protect the rights of citizens. This activity later culminated in large-scale plans for the hospital and educational sectors. With the same dream of more efficiently responding to citizens' needs, the 'procedure for the protection of fundamental rights' was established.

If we have to look for another significant milestone before arriving to the present day that is, without hesitation, the year 2007: the year of the presentation of the iPhone.

The iPhone represented the beginning of a new way of understanding life; a model of communication and social interaction that was widely copied and that is still valid today. In Spain, today, 90% of young people depend on a smartphone for their daily lives. It makes sense that, just a few months later, WhatsApp emerged, and with it, SMS died as a form of communication. In that year, the 'major players' consolidated in the global information market; especially Google, after having acquired services such as Android and YouTube. Around that time Amazon Web Services were born and soon after Google App Engine, which materialized the cloud or the Cloud Computing technology market, started its journey in the year 2000. In parallel, Netflix emerged.

That same year, Wikileaks began its activities and massive leaks of information were produced. The previous year had seen the largest data breach so far when information relating to 94 million credit cards were stolen, due to the company TJX's inefficient encryption system. The organization Anonymous intensified its activities and the Snowden scandal would come a few years later. All these events made citizens more aware of the danger of the massive accumulation of data in the hands of multinationals and States, especially in files accessible from the Internet, and the fragility of information security.

In 2007, half of the households in Spain had computers and the Internet at home. There were ten million users of social networks in our country: MySpace began to lose market share in favor of Facebook, which confirmed its rise, and Twitter was in its second year. Companies in the ICT sector in Spain doubled to more than 50,000. At that time 94% of companies already had access to the Internet and, in addition, broadband. New intrusive forms of data processing were spread in a massive way, particularly video surveillance systems, and citizens ceased to be passive subjects of the data and became active elements in the Information Society.

At the end of 2007, the Regulation for the Development of the Organic Law on Data Protection was published,

approved by Royal Decree 1720/2007. This Law established the principles for more 'rational protection' and for a more agile response by the Agency. Citizen complaints grew, passing from just under two thousand in 2006 to over seven thousand in 2009; more than double that accumulated in the first ten years of the Agency's existence. The sanctioning procedures also doubled, until they passed over six hundred per year; and up to 160 legal proceedings were started in four years.

To cope with these new demands, the Agency had to reinvent itself: it doubled its staff compared to 1999, introduced new procedures, improved the response to citizens and enhanced awareness activities with the preparation of guides and reports that legally interpreted the new technologies. Its staff had to adapt to these new challenges by increasing their productivity and leading international programs.

To finish this introduction, let's make a leap to this day. 2018 is a year marked by the effective application of the European Union's General Regulation of Data Protection, but also by the challenges posed by blockchain, iHealth, IoTA, Edge Computing, immersive reality .... Perhaps nothing can better describe the character of this moment than the following quote:

"It was the best of times and it was the worst of times; the age of wisdom and also of madness; the age of belief and unbelief; the age of light and darkness; the spring of hope and the winter of despair. We had everything, but we had nothing; We went straight to heaven and went astray in the opposite way ... "

C. Dickens "Tale of two cities"

And the Spanish Data Protection Agency can only successfully address these new challenges in one way: with a dream.

Mandates of the AEPD's directors

Juan José Martín-Casallo López (from 1993 to 1998). Appointed RD on 22 October 1993. BOE 23 October 1993.

Juan Manuel Fernández López (from 1998 to 2002). Appointed RD on 27 March 1998. BOE 31 March 1998.

José Luis Piñar Mañas (from 2002 to 2007). Appointed RD on 8 November 2002. BOE 9 November 2002

Artemi Rallo Lombarte (from 2007 to 2011). Appointed RD on 23 February 2007. BOE 26 February 2007.

José Luis Rodríguez Álvarez (from 2011 to 2015). Appointed RD on 17 June 2011. BOE 18 June 2011.

Mar España Martí (from 2015 to date). Appointed RD on 24 July 2015. BOE 25 July 2015.

II. The Agency's beginnings (1993-1999)

The 1978 Constitution already sensed the huge potential impact of new technologies and the unstoppable development of the media, by stating in article 18.4 that: "The law will limit the use of information technology to guarantee personal and family honor and the intimacy of citizens and the full exercise of their rights. "

On the other hand, the Council of Europe foresaw in Convention 108 of 1981 the existence of an independent authority that would supervize this right.

But it took 14 years for that constitutional provision to have a normative development. In October 1992, the Organic Law 5/1992, of October 29, on the Automated Treatment of Personal Data, LORTAD, which created the Data Protection Agency, was approved by the Congress of Deputies. Until the arrival of this law, it was the institution of the Ombudsman that was in charge of resolving issues related to the protection of this fundamental right.

The Law also created the Consultative Council as a collegiate advisory body for the management of the Agency, comprising ten members who are appointed for a period of four years.

Spain was therefore three years ahead of the international establishment of these types of institutions.

At that time, the mobile phone barely existed, the personal computer was a luxury item that coexisted with typewriters, and television was just starting to expand its offer.

The existence of the Internet was known, but it was not a tool in generalized use. People, especially when they lived distantly, wrote letters; by hand for personal letters and by typewriter at work, which were sent via the Post Office and took several days to reach their recipient.

If in the 1970s television was still a luxury item, which all households could not afford, in the '80s it became widespread as a home appliance. There was a television in every home. They were those huge box-shaped televisions, with which you had to get up to go to the button to turn up the volume or to change the channel.

After the early years in which broadcasts were in black and white, by the end of the '80s color television was widespread. But it is worth emphasizing: there was normally one television in the living room of each house. There were four general channels: two broadcast by RTVE and two private channels. There was no 24 hour a day broadcast, and the social interaction generated by television comprised comments among people; inside the house itself or the next day at work, or on the street.

You could watch the news at midday or in the evening, which many called "El Parte", and the movies were the classics of American cinema. Children's programming played a key role; children watched Sesame Street and Once upon a time...life and every weekend the first film after the daily news program at 3pm was suitable for minors.

In the mid-nineties, adult programming was moving towards new formats: new types of programs were emerging and there were new political and social discourses, analyses and debates. You could interact at a distance with the TV programs through contests in which you participated by letter.

This was daily life when the Spanish Agency for Data Protection began its journey in 1993.

The Agency was created as an independent public entity, with its own budget integrated in the General State Budget, and with full autonomy to carry out its duties.

The Statute of the Agency was approved by Royal Decree 428/1993, of March 26. This Decree outlined its powers, organizational structure, the functions of the Director and the Advisory Board, the operation of the General Registry of Data Protection, and the economic, patrimonial and personnel regime.

The Agency was structured into Data Inspection, the General Registry of Data Protection, the General Secretariat, and a Support Unit.

The Data Inspection office carried out the inspections and training functions necessary for the research and 'corrective powers' given to the Agency, within the framework of the permanent supervision of regulation compliance by those responsible for and in charge of the area of data processing.

The General Registry of Data Protection registered and publicized public and private files, promoted and registered codes of conduct, and processed authorizations for international data transfers.

For its part, the General Secretariat was responsible for economic and personnel management, supported the other units, and managed matters not attributed to them.

A few months after the approval of the Statute, specifically on October 23, 1993, the appointment of the Agency's first director, Mr. Juan José Martín-Casallo López, took place.

It was at that moment that the Agency was given the necessary infrastructure and the corresponding personnel and material means. But soon there was a need for more staff; mainly highly specialized personnel for the performance of the inspector and instructor functions that the Organic Law required, which is why, in 1994, the workforce grew to 49 posts.

Until May of that year, the Agency occupied, under lease, facilities assigned by the Ministry of Justice: specifically, the third, fourth and fifth floors of the building of number 41, Paseo de la Castellana, in Madrid.

1. The General Registry of Data Protection

At the time it began its activity, the priority of the Spanish Agency for Data Protection was to create and organize the General Registry of Data Protection.

The fundamental purpose of the Registry, which required companies to register data files, was to provide any citizen with free access to the information contained in those databases. In this way, citizens could identify the holders of the files in which their personal data had been included, and know the contact address of those responsible, the purposes for which the information would be used, the type of data incorporated in it, and the international transfers of data envisioned. And, once identified, they could exercise their right of access to know if they were included or not and, if so, what information had been incorporated.

Thus, if a person discovered that he was included in a record of arrears when going to a financial institution

to, for example, request a credit card or financing for the purchase of a vehicle, they could go to the Agency and request information free of charge on those files. Once the 'file owners' were identified, the citizen could exercise their right of access to obtain information on whether or not they were registered. And, if they were, to identify in which files they were listed, which entity had qualified them as a defaulter and had requested their inclusion onto that database, the amount of debt, and other relevant data, such as the evaluations and assessments of the affected person's risks that may have been undertaken in the six months prior, and the names and addresses of those to whom that information had been communicated.

If the affected party considered that inclusion to be unlawful, either because they had not had any relationship with the alleged creditor, or perhaps because they had no outstanding debts, they could exercise the 'right of deletion' both to the holder of the payment default file and to the entity that had supplied the information included in the file, a financial institution for example, so that they could have that data removed. And, if the request for deletion of the data from the file was not met, the individual could lodge a complaint with the Agency to investigate and, where appropriate, have the offender punished and the information in the file removed.

To this end, meetings, presentations and information days were held with numerous public and private organizations, backed up by telephone calls and the sending of information by post. Although in the beginning the registration process was carried out largely on paper, a computer application was developed in four weeks to notify the files to the Registry and diskettes were distributed for the recording and registration of the files by those responsible, through the tobacconist network of TABACALERA, SA.

Thus, a massive registration of files took place, which meant that between June and July 1994, more than 200,000 files from more than 100,000 private companies and most of the files of the General State Administration were registered; a figure that continued to increase until it reached 5,094,312 files at the close of the Registry, as a consequence of the full application of the European Data Protection Regulation.

2. The first consultations

As citizens' knowledge improved, inquiries about how to identify the identity of the file owners and how to guarantee their rights increased.

From the beginning, the Spanish Agency for Data Protection has been entrusted with the task of providing information to citizens about their rights in relation to the processing of their personal data.

For this reason, in April 1994, the 'Citizen Service Area' was opened, which provided telephone and face-to-face contact, as well as responses to questions in writing.

However, at first the Agency's efforts focused on providing information to those responsible for data processing, meaning that the impact on citizens was initially lower. Therefore, citizens had a relatively low level of knowledge of their legal rights and what the Agency could offer in terms of the possibilities of exercising them.

After this incipient period, however, there was a slow but gradual increase in the number of citizen consultations.

If data from the beginning of the period are compared with those at the end, stability in the number of consultations can be found over these years. Thus, in 1995 there were almost 10,000 responses given to telephone enquiries, over 1,500 face-to-face consultations and 598 in writing; while in 1999, there were 11,500 telephone, 1,150 face-to-face and 1,739 in writing.

Regarding the issues to be consulted, three main issues can be distinguished: the exercise of rights provided for in Law; the consultation of specific files and the transfer of data; with this latter issue progressively losing weight in favor of other issues such as general information about the Agency or enquiries about specific records in the Registry.

- Clear growth in the number of consultations relating to the exercise of rights can be identified, passing from 25% in 1996 to 50% in 1999. Specifically, the rights over which there were most questions were those related to access and cancellation. Which means that, initially at least, citizens' were particularly concerned about who had their information and how to have it removed.

- Regarding the consultation of specific files, asset solvency files predominantly and increasingly concerned the public throughout the period, passing from representing 38% of the total in 1996 to 70% in 1999.

Consultations in this period focused on the identity of the person in charge and on the rights of access, rectification, and especially on the right to deletion; given that citizens' primary concern is to not appear in these types of files.

Following these the following in importance, in terms of the volume of queries, were files for advertising purposes. The most frequent request the Agency received was the desire to not receive unsolicited commercial information sent by companies with which the affected party had no prior relationship. It is recommended to exercise the right for the subscriber to be excluded from Telefónica's subscriber listings and from those other companies in the sector, which are accessible to the public and can be used for advertising purposes.

- Regarding inquiries related to data transfers, most of them have to do with transfers between Public Administrations, which are often covered by laws, or with the transfers of data from the fiscal censuses of local entities, among others.

3. The first complaints and claims. The first inspections

The Agency began by managing a relatively small number of complaints, and now receives thousands of complaints every year. Some, related to processing carried out by large companies, affect more than 4,000 million Internet users. In the following sections we will explore in more detail how the Agency has adapted to the evolution of Spanish society and its demands.

The first notifications in writing that contained claims or complaints regarding data protection date back to the end of 1993, but it was not until the following year when the significant activity of the General Subdirectorate of Data Inspection began.

While 81 complaints were processed in 1994, only five years later, 195 'guardianship proceedings' had been resolved: 110 related to sanctions and 25 for Public

Administration infringements, which gives an idea of the significant increase in such a short period of time. When the file registration period in the General Data Protection Register ended, the Agency began to undertake significant activity in terms of the 'guardianship of rights' and the possibility of imposing sanctions.

The complaints and 'protection requests' in that first period show that citizens' concerns revolved around economic-financial data and, among these, those especially related to solvency, credit and debt. After that came issues related to direct advertising, and then, those referring to financial institutions and Public Administrations. Citizens' complaints were mostly directed towards entities or people based in Madrid, followed by those in Barcelona.

It is worth highlighting citizen concern about inclusion on a payment default file, due to the significant effect it has on people's financial lives. Specifically, appearance on one of these lists may significantly limit the possibilities of accessing any type of credit, or the possibility of restrictions in the contracting of other basic services such as telephony, in particular because these operators are one of the leading suppliers of information for these files.

In order to minimize these effects, and to strengthen citizen guarantees, the Agency developed rules relating to asset and credit solvency files.

On the other hand, despite the initially small number of complaints about sensitive data, the Agency has had a special interest in the processing of health data. Thus, during 1995 the first public inspections were carried out of hospital establishments, actions that have continued over the years, especially those related to accessing clinical history, to which reference will be made in subsequent sections.

If the figures for 1998 are compared with those of the previous year, we can see that the number of complaints received decreased, due to the fall in the number of complaints in the sectors that have traditionally had a greater incidence in the number of claims: asset solvency and credit (218 in 1997 against 148 in 1998), financial entities (84 versus 58) and direct mail (126 in 1997 compared to 100 in 1998).

This decrease must be attributed not only to the work that the Agency was doing, but also to the progressive knowledge of data protection legislation by the companies in the aforementioned sectors. This circumstance led to the establishment of procedures to ensure a better response to the rights of citizens, especially over access, rectification and deletion.

On the other hand, there was a fall in the number of complaints alleging the use of data from the electoral census in advertising campaigns. Additionally the Agency confirmed that use of these files for the preparation of advertising lists also fell by the same proportion.

In this period, several sectoral inspections were carried out to gain in-depth knowledge of the status and degree of compliance with the regulations on personal data protection in specific sectors of activity, with the ultimate aim of developing a preventive policy that better guarantees the rights of citizens.

As a consequence, in 1997, the files of several local police stations were reviewed and in 1998 Telefónica's information systems were revised in depth, as part of a more ambitious plan including a number of other telecommunication operators.

The systems of the largest entities dedicated to asset and credit solvency information and a selection of the largest Spanish insurance companies were also thoroughly reviewed.

Likewise, the Spanish SIRENE Office, a police collaboration body established within the framework of the Schengen Agreement, was reviewed and various bingo halls were inspected.

Also in 1998 and 1999 Inspections were carried out on large insurance companies, the State Agency for Tax Administration, the Traffic Department and the private investigation sector. Additionally, reviews were conducted in the field of health, including the psychiatric hospitals of Foncalent, Gómez Ulla military hospital, and the National Epidemiology Center.

Finally, in 1999, it is worth highlighting the implementation of a specific inspection plan in the Telecommunications Sector, such that inspections already carried out in the sector regarding compliance with the LORTAD were extended in relation to compliance with the new privacy protection regulations in the telecommunications sector. Thus, art. 50 of Law 11/1998, April 24, on General Telecommunications, established that operators that provide telecommunications services to the public, or exploit telecommunications networks accessible to the public, shall guarantee, in the exercise of their activity, the protection of personal data, in accordance with the provisions of the legislation on data protection.

III. The constitutional dimension of law. The new challenges of privacy: electronic communications (1999-2007)

In 1999 the euro was born, but it was not until 2002 when it officially replaced the peseta. The use of a common currency facilitated the exchange of goods and services, the use of macrosystems of information and the production of statistics referenced to a common index.

In this period, technology had already made televisions much smaller and flatter, and considerably cheaper, so there were often several in each house.

Additionally, there were many more programs that required the 'live' participation of viewers, either by phone call, or by sending short text messages (SMS), whether it was to hear the opinion of the viewers, vote for a favorite song or to collect money for a particular charity.

Television programmes also increased during the night and early morning hours. As an interactive tool, television had teletext, which allowed viewers to search for the programme guide, consult the weather forecast, and even their horoscope.

From the end of the nineties the use of the mobile phone became widespread. Some phones were used to call, and send SMS; nothing more and nothing less. They could not connect to the Internet, but from that moment on, people could be reached 24 hours a day.

A significant development that is worth mentioning in this period is the effect produced by the Security Measures Regulation, approved by Royal Decree 994/1999, of June 11, with Juan Manuel Fernández López at the head of the Agency.

The measure provided for an obligatory step-by-step triple level of security, for any data file, which became effective on December 26, 1999 (later extended to March of the following year). This resulted in a notable increase in activity at the Agency at the end of the year to respond to requests from citizens and an increase in file registrations in the General Data Protection Register.

1. The LOPD

The year 2000 brought together two events of special importance for the protection of personal data: on the one hand, the entry into force on January 14 of the Organic Law 15/1999, on the Protection of Personal Data, the LOPD, which replaced the LORTAD and became key to the system of guarantees of this right in our country and, on the other, the ruling of the Constitutional Court 292/2000, which will be explored in more detail below.

This pronouncement of the Constitutional Court coincided with the declaration of the European Union's Charter of Fundamental Rights, made at the Nice Summit on December 7 of the same year. Article 8 of the aforementioned Charter expressly recognizes the right to personal data protection.

Along with this recognition, Article 8 also makes reference to the principles of data processing ("that will be treated faithfully, for specific purposes"), to the legal basis thereof ("on the basis of consent of the person affected or by virtue of another legitimate foundation provided by law") and the rights comprising its core content ("Everyone has the right to access data collected about them, and their rectification").

And, especially, it adds a structural element to the system of guarantees for the protection of this right, of an institutional nature, by establishing that "respect for these norms will be subject to the control of an independent authority". In this way, the Charter "constitutionalizes" the independence of the control authorities.

The approval of the LOPD was a direct consequence of the transposition in Spain of the European Directive 95/46/CE, of October 24, 1995, regarding the protection of persons with regard to the processing of personal data and the free circulation of these data.

This Directive represented an important step in the regulation of the protection of personal data within the scope of the European Union, not only for the development of a broad system of guarantees for the protection of this right, but also to acknowledge a key objective in the European sphere, which is to guarantee the free circulation of personal data as a complement

to the free movement of goods, people, services and capital, for the establishment and functioning of the internal market.

To achieve this, the Directive sought a 'harmonized system of protection' while recognizing that Member States have some margin for maneuver in their national law.

With respect to its predecessor, the new Organic Law introduced significant changes in the regulation of data protection, expanding the scope of the Law by including all data files, whether computerized or not, within its remit.

The application of the Law to personal data collected in various media and, mainly on paper, completed the application of the guarantee to all personal data processing at a time when paper files were voluminous. This extension, aimed at avoiding serious risks of circumvention of the standard, only covered the manual files structured with specific criteria relating to people who had easy access to personal data, excluding unstructured folders.

Likewise, the principle regarding the data's end purpose was reinforced, since the purposes for which the data may be used must not only be legitimate, as required by the old law, but also specific and explicit, with it being necessary that the affected party clearly knows, in all cases, the purposes for which the data is being processed.

This specification of the principle of purpose was particularly relevant in some data processing such as those relating to advertising and marketing, around which there had been a greater volume of citizen complaints. And it demanded that the companies involved in this activity included in their information clauses the requirement of consent of a reference to the specific sectors for those who authorized the sending of commercial communications (such as financial products, insurance, telecommunications ...), which allowed those affected to opt for those that were of interest, or otherwise reject them.

Additionally, the information was disseminated to citizens, along with the option to prevent unwanted advertising in those cases where the law allowed it to be carried out without the consent of the recipients, for example, through the use of data from public sources such as telephone directories. In these cases it was required to include in each advertising communication, information about the origin of the data, the identity of the person who produced the advertising and the rights that the recipients had.

The rights of access, rectification and cancellation were completed with recognition of 'the right of opposition', when the consent of the affected party was not necessary for the treatment of the data, if there were well-founded and legitimate reasons for their specific personal situation.

2. The verdict of the Constitutional Court 292/2000

A second important event in this period was the verdict of the Constitutional Court, 292/2000. Its relevance lies in the fact that the right to the protection of personal data is established as an autonomous right and distinct from the right to privacy, which aims to give citizen's control over their personal data, both in relation to the private and public sectors.

The ruling is based on the consideration that, unlike the right to privacy, which allows the guaranteeing of a 'private sphere', the right to data protection attributes a power of disposition and control over personal information, even when it is accessible to third parties, both public and private.

On the other hand, for the exclusive sphere of data transfer between Public Administrations, the ruling restricts use to cases in which they exercise similar powers. Therefore, any transfer of data between Public Administrations can only be carried out if this condition is fulfilled, or is authorized by a regulation with formal legal status.

3. New responsibilities in the field of electronic communications. The Law on Services of the Information Society and Electronic Commerce (LSSI) and the General Telecommunications Law (LGT)

In 2003, a significant modification of the Organic Law on Data Protection occurred, with regard to the transparency of the Agency's actions: it was decided to publish its resolutions, preferably through computer or telematic means, which took place from January 1, 2004, through the website of the Agency.

The publication of its resolutions also contributed to increased 'legal security' because citizens were able to understand the criteria for the rule's application.

During this period, the regulatory framework for the protection of personal data was extended and updated to new technological environments through the approval of laws 34/2002, Services of the Information Society and Electronic Commerce (LSSI) and of Law 32/2003, on General Telecommunications (LGT). Both laws have been subject to further modifications to update guarantees for the protection of personal data.

These norms incorporated Directive 2002/58/EC on the treatment of personal data and the protection of privacy in the electronic communications sector into the legal structure.

The Directive took into account the introduction of new advanced digital technologies in public communication networks and new electronic communication services, as well as the importance of the Internet in providing a common global infrastructure for the provision of a wide range of services. And, in particular, it warned about the need to protect rights and freedoms in the face of the growing capacity of storage and computer processing of data related to subscribers and users of these services.

Consequently, the Directive addressed the challenge of harmonizing the legal provisions of Member States to update the protection of personal data in these environments and to avoid obstacles for electronic communications within the internal market, guaranteeing in any case that the promotion and development of new electronic communication services and networks were not hindered.

The common element of the two laws is their relationship with developments in advertising that go beyond traditional postal mail, either by directly regulating other advertising channels, or indirectly addressing the use of technologies that are essential for the use of personal information in the development of 'online' advertising.

Thus, after an initial draft in 2002, in which it limited itself to establishing guarantees on commercial advertising

communications, the LSSI was subject to various modifications that culminated in a new regulation of commercial communications by electronic means that required 'reinforced consent', in the sense that they had to be expressly requested or authorized by those who they were addressed to (this related to so-called junk mail or 'spam').

However, this reinforced regime provided for an exception when there was a prior commercial relationship with the customer and the advertising was about products or services similar to those contracted. In these cases, the customer should be offered in each commercial communication the possibility of not continuing to receive them through a simple and free procedure.

The requirement of reinforced consent with respect to that of the LOPD is justified by the technological changes that allow the sending of mass commercial communications by means of relatively simple and economic systems, and by the inconvenience and even the costs that these may involve for the recipient.

Also, within the regulatory developments of this period were the obligation to provide information to recipients by service providers that use data storage and recovery devices in terminal equipment (the best known are the so-called "cookies"). The importance of the use of these devices lies, among other aspects, in the fact that they allow Internet users' browsing to be tracked.

In this way, service providers are obliged to inform recipients in a clear and comprehensive manner about the use and purpose of the collection of the information, and to offer them the possibility of opposing the processing of the data through a simple and free procedure. In this way they facilitate the development of user habits and profiles to offer personalized advertising, in a business model based on the offer of free services on the Internet whose price is the data of users.

However, in practice, the guarantee based on the right of opposition was ineffective and forced a subsequent legal modification to provide a stronger guarantee for the use of these devices.

On the other hand, the General Telecommunications Law established specific guarantees for the processing of traffic and location data and their commercial use. And it also strengthened the rights of subscribers and users of these services to avoid unwanted advertising by requiring prior and informed consent to receive it through automatic calls or faxes. It also recognized the right to be excluded from electronic communication service guides and of the information services on the guides, preventing the information in them being used to advertise without the consent of those affected.

The Agency's new powers derived from the application of both laws immediately led to significant growth in its employees' workloads. The main cause of this increase came from complaints about spam, which since that time have been one of the biggest sources of complaints. To illustrate this, it is sufficient to point to the increase in the number of complaints for infringement of the Services of the Information Society Law, which have passed from 11 sanctioning procedures resolved, in 2005, to 110 infractions declared in 2017.

4. Increase in the Agency's Human Resources

The changes to the Spanish legal system resulted in an exponential growth of citizens' inquiries and complaints. In order to adequately attend to both, the Agency

increased its staff, not only reinforcing the technological profile of its workforce, but also incorporating specialists in information technology and citizen services.

The most significant increases in personnel occurred in 2003, when the Agency grew from 68 to 92 people, and in 2008, from 103 to 147.

Despite the fact that the evolution of complaints and protection has continued to grow every year in significant percentages, the Agency's workforce remained practically unchanged up until 2017, despite repeated requests for an increase from successive Directors, even in parliamentary headquarters.

Finally, in 2017, an increase of the workforce was authorized, up to the 180 posts that the Agency currently has.

5. Consultations

In 2000 a specific section of 'frequently asked questions' was included in the Agency's web page, which answered the most recurrent issues in consultations, namely: advertising mailings; telephone billing data; Data from Telephone Directories; and asset and credit solvency information files.

The list of 'frequently asked questions' has been expanded and now includes over 200.

Additionally, other resources were incorporated, such as the Agency's recommendations to Internet users and the Legal Department's main rulings.

From 2001 onwards, there has been an exponential growth in queries, with annual increases of between 20% and 30%: the 19,262 consultations that were responded to during 2000 turned into 35,251 in 2004. That increase had a decisive influence on the comprehensive remodeling of the Agency's website undertaken in 2003, which became the backbone of the normalization of knowledge of fundamental law.

On October 15, 2004, the 'intelligent telephone line' that selectively deals with citizen enquiries as part of the Citizen Attention Service, and the other Agency Units, became operational.
The Agency self-imposed the fulfillment of a series of quality commitments in responding to citizens: face-to-face consultations, with a waiting time of no more than 20 minutes; telephone calls, attended to as soon as the details of the consultation were known; and written requests, with answer periods not exceeding 30 and 20 business days for postal and electronic, respectively.

With regard to the quantitative evolution of the consultations, it was already clear how from 2000 to 2004 they increased by more than 80%. Later, at the end of the period, the number of annual consultations responded to reached 72,652; that is, from 1999 to 2008 they almost quadrupled.

In this period, the largest annual increase occurred between 2007 and 2008, no doubt due to the entry into force of the Regulation of the Organic Law on Data Protection. This increase was especially evident in the telephone service, passing from 11,500 calls in the year 2000 to 58,143 in 2008. Writing is the second most used route (9,722 queries in 2008 compared to 1,739 in 2000) and, thirdly, face-to-face (4,785 queries in 2008 compared to 1,150 in 2000).

With regard to the issues consulted, the fundamental concern of citizens relates to the exercising of rights,

which in certain years represents over half the total number of consultations.

In particular, the right that arouses most citizen interest is the exercise of the right of deletion, which accounted for more than half the consultations attended to in 2008 (a specific phenomenon related to the cancellation of data were the 'Books of Baptism', produced by the Catholic Church). Following cancellation, it is citizens' right of access that is the focus of people's concerns who, in short, want to know who is using data and what data are used, how and where to exercise their rights and, to a greater extent, prevent others from continuing to process their personal information.

Queries regarding specific issues, such as asset and credit solvency, mass faxes or calls without human intervention, and exclusion from telephone directories have also kept constant throughout the period. In these cases, citizens have enquired about their appearance in defaulter files despite having settled their debts. They have also been interested to know: how to find out if they are in payment default files; if one company can assign to another the personal data of its former clients to claim debts; and the procedure to stop unwanted advertising by mail.

6. Complaints and inspections

The volume of complaints lodged in 2000 was very similar to that of 1999. In particular, 146 sanctionary proceedings were initiated against private sector entities and 31 against the public sector.

However, over the following years these figures grew exponentially, such that in 2007 399 sanctioning procedures and 66 Public Administration offences were resolved. Also, 37 procedures were resolved in accordance with the LSSI and 2 with the LGT.

In the early years of this decade, with a particular impact in 2005, actions were increased due to fraud in the contracting of products and services, normally telephony and Internet access, in many cases due to deficiencies in the management of the distributors of those services.

In 2007, most of the inspections carried out affected telecommunications and financial entities, followed by video surveillance, with an increase of more than 400% in 2007 compared to 2006.

In this period advertising continued to be one of the sectors in which citizens raised a large number of complaints; it was also a sector in which there was a change in the trend in complaints as a result of changes in the technological environment. Thus, those relating to the postal system fell, while those connected to electronic channels increased, mainly involving e-mail or SMS messages, together with the possibilities of profiling Internet users.

The sending of commercial emails and faxes without consent is one of the areas in which most inspection activities were carried out.

Another of the key sectors in which complaints by citizens increased is that of financial institutions; and more specifically in relation to the information on asset solvency and credit, since a very significant part of the claims, more than 50%, refer to the inclusion of data in a payment default file, in many cases, without respecting the principles and guarantees provided in the data protection regulations.

The other major sector that focuses citizens' attention is that of telecommunication companies, for two reasons: on the one hand, because these companies are a source of information on the payment default files, to which their debtors communicate; and on the other, due to the increasingly frequent problems caused by the processing of personal data in this sector, which includes not only the most traditional processing related to telecommunication directories, but also those derived from technological development itself, among which is included data processing on the Internet or services, such as SMS.

In this period there was considerable growth in claims in this sector, in which inspections (216) occupied first place in 2004, followed by procedures (62), thereby surpassing those related to financial institutions. This increase is related to the new technological environment described in Directive 2002/58/EC, which has been explored in detail above.

Approximately 30% of the claims in the telecommunications sector relate to the existence of fraud in the contracting of products and services, normally telephony and Internet access.

The main cause of fraud involves the identity theft of the contracting person. This cause is significant in the telephone and online contracting of all types of services - not only telecommunications - to the point that, in 2013, the supply and marketing of water and energy sectors have come to occupy second place in terms of volume of sanctions, surpassing financial institutions.

On the other hand, there was a decrease in sanctioning in the: health, insurance, property owners' management, estate management, human resources and labor relations sectors; as well as the sending of commercial communications by fax.

With regard to this last aspect, by this time the use of fax was already minimal, and postal mail had lost its place to electronic mail. Thus, in the advertising sector, the interest of companies focused on commercial mailings through e-mail, either through mass mailing campaigns or through personalized mailings. Therefore, the profile of this sector can only be glimpsed.

Regarding the area of public administrations, inspections and 'statements of offence' fell in the local administration sphere, while they increased among the General State Administration and the Autonomous communities. Among the offences declared are those relating to non-inclusion in the 'fines bulletins' or infractions of the informative clause referred to in article 5 of the Organic Law on Data Protection, as well as those relating to a lack of information in the visitors' entry data forms in public buildings, and undue access to personal data in a public body.

The major debates within the Agency in 2007 were about whether it was possible to prevent the misuse of personal data on the Internet, if a video surveillance society and a more controlled work life was inevitable, if it is possible to cope with Internet piracy and protect personal data, and what privacy guarantees can be achieved in a globalized world.

These concerns can be considered the precursors of the activity of the Agency in the following period, while it was moving, together with other European authorities, towards international privacy standards.

Finally, it should be noted that new sectoral inspections were formally undertaken in the sectors of electronic commerce and the management of credit cards in large commercial areas.

7. The protection of rights

The early 2000s saw a large increase in requests about the protection of rights. Although the concerns of citizens remained basically the same, there was an inversion in the trend of previous years: interest in the right of deletion accounts for 53% of the requests, while the right of access drops to 42%, which shows that citizens' concern is not so much about the access to data or not, but to avoid these data being processed.

Requests relating to the exercise of the right of deletion mainly involved the following issues: improper inclusion in payment default files and deletion when the debt is paid; elimination of data once the services contracted with telecommunication operators has been completed; closure of the files of telecommunication operators when a subscriber has not given their consent to a change of company; clinical history; and deletion of data -especially photographs- on the Internet (forums, YouTube).

The most common demand over the right of access related to images taken by cameras on public roads, economic solvency assessments carried out by financial institutions, the medical history of a deceased family member and clinical histories that were considered to have been provided in an incomplete way.

Among the requests relating to the 'right of opposition' can be highlighted citizens' interest in data processing by medical companies that control time off work and the receipt of advertising from a company with which there has been a prior contract.

8. Agency Recommendations

At the end of this period, the Agency, based on its experience acquired in the exercise of its functions, published a series of recommendations to guarantee the privacy of citizens:

- Deberían delimitarse las actividades en las que puede resultar necesario el establecimiento de sistemas de denuncia interna en las empresas por los trabajadores, determinando sus finalidades, los procedimientos de auditoria y los periodos de conservación; garantizando la confidencialidad del denunciante y los derechos de los denunciados.
- The establishment of an internal companies complaint systems for workers may be necessary, which defines its purpose, any auditing procedures and the periods that information can be kept; while both guaranteeing the confidentiality of the complainant and the rights of those reported.
- The development of procedures that make compatible the rights of copyright protection and data protection.
- The need to regulate the anonymous publication of verdicts by legal bodies.
- The relevant Public Administrations should develop plans to protect minors' personal data on the Internet.
- The promotion of special precautions to avoid the unwanted exchange of sensitive personal data on the Internet through P2P networks. Users must be urgently made aware of the risks that arise from

spreading, often inadvertently, information stored on their computer equipment.

- The generalized use of the 'hidden copy' in the sending of emails should be promoted, as a guarantee of confidentiality.

- Promotion of good practice in the guarantee of privacy in all Bulletins and Official Journals. The information published usually includes personal data and is also captured by Internet search engines, multiplying the access possibilities and making it difficult to exercise the rights of deletion and opposition. It is recommended that procedures are developed that, without affecting the proper function of the official journals, limit the possibility of misuse by search engines on the Internet.

- The development of a local strategy aimed at adapting the installation of cameras for traffic control to the rules of personal data protection.

- Promote self-regulation in the media (written and audiovisual) to guarantee the protection of personal data. In general, the prevalence of freedom of information can be affirmed (Article 20 CE). If a particular piece of news has public relevance, the affected party has a duty to support it without being able to invoke the principles of protection of personal data. However, this does not prevent the promotion of more respectful practices regarding the personal data protection regulations. An appropriate instrument for this is self-regulation by the sector itself. Other possible conflicts must be resolved within the framework of the legislation for the protection of honor, privacy and one's own image.

IV. The regulation of the Organic Law of Data Protection: from 2008 to 25 may 2018

1. The Regulation for the development of the Organic Law of Data Protection

Following the early years of the implementation of the Organic Law, with the Agency at the time under the leadership of José Luis Piñar Mañas, the need was felt to develop the regulations to achieve higher levels of legal security when they were applied.

The Regulation finally saw light, soon after the mandate of Artemi Rallo Lombarte, through the publication of Royal Decree 1720/2007, of December 21.

The regulation contributed decisively to objectify the application criteria of the Organic Law, which benefited not only from the resolutions of the Agency itself, but, above all, the judgments of the Contentious-Administrative Chamber of the National Court and of the Supreme Court, and complied with the obligation to transpose Directive 95/46/EC.

One of the most outstanding novelties of the Regulation, in relation to the so-called solvency files, was that the requirements for inclusion of the data and to access the information in these files were specified.

Solvency processing usually involves four subjects: the debtor, the creditor who notifies the debt, the person responsible for the solvency treatment, and the entities that consult this information. To include the personal data of a person in a 'defaulters file', the following requirements must be fulfilled:

- That there is a specific debt, due, demandable, and unpaid.

- That six years have not elapsed since the date on which the payment of the debt or the expiration of the obligation or the corresponding installment payment was due.

- That there is a payment notice requirement, warning that if payment is not made, the person's name will be included in the defaulters file. Whoever notifies that the debt will be added to the file, must prove that they have provided this notice. The obligation will be fulfilled when the recipient rejects the missive and/or when it is sent to the address that appears in the contract.

The AEPD does not have the powers to resolve disputes about the existence of a debt. The consent of the owner of the data is not required to communicate the information to a debt collection management company. If a person does not know which solvency file they are included on, they can exercise the right of access to their personal data in the files - in the guide published by the Agency, accessible through its website, there are links to the most common files. Once the debt has been paid, the personal data must be deleted. If not, the right to have the data deleted can be exercised. This right of withdrawal can also be exercised if, after six years from the expiration of the unfulfilled obligation, the data continues in the non-payment files ('payment defaulter files').

Another significant novelty that the Regulation incorporates with respect to advertising processing was inclusion in the common files for exclusion from commercial communications. This so-called 'Robinson List' service was jointly presented on June 30, 2009 by the Agency and the current Spanish Association of the Digital Economy (ADIGITAL), the only entity that manages it to date.

This service allows those who join it to manage unwanted advertising – and in particular, so that parents or guardians can request that minors' data are not used to send advertising-, and also allows the possibility to choose the channels through which a person wishes to receive advertising, including by postcard, email, SMS and MMS messages and telephone. Within each of these channels it is possible to select several options regarding the identity of the person, their addresses, email addresses and phone numbers. At present there are over 600,000 citizens registered.

2. Modification of the Law of Services of the Information Society and Electronic Commerce and the General Law of Telecommunications

In 2014, there was a partial modification of the Law of Services of the Information Society and Electronic Commerce to strengthen the guarantees of citizens against the practice of profiling, in particular, for the purposes of 'online' advertising.

Faced with the inoperability of the system of opposition to the use of cookies or other similar devices, the new regulation required obtaining unequivocal consent from Internet users, transposing Directive 2009/136 EU.

On the other hand, the General Telecommunications Law was amended to oblige telecommunications operators to notify the Agency of security breaches in their information systems and, if applicable, also to the

interested parties themselves if they might have their rights infringed as a result.

3. Citizens' consultations

During this period, and significantly since 2014, there has been a rebound in the number of inquiries about improper inclusion in 'payment default' files, and also the acknowledgement of possible identity theft in the contracting of basic services such as telephony or the water and energy supply.

Additionally, citizens sought information about the: obligation to register files, which has disappeared with the entry into force of the EU Regulation on May 25, 2018; data protection in the management of property by owners; video surveillance; and how to make complaints and claims to the Agency.

Regarding consultations on the exercise of rights by citizens, 43.34% related to the right to deletion of data, and 12.38% to the so-called 'right to be forgotten' relating to links generated by search engines on the Internet.

With regard to the other rights, 31.36% related to rights of access, 8.73% to opposition, and 4.16% to rectification.

In 2016, the 'Frequently Asked Questions' list was reworked, drawing together more than 200 question-answers grouped by theme, among which questions on the new EU Regulation were already included, thus preparing for when it comes into force.

In short, the concern of the Spanish population for privacy has grown significantly in recent years. This is evidenced by the CIS Barometer of May 2018 in which 76% of respondents said that they were either 'very' or 'greatly concerned' about the protection of their personal data and its possible use by third parties.

In a field as common as commerce, respondents showed that they do not feel safe giving data about their bank card over the Internet; although curiously, financial institutions seem to be winning the battle against mistrust because although 31% of respondents feel that it is not safe for them to carry out Internet banking operations, 29% say they are quite safe.

Equally interesting is the identification of the data that the respondent would not provide, unless it were essential: a fingerprint (86.1%), medical records (66.9%), and financial information (87.6%).

Regarding information about tastes and opinions: 40.4% would give them easily, 27.4% would reluctantly give them and 30.7% would not give them, unless it was essential.

With regard to personal photos and videos, 22% would be reluctant to give them, and 70.7% said they would not, unless it was essential.

In general, the population does not habitually read Internet sites' privacy policies: 9.2% 'almost always' reads them; 21.7% sometimes; 29.4% rarely; and 33.3% never.

To conclude this review, the following points are revealing:

- In response to the statement: "Actually, it matters more to access the services provided by websites

Table 1
Evolution of citizen consultations on rights (period 2008-2017)

Source
Prepared by the author

YEARS	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Total consultations*	72.650	97.223	104.826	134.635	111.933	102.064	99.524	85.611	89.658	85.154
About rights	20.030	30.820	30.200	38.788	11.753	7.883	5.458	5.522	7.226	8.175

Table 2
Percentage of citizen consultations by type of right

Source
Prepared by the author

RIGHTS	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Access	12,3%	20,62%	23,63%	15,71%	13,1%	22,34%	25%	26,25%	7,92%	31,36%
Cancellation	53,01%	62,39%	40,64%	50,35%	50,35%	51,57%	55,11%	55,98%	79.9%**	55,72%**
Rectification	1,23%	2,42%	5,44%	3,57%	1,8%	3,23%	3,75%	2,31%	2,68%	4,16%
Opposition	2,82%	8,66%	25,51%	27,85%	30,9%	20,71%	15,03%	13,97%	9,5%	8,73%

** Includes the so-called “right to be forgotten’

than data privacy.” 11.4% ‘strongly agree’; 37.7% ‘quite agree’; 28.7% ‘barely agree’; and 17.8% ‘don’t agree’.

- In response to: “Have you ever regretted having posted something (comment, photo, video) on a social network?” 24.5% responded in the affirmative.
- And for: “Have you ever had problems with content that others have posted on the social network?” 12.2% said ‘yes’.

4. Complaints and Inspections

During this period, research files grew until 2013, when a decreasing trend was noted.

The formal sectoral inspections were very prominent in 2008, then sharply fell up to the 2016 to 2018 period, when they grew again significantly as a result of their inclusion in the Agency's Strategic Plan, as part of its preventive work.

Private sector sanctions have remained constant throughout the period, with a slight reduction from 2016.

On the other hand, the declaratory procedures related to public administration infringements have been very stable, except for slight upturns in the years 2009 and 2010, and a reduction in the period 2011 to 2013.

The procedures related to the application of the Services of the Information Society and Electronic Commerce Law (LSSI) and the General Telecommunications Law (LGT) during the period, are shown in Table 4.

Of the total of 975 actions in this area corresponding to the whole period, it is worth highlighting the increase in offences relating to cookies, which is connected to the modification of the LSSI due to Royal Decree-Law 13/2012, as well as that of spam (commercial electronic communications), especially the sanctioning resolutions during the period 2012-2016.

As regards sectors in which the largest number of inspections were carried out and most sanctions given during the period, those relating to telecommunications, financial institutions, video surveillance and payment default files continue to be

Table 3
Complaints and inspections

Source
Prepared by the author

YEARS	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018[1]
Guardianship claims	2.159	1.832	1.657	2.230	2.193	1.997	2.099	2.082	2.588	2.654	1.346
Complaints	3.073	5.310	5.045	7.648	8.594	8.607	10.074	8.489	7.935	7.997	5.311
Claims RGPD	-	-	-	-	-	-	-	-	-	-	4.407
Total	5.232	7.142	6.702	9.878	10.787	10.604	12.173	10.571	10.523	10.651	11.064

[1] Since the entry into force of the General Data Protection Regulation, a new classification category has appeared: the RGPD claims.

Table 4

Source
Prepared by the author

Procedure	Activity Group	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Pr. Apercibimiento	Cookies (LSSI)							22	28	12		
Pr. Apercibimiento	Spam (LSSI)						3	40	27	19	19	13
Pr. Infracción	Cookies (LSSI)					1		1	2			
Pr. Infracción	Spam (LSSI)	1								1		1
Pr. Sancionador	Cookies (LSSI)						7	17	10	14		1
Pr. Sancionador	LGT (fax y otros)	14	4	1	6	4	2	3	3			
Pr. Sancionador	Spam (LSSI)	49	35	52	31	62	76	81	102	63	39	32
T. Derechos	Cookies (LSSI)									1		
T. Derechos	LGT (fax y otros)					1						
T. Derechos	Spam (LSSI)	2	1			2	4	9	15	8	2	14
TOTAL		66	40	53	37	70	92	173	187	118	60	61

the most prominent, followed by those of spam and the Public Administration.

These data are in line with the evolution of the economic situation. If in 2007 the Survey of the Active Population showed an unemployment rate of 8.57%, in the following years this percentage shot up, with all the consequences that unemployment implied for households; particularly delays in, or even the impossibility of, meeting credit payments.

Another area that creates great citizen concern is telephone advertising. As a result, the AEPD carried out two formal mobile telephony sectoral inspections related to commercial calls and 'short messages'. The Agency noted the lack of mechanisms available to citizens to halt these communications and warned about how easy it is to unwittingly be paying for high rate calls.

2008, in particular, was associated with video surveillance, which was already an unstoppable phenomenon at the time. The sectors that had the most files opened were those of commerce, followed by tourism and hospitality, and then property owner management; displacing health to fourth position. In

line with the above, inspection and sanctioning in these areas increased significantly.

The notable growth of video surveillance files in the education sector is striking. In this context, we must mention the criteria adopted by the Agency in relation to video surveillance in schools, where the installation of cameras can serve children's best interests by contributing to greater security in playgrounds and in the dining room. However, this statement is not absolute, since competing interests must be balanced. Access to the images and recordings, for example, must be strictly controlled.

Agency criteria in relation to video surveillance evolved throughout this period. In this context it is worth mentioning the policy change in relation to simulated/non-functioning cameras. Specifically, the Agency used to sanction when its requirements were not met, but now it archives cases where there has been no actual processing of personal data.

As of 2008, several formal inspections were initiated due to information published in the media, about the appearance of documents containing personal information found on public roads. It is particularly worth noting, because of its special importance, inspections related to the discovery of legal documentation and health user cards on public roads. It should not be forgotten that making personal information available that should have been destroyed or kept confidential, and that sometimes contains sensitive or specially protected data, such as health records, reveals, not just ignorance, but a real neglect of citizen rights.

On the other hand, in the area of portfolio transfers between companies (sale of debt) in 2009, several disciplinary proceedings were undertaken that resulted in the imposition of fines that reached up to €420,000. These involved cases in which companies, mainly from the telecommunications sector, sold a debtor portfolio to another company that would then seek to recover the debts of thousands of customers. After verifying that in several cases the transfer of a non-existent debtor or debt had taken place, the aforementioned sanctioning decisions were adopted.

The dissemination of files containing personal data in P2P networks using work tools, usually with the e-mule program, was another of the Agency's main concerns. The inspections initiated by this practice, which affect both private entities and public bodies, included a gym, a union, a sports club, a psychosocial rehabilitation center, a political party and a law firm. The files disseminated included sensitive information, such as health data.

Throughout 2010, a project was also undertaken to prepare a report on compliance with the LOPD in hospitals, as these institutions are chiefly responsible for working with health data. This initiative came about as the result of alarming cases of legal non-compliance, mainly linked to security breaches, including the dissemination of clinical data through P2P file exchange networks; abandonment of health data on public roads; the storage of clinical information in unrestricted areas of health centers and, therefore, within the reach of anyone; the loss of clinical histories when automating systems in an electronic format; and the use of health data for unauthorized purposes, or their undue communication to third parties.

The Agency also analyzed information systems for citizens, procedures for the exercise of ARCO rights, the registration of files and the outsourcing of services.

The evaluation was carried out by sending a questionnaire to more than 600 centers registered in the List of National Hospitals, which had a 92% response rate. In general terms, the degree of compliance was greater in centers in private hands than in public ownership. In terms of security, the report shows that there was a significant difference between formal compliance with security measures and their effective implementation. Thus, although the vast majority of centers had a 'security document', there were deficiencies in the application of the measures. It was also concluded that there was a lack of diligence regarding access to medical records, namely whether those who use the data had adequate justification -fundamentally that access was necessary for patients health care -, as well as an absence of controls in the effectiveness of security measures.

Over time, health sector entities have made progress in the digitalization of their work processes. In Spain, public health care management is decentralized across the Autonomous Communities' Health Services. Since the mid-nineties these Communities have been implementing electronic processing in specific aspects of their work, such as the management of off-work disability reports, and gradually have been exploring other methods of working with data, such as electronic medical records, information systems in laboratories (LIS) and electronic prescriptions. This effort, undertaken at the beginning of the 21st century, focused on the interoperability of the different systems used by the autonomous health services; based on common standards. Currently, almost all the Autonomous Communities operate the Electronic Health Record System of the National Health System (HCE) in the implementation phase, and electronic prescription systems are very advanced.

The Agency's interest in hospitals' data processing continued in 2017 with the implementation of a new Office Inspection Plan. The Plan focuses on auditing aspects where shortfalls were detected in the 1995 and 2010 inspections and, specifically, in the security measures. To this end, the strategy centred on hospitals that: were starting from paper-based medical histories and have transferred them to electronic format; hospitals that still have paper-based medical histories and are immersed in automation processes; and hospitals that have had electronic medical records since their inception. The inspected hospital services include: Admissions, Emergencies, External Consultations, Pathological Anatomy, Intensive Care Units, Clinical Analysis Laboratories, Hospital Pharmacies, Departments of Information Technology, Patient Care, Social Services and Biobank.

Among the main conclusions of the analysis has been found, in general, a favorable trend regarding the gradual incorporation not only of the regulations, but of the principles and culture of data protection. The report shows that specific errors found in the treatment of data do not constitute general behavior, which represents a marked improvement in performance.

Among the aspects that can and should be improved, must be highlighted those relating to the information offered to patients and the strengthening of security measures.

The publication of this Inspection Plan is accompanied by basic rules that include key points of the data protection regulations aimed at the health and administrative staff of centers, with the ultimate goal of raising the level of compliance and generating confidence in the actions

of the health institutions in both the healthcare and research areas.

Apart from the legal actions, there was an increase in complaints in the health sector due to offences related to security breaches and unjustified and unauthorized access to medical records.

Finally, in order to highlight the most significant cases related to the Agency's reactive functions, the highest fines in its history are listed.

5. Rights protection

The figures relating to the Agency's work on the protection of rights have grown steadily, and were accentuated between the years 2012 and 2017.

Among them, the right to be forgotten on the Internet has become a growing demand since 2010. The increase in the use of deletion and opposition rights against those in charge of search engines demonstrate the intensity

Table 5
List of the most significant sanctions in the history of the Agency

Source
Prepared by the author

Case	Sanction	Date of resolution	Fine
PS/00082/2017	FACEBOOK, INC.	21/08/2017	1.200.000,00
PS/00095/2000	Zeppelin Televisión, S.A.	29/12/2000	1.081.821,79
PS/00345/2013	GOOGLE INC	18/12/2013	900.000,00
PS/00433/2017	J.V.L.F.G.	08/03/2018	800.000,00
PS/00169/2006	INVERTRED, S.L.	28/03/2007	602.214,12
PS/00146/2011	J.V.L.F.G.	21/09/2011	600.000,00
PS/00146/2011	SABERLOTODO INTERNET S.L.	21/09/2011	600.000,00
PS/00348/2005	COMERCIAL REDES SISTELCOM, S.A.	12/09/2006	450.000,00
PS/00006/2006	DATASUN 2, S.L.	19/07/2006	540.000,00
PS/00166/2008	INFORMACION EUROPEA ON-LINE, S.L.	19/06/2008	450.000,00
PS/00251/2005	Comercial Redes Sistelcom, S.A.	27/04/2006	450.000,00

of this demand, amounting to almost one hundred resolutions issued to protect these rights. 87% affect the Google search engine and the remainder relate to others, such as, Yahoo!, Lycos, Altavista, Bing and Terra. 75.5% of cases were resolved in favour of citizens.

In this respect, the year 2014 is marked in the data protection field by the European Union's Court of Justice ruling in the case of 'the Agency against Google', which will be described below in section V, regarding the right to data protection in Internet services.

V. The right to protect data in Internet services. The new challenges of privacy

We are immersed in a digital society, or information society, characterized by the existence of more information about people, and about more aspects of their lives, which can be stored, exchanged and processed for a large variety of purposes with great ease and with relatively low costs.

That is the scenario in which the fundamental right to the protection of personal data currently has to be developed. Huge amounts of information that is constantly generated and shared by all citizens in a highly technical context.

Some data, although they are on scales that are difficult to visualize, can help give an approximate idea of the dimensions of this phenomenon.

A study has recently been published according to which global traffic over the Internet will multiply by three between 2016 and 2021, reaching 3.3 Zettabytes per year in 2021.

In Spain, this traffic will reach 37 exabytes per year in 2021, from the 12 registered in 2016.

As those figures surely escape us all, it is worth saying that that would represent all the films produced in the world throughout history crossing the Spanish IP networks every two hours.

In Spain there will be 36.3 million Internet users in 2021 (79% of the population), from the 33.5 million recorded in 2016 (73% of the population).

And also in Spain there will be 345 million devices connected in 2021 (7 connections per inhabitant), from the 196 million posted in 2016.

At the same time, little can be said about the technological advances that we cannot perceive in our day to day life.

The development of the Internet is at the base of this advance. All the services of the Information Society are supported by the network and, at the same time, have contributed to its growth and to the universalization of its use.

One point worth highlighting is that the presence of the Internet is evident not only in the services provided entirely and directly 'online', but also in the increasingly frequent integration of 'off-line' activities with versions or utilities on line. In other words, the penetration of the 'on line' dimension in which we tend to define the 'real world' is growing; although both are in fact growing.

This is very evident in, for example, the financial and commercial sectors, where large spaces or banks unite their offer in physical establishments with alternatives on the Internet that are increasingly gaining in prominence.

Perhaps it is less obvious, but equally real, in many other activities. The simplest smart phone model has an information processing capacity superior to that of the large computers that a few years ago were only available to companies. And they also allow you to make phone calls.

The immediate future will offer many new developments in this field. Concepts such as 'big data', 'the Internet of things', 'artificial intelligence', 'blockchain' and the associated technologies that make them possible, are going to have, and already have, an enormous impact in the field of personal information.

Because regardless of the place we occupy through our professional, business or political activity, for a good part of our lives we all play the role of 'citizen holders' of such data. And we will be affected by the use that is made of them.

These effects can be analyzed from different perspectives, and one of them is the protection of the rights of people in the use of these data.

Modern technologies and their use of personal information have improved our lives, and they will undoubtedly do so even more in the coming years. They are a determining factor for change and innovation.

The access to information and training that we currently enjoy is unparalleled with that we were offered in the not too distant past.

And this information is also more plural and varied. There is no longer a limited number of actors in the communication process. It is now about open and multidirectional communication.

The Internet, and the use of our data, offer us much greater personal relationship possibilities and an enormous diversity of ways to manage our leisure time.

One cannot in anyway ignore its impact on economic activity. New businesses, new business models, a different way of managing company relationships with customers are all the result of the emergence of new technologies in the business environment.

Technologies are a fundamental factor in the generation of wealth within the framework of the digital economy.

And it is also necessary to allude to its effects in the field of public policies, including those related to security. Technologies and the analysis of information contribute significantly to a better identification of the needs of citizens and to better provision of the services they demand.

The impact is similar in the fight against crime, especially in its most serious manifestations, both in the preventive dimension and in the pursuit and prosecution of those responsible.

Its role in the development of scientific research in all fields is crucial, but in particular in the field of health. Thanks to these advances, and the capacity new technology offers to process large amounts of information, the causes, and also responses, to diseases that up to now were resistant to study by traditional methods are being identified.

But if the possibilities and advantages are great, so are the risks.

Some of these risks have to do simply with a matter of quantity and statistics. The more data there is circulating about more aspects of people's lives, the more likely it is that something will go wrong and that the problem will have serious consequences for those affected.

But other risks are associated, above all, with unforeseen, unfair or illegal uses of that information.

Unfortunately, the seemingly illegal use of data obtained through an application distributed on the social network Facebook, which originally had scientific research purposes, with the aim of manipulating electoral processes, is highly topical.

This is a perfect example of illegal and interested use of data provided in good faith and with the conviction that they would be used in the framework of scientific research. Not only is the right to privacy and data protection of the people involved affected, but states are also facing a direct attack on the very foundations of the democratic system.

And all this from unauthorized use of some information; a use over which their owners had no knowledge.

Many similar cases could be cited.

Many of them are due to reasons that have to do with the way in which the economy has been organized and has evolved in the digital environment.

It is a sector that has experienced an intense process of concentration in little more than a decade; with a small group of actors in dominant positions that store huge amounts of information.

At the same time, the business model of many, if not most, service providers of the information society is based on the monetization of the personal information of its users.

In principle, these data are marketed for commercial advertising purposes. But it might also be used for other types of purposes. For example, for companies that want to know the profiles of their potential customers to determine the prices at which they will offer their products or services.

Soon it will be five years since the revelations of Edward Snowden that showed how, starting from the very legitimate aims of fighting terrorism and other serious forms of organized crime, the US intelligence services had developed projects to access citizens' data managed by the big Internet companies.

Among these data were those of citizens in the European Union that would have been transferred to the United States in the framework of the so-called Safe Harbor Scheme. This was an instrument that was declared illegal by the European Union's Court of Justice, precisely as a consequence of the lack of limits and guarantees to access by the security services.

The possibilities that technologies offer for the collection and processing of personal information are presented to us as practically unlimited.

Many people say that they are willing to offer their personal information in exchange for services. But, at the same time, those same people tell us that they distrust digital services and want to regain control, or have more control, over the information they provide.

One of the main obstacles to the development of the digital economy is the lack of citizen trust. The set of challenges outlined above requires response. Responses that guarantee the rights of European citizens in a world of globalized services that often are provided from outside the European Union.

It was precisely to address all these challenges with confidence and generate the necessary trust among the different actors involved, that the Agency launched in 2016 the Unit of Evaluation and Technological Studies (UEET), as a specialized unit to analyze the implications of new developments, to carry out prospective studies and evaluate products and services in the market. All this is undertaken in collaboration with universities, technological research groups, industry and the public administrations empowered to promote ICT.

- **The right to be forgotten on the Internet: a necessity of our time**

Search engines have become an essential tool in the daily life of all Internet users. Without them, it would be enormously difficult to access existing information on the network. But, at the same time, their potential is increasingly problematic, because they allow us to be located instantaneously, overcoming all barriers of time and space, and provide information of all kinds relating to a person. The recovery and aggregation capabilities of search engines can cause considerable harm to individuals, both in their personal lives and in their social relationships.

One of the most important issues in the current debate on privacy on the Internet is related to what has been called the 'right to be forgotten'.

The resolutions of the Spanish Agency for Data Protection in terms of protection of rights, and particularly to the right of deletion, had been accepted at specific moments by those responsible for a number of web pages, but the same did not happen when a decision affected Google: in fact, the largest search service provider systematically challenged the Agency's decisions before the contentious-administrative jurisdiction.

The National Court decided on February 27, 2012 and before the resolution of the appeals filed by Google, to file a preliminary issue before the European Union's Court of Justice. It sought to re-interpret the European Court's interpretation of several sections of Directive 95/46/EC which were relevant for the resolution of more than 200 appeals pending before the Hearing; in particular, those relating to a number of key questions about the applicable law, the responsibility of search engines and of website owners, the powers of the data protection authorities and the possibility of avoiding the indexation of personal information.

On May 13, 2014, with the Director of the Agency, Mr. José Luis Rodríguez Álvarez, at its head, the Court of Justice of the European Union issued its ruling in case C 131/12 (Google Spain, SL, Google Inc. vs. The Spanish Agency for Data Protection (AEPD), Mario Costeja González), resolving the aforementioned question referred in 2012 by the National Audience.

The Judgment fully accepted the thesis that the Spanish Data Protection Agency had put forward, and its verdict led to a change in Google's privacy policy, making the Agency a reference worldwide among the Control Authorities.

In essence, the Judgment established that European law, and more specifically Spanish legislation, are applicable to Google, and requires the company to have an establishment in European territory.

On the other hand, the judgment considered that the technical operations performed by search engines to find information on the Internet are integrated into the definition of 'processing' offered by the Directive, and that the search engines themselves are responsible for that treatment because they decide on the means and on the ends.

The European Court also stressed that the activity of search engines has a significant impact on the fundamental rights of respect for privacy and protection of personal data, since in searches carried out on the Internet from the name of a person, it is possible to obtain a complete and structured view of all the existing information about them and this would allow more or less detailed profiles to be developed. For the Judgment, it is the universal dissemination and accessibility offered by the search engines that can lead to injury to the rights of people in a much more intense and serious way than the original publication of information.

The Court of Justice did not accept the thesis that the activity of the search engine would be, in some ways, legitimized by the right of freedom of expression. For the Court, the interest that the search engine has in processing information is merely economic and is insufficient to justify the serious interference with individual rights that it entails.

In general terms, the rights of the affected person would also prevail over that interest in locating a piece of information through nominative searches, but in each specific case that balance will depend on the relative weighting between the nature of the information in question, its sensitive nature for the private life of the affected person and the public interest in having the information. It is important to note that the Court expressly states that it is not necessary that harm be caused to exercise the right against the search engine.

In May 2015 the Agency, after the appropriate inspection actions, declared illegal Google's practice via which, through the Webmaster Tools service, it communicated to the people responsible for the different web pages what information on their websites was being removed from the results of a search. In this way, the editors of those web pages, simply by re-editing the information or with a small change in the URL, retrieved the deleted information, which reappeared immediately in Google searches.

- **The Street View service**

In October 2010, after an exhaustive preliminary investigation, the Agency initiated a sanctioning procedure against Google Inc. and Google Spain for the acquisition and storage of location data of open wireless networks (Wi-Fi networks) and of traffic data transferred to them by the vehicles used to obtain images for the Street View service.

However, the existence of an open criminal judicial procedure forced the Agency to suspend its sanctioning procedure. In 2017, once the decision of the Court that agreed to dismiss and archive criminal proceedings was known, the Agency resumed the administrative procedure.

It was found that Google collected information from users' open Wi-Fi, without those affected having knowledge that this data collection was taking place without their consent. It was not verified that Google dealt with specially protected data through these systems.

In October 2017, the Agency issued a resolution declaring the existence of a serious infringement and imposed a penalty of 300,000 euros on Google. As for the data being collected from open WiFi networks, the resolution specifies that "the fact that holders of WiFi networks do not ensure the encryption of these networks, to the detriment of the security of their data, does not authorize in any way the collection of the information carried out or any subsequent use thereof."

- **Google's privacy policy**

The Agency initiated a procedure to analyze the compatibility of Google's privacy policy and its conditions for use of services with the Spanish regulations on data protection. In the framework of this investigation, it was found that Google illegally collects and processes personal information, both on their authenticated users (registered in their services) and of those who are not; and even of mere "passive users" who have not requested their services but who access their pages, which include elements managed by the company without specifying it.

The inspection actions confirmed that Google collects citizens' personal information through almost a hundred services and products offered in Spain, without providing in many cases adequate information on what data is collected, for what purposes they are used and without obtaining the valid consent of its owners.

Thus, for example, Gmail users are not clearly informed that a filtering of the content of their emails and their attached files is done to insert advertisements. When it is reported, imprecise terminology is used, with generic and unclear expressions employed that prevent users from knowing the real meaning of what is being considered.

The lack of adequate information on the particular purposes that justify the processing of the data prevents specific and informed consent being considered and, consequently, being valid.

On the other hand, Google combines the personal information obtained through its various services or products and uses it for multiple purposes that are not clearly determined, and thereby violates the prohibition to use the data for purposes other than those for which they have been collected.

Contrary to what is required by Spanish law, Google stores and keeps personal data for indeterminate or unjustified periods of time. The preservation of data for an indefinite period of time, beyond the requirements that derive from the purposes intended at the time of collection, constitutes illicit treatment.

Finally, the Agency concluded that Google hinders - and in some cases prevents - the exercise of rights of access, rectification, deletion and opposition. The procedure that citizens must follow to exercise their rights or manage their own personal information forces them to go through a myriad of pages scattered across several links that are not available to all types of users and, sometimes, with names that do not always make reference to its object.

The AEPD declared the existence of three infringements of the LOPD and imposed a fine of 300,000 euros on Google for each, and required it to comply with the law without delay.

As a result of this action by the Agency, Google's privacy policy changed worldwide, and introduced significant changes in terms of information, consent and the exercise of rights.

- **Information in the cloud or "cloud computing"**

The provision of cloud computing services in its different 'cloud types' (public, private, hybrid, etc.) and service modalities (infrastructure as a service, platform as a service and software as a service) has modified traditional relationships between the clients -responsible for the treatment of the data- and those in charge of the treatment - providers of cloud computing services -.

The change of paradigm in these relations led to the Agency initiating a process of analysis on its implications and on the necessary modulations in the application of data protection regulations to guarantee the rights of citizens. This analysis concluded with the preparation of a guide on cloud computing, whose most outstanding aspects are the following:

- The applicable legislation on data protection is that of the customer who processes data in Spain.

- The provider of cloud computing services is a processor, even if it is a large multinational company. The client who contracts with the service provider is still responsible for the data processing and must act diligently in the choice of provider of cloud services. The service provider for its part must be diligent in providing guarantees for data protection. In this diligence, transparency plays an important role in obtaining information on these guarantees and, in particular, on those existing in the outsourcing of services and in international data transfers.

- The client must inquire about whether the security measures are adequate for the treatment of the data and obtain guarantees to audit them, even if it is through a (reliable and independent) third party.

- The client must obtain guarantees so that, at the end of the contract, s/he can recover the personal data, or transfer them to a new provider of these services.

- **The crisis of the Safe Harbor System**

On October 6, 2015, there was a crisis in the system that was employed as the basis for international data transfers from Europe to the United States. That day the ruling of the European Union's Court of Justice was published, which invalidated the European Commission Decision 2000/520/EC, known as the 'Safe Harbor' Decision, which regulated the transfer of data from the European Union to those entities established in the United States and were sheltered under the Safe Harbor system.

The Court's decision was the result of a claim by Maximiliam Schrems, an Austrian national and Facebook user, who had asked Facebook Ireland not to transfer the data to Facebook Inc., its parent company based in the United States.

The complainant alleged that the current United States law and practices did not guarantee sufficient protection of personal data kept in its territory against the surveillance activities practiced by its public authorities. Mr. Schrems made reference in this regard to Edward Snowden's revelations about the activities of the information services of the United States, in particular those of the National Security Agency (NSA).

Among the reasons for the Judgment was the revelation of the existence in the United States of several surveillance programs for the collecting and processing of large-scale personal data.

It was found that, as a consequence, for example, of the contracting of Internet services, the North American authorities had access to the personal data of European residents and that these data were used for different purposes and were incompatible with those that justified the transfers. It was also proved that the interested parties could not exercise any legal action to access their personal data and that their rectification or suppression was also vetoed.

The pronouncement affected Internet companies such as Google, Facebook, Microsoft, Apple and Yahoo, which have hundreds of millions of customers in Europe and transfer the personal data of those customers for processing from Europe to the United States.

The ruling was also influenced by Mr. Snowden's revelations about the activities of the National Security Agency (NSA), which, based on reasons of national security, public interest or compliance with American law, could access the data of Europeans that had been transferred to the United States, without any rule to limit possible interference with their rights.

The supervision of the actions of the information services is carried out through a secret and non-contradictory procedure. Once the personal data has been transferred to the United States, the NSA and other federal agencies, such as the Federal Bureau of Investigation (FBI), can access them in the context of surveillance and undifferentiated interceptions that they execute on a large scale.

For all these reasons, and some others, the Safe Harbor system was declared invalid. Therefore, between that date (October 6, 2015) and July 12, 2016, when the Commission approved the 'Privacy Shield' decision to replace the canceled one, the Spanish Agency deployed a series of actions aimed at alleviating the absence of guarantees for those whose data had been and were being transferred to United States' entities attached to the Safe Harbor system.

• The risks of geolocation

The proliferation of smart mobile devices has led to the emergence of a multitude of services to locate their owners. People use their mobiles to learn about the weather forecast, find a street, locate friends or search for a specific service in a specific place.

The technology used by these mobile terminals, which are closely linked to people, allows geolocation service providers, through the capture of signals from base stations and Wi-Fi hotspots, to obtain details of the habits and behavioral patterns of the owner of the mobile, and, therefore, to establish exhaustive profiles of these users.

The Agency participated in an analysis of this phenomenon carried out by the Working Group of Article

29 of the European Committee for Data Protection, which concluded in the 'Verdict on geolocation services' that was approved in May 2011 (WP 185).

In this same area, several media outlets reported that Google collected information on the location of mobile terminals with Android operating systems, regardless of whether the user had authorized it in the system settings, and even if the geolocation system was deactivated from the terminal.

The Agency concluded after the corresponding investigation that Google only uses the information transmitted by these terminals to establish connections, but it does not register the servers of the entity, nor is it used to track the location of users.

- **Advances in facial recognition**

In recent years there has been a rapid increase in the availability and accuracy of facial recognition technology. This technology has been integrated into online services and mobile devices that allow users to capture images and link them in real time to a wide variety of online services. As a result, users can take pictures with their mobile phone, tag people - who may or may not be registered in the service -, and share the images with other users.

The popularization of these services, their implantation in social networks and in facial recognition services and the labeling of photographs, such as through Google's 'Find my Face', entails a series of challenges for privacy. These include the processing of digital images of people who do not use the service and have not given their consent for it, the use of images for purposes other than which they were taken, or the possibility of looking for people by introducing their image in a search engine and obtaining matching images or the profile of the person in social networks as a result.

- **The collection of data by social networks (Facebook)**

In September 2017, the Agency concluded its investigation initiated to analyze whether the data processing carried out by the social network Facebook is in line with the data protection regulations.

In the framework of the research carried out, the Agency verified that Facebook gathered information about ideology, sex, religious beliefs, personal tastes and navigation without clearly informing people about the use and purpose that it was going to give to them. Specifically, it was verified that the social network processed specially protected data for advertising purposes, among others, without obtaining the express consent of the users as required by the data protection regulations.

The investigation also made it possible to verify that Facebook did not inform users in a comprehensive and clear way about the data that it was going to collect and the processing that it intended to carry out, but that it simply limited itself to giving some examples. In particular, the social network collected data derived from the interaction carried out by users on the platform and on third-party sites without their being able to clearly perceive the information that Facebook collects about them or for what purpose they are going to use it.

The Agency also confirmed that users were not informed that their information was going to be processed through the use of cookies - specifically used for advertising

and other secret use by the company - when browsing through non-Facebook pages and that contain the 'Like' button.

This situation also occurred when users were not members of the social network but had once visited any of its pages, and when a user registered on Facebook navigated through third-party sites, even without logging into Facebook. In these cases, the platform added the information collected in these pages to the information associated with their account in the social network.

For all these reasons, the Agency considered that the information provided by Facebook to users did not comply with the data protection regulations. It was also found that Facebook's privacy policy contained generic and unclear expressions, and obliged users to access a multitude of different links to learn about it.

The social network made very imprecise reference to the use it gave to the data it collected, so that a Facebook user with medium-level technological knowledge was unaware of the data being collected, of its storage and subsequent treatment, or why they were going to be used.

In relation to the conservation of data, when a user of the social network has deleted their account and requests deletion of the information, Facebook captures and processes that information for more than 17 months, such that the data is not deleted in its entirety, even when they have ceased to be useful for the purpose for which they were collected, nor when the user explicitly requests their removal.

Consequently, the Agency fined Facebook 1,200,000 euros.

• Facebook Messenger case

In May 2016, a Facebook user complained to the Agency that Facebook accounts have an integrated messaging service, called Chat, that allows a Facebook user to know when other users are online or when their last connection was, and that the user does not have the ability to prevent others from monitoring their activity.

The Agency initiated an inspection, which is ongoing as of the closing date of this book, in which it has been possible to verify the operation of this service. Specifically:

- *When a user's 'friend' has a session open on Facebook and the Chat service activated, in the user's account and associated with the name of the 'friend' a signal appears, a green indicator, which reveals that the 'friend' has a session open at that time. If the 'friend' is not connected, the green indicator does not appear, but a numerical value does, which reveals how many minutes the session was previously open for.*

- *On the main page of the privacy policy of Facebook there is no explicit and complete information on the disclosure of the connection information and its subsequent use or disclosure to third parties or a reference on how to manage the recording of connection times, among others.*

• Changes in the privacy policy and Whatsapp terms of service after the Facebook purchase

When Facebook acquired the WhatsApp messaging service in October 2016, the Spanish Data Protection Agency decided to open a formal action to determine the general data processing model, the extent of the data

transferred, the processing scope and the legal basis of the communication of data in which both WhatsApp and Facebook were involved.

Facebook imposed as mandatory the acceptance of new conditions to be able to make use of the messaging application that allowed it to use personal data for purposes that are not related to those originally established, without adequate information and without the possibility of opposition. By requiring that users give their consent in these terms and, taking into account the social establishment of the messaging application, consent given cannot be considered free and, therefore, valid.

During the actions of the Agency, both entities admitted that they share information about the users of the WhatsApp application. Specifically, WhatsApp confirmed that it 'currently' shares information with Facebook about all WhatsApp users, whether or not they are Facebook users, and that this information is transmitted in real time.

Specifically, both entities detailed that they share the identifier of the WhatsApp user account, including a common identifier included in the Facebook and WhatsApp applications; information about the device, the prefix and code of the country's mobile network, information about the platform, and the version of the application that allows acceptance of the application update and control options to be monitored; the 'last connection state' of the user, that is, information about the last time the user used the service and the date when the user signed up for their WhatsApp account.

On the other hand, it was found that the transfers or communications of personal data between WhatsApp and Facebook that do not relate to the purposes that determined their collection, are made without offering users any way to indicate their refusal, because WhatsApp only enable mechanisms to accept the transfer of information in order to "improve the experience with products and advertising on Facebook" and only in the case of existing users. Therefore, the 'consent' conceded with the acceptance of the Privacy Policy and Terms of Service cannot be considered free; and this means that the consent given cannot be considered valid.

It should be added that the information about the possible recipients of the data, about the purposes for which it is assigned, or the use that the assignees will make of them, is offered in an unclear way, with imprecise and inconclusive expressions that do not allow it to be deduced, without doubt or mistake, the purpose for which the data will be transferred.

Therefore, in September 2017 the Agency initiated a sanctioning procedure for WhatsApp, and Facebook, which resulted in the imposition of a 300,000 euros fine to each of the entities.

- **The Strategic Plan of the Spanish Agency for Data Protection**

In November 2015 the Agency adopted a Strategic Plan that will guide its actions in the 2015-2019 period. The Plan has five main sections: prevention; innovation; transparency and participation; closeness to those responsible and to the 'privacy professionals'; and agility and efficiency .

The Strategic Plan responds not only to a necessary updating after twenty-five years of operation, but

also, and above all, to the requirement to provide the Agency with a solid basis to face the additional effort of adapting to European Regulations, both for the Spanish legal system, and the Agency's own structure and procedures for action.

This was understood by the main recipients of the Strategic Plan who made almost four hundred contributions during the public consultation process that took place during its preparation.

The Strategic Plan initially contained 113 initiatives, which have been successively increased to the 145 that currently exist.

Thus, the Agency has rolled out an intensive information and dissemination plan on privacy culture aimed at citizens, with the objective being to raise awareness about their rights and how to enforce them.

To this end, the Agency has developed several guides on: privacy and security; citizen's rights; teaching centers; secure purchases on the Internet; data protection and crime prevention; property administration; patients and users of health systems; and video surveillance.

Microsites have also been created on the Agency's website for specific topics; in particular, on claims regarding telecommunications and unwanted advertising.

The Agency is committed to the protection of data being a subject that is regularly raised in the traditional media. Thus, the Agency has launched a specific campaign to raise awareness about the implications of the entering into force of the new EU Regulation; a campaign that was declared of 'public service' and, therefore, had free diffusion on A3media, Mediaset, TVE1 and Radio5.

Work in the digital field has also been very significant: the Agency's new website, which houses a Blog that contains key analyses on privacy; the improvement and updating of the 'frequently asked questions' section; the re-design of the citizen service channel; and, finally, the regular presence of the Agency on Twitter; on which, of all the social networks, the Agency intends to continue advancing.

An important part of the Agency's prevention policy is a consequence of the conclusions drawn from the so-called Sectorial Inspection Plans. Consequently in recent years, specific work has been carried out in public hospitals; cloud computing services in the education sector; remote contracting; financial entities, and the social healthcare sector.

Specifically, the Agency has sought to focus its prevention work in three sectors: technology, advertising and minors.

In September 2017, the Spanish Agency for Data Protection and the Association for the Self-Regulation of Commercial Communication (Autocontrol) signed a Protocol of action, for the implementation of a new system of voluntary mediation in which Movistar, Orange / Jazztel, Simyo, Yoigo / Masmóvil / Pepephone / Happy / Llamaya, Vodafone and Ono participate.

According to this procedure, citizens who have filed a claim regarding identity theft or the reception of unwanted advertising from these companies, and who have not obtained a satisfactory response, can resort to Autocontrol's mediation.

Once the claim has been received, Autocontrol will verify that it complies with the established requirements and, if so, will initiate a mediation process to try to help the parties reach an agreement and resolve the dispute.

This mediation system is perfectly compatible with, and independent of, the claims that citizens may continue to make to the Agency.

The Agency has also worked especially in the field of publicity with the aim of expanding the rights of citizens against unwanted advertising. The advertising exclusion service known as the Robinson List, managed and rendered by ADIGITAL, has been strengthened and already has more than 600,000 registered citizens.

In particular, citizens now have more possibilities to halt unwanted advertising, through a greater selection of their preferences. So a citizen can now decide that they do not want advertising by e-mail, but via their mobile phone, or that they want to be sent advertising about travel or electronics, for example, but not about other matters.

The protection of the rights and freedoms of minors in relation to the processing of their personal data constitutes one of the constant preoccupations of the Agency; a concern that has increased with the rise of Internet services, particularly social networks.

The Agency developed in 2007 the "Plan for the Protection of the personal data of minors on the Internet" and, in 2008, the "Safe surfing" guide on the rights of children and the duties of parents.

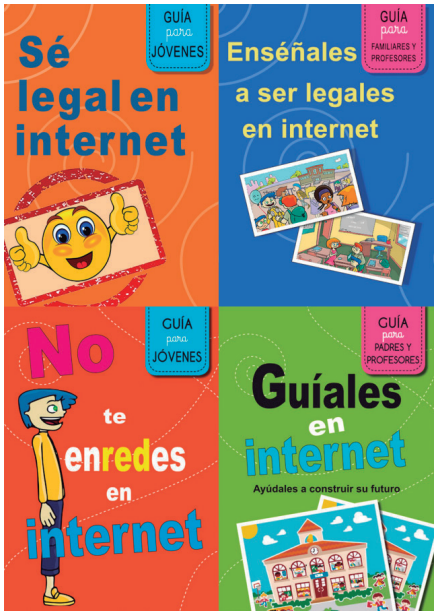
The Agency endorsed society's concern regarding the risks of Internet use reflected in the CIS barometer of September 2009, in which more than 80% of citizens stated that their concern is even greater with respect to minors.

Since then the Agency has directed its actions in this field to the training, awareness and sensitization of minors, parents and an educational system that has more than 8 million students.

Various data protection authorities, the Basque, Catalan, and Community of Madrid, plus a number of Spanish agencies, have collaborated in the development of a training resource on data protection and privacy in relation to minors. In addition, the Agency urged Facebook to establish the admission age for the social network in Spain at 14 years old, when in its North American terms and conditions of use it is established at 13.

In 2013, the portal "You decide on the Internet" (www.tudecidesenInternet.es) was created, with contents aimed at educating and sensitizing youth about the importance of privacy and the value of personal data for their safeguard.

In 2015, the portal was revised not only from the point of view of its image, but also incorporating new materials and resources (new guides, videos, help channels, children's contests, workshops ...), and it had received over 335,000 visits at the time this book was written.



In addition, work has been undertaken in this field of online child protection with various public agencies (the Ministries of Education, Justice, Health and Social Services, and Interior; the Child Prosecutor's Office; Red.es; INCIBE; INJUVE; and the CNMC) and also private entities (including the ANAR Foundation, the Observatory of Audiovisual Content, Pantallas Amigas, and Telefónica, Orange, Google, RTVE, Mediaset and Atresmedia).

To promote the dissemination and knowledge of data protection and the importance it has for the education and development of minors - in addition to seminars, informative and awareness raising sessions and workshops - outreach campaigns through television have been carried out. The collaboration of TVE's Clan channel and the Mediaset group has been obtained for the diffusion of 'key tips' to enjoy safe navigation over the Internet.

In 2015, the Spanish Data Protection Agency established a specific channel to inform and advise families, teachers, monitors and the minors themselves about privacy issues.

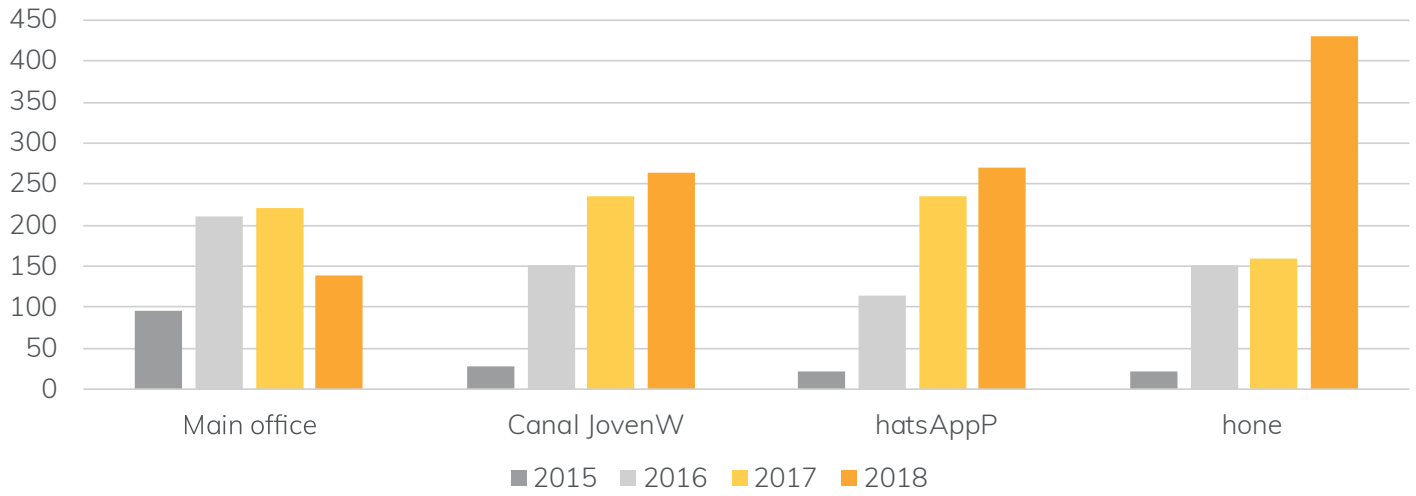
This channel has an email address (canaljoven@agpd.es), a personal attention telephone number (901 233 144) and a WhatsApp system (616 172 204).

The most frequent queries relate to images of minors. Specifically, they deal with: disputes between divorced parents over the publication of images of their children on social networks; use of images of children under 14 on social networks, mainly on Facebook and Instagram, without the consent of their parents or legal guardians; publication on the Internet of images of minors that have been obtained from WhatsApp groups, or from social network accounts; the processing of minors' data by educational centers and AMPAS (basically the publication of images both on their own websites and on social networks or the use of educational platforms by educational centers).

The deficit in the levels of training and awareness of minors in the responsible use of personal information on the Internet is the reason why the Agency, like other institutions, has insisted on the inclusion of training on personal data protection, privacy and the Internet in study plans and in the academic curricula.

Graph 1
Evolution of minor queries

Source
Prepared by the author

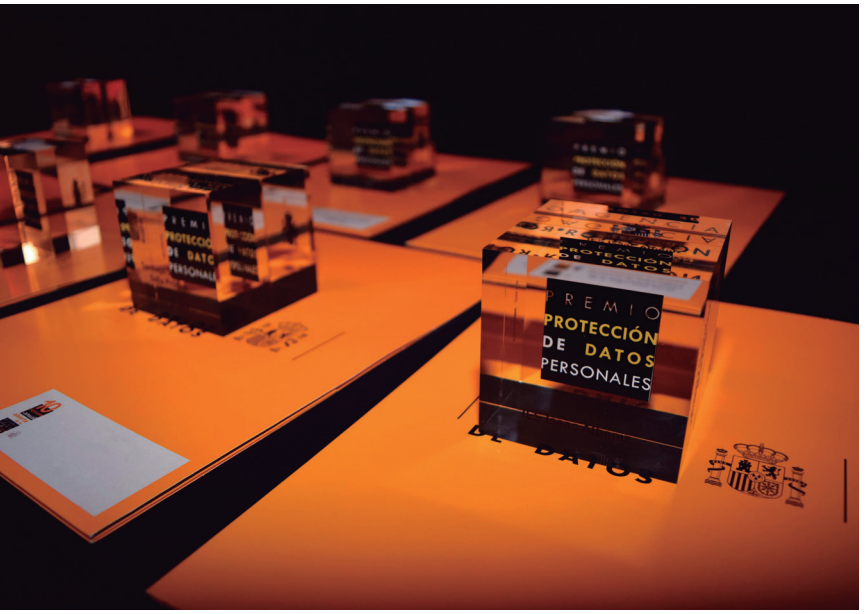


This is an objective that has finally been established in the Organic Law of Protection of Personal Data and Guarantees of Digital Rights, whose article 83.1 confirms that the educational system will guarantee the full insertion of students into the digital society. This includes learning to use digital media in a way that is safe and respectful of human dignity, respects constitutional values, fundamental rights and, particularly, guarantees personal and family privacy and the protection of personal data. Likewise, it ensures that teachers receive digital skills and the necessary training for their teaching.

To this constant task of raising awareness about the dangers that threaten our privacy, the Data Protection Agency offers an annual call for Awards on various themes: communication, good educational practice on the Internet, good practice in adapting to EU Regulations, and a research prize in the protection of personal data «Emilio Aced».

Also, the Agency has offered to accompany people, entities and administrations on the road to compliance with data protection regulations. To make this path easy to travel, tools and guides have been developed that aim to facilitate compliance:

- «FACILITA_RGPD», which is a free tool for the self-assessment of risks for SMEs with very low risk processing; and infographics with guidelines on



the steps to follow to adapt to the EU Regulation by those companies that cannot do so with the FACILITA_RGPD tool.

- "Guide to the General Data Protection Regulation for data controllers", with the information and explanations necessary to prepare and adopt the corresponding measures to comply with the provisions of the EU Regulation.

- "Guidelines for the development of contracts between managers and processing managers", to identify the key points to bear in mind when establishing the relationship between the data controller and the processor, as well as the issues that directly affect the management of the relationship between both.

- "Guide for the fulfillment of the duty to inform", which is a guide that offers best practice on informing interested parties, by virtue of the principle of transparency, about the circumstances and conditions of the data processing to be carried out, as well as their corresponding rights.

- "Guidance and guarantees in procedures for the anonymization of personal data", which seeks to guarantee the protection of personal data in the development of studies and research of social, scientific and economic interest, and to promote its development and dissemination.

- "A practical guide to risk analysis", a roadmap focused on the management of potential risks associated with the processing of data from its design stage, through to the establishment of security and control measures to guarantee the rights and freedoms of individuals.

- "A practical guide for impact evaluations in the protection of data subject to the EU Regulation"

- «A list of regulatory compliance to facilitate adaptation to the EU Regulation»

- "Security breaches guide", which is addressed to those responsible for processing personal data, with the aim of facilitating the interpretation of the EU Regulation as regards the obligation to notify the competent authority and, where appropriate, those affected, so that the notification to the authority is made through the appropriate channel. It contains useful and precise information for statistical and monitoring purposes, and is adapted to the new requirements of the Regulation.

- "Adaptation of the Risk Assessment Tool for Public Administrations (PILAR) to the requirements of the Regulation."

- Documents «The impact of the RGPD on the activity of Public Administrations», and «The Representative for Data Protection in Public Administrations».

- "Guide on data processing in the field of Local Administrations."

Different initiatives have also been developed with the most representative business organizations in the field of SMEs and for the self-employed (CEPYME, ATA, UPTA ...). In particular, the Protocol signed between the AEPD, CEOE and CEPYME should be highlighted, as it seeks to promote the dissemination of the RGPD and those tools, publications, and guides published by the Agency that can help SMEs to fulfil their obligations. This collaboration has resulted in an intense program of public events developed by the AEPD in all the Autonomous Communities for the dissemination among CEPYME's partners of the aforementioned resources, especially the FACILITA_RGPD tool.

The adaptation to the new requirements of the EU Regulation is especially expensive for self-employed workers and SMEs, which constitute Spain's principal business fabric. For this reason, the Agency, beyond the FACILITA tool, has been offering numerous training and dissemination days around the guides and tools developed by the Agency with the most representative business organizations (CEOE, CEPYME, ATA, UPTA, ...).

On the other hand, in the first months that the EU Regulation came into force, special attention has been paid to the post of the Representative for Data Protection, a mandatory figure for public administrations and for a good number of other companies and entities.

Thus, with the aim of guaranteeing a quality reference in the market, the Agency launched in July 2017 in collaboration with the National Accreditation Entity (ENAC), a certification scheme for Data Protection Representatives, thereby becoming the first European authority that has developed a frame of reference for this figure.

In our legal system this certification is not the only way to be a Representative, but the Agency believes it is necessary to provide a reference on the subject matter and elements required to certify the qualification and professional capacity of a Data Protection Representative.

A significant effort has also been made to train public administrations' Data Protection Representatives, in collaboration with the INAP, the training institutes for public employees of all the Autonomous Communities, the Spanish Federation of Municipalities and Provinces, and the Official School of Secretaries, Auditors and Treasurers of the Local Administration.

Additionally, a training plan has been developed with the INAP for officials from the three public administrations, of which an online course is part, which will have 9 editions in 2018. A specific program has also been added to this –online and face to face- that includes specialized training for Data Protection Representatives in the three administrations.

Another line of work is represented by the different professional associations. The Agency has signed a

Protocol with the Professional Union, an entity that brings together the General and Superior Councils and national professional associations, with more than one and a half million professionals, to disseminate among their organizations all the tools, guides and materials developed by the Agency to help fulfill the obligations arising from the EU Regulation.

Finally, the Agency launched in 2017 a specific channel ("INFORMA RGPD") to answer inquiries from data managers, managers and delegates; they have already received more than three thousand queries.

VI. The Agency of the future

The General Regulation of Data Protection. Main novelties. New Rights

On May 25, 2016, the new General Regulation for Data Protection was approved, a standard with which the European Union intends to respond to the challenges posed by the widespread use of information and communication technologies.

The Regulation can be considered an evolution of Directive 95/46/EC, which it replaces, and which collects together and reinforces the basic principles of data protection and the rights of interested parties.

Additionally, from the point of view of protection procedures and mechanisms, the Regulation contains important novelties.

The first is that the Regulation is a norm that is applied directly in the Member States, without the need for transposition rules. States may, however, develop rules in cases where the Regulation enables them to do so.

This has happened in Spain with the Organic Law on the Protection of Personal Data, whose parliamentary procedure concluded in November 2018.

From the point of view of citizens, this norm, which standardizes the European data protection law, guarantees a similar level of protection throughout the Union. It is also the only case of a fundamental right regulated by an EU Regulation.

Another of the key novelties is that its precepts are applicable to processing that affect citizens residing in the European Union, regardless of whether the person responsible or in charge of the data processing is established or not in the Union. In cases where they are not established in the Union, the Regulation will be applicable provided that the processing is related to the offer of goods and services to citizens in the Union or with activities to control their behavior when they are in the Union.

Also, the control that citizens have over their personal data has been strengthened. Thus, a better regulation of consent is established, which must be provided unequivocally by means of clear statements or affirmative actions, or by the provision of information - that is now a right - linked to the principle of transparency. Additionally new rights are recognized such as the limits on processing and portability.

The Regulation also mentions the 'right to be forgotten'. However, it was decided not to try and establish it as an autonomous right, following the line of the European Union's Court of Justice in the judgment on the Google Spain case, where it was pointed out that this right is an adaptation to the activity of the search engines for 'classic rights' such as deletion and opposition.

The Regulation also includes a novelty in the case of the right of opposition, stating that it will be the responsibility of the person in charge to demonstrate that their interests prevail over the rights, freedoms and interests of the interested party in relation to their specific circumstances.

Regarding the obligations of those responsible and in charge of the processing, the Regulation is committed to a new model of compliance, which pivots on the proactive conduct of managers from the perspective of the risks that data processing can pose for the rights and the freedoms of the interested parties.

This new approach represents a substantial change in the way in which compliance with data protection regulations is understood. In the system in force to date, the focus of regulators and regulated entities has been placed on results. Data processors have sought to comply with the legislation to avoid possible offences. The supervisory role of the regulators has begun as a general rule when an offence has occurred.

The new Regulation, on the other hand, places the obligation on those in charge, and also on the supervisors, to be proactive, and introduce preventive measures, which must be adopted to ensure that those responsible are in a position to comply with its provisions.

This preventive approach unites with the risk assessment approach to determine the actions that organizations should take. The confluence of both supposes that the organizations must document and be able to demonstrate that they have analyzed the risks of the data processing they are carrying out, and have applied the appropriate measures to eliminate them or bring them in line with 'acceptable levels'.

These measures include: the protection of data from the design stage and by default; the maintenance of a processing register; the need to apply security measures that are appropriate to the risk derived from the processing; the undertaking of impact evaluations regarding the protection of data processing that a priori seem to entail a high risk for the rights and freedoms of the interested parties; and the obligatory appointment of a data protection representative in all public and

private organizations that carry out specific processing activities.

Another of the most significant developments of the EU Regulation, which is clearly different from the Directive, is that relating to the new supervision model, which goes from concentrating on verifying whether an infringement has occurred, or correctly applying the assessed measures that the legislation foresees, to have to assess, together with the responsible person and those in charge, the processes of risk analysis and the decisions on the application of the measures that minimize them.

It is also a more flexible system, insofar as it opens up greater possibilities for the supervisory authorities to a broader range of corrective measures (cautions, warnings, etc.) whose application must be assessed according to the specific case, before considering the imposition of economic sanctions.

All this does not exclude the fact that the Regulation provides for very severe economic sanctions, which can reach up to 20 million euros or an amount equivalent to 4% of the total annual global business volume of the company in the previous financial year. Sanctions that may have a dissuasive effect and whose application will depend on the level of diligence adopted to comply with the Regulation and various other circumstances related to their impact on the rights and freedoms of citizens.

It is, at the same time, a model of supervision that could be described as cooperative, since the authorities will be obliged to cooperate not only in the establishment of the criteria for its interpretation, but also in its application to a specific case when several authorities may be affected as a consequence of a particular processing issue. This obligation of cooperation is regulated in the complex procedures of cooperation and coherence. In this procedure, the European Committee for Data Protection plays an especially important role and, ultimately, the European Union's Court of Justice.

This legal framework has yet to be completed by two other important European standards pending transposition or approval: Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of citizens as regards the processing of personal data by the competent authorities for purposes of prevention, investigation, detection or prosecution of criminal offenses or execution of criminal penalties, and the free movement of such data, pending transposition; and the E-privacy Regulation, currently in process, which aims to update the still current Directive 2002/58/EC to apply the principles and requirement of the General Data Protection Regulation to the field of electronic communications.

The combined effect of all these measures must ultimately have an effect on the data protection culture of organizations and on the better protection of citizens' rights.

The Organic Law on Data Protection

The recently approved Organic Law for the Protection of Personal Data and the Guarantee of Digital Rights aims to fulfill five basic objectives: to adapt Spanish law to the model established by the Regulation; to introduce innovations and improvements by developing some of the matters contained in it; to reinforce the rights of citizens; to clarify concepts; and to provide legal security for those who process data.

It is important to firstly highlight the aspects relating to citizens' rights.

The legal text facilitates, in general, the exercise of rights by requiring, in particular, that the means for their performance be easily accessible by those affected.

It recognizes, for example, the right of access to the data and, where appropriate, rectification or deletion by people linked to the deceased and their heirs, for family or de facto reasons, by addressing an omission in the previous Law that generated conflict, especially on the Internet, which is beyond the protective scope of the Agency. This relates to rights that may be exercised except in the case that the deceased had expressly prohibited it.

The Law has introduced a significant change, which even affects the title holder of the standard, relating to what it calls digital rights, regulated in heading X. Under that heading, two distinct blocks of rights can be distinguished, depending on whether the guardianship is, or is not, the responsibility of the Agency.

Of these, the powers of the Spanish Agency for Data Protection are limited to those regulated in articles 89 to 94 of the Organic Law.

It should also be noted, regarding these Regulations, that the Law updates guarantees to the right to privacy relating to the use of video surveillance devices and sound recording in the workplace, as well as the right to privacy - both for ordinary workers and public employees - in the use of digital devices at their disposal, complementing this right with the right to privacy rule when geolocation systems are employed in the workplace. These are now considered to be workplace rights that can be reinforced through collective agreements.

In the sphere of the Internet, social network services and other similar tools of the information society, the regulation has systematized the criteria of the verdict of the European Union's Court of Justice of May 13, 2014 in the case of the Agency against Google regarding the right to be forgotten in internet searches, in order to facilitate its application and increase legal security.

In addition, the organic law regulates the right to be forgotten in social network services and equivalent information society services, limiting itself to allow the deletion of personal data when they have been provided by the interested party; deletion that in many cases may be carried out without the need for a request to the person responsible. Additionally, this data may be deleted when they have been provided by third parties; applying the same principles established in the aforementioned judgment.

In any case, any deletion is exempt from the Regulation when it has been facilitated by individuals exercising their personal or domestic duties.

The purpose of this provision is also to facilitate operators' understanding, and guarantee legal certainty.

It is worth making special mention of the regulation regarding minors in which the following aspects stand out, even though in some cases the Agency does not have responsibility:

The age at which minors can 'autonomously consent' is fixed at 14 years.

The right to have deleted, by a simple request, the data provided to social networks or other similar services of the information society by the minor themselves, or by third parties representing them, is expressly regulated.

The duties of the education system are reinforced, very clearly, to ensure the full insertion of students in the digital society and to help them learn about digital media, safely and appropriately, in a way that ensures their privacy, including specific training in the academic curricula. It also requires that teachers receive adequate training in this area.

To this end, the Government must submit within one year from the entry into force of the Law, a bill specifically aimed at guaranteeing these rights, and educational administrations will have the same deadline for the inclusion of this training in the curriculum.

Finally, measures for the protection of data on the Internet are contemplated, in order to ensure that parents or legal representatives guide minors to use digital devices in a balanced and responsible way. Additionally, the Regulation provides for the intervention of the Public Prosecutor when the use or dissemination of images, or the personal data, of minors in social networks or services of the information society involves illegitimate interference with their rights.

Regarding new aspects and improvements, it is worth mentioning the regulation of credit information systems, known as default payment files, in which the maximum period of inclusion of debts is reduced from 6 to 5 years and a minimum amount of 50 euros is required to incorporate debts into those files. In this way, any adverse effects are limited, which in the past have generated discriminatory situations, especially regarding access to financial or telecommunications services, in cases of illegal inclusion or inclusion for very small amounts, which may only be cents.

The legal text also updates regulation of the Robinson List, which is an advertising exclusion file in which those who wish to avoid unwanted advertising through postal, telephone and electronic channels can register voluntarily.

The law of unfair competition has been modified to control illegitimate organizations that seek to supplant the identity of the Agency or its functions; describing these as 'aggressive practices'. It also seeks to regulate these organizations' 'advice', sometimes referred to as "adaptation to the Regulation at zero cost" in order to limit advice to companies of very small quality.

Likewise, the means are provided so that companies can confirm the legality of a particular procedure before possible cases of criminal responsibility, by regulating their internal complaint systems; which may now even include anonymous complaints.

One of the main novelties is the regulation of data processing in the field of health research, which now offers more flexibility over the ways in which health information can be used, accessed and reused, with adequate guarantees. In this way, it responds to concerns that this new regulation had raised in the scientific field.

In order to promote legal certainty, the new regulation requires a standard with the formal status of a law in cases where the legitimacy of the processing is based on public interest or the exercise of public powers; it facilitates the processing of contact data by 'legal persons', individual businessmen and liberal

professionals; as well as data processing in corporate operations, based on a presumption of 'legitimate interest' for those responsible for the processing.

Additionally, it updates the regulation of processing for video surveillance purposes.

And, with respect to the new and important figure of the Representative for Data Protection, it details, in an exemplary manner, the cases in which their appointment is mandatory. In particular, it clarifies that they will not be responsible for breaches in data processing; as this responsibility will fall on the entity which provides the services.

On the other hand, the organic law clarifies certain specific concepts such as the presumption of accuracy in the processing of data in certain cases and, above all, states that consent must be expressed through a clear affirmative statement, excluding 'tacit consent', and that this will not be dependent on the execution of a contract by the affected party 'consenting' to the processing of data unrelated to it, since it is understood that this would not be free consent.

Finally, it is worth highlighting some key aspects of the regulation relating to Public Administrations.

As a measure of transparency, the regulation requires that administrations make public their processing activities, which replaces the previous requirement that obliged them to 'advertise' the creation of files. In this way citizens can know who is processing their data, and with what purpose; as well as the legal basis that legitimizes it. It also updates the relationship between the right to data protection and that of transparency and access to public information.

In the case of advertisments and publications of administrative acts through the official bulletins, it limits identification data, such as the DNI number, and other official documents that may be published, and prohibits the publication of names and surnames together with the full number of the aforementioned documents. In this way it reduces risk for victims of gender violence and the possibilities of identity theft.

Regarding the right of interested parties not to provide documents that are in the possession of the administration - unless there is express opposition from the interested party or the law requires their express consent - the regulation legitimizes data processing in compliance with legal obligations, without the need for interested parties to give express or implied consent, which is expressly prohibited by the European Regulation.

The legal text regulates security measures in the public sector, through the National Security Scheme, which has been adapted to the European Regulation and enables the notification of security incidents to computer emergency response teams (CERT) or computer security incidents (CSIRT).

Likewise, the Law reinforces the powers of Public Administrations by allowing the verification of personal data held by them, to confirm their accuracy when requests are made by interested parties, by any means.

In terms of infractions and sanctions by Public Administrations, the Law has chosen not to impose economic sanctions in case of non-compliance, limiting itself to the issuing of warnings so that corrective measures can be taken. However, the Regulation provides for the possibility of disciplinary action against

public employees that have committed infractions or a public reprimand to directors whose conduct may have given rise to the offence, in spite of having received information about the possible regulatory breach. These verdicts will in any case be published in the official bulletins.

In the institutional sphere, the Law considers the Spanish Data Protection Agency as the supervisory authority, which will modify its composition when the appointments of a President and an Assistant redefine its powers and functions.

The appointment procedure, in which the Government preselected the candidates, has been modified and sent to the Congress of Deputies with a report providing the reasons.
Congress must ratify these candidates by means of qualified majorities, and those selected will then subsequently be appointed by the Government.

The Agency's members' mandates have been modified by extending them to five years, renewable once only; and the reasons for their cessation also now have to provided.

The Law expands composition of the Consultative Council to allow for the incorporation of representatives from new sectors related to the protection of personal data.

Likewise, cooperation procedures have now been established with the Autonomous Data Protection Authorities in the internal sphere and in the European Committee for Data Protection. The law includes out-of-court conflict resolution systems and 'specialties' in the administrative procedures contemplated in Royal Decree Law 5/2018, of July 27, including those that allow for cooperation and coherence with the European Committee for Data Protection.

And finally, the Law establishes a statute of limitations for infractions and sanctions, relating it to an exemplary description of those foreseen in the European Data Protection Regulation.

The Agency of the future

The Agency of the next few years must be in a position to face with decisiveness and effectiveness the great challenges, current and future, that privacy faces.

The fulfillment of this objective will mean aligning its activity and operating mode to the fundamental assumptions established in the General Data Protection Regulation, prioritizing diligence and proactivity and applying a new supervision model with preventive, corrective and - when appropriate – dissuasive action; when faced with breaches by those in charge.

This is without forgetting the data protection authorities' responsibility for the investigative abilities common to all of them, in order to effectively carry out their functions and, where appropriate, impose dissuasive economic sanctions to ensure that the law is respected.

The Spanish Agency is making an enormous effort to adapt the entire organization to respond to these challenges.

Along with the requirements that the Agency must specifically fulfill as a mandatory subject (the creation of processing activity records, prior risk analysis, impact evaluation, adaptation of forms for security breaches, informative clauses, manager contracts, new models of codes of conduct ...), a wide group of initiatives aimed at internal training, the redesign of management procedures and, ultimately, the adaption of the organization to the new regulatory framework have been foreseen in its Strategic Plan.

This will undoubtedly be a major challenge for the Agency, but at the same time a magnificent opportunity to carry out a necessary 'updating' after more than twenty-five years of operation in a period that has undergone such profound changes.


aepd
agencia
española
protección
datos

agencia española protección datos

25th Anniversary

1994	1995	1996	1997	1998
1999	2000	2001	2002	2003
2004	2005	2006	2007	2008
2009	2010	2011	2012	2013
2014	2015	2016	2017	**2018**

www.aepd.es

@AEPD_es