La Soberanía de los Datos

INFORME XXVI

FUNDACIÓN DISENSO

FUNDACIÓN DISENSO

Pº. del General Martinez Campos 21, 1ºA.
28010, Madrid
info@fundaciondisenso.org
prensa@fundaciondisenso.org

Índice

RESUMEN

La soberanía de los datos es un concepto que ha ido ganando importancia tanto en el ámbito personal como en el nacional, especialmente en el contexto de la globalización digital y las implicaciones de los datos personales sobre la privacidad y seguridad. El presente informe se interesa por esta cuestión en una doble dimensión: la de soberanía personal, desde la que se explora el dominio de los españoles como usuarios del mercado digital; y la de soberanía nacional. Desde la primera, se destaca cómo los ciudadanos mantienen relaciones desequilibradas con las transnacionales tecnológicas cuando se intercambia información personal por servicios en el mercado digital, fruto de un desconocimiento del valor de la primera. Por otro lado, desde la perspectiva de la soberanía nacional, se resalta cómo la falta de regulación en la circulación de datos compromete directamente a la seguridad del Estado, al exportar información sensible que pone en riesgo elementos estratégicos clave en el ámbito de la seguridad y la defensa, y en otros aspectos que afectan directamente la soberanía de España.

Este informe comienza con una aproximación teórica a los conceptos anteriores y, a continuación, los analiza desde el punto de vista económico y regulatorio, con algunos apuntes del contexto europeo. Por último, aporta una serie de recomendaciones que pueden conducir a una mayor protección de la privacidad de los españoles y del dominio que ostentan sobre sus datos personales, así como también contribuir a una mejora en materia de seguridad nacional, de forma que se reduzca la vulnerabilidad actual de España en este aspecto.

1. INTRODUCCIÓN

El desarrollo tecnológico derivado de la Cuarta Revolución Industrial en la que nos hallamos inmersos es fundamentalmente de índole digital, lo que hace que la información, su activo más importante, sea especialmente líquido y maleable. A esto contribuye también el carácter transnacional de las principales corporaciones tecnológicas, que si bien disponen de un domicilio societario principal —a menudo, el fundacional[1]—, operan como empresas verdaderamente globales a través de un complejo entramado societario construido para la elusión fiscal y la maximización de beneficios.

Este contexto ha supuesto una creciente preocupación por la denominada «soberanía de los datos», «soberanía tecnológica» o «soberanía digital». Se trata de un término que surgió a principios de los 2000 pero que ha ido cobrando cada vez más importancia. En su acepción más canónica, este es un concepto que se refiere a la idea de que los datos están sujetos a las leyes y estructuras de gobernanza de la nación donde se generan o almacenan. Se trata así de un término eminentemente legal, que define las normas que rigen cómo se manejan los datos, y vinculado estrechamente con la protección de datos.

Sin embargo, de esta primera acepción se deriva otra de carácter personal y que afecta tanto a empresas o personas jurídicas como a particulares. Y es que la «soberanía de los datos» también se puede referir a la capacidad de los individuos y empresas para decidir cómo y para qué propósitos se pueden utilizar sus datos, así como a qué precio, en caso de que decidan compartirlos. En definitiva, indica quién tiene la autoridad y control sobre los activos tecnológicos de una persona u organización. Pues bien, el presente informe se interesa también por la importancia del empoderamiento de las personas con respecto a su privacidad, tratando de averiguar en qué medida somos dueños de nuestro destino digital.

Las siguientes páginas examinan así la cuestión de la soberanía de los datos desde dos perspectivas fundamentales: la soberanía personal y la soberanía nacional. Ambos conceptos, en diferentes niveles de análisis, reflejan la capacidad de tomar el control de las propias decisiones sin interferencias de terceros, algo en gran medida obstaculizado por la peligrosa combinación de

1 Si bien también es frecuente que, con el tiempo, busquen nuevas sedes en jurisdicciones relativamente poco opacas en términos de transparencia y que presentan unas condiciones fiscales muy deseables para la compañía, llegando en ocasiones a tratarse de verdaderos paraísos fiscales.

un mundo cada vez más y mejor conectado en el que la regulación del movimiento y empleo de los datos es siempre compleja, junto con una era de la exposición voluntaria de nuestra privacidad en la esfera digital por parte de los consumidores y usuarios. Complejidad que se ve acentuada, a su vez, por la convergencia entre dos fuerzas históricamente antagónicas, pero hoy aliadas. A saber, el Estado y el mercado.

En primer lugar, dentro de la perspectiva de la soberanía personal, se reflexiona acerca de cómo las grandes empresas se aprovechan de la cesión de datos personales derivada de la pérdida del sentido de la intimidad característico de la sociedad exhibicionista actual; en un proceso de mercantilización en el que la concentración de mercado y una regulación laxa dejan a las personas o usuarios a la intemperie. Como resultado, se producen relaciones jurídicas sin contraprestación dineraria en las que el usuario es un contratante débil al intercambiar su privacidad por un producto en el mercado digital, sin saber realmente cuánto vale la primera.

Por su parte, dentro de la soberanía nacional, se aborda cómo el empleo de los datos en ausencia de un marco regulatorio apropiado compromete directamente a la seguridad de nuestros conciudadanos y de la nación. La triangulación arbitraria y la exportación de nuestra información por parte de trasnacionales se convierte en información sensible desde un punto de vista estratégico y de seguridad, además de ser potencialmente utilizable en contextos de alta volatilidad como en los períodos electorales.

El informe incluye también una serie de propuestas con el fin de contribuir a la salvaguarda de la soberanía en cada una de estas dos acepciones; propuestas que abordan elementos de voluntad política y de desarrollo legislativo o regulatorio, tanto en un contexto español como europeo. A este apartado propositivo le sigue otro a modo de apunte final que versa sobre uno de los grandes temas de nuestro tiempo, y que está íntimamente ligado al ámbito digital: la inteligencia artificial. Por último, este informe cierra con una conclusión a modo de recapitulación, seguido de un apartado bibliográfico.

2. LA PROPIEDAD DE LOS DATOS Y LA SOBERANÍA: DOS PERSPECTIVAS

2.1 La soberanía personal

2.1.1 Sobre el concepto de soberanía personal

Se llama soberanía personal a la capacidad de cada persona de autodeterminarse y ejercer control sobre su vida en línea con sus valores, tradiciones y creencias. Es decir, al derecho de tomar decisiones personales, siempre y cuando estas no interfieran con los derechos y las libertades de nuestros conciudadanos y no comprometan la seguridad de la nación. Se trata de un principio fundamental de cualquier sociedad libre dado que afecta directamente la libertad de opinión, de expresión, de credo... Un concepto de un profundo significado a nivel filosófico[2] y de numerosas ramificaciones en su aplicación práctica. Sin embargo, a los efectos de este informe, la soberanía personal se entiende como capacidad de decisión, de control, sobre nuestra huella digital. Y es que en los datos que circulan por la red y que son almacenados en los servidores de empresas y estados se encuentran cristalizados los gustos y preferencias —de mercado y vitales— de las personas.

En este contexto, la relación que mantiene la soberanía personal con la privacidad y la intimidad es intrínseca y bidireccional, pues las segundas son condición para que se dé la primera, y viceversa. Bajo un prisma de soberanía personal «perfecta», cada usuario debería poder mantener los datos que reflejan su esfera personal alejados de la mirada pública o del escrutinio no deseado. Sólo así se podría salvaguardar una autonomía plena. A su vez, la soberanía personal incluye el derecho de admisión o exclusión; es decir, la capacidad de controlar quién tiene acceso a estos datos y cómo se utilizan. En otras palabras, la privacidad es poder. Es autogobierno. Es soberanía.

2.1.2 La soberanía personal en materia de datos

La acepción de soberanía de datos en clave digital ha sido un tema de preocupación para muchos responsables políticos y expertos en política pública. El motivo principal es que la persona —en clave digital, el «usuario»—, se halla

2 La agencia, o autonomía, es uno de los pilares fundamentales de la filosofía política liberal, cristalizada en el «unencumbered self» Rawlsiano como individuos carentes de ataduras, lazos o condicionantes de partida; hechos a sí mismos.

en una encrucijada en la que su privacidad se encuentra enfrentada con el interés económico del mercado tecnológico y el de vigilancia de los Estados, bien por motivos legítimos de seguridad, bien por motivaciones espurias, extralimitándose en sus competencias y atribuciones.

Corresponde así examinar los diferentes caminos que convergen en esta encrucijada. Todos ellos revisten complejidad, pues en ella se produce una colisión de derechos, libertades e intereses. Del individuo, de la empresa, y del estado.

En la sociedad actual, la corporalidad ha perdido importancia y el formato del poder ha cambiado. La información siempre ha sido una fuente de poder, pero más aún en un mundo donde la capacidad para analizar información, para almacenarla, transmitirla y diseñar estrategias y acciones con base en ella, es cada vez mayor. En el sector privado, este poder equivale a más facturación y, en el sector público, a un mayor control. Así, ante tan enormes posibilidades, Estado y mercado buscan con ahínco hacerse con la mayor cantidad posible de datos.

En sistemas políticos autoritarios o totalitarios, la injerencia en la privacidad es siempre más evidente, pues se basa en el principio de coerción mediante la amenaza de un castigo. En cambio, en Occidente, hogar de sociedades libres y gobiernos elegidos democráticamente, estas injerencias siguen el camino de la gratificación o el cuidado. En el caso del mercado, la recompensa es la satisfacción que trae consigo el uso de una tecnología; satisfacción que, a su vez, puede traducirse o no en una instrumentalización o empleo de esa tecnología con usos profesionales. En el caso del Estado, esa satisfacción se da cuando se resuelve la disyuntiva clásica entre privacidad y seguridad en favor de la segunda. En ambas ocasiones, sin embargo, es el usuario el que entrega libre y voluntariamente esos datos, en un fenómeno que es ya característico de la actual sociedad de la transparencia o sociedad del exhibicionismo. A todo, lo público y lo privado, se le da visibilidad compartiéndolo en línea.

La persona pierde así poder; se desprende su soberanía, y queda más vulnerable a los abusos de poder o a la manipulación —aunque no siempre sea consciente de ello— del Estado o el mercado.

El papel del mercado en la soberanía personal

En nuestra sociedad, la comodidad y la preferencia por el empleo de herramientas digitales de compra de productos o servicios online trae consigo la

consecuente cesión de datos personales y preferencias de mercado. Asimismo, como se señalaba anteriormente, vivimos en una cultura de la imagen y la exhibición de aspectos personales de la vida de las personas. En ambos casos hay algunas críticas que pueden y deben dirigirse a los consumidores y usuarios. Una crítica moral y también de prudencia y sentido común, en especial en lo que se refiere al uso de las redes sociales o del libre acceso a internet de los menores de edad, así como en la búsqueda denodada de la gratificación instantánea. No obstante, estas cuestiones exceden de los umbrales del presente informe, con una salvedad de corte funcional, como es el fenómeno de la información imperfecta.

En teoría económica, la información imperfecta se da cuando los agentes económicos carecen de información sobre un bien o cualquier otra información relevante para la transacción. El término información imperfecta significa que los compradores o vendedores no tienen toda la información necesaria para tomar una decisión informada. Esto es algo relativamente habitual en las transacciones económicas, pues el vendedor y comprador rara vez tienen la certeza sobre las cualidades de lo que están comprando o vendiendo.

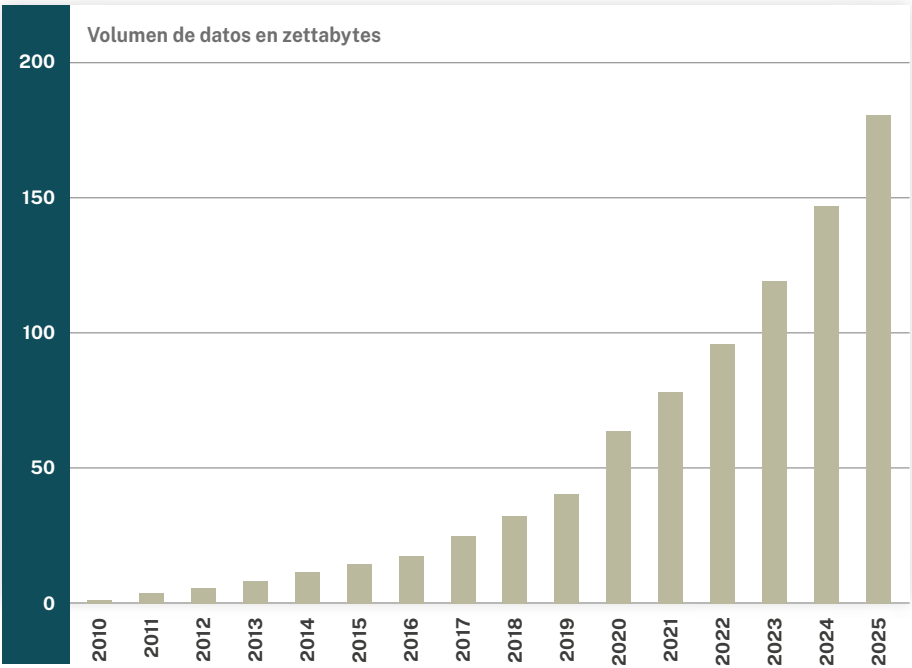
Sin embargo, en el caso del mercado de los datos, hay dos elementos que hacen que el problema de la información imperfecta revista una especial complejidad. En primer lugar, destaca el propio activo que se compra y se vende en uno de los extremos de la contraprestación, que es la información personal —pues no siempre hay un pago implícito en la relación, como es el caso de las redes sociales, de carácter «gratuito»—. En segundo lugar, hay una notable desproporción entre la información de la que disponen las empresas acerca de la transacción y la que obra en poder de los consumidores y usuarios. Así, la información es especialmente imperfecta en las transacciones digitales por parte de estos últimos, lo que trae consigo una situación de información asimétrica, en la que una parte de la transacción tiene más información que la otra.

Los usuarios son por lo general conscientes de su propia función de utilidad; o la satisfacción que le proporciona el acceso a una herramienta de software que emplea en su desempeño profesional, la lectura de un periódico digital o el uso de una red social. Sin embargo, por lo general, los usuarios ignoran la función de utilidad de las empresas tecnológicas o que prestan servicios digitales.

De 8.000 millones de personas que hay en el mundo, más de 4.000 millones son usuarios de redes sociales que, además, tienen una media de 9 cuentas

(en una o varias de estas redes sociales). Se estima que para 2024 se creen, copien y consuman 149 zettabytes[3] de datos en todo el mundo.

Gráfico 1. Volumen de datos/información creados, capturados, copiados y consumidos en todo el mundo de 2010 a 2022, con previsiones de 2023 a 2025 (en zettabytes)



Fuente: Elaboración propia a partir de datos de Statista.

Ante semejante volumen de datos y usuarios, su cuantificación económica resulta un ejercicio complejo y, por ende, también lo es el de averiguar el valor de nuestra información personal. No obstante, hay fórmulas de aproximación más y menos sofisticadas. Una de estas, y quizá la más empleada, es la métrica ARPU[4] (del inglés *Average Revenue Per User*), que muestra los ingresos promedio generados por usuario en una plataforma determinada.

3 Un zettabyte, son 1.000.000.000.000.000.000.000 bytes de información.

4 ARPU es una métrica que muestra los ingresos promedio generados por usuario en una plataforma determinada. Se calcula como los ingresos totales divididos por el número total de usuarios. Es una medida fundamental ya que indica el valor financiero que cada usuario aporta al negocio.

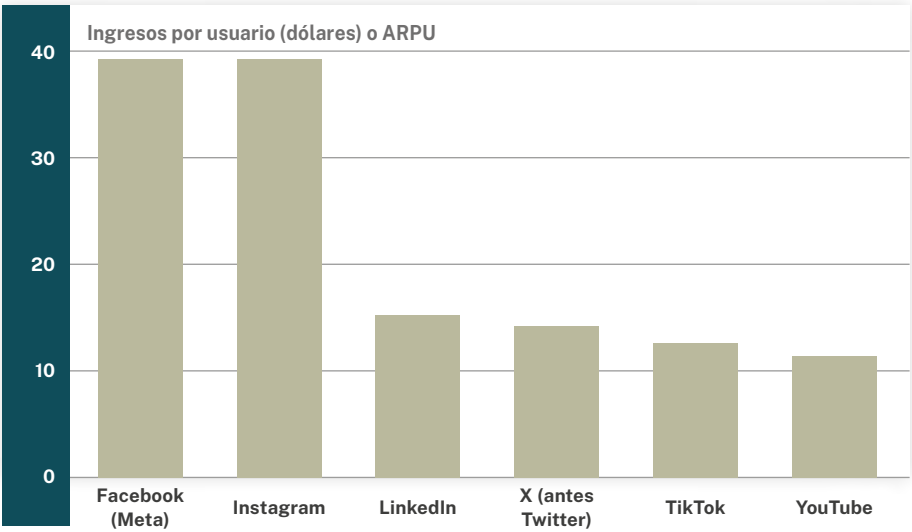
Tabla 1. Ingresos, número de usuarios activos y ARPU por red social (2022)

Red social	Ingresos (millones de dólares)	Número de usuarios activos (millones de dólares)	Ingresos por usuario (dólares) o ARPU
Facebook (Meta)	120000	3050	39,34
Instagram	51400	1300	39,54
LinkedIn	13200	875	15,09
X (antes Twitter)	5220	368	14,18
TIkTok	9400	755	12,45
YouTube	29240	2600	11,25

Fuente: Elaboración propia a partir de datos fiscales de las empresas a cierre del ejercicio 2022.

Así, se observa que la empresa que presenta un ARPU mayor es Facebook, con casi 40 dólares por usuario[5], seguido de Instagram y a gran distancia de LinkedIn y X (antes, Twitter), que rondan los 15 dólares por usuario.

Gráfico 2. ARPU por red social (2022)



Fuente: Elaboración propia a partir de datos fiscales de las empresas a cierre del ejercicio 2022.

5 Es preciso señalar que esta métrica es una media global que presenta grandes fluctuaciones en función del país por el perfil socioeconómico del usuario y la publicidad que a él se dirige.

El valor de los datos personales puede variar significativamente dependiendo de varios factores, incluido el tipo de datos, su calidad y el contexto en el que se utilizan, pudiendo oscilar considerablemente. Por ejemplo, algunos tipos de datos personales como la información financiera (como el historial de pagos recientes) o los registros médicos (que dan detalles de salud) son muy valiosos, y por eso algunas importantes plataformas de servicios en línea gastan miles de millones de dólares anualmente para adquirir datos de clientes de terceros. En cambio, la información demográfica básica como la edad el sexo (que se ubica normalmente en unos 0,0005 dólares por persona) es menos valiosa. A su vez, la calidad —precisión, actualización— y el volumen también son determinantes en la valoración de los datos personales, como también es el caso de la demanda del mercado y su potencial de monetización.

Una forma de cuantificación o valoración de esta información es el precio de mercado de este tipo de datos en la *Dark Web*, como se denomina a una porción de Internet intencionalmente oculta a los motores de búsqueda, con direcciones IP enmascaradas y habitualmente relacionada con actividades criminales.

También se puede estimar el valor de la información del usuario a partir del precio de mercado de una multinacional tecnológica. Microsoft compró LinkedIn por 26.200 millones de dólares cuando el segundo tenía más de 400 millones de usuarios. Con esta información se puede estimar que el valor de los datos personales de cada usuario estaba valorado en 65 dólares. Siguiendo la misma lógica, lo que es ahora Meta compró WhatsApp por 21.800 millones de dólares, pagando 39,6 dólares por cada usuario de los 500 millones que tenía la segunda compañía en el momento. Google adquirió YouTube por 1.650 millones de dólares. Pues bien, Meta, Google o Microsoft no desembolsaron esas enormes cantidades por la estructura tecnológica de estas plataformas, sino por el número de usuarios que traían consigo, con su correspondiente información personal. Y estas cantidades son inmensas. Por ejemplo, los usuarios de Meta, que incluye Facebook, WhatsApp e Instagram, superan los 4.000 millones de usuarios en todo el mundo. En otras palabras, más de la mitad de la población mundial.

Otro mecanismo de valoración consiste en acudir a la facturación de estos gigantes tecnológicos. Solo en nuestro país, y por citar algunos ejemplos, Google España y Apple España facturaron 214 y 551 millones de euros respectivamente, en 2021. Sin embargo, llegados a este punto, es preciso recordar que las empresas tecnológicas introducen un elemento básico para la creación de valor, que es el *know how*, o las competencias para poder mercadear con

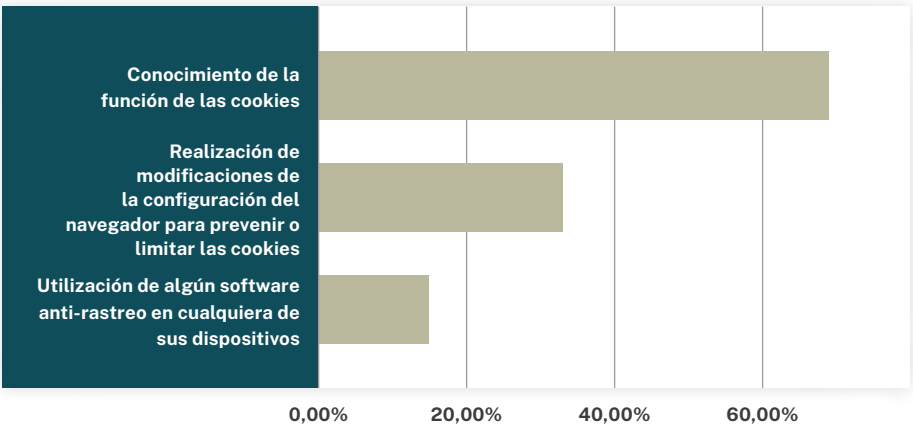
la información de sus usuarios. Ese es su valor añadido; su capacidad para monetizar a sus usuarios.

En el foro digital, donde todo se compra y se vende, con un clic lo privado se hace público y la libertad queda redibujada en la economía del dato. Sin embargo, en esa transacción, el consentimiento que presta el usuario es a menudo a ciegas, pues no conoce realmente el valor que su privacidad aporta a estas entidades y tampoco es del todo consciente de los términos legales que regulan el modo y alcance del empleo de sus datos por parte de las empresas a las que los cede.

Es cierto que el usuario, cada vez más, tiene a su disposición buena parte de la información que necesita para tomar mejores decisiones de mercado en la propia política de privacidad de las organizaciones a las que cede sus datos a cambio del uso de software. Sin embargo, es preciso señalar que el acceso no conlleva su comprensión. Este es particularmente el caso de la política de cookies y privacidad de las empresas, cuya complejidad técnica y extensión conducen a una aceptación de las mismas sin una lectura previa. En especial, una comprensión cierta del contrato que se está firmando.

Así, en España, son muy pocos los ciudadanos que activamente buscan alternativas para proteger sus datos personales más allá de la política de cookies. El Gráfico 3 muestra esta información a partir de datos recabados por el Instituto Nacional de Estadística.

Gráfico 3: Concienciación de políticas de cookies en España.



Fuente: Instituto Nacional de Estadística

El ciudadano promedio, frente a la política de cookies o de privacidad de las compañías tecnológicas, se halla habitualmente ante la tesitura de consentir sin conocer del todo aquello que está aceptando o dedicar un tiempo y esfuerzo muy considerable a comprender las implicaciones de su consentimiento. A su vez, no existe información —ni interés, en ocasiones— acerca del valor de esos datos para las compañías, como tampoco existe un análisis sobre el coste de ceder nuestra privacidad; nuestra soberanía. Todo ello se alimenta, a su vez, de una cuestión puramente operativa, y es la licencia para operar en el mercado profesional que supone el acceso y conocimiento acerca del funcionamiento de diferentes dispositivos tecnológicos de software o hardware. El empresario o trabajador que tenga habilidades o conocimientos digitales tiene una ventaja competitiva cierta sobre los que no. Un motivo más para que el usuario no examine cuestiones críticas como el valor de los datos o la privacidad en sí misma, no resulte que esto impida que se tome a la ligera una decisión que, como puede observarse, es de gran calado.

Como puede observarse, la información imperfecta, la propia naturaleza digital de los datos, y la difícil comprensión de los compromisos legales adquiridos convierten al ciudadano en un contratante débil; en un usuario vulnerable y poco soberano que queda a la intemperie frente al poderoso mercado. Un mercado que crece rápidamente en su capacidad —al menos potencial— de abuso de los consumidores y usuarios por dos factores principalmente.

El primero es la envergadura que presentan algunas compañías tecnológicas en cuanto a su peso relativo dentro del mercado empresarial y cotizado norteamericano. Tan solo 7 empresas —Apple, Microsoft, Alphabet/Google, Amazon, Nvidia, Tesla y Meta/Facebook— suponen el 28% del S&P 500 con una capitalización de más de 10 billones de euros[6]; es decir, casi 10 veces el Producto Interior Bruto (PIB) de España.

6 Menton, J. & Popina, E. (2023). 'History Says Big Tech's Rule Over US Stocks Shouldn't Be Feared', *Bloomberg*. 9 de julio de 2023. Disponible en: https://www.bloomberg.com/news/articles/2023-07-09/history-says-big-tech-s-dominance-over-us-stocks-poses-no-risk

Tabla 2. Ranking de países y empresas por su PIB o valoración (2022)

País o compañía	PIB nacional o Valoración (miles de millones de dólares)
Estados Unidos de América	26,95
China	17,7
Alemania	4,43
Japón	4,23
India	3,73
Reino Unido	3,33
Apple	3,06
Francia	3,05
Microsoft	2,77
Alphabet (Google)	2,72
Italia	2,19
Saudi Aramco	2,13
Brasil	2,13
Canadá	2,12
Rusia	1,86
México	1,81
Corea del Sur	1,71
Australia	1,69
Amazon	1,59
España	1,58
Indonesia	1,42

País o compañía	PIB nacional o Valoración (miles de millones de dólares)
Nvidia	1,22
Turquía	1,15
Países Bajos	1,09
Arabia Saudita	1,07
Meta (Facebook)	0,9
Suiza	0,9

Fuente: Elaboración propia a partir de datos del Fondo Monetario Internacional. Disponibles en: https://www.imf.org/external/datamapper/profile

En segundo lugar, el sector digital se caracteriza también por una creciente concentración de mercado, lo que presenta una doble amenaza. Por un lado, como en cualquier situación de monopolio u oligopolio, el consumidor sufre las consecuencias desde la perspectiva del precio, que todavía no se hace notar dada la férrea competencia entre los gigantes tecnológicos y por la fase actual de democratización tecnológica que exige hacer productos asequibles por las clases medias. Por otro, porque el escaso número de empresas y su envergadura permite que las empresas se encuentren con una gran capacidad para influir en los organismos reguladores de la competencia[7] y del legislador. Esta cercanía al legislador es quizá el mejor ejemplo de cómo las grandes corporaciones tecnológicas están difuminando la divisoria clásica entre el Estado y el mercado.

Examinemos ahora a este segundo actor; el Estado, su papel en el mercado de los datos y en qué medida esa actuación afecta en un sentido u otro a la soberanía personal.

El papel del Estado en la soberanía personal

7 Esto trae consigo, a su vez, un efecto bola de nieve en el que esta concentración de mercado va en aumento, pues las barreras de entrada para nuevos actores son cada vez más difíciles de sortear. También puede motivar la posible actuación de cartel por parte de las organizaciones hegemónicas del sector, bien para la fijación de precios, o bien para la difusión de cuestiones de índole moral e ideológica, como es la visión del mundo *woke*.

El ejercicio en libertad de los derechos y obligaciones de los españoles solo es posible si el Estado, en cumplimiento su principal responsabilidad, asegura que se toman medidas eficaces que garanticen la seguridad de los españoles. Es obligación constitucional del aparato estatal dotar de protección a sus ciudadanos y empresas.

En definitiva, el Estado desempeña un papel de protección que se articula en torno a dos grandes bloques: regulación y vigilancia. En otras palabras, la elaboración de leyes y velar por su cumplimiento.

El primero de estos bloques; el regulatorio, se centra principalmente en el diseño de las normas que regulan el mercado digital, con especial atención en garantizar la competencia, de forma que no haya posición de dominio, u oligopolios que den lugar a prácticas de cartel, etc. Junto a esto, destaca también el apartado fiscal, bajo la máxima de que las organizaciones —en especial, las internacionales— tributen en proporción con la facturación obtenida en el país en cuestión.

Las empresas tecnológicas multinacionales, como muchas otras grandes corporaciones, han sido objeto de escrutinio por sus prácticas fiscales en varios países, incluida España, por sus prácticas de «optimización fiscal», falta de regulación (que acostumbra a no seguir el ritmo del avance tecnológico), etc. En respuesta a estas prácticas, y en una carrera en la que la iniciativa privada le lleva unos años de ventaja al regulador, tanto España en el ámbito nacional como la Unión Europea y otros organismos internacionales han aprobado leyes y reformas que se ajusten a la realidad del mercado y el impacto —intencionado o no— que estas empresas están teniendo. En este sentido, destaca el Reglamento General de Protección de Datos[8] (GDPR por sus siglas en inglés) de las personas físicas.

Asimismo, se está realizando un esfuerzo por reformar las regulaciones fiscales —de nuevo, tanto española como europea— para asegurar que las empresas multinacionales queden sometidas al régimen fiscal del país en el que desarrollan su actividad. De forma similar, también se ha tratado de armonizar para cerrar lagunas fiscales y establecer normas impositivas mínimas globales.

8 El Reglamento General de Protección de Datos es el reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos en la UE y el Espacio Económico Europeo.

En España, el mayor intento de adecuación a las exigencias del mercado en materia fiscal de los últimos años ha sido la Ley 4/2020 de 15 de octubre, sobre Determinados Servicios Digitales, más conocida como «Tasa Google». Este impuesto fue objeto de numerosas críticas que ponían de manifiesto su falta de calidad técnica como medida fiscal a la par que discriminatoria, pues afectaba a un número muy reducido de empresas dado que tan solo se aplicaba a aquellas cuyo importe neto de cifra de negocios en el año natural anterior superase los 750 millones de euros y que el importe total de sus ingresos derivados de prestaciones de servicios digitales sujetas al impuesto fuese mayor de 3 millones de euros. Además, la «Tasa Google» también ha resultado en un fracaso de recaudación. El impuesto, que gravaba los servicios digitales en un 3%, ha tenido con una recaudación muy inferior a la prevista por el gobierno del Partido Socialista. Según las primeras estimaciones, antes de que se aprobara oficialmente, este impuesto iba a servir para recaudar unos 1.200 millones de euros anuales. Posteriormente, una vez recogida en los Presupuestos de 2021, la 'tasa Google' se suponía que iba a recaudar unos 968 millones al año. Sin embargo, los resultados finales fueron bien distintos. El primer año se recaudaron únicamente 166 millones de euros, pues muchas empresas no llegaron a implementarla y tampoco estuvo presente durante todo el año. En 2022, el resultado fue de 278 millones de euros, según la Agencia Tributaria.

Por otro lado, este impuesto ha traído consigo toda una serie de efectos no intencionados, como la repercusión del impuesto a lo largo de la cadena de valor y también al consumidor, como sucedió con el recargo del 2% que comenzó a aplicar Google a los usuarios de publicidad que contratasen con Google Ads. También en el caso de Google, el impuesto supuso un cambio de criterio de localización empresarial, potenciando en Portugal un centro internacional de operaciones que ha creado 1.300 empleos tras descartar implantarlo en España (en claro contraste con los 200 empleados del gigante tecnológico que había entonces en España).

La eliminación del impuesto proviene de la presión estadounidense —donde están domiciliadas la amplísima mayoría de este tipo de corporaciones—, que a su vez cristalizó en uno de la OCDE para crear una «tasa Google» a nivel global. De tal forma, 130 países de la OCDE pactaron la creación de un impuesto mínimo global del 15% para las multinacionales. Un baremo que serviría para unificar criterios y evitar que estas grandes empresas opten por irse a los países donde se pagan menos impuestos, y que deberá aplicarse en 2024.

A su vez, la Unión Europea está endureciendo su marco regulatorio para con las principales corporaciones tecnológicas globales. Históricamente, estas han

demostrado ser oponentes formidables para quienes nada está prohibido, ya sea en términos de prácticas anticompetitivas, evasión fiscal o uso cuestionable de datos personales recurrentes. Y en la última década han preferido pagar sanciones por infracciones de elusión fiscal o competencia desleal antes que plegarse a la legislación vigente.

Frente a estas repetidas violaciones, Europa está endureciendo su postura hacia los gigantes de Internet. La presión de la Unión Europea empieza a dar sus frutos, especialmente respecto a Amazon, que se ha visto obligada a pagar impuestos en todos los países donde la empresa tiene filiales, mientras que antes el grupo centralizaba sus ingresos en Luxemburgo. La reciente Ley de Mercados Digitales (DMA por sus siglas en inglés) de 2022, da fe de esta nueva posición, sometiendo a las grandes plataformas digitales a un régimen regulatorio que prevé, con obligaciones especiales, la prohibición de determinadas conductas y un estricto régimen sancionador que en gran medida replica el régimen aplicable a las infracciones de las normas de competencia.

El segundo de estos bloques es el fiscalizador, que hace referencia a las diferentes agencias y administraciones públicas —como la Agencia Estatal de la Administración Tributaria— y Fuerzas y Cuerpos de Seguridad del Estado que velan por el cumplimiento de la normativa vigente como la anteriormente mencionada.

Así, como puede observarse, el Estado juega un papel fundamental en el ámbito digital y, como resultado, tiene un impacto o incidencia en la esfera de soberanía personal de los usuarios. Sin embargo, en estas actuaciones, motivadas en un principio por un interés genuino de protección, están suponiendo también en muchas ocasiones una amenaza a la libertad de las personas. Esta intromisión por parte del Estado —real, en muchos casos, y potencial, siempre— en la libertad de las personas, o el control o coerción sobre sus decisiones, también responden a una aceptación, por parte de la ciudadanía, de que para salvaguardar su seguridad o comodidad, es preciso ceder parte de su privacidad o su libertad. En especial, en medio de un clima adverso y un contexto de creciente incertidumbre e inseguridad.

De nuevo, la concentración de mercado en el sector digital y su capacidad de influir en el legislador o el tomador de decisiones resulta ser una grave amenaza, pues la connivencia de ambos y su colaboración interesada en operaciones que están fuera de la legalidad es muy conveniente para los dos, en detrimento del ciudadano o usuario. El mejor ejemplo es la vigilancia masiva a la que los Estados están sometiendo a la práctica totalidad de sus sociedades. La NSA,

por ejemplo, obtiene comunicaciones —como mensajes internacionales, correos electrónicos y llamadas por Internet— directamente de empresas de tecnología y redes sociales estadounidenses como Facebook, Google, Apple y Microsoft. El gobierno identifica las cuentas de personas no estadounidenses que desea monitorear y luego ordena a la empresa que divulgue todas las comunicaciones y datos hacia y desde esas cuentas, incluidas las comunicaciones con personas estadounidenses.

Este tipo de operaciones de vigilancia masiva han alcanzado en algunos países proporciones que hasta hace pocos años parecerían de ciencia ficción, como el sistema de crédito social impuesto en China, que expande la vigilancia digital a todos aspectos de la vida por el que las personas son calificadas según su comportamiento social y financiero.

Si bien los aspectos financieros y sociales del sistema de puntuación de China generalmente se consideran separados, las actividades no financieras pueden afectar su situación financiera y viceversa. En definitiva, la puntuación de los ciudadanos afecta su credibilidad y capacidad para operar en la sociedad. Así los delitos menores que afectan la puntuación de un ciudadano incluyen:

1. Comer en trenes
2. Comprar demasiados videojuegos
3. Hacer trampa en videojuegos en línea
4. Gastar ‹‹frívolamente››
5. Esparcir rumores
6. Publicar ‹‹noticias falsas››
7. Participar en prácticas religiosas.
8. No visitar a los padres ancianos con frecuencia

Las personas con una puntuación de crédito social más alta disfrutan de un trato preferencial, apoyo comercial y mejores opciones de viaje. Aquellos con puntuación de crédito social más baja pueden tener dificultades para encontrar trabajo, vivienda o buenas escuelas para sus hijos, y pueden verse restringidos en algunas formas de viajar.

El sistema de puntuación de China no concierne únicamente a los ciudadanos individuales, sino que también afecta a empresas y organismos gubernamentales. Sin embargo, lo que ha causado la mayor protesta es cómo el sistema afecta la privacidad y los derechos humanos básicos de los ciudadanos comunes y corrientes.

Pues bien, estas actuaciones vienen facilitadas por la capacidad técnica de las grandes corporaciones tecnológicas y los datos que obran en su poder. Actuaciones que vienen siempre justificadas por un discurso de seguridad nacional, lo que nos lleva a la siguiente sección, en la que se examinará la soberanía de los datos desde una perspectiva de soberanía nacional.

2.2 La soberanía nacional

2.2.1 *Sobre el concepto de soberanía nacional*

La soberanía nacional es el poder político que posee un Estado independiente y que le confiere la legitimidad política y autoridad necesaria para tomar autónomamente sus propias decisiones. Dicha autoridad reside tradicionalmente en la nación y se encuentra contenido en la constitución nacional. En este sentido, la soberanía consiste en la capacidad de un Estado de gobernarse a sí mismo sin interferencias externas y es fundamental para la supervivencia de la nación en términos de seguridad y prosperidad. Es lo que permite al Estado defender sus intereses nacionales tanto dentro como fuera de sus fronteras al tiempo que protege a sus ciudadanos.

Además, la soberanía nacional es un valor moral. Un Estado soberano es capaz de gobernarse a sí mismo de acuerdo con sus propias leyes y valores. En definitiva, la soberanía nacional es también, como lo era la soberanía personal del apartado anterior, sinónimo de independencia. Precisamente por este motivo, la mayor amenaza hacia esta independencia es la obstaculización o ataque, por parte de terceros Estados, de organizaciones supranacionales o empresas transnacionales que, con su actividad, compromete la autodeterminación, que es causa y consecuencia de la soberanía nacional. Así, el *cloud* o la *big data* no son sólo una cuestión de tecnología o de técnica, sino de gobernanza.

Como se ha señalado en la introducción, la expresión «soberanía digital» en clave «nacional» también se refiere a la capacidad de los Estados de garantizar que sus normas sean respetadas por los distintos actores del mundo digital. En este sentido, esta noción expresa las dificultades a las que a veces se enfrentan los Estados para ejercer sus funciones tradicionales frente a poderosos actores transnacionales con un liderazgo tecnológico indiscutible. Estas dificultades son más importantes en la medida en que los Estados a veces dependen de estos actores, porque necesitan servicios tecnológicos —como la computación en la nube— para desempeñar sus funciones públicas. Así, la

expresión «soberanía digital» tiene indiscutiblemente un aspecto jurídico, ya que se refiere a las prerrogativas del Estado y su capacidad para regular a los gigantes tecnológicos contemporáneos.

Este desarrollo legislativo o regulatorio que acompaña —de nuevo, a menudo con cierta distancia por detrás— al desarrollo tecnológico, es especialmente contundente cuando su justificación obedece a cuestiones que afectan a la seguridad nacional. Por eso, resulta problemático que, por ejemplo, el 92% de todos los datos del mundo occidental se almacenen en servidores de propiedad estadounidense.

Esos servidores pueden contener información sensible tanto de usuarios como de sectores estratégicos clave para la seguridad de un país, como sus telecomunicaciones, sector energético, puertos y aeropuertos, etc. De ahí que se apele a la soberanía nacional articulando el discurso de que, si los datos son de un país, deben permanecer en dicho país o bajo el control del mismo.

Sin embargo, como se ha señalado en el caso de China, las alusiones a la soberanía nacional en algunas ocasiones esconden motivos espurios de vigilancia y control y, en otras, entran en una dinámica de extralimitación de funciones. Ese es el caso de la vigilancia masiva a la que algunas democracias liberales están sometiendo a sus ciudadanos. El gobierno de EE. UU., por ejemplo, con la ayuda de los principales operadores de telecomunicaciones, incluido AT&T, ha participado en una vigilancia masiva e ilegal de las comunicaciones nacionales y los registros de comunicaciones de millones de estadounidenses comunes y corrientes desde al menos 2001. Otro ejemplo es el señalado antes de la NSA.

Otro argumento para la intervención estatal en materia digital amparado bajo el discurso de seguridad nacional es la creciente injerencia de terceros estados en procesos electorales o democráticos. En 2019, a pocos meses de las elecciones presidenciales norteamericanas de 2020, 19 de las 20 páginas principales 'cristianas' en Facebook estaban dirigidas por granjas de trolls de Europa del Este en el extranjero[9]. Los datos muestran que la gran difusión de información errónea en Facebook está impulsada en gran medida por esfuerzos coordinados entre profesionales extranjeros que trabajan juntos para difundir contenido provocativo en los EE. UU.

9 Hao, K. (2021). 'Troll farms reached 140 million Americans a month on Facebook before 2020 election, internal report shows', *MIT Technology Review*. Disponible en: https://www.technologyreview.com/2021/09/16/1035851/facebook-troll-farms-report-us-2020-election/

Estos grupos, basados principalmente en Kosovo y Macedonia, tuvieron un gran éxito atacando a los cristianos estadounidenses. Aunque dividieron sus esfuerzos entre varias páginas, en su mayoría eran operadas por los mismos grupos. En conjunto, sus páginas cristianas de Facebook llegaron a unos 75 millones de usuarios al mes, una audiencia 20 veces mayor que la siguiente página cristiana más grande de Facebook.

De forma similar, Rusia influyó notablemente en favor del separatismo catalán a través de campañas de desinformación masiva y propaganda destinadas a seguir impulsando el movimiento separatista y polarizar la sociedad, como han constatado numerosos estudios[10].

El equilibrio entre seguridad y libertad —y, por descontado, el imperio de la ley—, radica en saber distinguir entre datos inofensivos o no sensibles, que verdaderamente ayudan a mejorar la experiencia digital del usuario, de aquellos que comprometen la soberanía nacional; los datos sensibles. Por naturaleza, los principios básicos de protección a la privacidad de las personas se aplican en diferente medida en función de la tipología de los datos personales en cuestión.

En primer lugar, los datos de carácter personal son la información sobre una persona física identificable. Estos son indiscutiblemente necesarios para que haya un contrato electrónico con el cliente. Sin embargo, las empresas tecnológicas trasnacionales quieren ir mucho más allá de la mera venta de sus productos; sino que desean elaborar estudios de mercado con información privada y lucrarse a partir de ellos.

De la primera tipología de datos se puede derivar mucha información sensible como lugar de residencia o patrones de comportamiento y preferencias culturales. El resultado de esto es la construcción de una identidad digital de cada usuario, que puede ser o no cierta. La veracidad o no de la información que 'vertimos' en la red es un elemento extremadamente relevante a efectos comerciales, pero, sobre todo, a efectos de seguridad nacional.

Pues bien, las corporaciones realizan un ejercicio de triangulación arbitraria de la información disponible, con lo que logran obtener información sensible

10 Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso Villota, M., Lebrun, M., Aho, A. and Giannopoulos, G. (2023). 'Hybrid Threats: A Comprehensive Resilience Ecosystem', *Publications Office of the European Union*, Luxemburgo, 2023.

a partir de información que no proviene de los datos cedidos por la persona. Este proceso deductivo puede llevarse a cabo también en clave de seguridad nacional, pero estas presunciones ya no son de cliente, sino delictivas, revirtiendo la carga de la prueba y el principio de presunción de inocencia, lo que, de nuevo, resulta muy problemático.

Conviene resaltar que, cuando se habla de datos sensibles, es erróneo caer en un individualismo extremo cuando se habla de derechos personales, pues rara vez existe el 'dato individual'. La información sensible está compuesta, aunque parezca paradójico, de datos personales colectivos y políticos que comprometen a nuestros conciudadanos y a la seguridad del Estado: cuando se da información de ubicación, se expone al vecino; cuando se dan datos de gustos, se expone a quienes los comparten; cuando se dan datos de genética, se expone a la familia y los antepasados, etc.

2.2.2. Entre la privacidad y la seguridad

El equilibrio o las tensiones entre privacidad y seguridad están presentes en múltiples instancias de nuestra vida. En clave digital, la seguridad en la tecnología de la información se concentra en salvaguardar los datos, que en realidad es la prevención en el acceso a esos datos y el anonimato de la identidad del usuario.

Por lo general, la ciudadanía en las sociedades abiertas es celosa de su privacidad y reivindica la protección de sus derechos y libertades, como la libertad de expresión, que quedan garantizados a través de la privacidad. Sin embargo, en periodos de convulsión y tensión, se da el fenómeno contrario, y se está más predispuesto a ceder cuotas de privacidad a cambio de una mayor protección. Así lo señalan, por ejemplo, multitud de encuestas realizadas en Estados Unidos[11] desde los ataques terroristas del 11 de septiembre de 2001. En estas, generalmente se ha demostrado que en este tipo de periodos se favorece —tanto desde la ciudadanía como desde las instituciones– un enfoque centrado en la seguridad.

Sin embargo, a la luz de algunos sucesos que han trascendido a la opinión pública, la ciudadanía cada vez es más consciente de la extralimitación por parte

11 Por ejemplo, encuestas del Pew Research Center. Ver Maniam, S. (2016). 'Americans feel the tensions between privacy and security concerns', *Pew Research Center*. Disponible en: https://www.pewresearch.org/short-reads/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/

de las agencias de inteligencia y los servicios de seguridad en la injerencia sobre la esfera privada[12].

A su vez, la expresión de este activismo tecnológico, político y legal sentó las bases de un apetito por una soberanía digital compartida. En esta versión de soberanía, el énfasis radica en mantener el respeto, la integridad y la confidencialidad de los datos frente a gobiernos cada vez más codiciosos y frente a gigantes de Internet. Sin embargo, este impulso de recuperar la soberanía está en desacuerdo con los imperativos de la cooperación internacional, por ejemplo, en la lucha contra el cibercrimen o el terrorismo internacional.

En definitiva, en los últimos años, la sociedad ha despertado de un aletargamiento centrado en la seguridad y reclama con cada vez más fuerza su espacio de privacidad y, con ella, de libertad. Así lo señalan las encuestas en EE. UU.[13] y en muchas otras democracias liberales como España. También ha sucedido con especial intensidad a raíz de la respuesta gubernamental en Occidente a la pandemia de coronavirus. Somos más conscientes de que estamos siendo vigilados y declaramos que vemos en ello más riesgos que beneficios. De esta forma, la tensión entre seguridad y privacidad vuelve a aumentar. Una tensión, no obstante, por resolver y de difícil solución, pues:

> «[C]iertas exigencias de seguridad pueden configurar límites legítimos a los derechos fundamentales. Se puede afirmar, sin ánimo ahora de entrar en mayores profundidades, que no hay derechos fundamentales absolutos, todos tienen límites. El problema está en precisar correctamente estos límites y hacer un traslado adecuado de los mismos a la realidad práctica» (Fernández Rodríguez, 2010).

Como se puede observar, en ocasiones será necesario restringir el ejercicio de los derechos fundamentales en Internet en aras de la seguridad, pero esta restricción debe ser siempre y en todo caso proporcional y razonable. Estos

12 El caso Snowden marcó en este sentido un punto de inflexión. Destapó la vigilancia masiva de la Agencia Central de Inteligencia y de la Agencia de Seguridad Nacional sobre la población estadounidense, aumentando significativamente la conciencia política como resultado de las revelaciones de Wikileaks.

13 Auxier, B. (2020). How Americans see digital privacy issues amid the COVID-19 outbreak, *Pew Research Center*. Disponible en: https://www.pewresearch.org/short-reads/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/

criterios, lejos de ser elementos objetivos altamente consensuados, presentan también un amplio margen de maniobra en su definición, quedando en gran medida dentro de la discrecionalidad del poder —legislativo, ejecutivo y judicial—. Se trata, en definitiva, de una cuestión compleja, caracterizada por la ponderación de derechos e intereses y sobre la apenas pueden aportarse una serie de recomendaciones como las que recoge el siguiente apartado.

3. PROPUESTAS. VISIÓN Y REGULACIÓN

El panorama que ofrece el estado de ebullición actual del sector digital es verdaderamente sobrecogedor; como también lo es el creciente poder de las grandes corporaciones tecnológicas frente a los usuarios y los propios Estados, así como el de estos últimos tanto con fines que atienden a criterios de responsabilidad o altruistas, como a otros de índole espuria.

Así, frente a semejante estado de cosas, la observación, tanto descriptiva como crítica siempre es más sencilla que el comentario propositivo. Sin embargo, éste es el que aporta más valor y son tan grandes los desafíos que presenta «la soberanía de los datos» que no podemos, pues no debemos, dejar de realizar una serie de recomendaciones para cada uno de los dos apartados analizados: «la soberanía personal» y la «soberanía nacional».

3.1. Soberanía personal: hacia un empoderamiento ciudadano

En el ámbito de la soberanía personal, la privacidad e intimidad del usuario debe estar en el centro del debate, y ser tenida en consideración como prioridad absoluta. Esto no quiere decir que deba consagrarse la inviolabilidad de la misma, pues como se ha mencionado anteriormente, en ocasiones será necesario restringir ciertos derechos y libertades.

Sin embargo, lo capital es que las nuevas tecnologías, como es internet en general, estén al servicio de la eficaz garantía de los derechos fundamentales y no de su detrimento. Siempre debe haber un núcleo inviolable e infranqueable, por parte de los Estados y las empresas, y que debería ser también indisponible e irrenunciable, por parte de los usuarios, lo que puede resultar un desafío aún mayor que poner cortapisas a la intromisión de terceros.

A la vista de esta prioridad, nuestra propuesta se basa en el empoderamiento ciudadano o, en clave digital, del usuario, que se vertebra en torno a dos líneas de acción:

(i) La educación y formación de las personas que sean o puedan ser usuarios de internet en materia de privacidad, información sensible o íntima, pudor, etc. con un foco particular en los menores de edad y en los mayores, como grupos poblacionales especialmente propensos a sufrir abusos.

(ii) La articulación de reformas que conduzcan a una transparencia por parte de las compañías tecnológicas y también de los Estados y que, a su vez, redunden en una mejor comprensión de los intercambios de mercado o contraprestaciones en tres ámbitos principalmente:

(ii. a) En el ámbito técnico, como por ejemplo en materia de política de cookies o privacidad, que debe quedar reflejada de una forma clara y sintética que permita su comprensión por una mayoría social independientemente de su conocimiento de la materia. Otro ejemplo es dotar a los usuarios de instrumentos para conocer y decidir sobre la forma en que se utilizan sus datos una vez cedidos al proveedor[14].

(ii. b) En ámbito jurídico, haciendo hincapié en la importancia de los derechos civiles y reforzando el conocimiento de las herramientas legales de las que disponen los usuarios para hacer valer estos derechos frente a posibles abusos de corporaciones y administraciones públicas.

(ii. c) En el ámbito económico, buscando que los usuarios dispongan de la información económica relevante que les permita interactuar en el foro digital con referencias claras del valor que sus datos personales aportan a las grandes tecnológicas (en especial, en materia de redes sociales) con el fin de que se superen los problemas derivados de la información asimétrica y se tomen decisiones de mercado informadas, y sean partícipes de los beneficios publicitarios.

3.2. Soberanía nacional: seguridad en libertad

Por otra parte, en el ámbito de la soberanía nacional, la seguridad en un mundo crecientemente hostil sigue y seguirá ejerciendo un fuerte contrapeso a la libertad de usuarios y empresas, por lo que el foco es el de hallar un equilibrio en el que ambas facetas estén satisfechas. Y no tanto por estar estos dos ámbitos en igualdad de condiciones, sino por ser la seguridad el presupuesto para vivir en libertad, y la libertad el fruto al que aspira la seguridad. Por lo tanto, consideramos oportuno que se avance en los siguientes frentes:

(iii) Definir qué tipo de información resulta sensible en materia de seguridad (ej. militar, energía, infraestructuras, etc.), de forma que el Estado esté legalmente amparado para intervenir, vigilar y censurar la actividad o información de los

14 Empresas que muestran a los usuarios el valor de sus datos en la red, como *Rita Personal Data*.

usuarios en internet. Esta definición resulta también clave para estos últimos, puesto que garantiza que conozcan tanto sus derechos como los límites de los mismos y puedan defenderse de los abusos de poder de la administración pública.

(iv) Diseñar una regulación que encuentre el equilibrio entre la libre circulación de datos personales y el dominio del Estado del que proceden sobre ellos. La autorización previa de España para la exportación de los datos de sus nacionales resulta fundamental para salvaguardar la soberanía nacional, y para proteger la soberanía de los usuarios —en este caso, los españoles—. Esta condición de autorización debe existir, en particular, en los supuestos de venta o cesión de estos datos, por parte de las empresas que los han obtenido, a terceros. Autorización que debe predicarse, por otra parte, principalmente de los usuarios y, de tratarse de información sensible en materia de seguridad nacional, también del Estado.

Es también de obligada mención el peligro que entraña la denominada «balcanización de internet» o «ciberbalcanización» frente a los que propugnan una «autarquía» o «aislacionismo digital». No cabe duda de que resulta tentador levantar fronteras digitales para garantizar que los datos personales estén protegidos de la vigilancia, la propaganda y la manipulación por parte de gobiernos extranjeros o empresas multinacionales. Sin embargo, esta postura trae consigo también riesgos muy notables, como es la posible captura o secuestro de la ciudadanía por parte de diferentes regímenes o gobiernos (véase Corea del Norte o, en menor medida, China). Así, con los mecanismos prudenciales debidos, conviene apostar por el uso de mercados abiertos y cadenas de suministros que eviten dependencias excesivas de sistemas propietarios o de la amenaza totalitaria.

(v) Por último, en el campo de la soberanía personal y la soberanía nacional, conviene acometer una serie de cambios en materia regulatoria, tanto en el ámbito español como de la UE.

(v. a) Agilizar el proceso regulatorio. Como se ha mencionado previamente, el Estado o la legislación acostumbra a seguir al mercado o la libre iniciativa empresarial, caracterizada por un enorme poder creativo. Sin embargo, si el lapso de tiempo entre una realidad y su encaje jurídico en nuestras sociedades es muy grande, la regulación corre el riesgo de nacer ya obsoleta. Un ejemplo es el propio Reglamento General de Protección de Datos que, si bien fue aprobado en 2016, entró en vigor en 2018. Dos años de ventaja para un sector

que no necesita ventaja alguna para llevarle la delantera al regulador. Resulta excesivo, por lo que es preciso dar con un mecanismo regulador más eficiente y que, por tanto, produzca mejores resultados.

(v. b) Desde un punto de vista de competitividad, frente al *Wild West* de Silicon Valley y al capitalismo de estado de China, la Unión Europea se encuentra en una posición en gran medida irrelevante en materia digital. No existen gigantes tecnológicos europeos ni la revolución digital se está produciendo en nuestro continente. Ahora bien, la intrascendencia actual de la Unión Europea no tiene por qué resultar inevitable. En este sentido, el abanico de posibilidades por parte de las instituciones europeas con el fin de reaccionar al desarrollo tecnológico, así como también al desarrollo legislativo en otras latitudes, es muy amplio.

En cualquier caso, la UE está rápidamente convirtiéndose en un referente en materia regulatoria, como se ha señalado previamente en materia de regulación del mercado digital. Otro buen ejemplo es el reciente impulso regulador de la UE para con la Inteligencia Artificial. A principios de diciembre de 2023, la UE acordó el diseño y aprobación de una nueva y amplia ley para regular la inteligencia artificial en uno de los primeros intentos del mundo para limitar el uso de una tecnología en rápida evolución que tiene implicaciones sociales y económicas de amplio alcance. La ley, denominada *A.I. Act*, establece un nuevo punto de referencia global para los países que buscan aprovechar los beneficios potenciales de la tecnología, al mismo tiempo que intentan protegerse contra sus posibles riesgos, como la automatización de empleos, la difusión de información errónea en línea y poner en peligro la seguridad nacional.

Queda, sin embargo, mucho recorrido y territorio por explorar en materia regulatoria. Un recorrido que vertebre, a su vez, un mecanismo de protección en favor de la soberanía digital. En materia de soberanía personal tampoco faltan desarrollos legislativos que blindan esta dimensión y que están sirviendo de guía en otras jurisdicciones, como es el caso de la California Consumer Privacy Act de 2018 (CCPA) (Ley de Privacidad del Consumidor Californiano)[15] que

15 Esta ley brinda a los consumidores más control sobre la información personal que las empresas recopilan sobre ellos y también da orientación sobre cómo implementar la ley. Esta ley histórica garantiza nuevos derechos de privacidad para los consumidores de California, que incluyen:

- El derecho a conocer la información personal que una empresa recopila sobre ella y cómo se utiliza y comparte;
- El derecho a eliminar la información personal recopilada de ellos (con algunas excepciones);

penaliza a las empresas infrinjan la normativa de privacidad de datos con la compensación económica a los consumidores y usuarios[16].

Apunte final. En torno a la Inteligencia Artificial

La Inteligencia Artificial se erige como punta de lanza de la revolución tecnológica, en la que se presentan una serie de encrucijadas técnicas, así como también otras de índole moral. De entre estas últimas, hay dos que destacan especialmente por la gravedad que revisten. La primera es el riesgo que entraña un juego en el que el ganador se lo lleva (potencialmente) todo (*winner-takes-all)* dejando a la competencia, bien empresas, bien Estados, fuera de juego en gran medida —motivo de más para regular rápido, y regular los primeros—. En este juego en el que el ganador se lo lleva todo, como sucede en el sector digital en general, unas pocas empresas dominantes, como OpenAI, Google y Microsoft, tienen cuotas muy significativas del mercado y los recursos, mientras que los jugadores más pequeños luchan por competir e incluso, en un estadio previo, por entrar en el mercado. Un mercado que presenta unas barreras de entrada muy difíciles de superar, como es la gran cantidad de datos y la potencia informática necesaria para entrenar grandes modelos de IA, así como la necesidad de contar con un gran equipo técnico de investigadores e ingenieros. En definitiva, en materia de IA existe el riesgo de la «velocidad de escape» por parte de actores públicos y privados; de actores nacionales o supranacionales. Y ese es un riesgo de fatales consecuencias para los derechos y libertades, para la desigualdad, etc.

Por último, la revolución digital y su vanguardia, la IA, habrían de ponernos en guardia en lo que se refiere a las repercusiones filosóficas o ideológicas que de ésta se pueden desprender. Y es que, a lo largo de la historia, las revoluciones tecnológicas —sean industriales o digitales— han traído consigo nuevas

- El derecho a optar por no vender o compartir su información personal; y
- El derecho a la no discriminación por ejercer sus derechos CCPA.

En noviembre de 2020, los votantes de California aprobaron la Proposición 24, la CPRA, que modificó la CCPA y agregó nuevas protecciones de privacidad adicionales que comenzaron el 1 de enero de 2023. A partir del 1 de enero de 2023, los consumidores tienen nuevos derechos además de los anteriores, como:

- El derecho a corregir información personal inexacta que una empresa tenga sobre ella; y
- El derecho a limitar el uso y divulgación de información personal sensible recopilada sobre ellos.

16 Es preciso señalar que esta ley se inspiró en gran medida en el Reglamento General de Protección de Datos (GDPR) de 2026 de la Unión Europea.

realidades y los problemas que los acompañaban, y, junto con estos, nuevas respuestas, nuevas formas de entender al ser humano y su organización social y política. Así, no se entiende el marxismo si no es de la mano de la revolución industrial, el éxodo rural, o el advenimiento de la clase obrera y la clase burguesa-capitalista. De igual forma, la revolución digital que marcará nuestra era hará emerger novedosas y desafiantes concepciones antropológicas y políticas a las que también habremos de dar respuesta.

4. CONCLUSIÓN

La «soberanía de los datos» es un concepto que ha ido cobrando importancia de la mano del rápido avance de la revolución digital de nuestro tiempo. En especial, debido a las implicaciones que este desarrollo está teniendo sobre la privacidad y la seguridad. Estos dos 'bienes' deben ser debidamente ponderados en un equilibrio de compleja gestión y aún más difícil resolución, pero esa habría de ser la meta para el regulador nacional y europeo a la vista de los riesgos potenciales y abusos reales que se producen sobre los usuarios, así como las amenazas de seguridad nacional que se ciernen sobre los estados.

Tras una breve aproximación teórica a estas cuestiones, este informe ha examinado los principales elementos que se hallan bajo el marco de los conceptos de «soberanía personal» y «soberanía nacional», entendidos ambos en clave de independencia o autodeterminación de usuarios y estados-nación respectivamente, y que han servido de eje vertebrador de este estudio. Se ha puesto de manifiesto cómo las personas —a los efectos, usuarios o consumidores— mantienen relaciones desiguales con las empresas y, en particular, con las multinacionales tecnológicas; relaciones caracterizadas por una cierta opacidad e información imperfecta.

Se ha puesto el foco también sobre la complejidad que reviste una regulación en línea con la salvaguarda de los derechos y libertades —en especial, la privacidad e intimidad— y, a la par, que sea respetuosa con la soberanía nacional y no ponga en riesgo el interés nacional —por ejemplo, en materia de seguridad y defensa, o en procesos electorales—. A su vez, se apunta hacia una posible visión proactiva en materia de regulación, que habría de protagonizar la UE.

El informe alerta de la conjunción entre el estado —en su dimensión nacional o multilateral— y el mercado, en particular, las grandes corporaciones digitales, como una amenaza real tanto sobre usuarios como sobre otros estados. Esto es algo característico de nuestro tiempo, definitorio de un escenario donde las empresas no siempre representan un contrapoder frente a lo público, sino que bien están al servicio de lo público, bien tratan de acometer su 'captura'. Por último, el informe se aventura a predecir movimientos tectónicos en el campo de las ideas y la antropología, haciendo alusión a la IA como punta de lanza —o canario en la mina— de lo que será un punto de inflexión ideológico que presenta un reto de enormes proporciones pero al que también habremos de dar respuesta.

Cada paso que descubre un nuevo horizonte en materia digital conlleva también una nueva exigencia de responsabilidad. Responsabilidad que debe ser asumida y exigida por los usuarios y las naciones en un mundo de creciente hostilidad e incertidumbre y en la que el margen de error para evitar consecuencias catastróficas es muy reducido. Es imperativo que los españoles como usuarios, España como nación y Europa como ecosistema en el que ésta se desarrolla despierten de su letargo digital antes de que sea tarde.

5. BIBLIOGRAFÍA

- Auxier, B. (2020). How Americans see digital privacy issues amid the COVID-19 outbreak, *Pew Research Center*.
  Disponible en: https://www.pewresearch.org/short-reads/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/

- Beard, A. (2022). 'Can Big Tech Be Disrupted?', *Harvard Business Review*. Disponible en: https://hbr.org/2022/01/can-big-tech-be-disrupted

- Fernández Rodríguez, J.J. (2010). 'Seguridad y libertad: ¿equilibrio imposible?: un análisis ante la realidad de Internet', en *Internet, un nuevo horizonte para la seguridad y la defensa*. Universidad de Santiago de Compostela, Colección Cursos e congresos, 189, pp. 9-26.

- Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso Villota, M., Lebrun, M., Aho, A. and Giannopoulos, G. (2023). 'Hybrid Threats: A Comprehensive Resilience Ecosystem', *Publications Office of the European Union*, Luxemburgo, 2023.

- Hao, K. (2021). 'Troll farms reached 140 million Americans a month on Facebook before 2020 election, internal report shows', *MIT Technology Review*.
  Disponible en: https://www.technologyreview.com/2021/09/16/1035851/facebook-troll-farms-report-us-2020-election/

- Maniam, S. (2016). 'Americans feel the tensions between privacy and security concerns', *Pew Research Center*.
  Disponible en: https://www.pewresearch.org/short-reads/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/

- Menton, J. & Popina, E. (2023). 'History Says Big Tech's Rule Over US Stocks Shouldn't Be Feared', *Bloomberg*. 9 de julio de 2023.
  Disponible en: https://www.bloomberg.com/news/articles/2023-07-09/history-says-big-tech-s-dominance-over-us-stocks-poses-no-risk

6. ANEXOS

Tabla A. Tabla correspondiente al Gráfico 1. Evolución del volumen de datos (zettabytes) en el periodo 2010-2025.

Año	Volumen de datos en zettabytes
2010	2
2011	5
2012	6,5
2013	9
2014	12,5
2015	15,5
2016	18
2017	26
2018	33
2019	41
2020	64,2
2021	79
2022	97
2023	120
2024	147
2025	181

Tabla B. Tabla correspondiente al Gráfico 2. ARPU por red social (2022)

Red social	Ingresos por usuario (dólares) o ARPU
Facebook (Meta)	39,34
Instagram	39,54
LinkedIn	15,09
X (antes Twitter)	14,18
TIkTok	12,45
YouTube	11,25

DISENSO
FUNDACIÓN

Actividad subvencionada por el Ministerio de Cultura

fundaciondisenso.org