COMISIÓN
EUROPEA

Bruselas, 10.1.2017
COM(2017) 9 final

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES

«LA CONSTRUCCIÓN DE UNA ECONOMÍA DE LOS DATOS EUROPEA»

{SWD(2017) 2 final}

«LA CONSTRUCCIÓN DE UNA ECONOMÍA DE LOS DATOS EUROPEA»

1. INTRODUCCIÓN

Los datos se han convertido en un recurso esencial para el crecimiento económico, la creación de empleo y el progreso social. El análisis de datos facilita la optimización de procesos y decisiones, la innovación y la predicción de acontecimientos futuros. Esta tendencia mundial presenta un potencial enorme en diversos campos, que van desde la salud, el medio ambiente, la seguridad alimentaria, el clima y la eficiencia en los recursos hasta la energía, los sistemas de transporte inteligentes y las ciudades inteligentes.

La «economía de los datos»[1] se caracteriza por un ecosistema en el que diferentes tipos de agentes del mercado –como fabricantes, investigadores y proveedores de infraestructuras– colaboran para garantizar que los datos sean accesibles y utilizables. Esto permite a dichos agentes extraer valor de esos datos, creando toda una gama de aplicaciones con un gran potencial para mejorar la vida cotidiana (por ejemplo, la gestión del tráfico, la optimización de las cosechas o la atención sanitaria a distancia).

Según estimaciones, el valor de la economía los datos de la UE ascendía a 257 000 millones EUR en 2014, lo que equivale al 1,85 % del PIB de la UE[2]. La cifra aumentó hasta los 272 000 millones EUR en 2015, equivalente al 1,87 % del PIB de la UE (crecimiento interanual del 5,6 %). La misma estimación prevé que, si se implantan a tiempo las condiciones marco políticas y jurídicas para la economía de los datos, su valor se situará en los 643 000 millones EUR para 2020, lo que representaría el 3,17 % del PIB total de la UE.

De conformidad con el Reglamento general de protección de datos (RGPD)[3], a partir de mayo de 2018 habrá un conjunto único de normas paneuropeas, en contraposición a las 28 legislaciones nacionales actuales. El recién creado mecanismo de ventanilla única[4] garantizará que una sola autoridad de protección de datos (en lo sucesivo, «APD») sea responsable de la supervisión de las operaciones de tratamiento de datos transfronterizas efectuadas por cualquier empresa en la UE. Quedará garantizada la coherencia en la

---

1 La economía de los datos mide la repercusión global del mercado de los datos –es decir, el mercado en que se intercambian datos digitales como productos o servicios derivados de los datos brutos– en el conjunto de la economía. Implica la generación, recogida, almacenamiento, procesamiento, distribución, análisis, elaboración, entrega y explotación de los datos que hacen posibles las tecnologías digitales (*European Data Market study*, SMART 2013/0063, IDC, 2016).

2 *European Data Market study*, SMART 2013/0063, IDC, 2016.

3 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/56/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1).

4 Artículo 56 del RGPD.

interpretación de las nuevas normas. En particular, en los casos transfronterizos en que estén implicadas varias APD, se adoptará una única decisión para cerciorarse de que los problemas comunes reciben soluciones comunes. Además, el RGPD crea unas condiciones de competencia equitativas entre las empresas de dentro y fuera de la UE, ya que estas últimas tendrán que aplicar las mismas normas que las empresas europeas si ofrecen bienes y servicios o siguen el comportamiento de las personas en la UE. Un mayor nivel de confianza por parte de los consumidores resultará beneficioso para los operadores comerciales tanto exteriores como de la UE.

La Directiva sobre la privacidad en las comunicaciones electrónicas se refiere a la confidencialidad de esas comunicaciones en la UE. La revisión de dicha Directiva, que se propone en paralelo a la presente Comunicación en forma de Reglamento[5], pretende garantizar un elevado nivel de protección en plena coherencia con el RGPD. Unas normas estrictas de protección de datos generarán la confianza que permita a la economía digital desarrollarse en todo el mercado interior.

Como destacó el presidente Juncker en su discurso sobre el estado de la Unión Europea el 14 de septiembre de 2016, «*[s]er europeo conlleva el derecho a que nuestros datos personales estén protegidos por estrictas leyes europeas. Porque a los europeos no nos gusta que unos drones sobrevuelen nuestras cabezas registrando todos nuestros movimientos, ni que las empresas registren cada vez que hacemos clic en nuestro ordenador. Por este motivo, en mayo de este año el Parlamento, el Consejo y la Comisión aprobaron un reglamento de protección de datos. Es esta una norma común europea que se aplica a las empresas con independencia de dónde tengan su sede y cuándo traten sus datos. En Europa, valoramos la intimidad: es una cuestión de dignidad humana*».

En su Comunicación de 2012 titulada «La protección de la privacidad en un mundo interconectado – Un Marco Europeo de Protección de Datos para el siglo XXI»[6] y en su Comunicación de 2014 titulada «Hacia una economía de los datos próspera»[7], la Comisión reconoció que hacen falta unas normas modernas y coherentes en toda la UE para que los datos circulen libremente de un Estado miembro a otro, que la economía digital europea ha tardado en acoger la revolución de los datos en comparación con EE. UU. y que carece también de una capacidad industrial comparable. Llegaba a la conclusión de que la ausencia de un marco jurídico adaptado a los intercambios de datos dentro de la UE podía contribuir a que el acceso a los grandes conjuntos de datos resultase insuficiente, crear posibles obstáculos a la entrada en el mercado de nuevas empresas y ahogar la innovación.

Es probable que las **restricciones injustificadas a la libre circulación de datos** limiten el desarrollo de la economía de los datos en la UE. Estas restricciones se refieren a los requisitos impuestos por las autoridades públicas a la localización de los datos con fines de almacenamiento o procesamiento. La cuestión de la libre circulación afecta a todos los tipos de datos: las empresas y los agentes de la economía de los datos manejan datos industriales y generados por máquinas, personales o no, así como datos creados por la

5 COM (2017) 10.

6 COM (2012) 9.

7 COM (2014) 442.

actividad humana. La Comisión anunció en su Estrategia para el Mercado Único Digital que iba a proponer una iniciativa para combatir las restricciones a la libre circulación de datos por motivos distintos de la protección de los datos personales en la UE, así como las restricciones injustificadas a la localización de los datos para su almacenamiento o procesamiento. Entre dichas restricciones figuran las disposiciones legislativas adoptadas por los Estados miembros, así como las normas y prácticas administrativas que tengan el mismo efecto. Su número tiende a crecer a medida que la economía de los datos se expande, generando así incertidumbre en cuanto a dónde se pueden almacenar o procesar los datos. Esto puede tener repercusiones en todos los sectores de la economía, tanto en las organizaciones del sector público como del privado, que podrían tener dificultades para acceder a servicios de datos más innovadores o más baratos. Las restricciones injustificadas impuestas a la localización de los datos obstaculizan la libre prestación de servicios y la libertad de establecimiento amparadas por el Tratado y vulneran también la legislación derivada pertinente. Se corre el riesgo de fragmentar el mercado, reducir la calidad de servicio para los usuarios y menoscabar la competitividad de los proveedores de servicios de datos, en particular de las entidades de pequeña envergadura.

La localización de datos injustificada forma parte también de los debates entre la UE y sus socios comerciales, dada la importancia creciente de los datos y de los servicios de datos en la economía mundial y las actitudes potenciales de los terceros países con respecto a esta cuestión. Las normas de protección de datos de la UE no pueden ser objeto de negociación en un acuerdo de libre comercio. Como se explica en la Comunicación sobre el intercambio y la protección de los datos personales en un mundo globalizado[8], los diálogos sobre la protección de datos y las negociaciones comerciales con terceros países deben seguir vías separadas. Aparte de esto, como se indica en la Comunicación «Comercio para todos»[9], la Comisión intentará utilizar los acuerdos comerciales de la UE para establecer normas sobre comercio electrónico y flujos de datos transfronterizos, así como para combatir las nuevas formas de proteccionismo digital, respetando plenamente las normas sobre protección de datos de la UE y sin perjuicio de ellas.

Además, a medida que la transformación impulsada por los datos penetra en la economía y la sociedad, cada vez son mayores los volúmenes de datos generados por máquinas o procesos basados en tecnologías emergentes como la internet de las cosas (IoT, por su sigla en inglés), las fábricas del futuro y los sistemas conectados autónomos. La propia conectividad modifica la forma en que se puede acceder a los datos: aumenta la medida en que datos a los que solía accederse mediante conexiones físicas resultan ya accesibles a distancia. La enorme diversidad de fuentes y tipos de datos, y las abundantes oportunidades para aplicar el conocimiento derivado de estos datos en variados ámbitos, incluida la elaboración de políticas públicas, están solo en sus comienzos. Para sacar partido de estas oportunidades, los actores públicos y privados en el mercado de los datos necesitan tener acceso a conjuntos de datos amplios y diversos. Las cuestiones del acceso y la transmisión en relación con los datos generados por estas máquinas o procesos desempeñan, por consiguiente, un papel básico en la creación de una economía de los datos y exigen una evaluación detenida.

[8] COM (2017) 7.

[9] COM (2015) 497.

Otras cuestiones nuevas que se plantean guardan relación con la aplicación de la normativa sobre responsabilidad por los daños y perjuicios resultantes de un fallo de un dispositivo conectado o un robot y con la portabilidad y la interoperabilidad de los datos. En el contexto de las nuevas tecnologías, como la IoT o la robótica, existen interdependencias complejas y sofisticadas tanto dentro de cada producto (basado en equipos y programas informáticos) como entre dispositivos interconectados. Por otra parte, también pueden plantear problemas nuevos las máquinas autónomas, cuyo comportamiento imprevisto o no deseado podría causar daños a personas y objetos. Estos fenómenos podrían crear inseguridad jurídica en relación con la aplicación de la normativa vigente en materia de responsabilidad y seguridad.

Como se anunció en la Estrategia para el Mercado Único Digital, la Comisión pretende crear un marco político y jurídico claro y adaptado para la economía de los datos, que elimine los obstáculos a la libre circulación de datos que aún persisten y remedie la inseguridad jurídica creada por las nuevas tecnologías de datos. Otros objetivos subyacentes en la presente Comunicación son aumentar la disponibilidad y utilización de los datos, fomentar nuevos modelos empresariales basados en los datos y mejorar las condiciones de acceso a los datos y el desarrollo del análisis de datos en la UE. A tal efecto, la Comisión presenta ciertos temas de debate específicos con vistas a la «construcción de una economía de los datos europea».

En consecuencia, la presente Comunicación explora los siguientes aspectos: la libre circulación de datos; el acceso y la transferencia en relación con los datos generados por máquinas; la responsabilidad y la seguridad en el contexto de las tecnologías emergentes; y la portabilidad de los datos no personales, la interoperabilidad y las normas. La presente Comunicación ofrece también sugerencias para experimentar con soluciones normativas comunes en un entorno realista.

La Comisión ha puesto en marcha un amplio diálogo con las partes interesadas sobre las cuestiones exploradas en la presente Comunicación. El primer paso de este diálogo es una consulta pública, iniciada paralelamente al paquete sobre la economía de los datos[10].

2. LIBRE CIRCULACIÓN DE DATOS

Una economía de los datos dinámica y con un correcto funcionamiento exige permitir y proteger el flujo de datos en el mercado interior. En un contexto tecnológico en rápida evolución, la circulación libre, segura y fiable de los datos resulta fundamental para la protección de las cuatro libertades fundamentales del mercado único de la UE consagradas en los Tratados (mercancías, trabajadores, servicios y capitales). Los servicios de datos están creciendo rápidamente en la UE y en todo el mundo. Un mercado único eficiente y sin barreras en este sector generaría importantes oportunidades de empleo y crecimiento adicionales.

Este crecimiento y la innovación en la economía de los datos, así como la implantación de servicios públicos transfronterizos, podrían verse amenazados por obstáculos a la libre circulación de datos en la UE tales como los requisitos injustificados de localización de los datos impuestos por las autoridades públicas. Las medidas de localización de los

[10] https://ec.europa.eu/digital-single-market/news-redirect/52039

datos suponen la reintroducción efectiva de unos «controles fronterizos» digitales[11]. Pueden ir desde los requisitos, impuestos por las autoridades de supervisión, de que los prestadores de servicios financieros almacenen sus datos a nivel local hasta la aplicación de normas sobre secreto profesional que impliquen el almacenamiento o el procesamiento locales de los datos, e incluso los reglamentos globales que exijan el almacenamiento local de la información archivada generada por el sector público, con independencia de que tengan o no carácter confidencial.

La preocupación por la privacidad es legítima, pero las autoridades públicas no deben utilizarla como motivo para restringir de forma injustificada la libre circulación de datos. Como se ha indicado anteriormente, el RGPD establece un conjunto único de normas que brindan un elevado nivel de protección de los datos personales en toda la UE. Esto consolida la confianza de los consumidores en los servicios en línea, y garantiza una aplicación uniforme de las normas en todos los Estados miembros a través del refuerzo de las autoridades nacionales de protección de datos. El RGPD fomenta la confianza necesaria para el tratamiento de datos y constituye el fundamento de la libre circulación de datos personales en la UE. Asimismo, prohíbe las restricciones a la libre circulación de datos personales dentro de la Unión basadas en motivos relacionados con la protección de los datos personales[12]. No obstante, las restricciones basadas en motivos distintos, por ejemplo en virtud de las leyes fiscales o contables, no están cubiertas por dicho Reglamento. Por otra parte, los datos de carácter no personal, es decir, los datos no se refieran a una persona física identificada o identificable[13], quedan fuera del ámbito de aplicación del RGPD y pueden referirse, por ejemplo, a los datos no personales generados por máquinas.

Las restricciones de localización de datos pueden resultar de disposiciones legales o de directrices o prácticas administrativas que exijan que el almacenamiento o el procesamiento de los datos[14] en formato electrónico[15] se circunscriban a determinada zona geográfica o jurisdicción. A veces los Estados miembros imponen estas restricciones en la creencia de que las autoridades de control pueden supervisar más fácilmente los datos almacenados localmente. La localización también se utiliza como prenda de garantía en términos de privacidad, auditoría y cumplimiento de la ley, así como de seguridad de los datos. Sin embargo, en la práctica, dichas medidas rara vez contribuyen a alcanzar los objetivos que se pretende.

La seguridad de la información depende de una serie de factores, aparte del lugar en que se almacenan físicamente los datos, tales como la preservación de su confidencialidad e

---

11 OCDE, *Emerging Policy Issues: Localisation Barriers to Trade*, 2015 y trabajos en curso.

12 Artículo 1, apartado 3. Por ejemplo, una dirección IP dinámica registrada por un proveedor de servicios de medios en línea cuando una persona accede a un sitio web que el proveedor pone a disposición del público podrá considerarse un dato personal, en relación con dicho proveedor, cuando este disponga de medios legales que le permitan identificar al interesado con la información adicional que tiene sobre dicha persona el proveedor de servicios de internet. Véase la sentencia del asunto C-582/14, Breyer, ECLI:EU:C:2016:779, apartado 49.

13 Según se define en el artículo 4, apartado 1, del RGPD.

14 Datos en manos tanto públicas como privadas.

15 Incluidas las copias de los conjuntos de datos.

integridad cuando quedan disponibles fuera de su instalación de almacenamiento. A este respecto, más que las restricciones en cuanto a la localización de los datos, los factores que realmente contribuyen a la seguridad del almacenamiento y procesamiento de los datos son las mejores prácticas de gestión de las TIC más avanzadas a una escala mucho mayor que los sistemas individuales. Por ejemplo, para proteger los datos ante catástrofes naturales o ciberataques, las instalaciones de almacenamiento de datos situadas en Estados miembros diferentes pueden respaldarse mutuamente y hacer uso de las medidas técnicas y organizativas previstas en la Directiva sobre la seguridad de las redes y los sistemas de información[16]. Por otra parte, la disponibilidad de los datos para fines de reglamentación o supervisión, que no se cuestiona en modo alguno, podría garantizarse mejor reforzando la cooperación entre autoridades nacionales, o entre dichas autoridades y el sector privado, que mediante restricciones de localización. En realidad, en ámbitos caracterizados por una estrecha cooperación entre las autoridades de control, tales como el de los servicios financieros, los requisitos de localización de datos podrían resultar contraproducentes[17].

No obstante, los requisitos de localización de datos pueden resultar justificados y proporcionados en contextos particulares o en relación con determinados datos (especialmente antes de que se pongan en marcha mecanismos eficaces de cooperación transfronteriza), por ejemplo para garantizar la seguridad en el procesamiento de ciertos datos relativos a las infraestructuras energéticas críticas, la disponibilidad de pruebas en formato electrónico (por ejemplo, en forma de copias localizadas de conjuntos de datos) para las autoridades policiales, o el almacenamiento local de los datos contenidos en algunos registros públicos.

Lamentablemente, la tendencia, tanto a nivel mundial como en Europa, es hacia una mayor localización de los datos, apoyándose a menudo en la idea equivocada de que los servicios localizados son automáticamente más seguros que los transfronterizos. Además, el mercado de servicios de datos se ha visto influido sustancialmente por la ausencia de normas transparentes y por una viva percepción de la necesidad de localizar los datos. Esto puede limitar el acceso de empresas y organizaciones del sector público a servicios de datos más baratos o innovadores, u obligar a las empresas que desarrollen actividades transfronterizas a disponer de un exceso de capacidad de almacenamiento y procesamiento de datos. También podría impedir a las empresas basadas en los datos, en particular pymes o empresas de nueva creación, aumentar la escala de sus actividades, entrar en nuevos mercados (por ejemplo, por tener que invertir en centros de datos en 28 Estados miembros) o centralizar sus capacidades de datos y de análisis a fin de desarrollar nuevos productos y servicios.

En la actualidad, Europa satisface internamente, dentro de la UE, el 84 % de su demanda final de «servicios relacionados con las TIC» (consulta, alojamiento, desarrollo). Si estos

---

16 Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DO L 194 de 19.7.2016, p. 1).

17 Una serie de disposiciones de la UE en materia de servicios financieros, así como el sistema europeo de supervisión financiera, exigen que los supervisores tengan acceso a los datos sobre las instituciones y las transacciones financieras en cualquier parte del territorio de la UE. Los requisitos que exijan que los datos se conserven en un determinado territorio nacional, o que condicionen el acceso con fines de control a procedimientos administrativos, podrían reducir el acceso de las autoridades de control a datos que les son indispensables para el cumplimiento de su misión.

servicios pudieran también operar más fácilmente a través de las fronteras interiores de la UE mediante la supresión de las restricciones de localización de datos, podría obtenerse un incremento del PIB de hasta 8 000 millones EUR anuales en ahorro de costes y mejora de la eficiencia[18].

La localización de los datos obstaculiza también la mayor difusión de la computación y el almacenamiento en la nube. Esto podría tener asimismo repercusiones sociales más amplias. En efecto, un uso más eficiente de los recursos informáticos podría contribuir a la reducción del consumo de energía y de las emisiones de carbono en un 30 % neto o más. Una pequeña empresa que se traslade a la nube podría reducir su consumo de energía y sus emisiones de carbono en más de un 90 %, ejecutando sus aplicaciones empresariales en la nube en vez de en infraestructura propia. Se espera que el mercado mundial de centros de datos energéticamente eficientes crezca hasta rondar los 90 000 millones EUR a finales de 2020. La fragmentación del mercado de servicios de datos puede constituir un obstáculo al pleno desarrollo en la UE de estos servicios más eficientes desde el punto de vista energético y socavar la voluntad de invertir.

Con el fin de abordar los problemas y las restricciones antes señaladas y de aprovechar plenamente el potencial de la economía de los datos europea, cualquier acción de un Estado miembro que afecte al almacenamiento o al procesamiento de datos debe estar guiada por un «**principio de libre circulación de los datos en el interior de la UE**», como corolario de las obligaciones que le incumben en virtud de las disposiciones sobre libre circulación de servicios y libertad de establecimiento contenidas en el Tratado y en el Derecho derivado pertinente. Cualquier restricción existente o nueva en materia de localización de datos exigiría una sólida justificación en virtud del Tratado y del Derecho derivado pertinente que avale su necesidad y proporcionalidad para alcanzar un objetivo imperioso de interés general, como la seguridad pública[19].

El principio de la libre circulación de los datos personales[20] consagrado en el Derecho primario y secundario también debe aplicarse en los casos en que el RGPD permite a los Estados miembros regular cuestiones específicas. Debe alentarse a los Estados miembros a no hacer uso de las cláusulas de apertura del RGPD para restringir aún más la libre circulación de datos.

---

18 *Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States*, ECIPE, 2016, cálculo basado en una mayor presión competitiva en el marco de un mercado único digital «industrial» con precios plenamente transparentes.

19 Teniendo en cuenta que las excepciones al Tratado deben interpretarse restrictivamente. El Derecho derivado pertinente incluye el RGPD, la Directiva 2000/31/CE (Directiva sobre comercio electrónico), la Directiva 2006/123/CE (Directiva sobre servicios), y, por lo que se refiere a los proyectos de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información, la Directiva 2015/1535 (Directiva sobre transparencia).

20 La libre circulación de los datos personales figura en el artículo 16 del Tratado de Funcionamiento de la Unión Europea, y las normas relativas a la libre circulación de los datos personales se recogen en la actual y futura legislación de la UE sobre protección de datos. El artículo 1, apartado 3, del Reglamento general de protección de datos establece lo siguiente: «La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales».

En sus conclusiones de 15 de diciembre de 2016, el Consejo Europeo hizo un llamamiento en favor de la eliminación de los obstáculos que persisten en el seno del mercado único, incluidos los que impiden la libre circulación de datos[21].

Con vistas a aplicar el principio de libre circulación de datos, la Comisión dará los dos pasos siguientes:

- Tras la publicación de la presente Comunicación, la Comisión mantendrá diálogos estructurados con los Estados miembros y otras partes interesadas sobre la justificación y la proporcionalidad de las medidas de localización de datos, tomando como punto de partida las restricciones detectadas hasta el momento por la Comisión.

- A la vista de los resultados de los diálogos y de la recogida de información sobre el alcance y la naturaleza de las restricciones sobre la localización de los datos y su incidencia, en particular sobre las pymes y las empresas de nueva creación, entre otras cosas a través de la consulta pública al respecto, la Comisión pondrá en marcha, en caso necesario, procedimientos de infracción para hacer frente a las medidas de localización de datos injustificadas o desproporcionadas y, si procede, podrá también tomar otras iniciativas sobre la libre circulación de datos. En este contexto, cualquier medida continuadora se emprenderá ateniéndose a los principios de «legislar mejor».

3. EL ACCESO A LOS DATOS Y SU TRANSFERENCIA

No dejan de aumentar los volúmenes de datos generados por máquinas o procesos basados en tecnologías emergentes como la IoT. Estos datos se utilizan cada vez en mayor medida como componentes clave de servicios nuevos e innovadores, con el fin de mejorar los procesos de producción o los productos y de prestar apoyo a la toma de decisiones.

La diversidad de los datos generados por estas máquinas o procesos ofrece abundantes oportunidades para que los agentes del mercado de los datos innoven y saquen partido de ellos. Por ejemplo, los datos capturados por los sensores utilizados en las explotaciones agrarias modernas podrían utilizarse para crear una aplicación que optimizase las cosechas, o los datos generados por los sensores de los semáforos podrían utilizarse para crear una aplicación de gestión del tráfico o de optimización de rutas.

A fin de aprovechar al máximo este tipo de datos, los agentes del mercado necesitan tener acceso a conjuntos de datos amplios y diversos. Sin embargo, esto resulta más difícil de lograr si los productores de los datos los reservan para sí mismos y, en consecuencia, los datos se analizan en compartimentos estanco. Los problemas asociados al acceso y la transferencia en relación con los datos brutos (es decir, que no han sido procesados ni modificados luego de su obtención) generados por estas máquinas o procesos desempeñan, por consiguiente, un papel básico en la creación de una economía de los datos y exigen una atenta evaluación.

[21] http://www.consilium.europa.eu/eu/en/press-releases/2016/12/15-euro-conclusions-final/

La cuestión del acceso a datos generados por máquinas se está estudiando en varios sectores, como el transporte, los mercados energéticos, los entornos vitales inteligentes y el sector sanitario y asistencial.

Antes de examinar la situación actual por lo que se refiere al acceso a los datos en la UE, es importante aclarar el tipo de datos considerados en este contexto.

3.1. Tipo de datos considerados

En términos generales, los datos pueden ser personales o no personales. Por ejemplo, los datos generados por los sensores de temperatura domésticos pueden ser personales si resulta posible relacionarlos con una persona viva, mientras que los datos sobre la humedad del suelo no son personales. Los datos personales pueden convertirse en datos no personales a través del proceso de anonimización. En caso de que unos datos puedan calificarse de personales[22], será de aplicación el marco de protección de datos, en particular, el RGPD.

Los datos generados por máquinas se crean sin intervención humana directa a través de procesos informáticos, aplicaciones o servicios, o mediante sensores que procesan los datos recibidos de equipos, programas informáticos o máquinas, ya sean virtuales o reales.

Los datos generados por máquinas pueden ser personales o no personales. Cuando permiten la identificación de una persona física, pueden considerarse datos personales, motivo por el cual será de aplicación toda la normativa sobre datos personales hasta que hayan sido totalmente anonimizados (por ejemplo, los datos de localización de las aplicaciones móviles).

Un aspecto común que vincula la libre circulación de datos con las cuestiones emergentes del acceso y la transmisión de datos es que las empresas y agentes de la economía de los datos tratarán tanto datos personales como no personales, y que los flujos y los conjuntos de datos contendrán habitualmente ambos tipos. Cualquier medida deberá tener en cuenta esta realidad económica, así como el marco jurídico relativo a la protección de los datos personales, respetando al mismo tiempo los derechos fundamentales de las personas.

3.2. Acceso limitado a los datos

A fin de estudiar esta cuestión emergente es preciso analizar, en primer lugar, cómo pueden acceder las empresas y demás agentes del mercado a los conjuntos de datos amplios y diversos necesarios en la economía de los datos.

La información disponible[23] revela que las empresas que disponen de grandes cantidades de datos suelen utilizarlos principalmente en sus capacidades de análisis de datos internas. En la mayoría de los casos, los datos son generados y analizados por la misma

[22] Según se definen en el artículo 4, punto 1, del RGPD.

[23] IDC, *European Data Market Study, First Interim Report*, 2016; *Impact Assessment support study on emerging issues of data ownership, interoperability, (re)usability and access to data, and liability, First interim report*, 2016; Conferencia de alto nivel de la DG Connect, 17 de octubre de 2016.

empresa, e incluso cuando se subcontrata su análisis, es posible que no se reutilicen más los datos. Además, en algunos casos los fabricantes, las empresas prestadoras de servicios u otros agentes del mercado que poseen datos reservan para sí mismos los datos generados por sus máquinas o a través de sus productos y servicios, lo que puede restringir su reutilización en mercados descendentes. Muchas empresas no se benefician de interfaces de programas de aplicación o API[24] (que especifican cómo deben interactuar las diferentes aplicaciones) fáciles de usar ni las permiten, cuando podrían servir de puerta de entrada segura para usos nuevos e innovadores de los datos que poseen las empresas.

Así pues, el intercambio de datos sigue siendo actualmente limitado en términos generales. Los mercados de datos están emergiendo lentamente, pero no se utilizan de forma generalizada. Las empresas pueden no estar equipadas con los instrumentos y las competencias adecuadas para cuantificar el valor económico de sus datos, y pueden temer la pérdida o menoscabo de su ventaja competitiva si los datos quedan a disposición de los competidores.

3.3. Datos en bruto generados por máquinas: situación jurídica a escala nacional y de la UE

Los datos en bruto generados por máquinas no están protegidos por los derechos de propiedad intelectual existentes, ya que no se considera que resulten de un esfuerzo intelectual o posean alguna originalidad. El derecho *sui generis* de la Directiva sobre bases de datos (96/9/CE) –que faculta a los fabricantes de bases de datos para impedir la extracción o reutilización de la totalidad o de una parte sustancial del contenido de una base de datos– proporciona protección únicamente a condición de que la creación de tal base de datos implique una inversión sustancial en la obtención, verificación o presentación de su contenido. La recientemente adoptada Directiva sobre protección de secretos comerciales (2016/943/UE), que debe ser transpuesta al Derecho nacional a más tardar en junio de 2018, protegerá los secretos comerciales de su obtención, utilización y divulgación ilícitas. Para los datos que puedan considerarse «secreto comercial», han de adoptarse medidas para proteger la confidencialidad de la información, que representa el «capital intelectual de la empresa».

En virtud de la legislación de diferentes Estados miembros, solo pueden aplicarse a los datos pretensiones jurídicas cuando cumplan determinadas condiciones que permitan ampararlos, por ejemplo, en el derecho de propiedad intelectual, de bases de datos o de secretos comerciales. Sin embargo, igual que a nivel de la UE, los datos en bruto generados por máquinas no suelen cumplir las condiciones asociadas.

Por consiguiente, no existen actualmente marcos políticos integrales a escala nacional ni de la Unión en relación con los datos en bruto generados por máquinas que no puedan considerarse datos personales, ni con las condiciones de su explotación económica y comerciabilidad. La cuestión se relega básicamente a soluciones contractuales. La utilización de los instrumentos existentes en el Derecho contractual general y en el Derecho de la competencia de la Unión podría constituir respuesta suficiente. Además, podrían contemplarse en determinados sectores acuerdos marco o voluntarios. No

[24] Por ejemplo, https://developer.lufthansa.com/; https://data.sncf.com/api; https://api.tfl.gov.uk/; https://dev.blablacar.com/

obstante, cuando la capacidad de negociación de los distintos participantes en el mercado sea desigual, las soluciones basadas en el mercado podrían no bastar por sí solas para garantizar unos resultados justos y que favorezcan la innovación, facilitar la entrada en el mercado de nuevos agentes y evitar las situaciones de cautividad.

3.4. Situación en la práctica

En algunos casos, los fabricantes o proveedores de servicios pueden convertirse en «propietarios» *de facto* de los datos que generan o procesan sus máquinas, incluso si dichas máquinas son propiedad del usuario. El control *de facto* de estos datos puede ser fuente de diferenciación y ventaja competitiva para los fabricantes. Sin embargo, pueden surgir problemas, ya que a menudo el fabricante impide al usuario autorizar la utilización de los datos por un tercero.

Los diversos agentes del mercado que controlan los datos, en función de las particularidades de los mercados, pueden aprovechar así las lagunas del marco regulador, o las incertidumbres jurídicas antes descritas, imponiendo a los usuarios cláusulas contractuales abusivas o a través de medios técnicos, tales como los formatos propietarios o el cifrado. Aunque varios Estados miembros han hecho extensiva también a las transacciones entre empresas la aplicación de la Directiva sobre las cláusulas abusivas en los contratos celebrados con consumidores, no todos lo han hecho. Esto podría suponer, por ejemplo, que usuarios y empresas quedasen atrapados en acuerdos exclusivos de explotación de datos. Podría surgir una puesta en común voluntaria de los datos, pero la negociación de estos contratos podría acarrear unos costes de transacción considerables para las partes más débiles cuando exista una posición negociadora desigual, o debido a los importantes costes del asesoramiento jurídico.

3.5. Un futuro marco de la UE para el acceso a los datos

Algunos Estados miembros exploran actualmente la posibilidad de garantizar el acceso a los datos generados por máquinas, y pueden decidir regular esta cuestión por sí mismos. Una actuación descoordinada plantea un riesgo de fragmentación y sería nociva para el desarrollo de la economía de los datos en la UE y el funcionamiento de los servicios y tecnologías de datos transfronterizos en el mercado interior.

Por consiguiente, la Comisión tiene intención de iniciar un diálogo con los Estados miembros y demás partes interesadas para explorar un posible futuro marco europeo para el acceso a los datos. En opinión de la Comisión, este diálogo debería girar en torno a los medios más eficaces para alcanzar los objetivos siguientes:

- **Mejorar el acceso a datos anónimos generados por máquinas**: Mediante su puesta en común, reutilización y agregación, los datos generados por máquinas se convierten en una fuente de creación de valor, innovación y diversidad de modelos empresariales[25].

[25] En lo que afecta a los datos personales, será aplicable el RGPD.

- **Facilitar e incentivar el intercambio de estos datos**: Cualquier solución futura debe fomentar un acceso efectivo a los datos, teniendo en cuenta, por ejemplo, las posibles diferencias de poder negociador entre los agentes del mercado.

- **Proteger las inversiones y los activos**: Cualquier solución futura debe también tener en cuenta los intereses legítimos de los agentes del mercado que invierten en el desarrollo de productos, garantizar un rendimiento razonable de sus inversiones y contribuir, por ende, a la innovación. Debe garantizar al mismo tiempo una distribución equitativa de los beneficios entre los titulares de los datos[26], sus procesadores y los proveedores de aplicaciones dentro de las cadenas de valor.

- **Evitar la revelación de datos confidenciales**: Cualquier solución futura debe atenuar los riesgos de revelación de datos confidenciales, en particular a competidores existentes o potenciales. A este respecto, debe también permitir la realización de una correcta clasificación de los datos, previa a la determinación de si se pueden compartir o no determinados datos.

- **Minimizar los efectos de cautividad**: Debe tenerse en cuenta el desigual poder negociador de las empresas y los particulares. Hay que evitar las situaciones de cautividad, especialmente para las pymes, las empresas de nueva creación y los particulares.

En los diálogos con las partes interesadas, la Comisión tiene intención de examinar las siguientes posibilidades para abordar la cuestión del acceso a los datos generados por máquinas, que difieren en cuanto a grado de intervención:

- **Orientaciones para incentivar a las empresas a compartir datos**: Con el fin de atenuar los efectos de las normativas nacionales divergentes y ofrecer una mayor seguridad jurídica a las empresas, la Comisión podría publicar orientaciones sobre cómo deben abordarse en los contratos los derechos de control de los datos no personales. Dichas orientaciones se basarían en la legislación vigente, en particular los requisitos de transparencia y equidad establecidos por la legislación de la UE sobre comercialización y consumidores, la Directiva sobre el secreto comercial y la legislación en materia de derechos de autor, especialmente la Directiva sobre bases de datos. La Comisión tiene previsto poner en marcha una evaluación de esta última Directiva en 2017.

- **Fomento del desarrollo de soluciones técnicas para la fiabilidad de la identificación y el intercambio de datos**: La trazabilidad y la identificación clara de las fuentes de datos constituyen un requisito previo para un verdadero control de los datos en el mercado. La definición de protocolos fiables y posiblemente normalizados para la identificación persistente de las fuentes de datos puede ser necesaria para crear confianza en el sistema. Las interfaces de programas de aplicación (API) también puede fomentar la creación de un ecosistema de desarrolladores de aplicaciones y algoritmos interesados en los datos que poseen las empresas. Las API puede contribuir a que las empresas y las autoridades públicas descubran diferentes tipos de reutilización de los datos que poseen y saquen partido de ello. Sobre esta base, podría contemplarse un mayor uso de API

[26] La entidad que gestiona y conserva los datos generados por máquinas en la práctica.

abiertas, normalizadas y bien documentadas, mediante directrices técnicas, incluida la identificación y difusión de las mejores prácticas para las empresas y los organismos del sector público. Esto podría incluir la oferta de datos en formatos legibles por máquina y el suministro de los correspondientes metadatos.

- **Normas contractuales por defecto**: Unas normas por defecto podrían describir una solución de referencia equilibrada para los contratos relativos a los datos, teniendo también debidamente en cuenta el control de adecuación en curso sobre el funcionamiento general de la Directiva sobre cláusulas contractuales abusivas. Podrían combinarse con la introducción de un control de la equidad en las relaciones contractuales entre empresas[27] que invalidase las cláusulas contractuales que se apartasen en exceso de las normas por defecto. Asimismo, podrían completarse con una serie de cláusulas contractuales normalizadas recomendadas diseñadas por las partes interesadas. Este enfoque podría reducir los obstáculos jurídicos con que tropiezan las pequeñas empresas, así como el desequilibrio en las posiciones negociadoras, y permitir, no obstante, un elevado nivel de libertad contractual.

- **Acceso para fines científicos y de interés público**: Debería otorgarse a las autoridades públicas acceso a los datos cuando ello redundase en el «interés general» y permitiera mejorar considerablemente el funcionamiento del sector público, por ejemplo, el acceso de los institutos de estadística a los datos comerciales o la optimización de los sistemas de gestión del tráfico sobre la base de los datos obtenidos en tiempo real de vehículos privados. El acceso a los datos comerciales por parte de las autoridades estadísticas contribuiría normalmente a aliviar la carga de información estadística impuesta a los operadores económicos. Del mismo modo, el acceso a datos procedentes de fuentes diversas y la posibilidad de combinarlos resulta fundamental para la investigación científica en ámbitos como las ciencias médicas, sociales y medioambientales.

- **Derechos de los productores de datos**: Podría otorgarse al «productor de datos», es decir, el propietario o usuario a largo plazo (arrendatario) del dispositivo, el derecho a utilizar y autorizar la utilización de los datos no personales. Este enfoque tendría como objetivo aclarar la situación jurídica y ofrecer más opciones al productor de datos, al abrir la posibilidad de que los usuarios utilicen sus datos y, por ende, contribuyan a desbloquear los datos generados por máquinas. Sin embargo, las excepciones deberían estar claramente especificadas, en particular el suministro de acceso no exclusivo a los datos por parte del fabricante o de las autoridades públicas, por ejemplo para la gestión del tráfico o por razones medioambientales. En los casos en que se vean afectados datos personales, el particular conservará su derecho a retirar su consentimiento en cualquier momento después de haber autorizado la utilización. Los datos personales tendrían que ser anonimizados de forma que la persona no sea o no sea ya identificable, antes de que se pudiera autorizar su uso por la otra parte. En efecto, el RGPD sigue siendo aplicable a todo dato personal (generado o no por una máquina) hasta que los datos hayan sido anonimizados.

[27]. Obviamente, en el caso de las relaciones entre empresas la referencia en cuanto al nivel de inequidad tendría que ser distinta que en el de las relaciones entre empresas y consumidores, traduciendo un mayor grado de libertad contractual.

- **Acceso remunerado**: Podría elaborarse un marco basado potencialmente en determinados principios fundamentales, tales como las condiciones justas, razonables y no discriminatorias (FRAND, por su sigla en inglés), para que los titulares de datos, tales como fabricantes, proveedores de servicios u otras partes, proporcionasen un acceso remunerado a los datos que poseen después de su anonimización. Habría que tener en cuenta los intereses legítimos pertinentes, así como la necesidad de proteger los secretos comerciales. Podrían también contemplarse regímenes de acceso diferentes para sectores o modelos de negocio diferentes, a fin de tener en cuenta las particularidades de cada sector. Por ejemplo, en algunos casos, el acceso abierto a los datos (parcial o total) podría ser la opción preferida, tanto para las empresas como para la sociedad.

La Comisión consultará a las partes interesadas sobre las cuestiones que se acaban de exponer con vistas a recabar más información sobre el funcionamiento de los mercados de datos por sector y explorar posibles soluciones. En este contexto, resulta esencial un amplio debate a nivel macroeconómico para debatir las posibles soluciones y evitar efectos secundarios no deseados que podrían asfixiar la innovación u obstaculizar la competencia. Además, se celebrarán debates sectoriales con las partes pertinentes de la cadena de valor de los datos.

4. RESPONSABILIDAD

Otra cuestión novedosa es la aplicación de las actuales normas sobre responsabilidad en la economía de los datos a los productos y servicios basados en tecnologías emergentes como la IoT, las fábricas del futuro y los sistemas conectados autónomos. La IoT es una red en rápido crecimiento constituida por objetos cotidianos, tales como relojes, vehículos o termostatos, que están conectados a internet. Los sistemas conectados autónomos, como los vehículos de conducción automática, actúan con independencia de los seres humanos y son capaces de comprender e interpretar sus entornos. Estas tecnologías emergentes utilizan sensores para obtener los numerosos tipos de datos a menudo necesarios para que funcione el producto o servicio.

Es probable que todas estas innovaciones contribuyan a aumentar la seguridad y la calidad de vida, pero, inevitablemente, los errores de diseño, el funcionamiento defectuoso o la manipulación siguen siendo posibles en cualquier dispositivo. Ello podría dar lugar a que un sensor transmitiera datos erróneos, debido, por ejemplo, a defectos en la programación, problemas de conectividad o funcionamiento incorrecto de la máquina. Dada la naturaleza de estos sistemas, puede ser difícil determinar el origen exacto de un problema del que derivan daños, lo que plantea la cuestión de cómo garantizar que estos sistemas sean seguros para los usuarios, con objeto de minimizar los daños, y de quién debe ser considerado responsable en caso de que se produzcan.

La cuestión de cómo proporcionar certidumbre tanto a los usuarios como a los fabricantes de estos productos en relación con su responsabilidad potencial es, por tanto, de importancia crucial para la aparición de una economía de los datos.

4.1. Normas sobre responsabilidad de la UE

El Derecho civil suele distinguir dos tipos de responsabilidad: contractual, cuando la responsabilidad por el daño deriva de la relación contractual entre las partes; y

extracontractual[28], cuando las responsabilidades se establecen fuera de un contrato. Un tipo importante de responsabilidad extracontractual es la relativa a los daños causados por productos defectuosos. A nivel de la UE, la Directiva sobre la responsabilidad por los daños causados por productos defectuosos (85/374/CEE) (en lo sucesivo, «Directiva sobre responsabilidad por productos defectuosos») establece el principio de responsabilidad objetiva, es decir, responsabilidad sin culpa: cuando un producto defectuoso provoque un daño a un consumidor, los fabricantes pueden ser responsables incluso en ausencia de culpa o negligencia por su parte. Sin embargo, puede resultar difícil o poco claro cómo aplicar las disposiciones de esta Directiva[29] en el contexto de la IoT y los sistemas conectados autónomos (por ejemplo, robóticos), por los siguientes motivos: las características de estos sistemas, por ejemplo una compleja cadena de valor del producto o servicio, con interdependencias entre proveedores, fabricantes y otros terceros; la incertidumbre en cuanto a la naturaleza jurídica de los dispositivos de la IoT, es decir, si son productos, servicios o productos asociados a la venta de un servicio; y el carácter autónomo de estas tecnologías.

La Comisión ha puesto en marcha una amplia evaluación de la Directiva sobre responsabilidad por productos defectuosos, con el fin de evaluar su funcionamiento general y si sus normas, elaboradas para un contexto muy diferente, siguen siendo adecuadas para tecnologías emergentes como la IoT y los sistemas conectados autónomos.

4.2. Posibles soluciones

El objetivo de la Comisión es mejorar la seguridad jurídica con respecto a la responsabilidad en el contexto de las tecnologías emergentes y, de este modo, crear unas condiciones favorables para la innovación. Aparte de mantener la situación actual[30], podrían explorarse enfoques diversos, entre ellos:

- **Enfoques de generación del riesgo o de gestión del riesgo**: En virtud de estos enfoques, la responsabilidad podría asignarse a los agentes del mercado que generen un riesgo importante para otros o a los que estén mejor situados para minimizar o evitar la materialización de tal riesgo.

- **Regímenes de seguro voluntarios u obligatorios**: Estos regímenes podrían combinarse con los enfoques en materia de responsabilidad citados. Se compensaría a las partes que hubieran sufrido los daños (por ejemplo, el consumidor). Este planteamiento tendría que ofrecer protección jurídica a las inversiones realizadas por las empresas y tranquilizar a las víctimas asegurándoles una compensación equitativa o un seguro adecuado en caso de daños.

---

28 Las normas sobre responsabilidad de la UE solo se refieren a las responsabilidades extracontractuales.

29 Se hace referencia a la responsabilidad objetiva del productor en caso de productos defectuosos en otros actos legislativos sobre seguridad de los productos, por ejemplo la Directiva sobre equipos radioeléctricos (2014/53/UE), los reglamentos sobre productos sanitarios, la Directiva sobre máquinas (2006/42/CE) y la Directiva relativa a la seguridad general de los productos (2001/95/CE).

30 La Comisión podría formular orientaciones sobre la aplicación a la IoT y a la robótica de las normas de la UE en materia de responsabilidad.

En cualquier caso, habría que tener en cuenta la actuación de la persona que utilice la tecnología, y más concretamente definir el papel de los usuarios de dicha tecnología.

La Comisión consultará a las partes interesadas sobre la idoneidad, en el contexto de la IoT y los sistemas conectados autónomos, de las normas sobre responsabilidad vigentes actualmente en la UE, así como sobre posibles enfoques que permitan superar las dificultades actuales a la hora de asignar la responsabilidad. También se está llevando a cabo en paralelo una consulta pública sobre la evaluación global de la aplicación de la Directiva de responsabilidad por productos defectuosos. La Comisión evaluará los resultados y estudiará las opciones para una futura actuación.

5. PORTABILIDAD, INTEROPERABILIDAD Y NORMAS

Otras cuestiones novedosas en la economía de los datos son la portabilidad de los datos no personales, la interoperabilidad de los servicios que permiten el intercambio de datos y las normas técnicas apropiadas para implementar una portabilidad auténtica.

5.1. Portabilidad de los datos no personales

La portabilidad de los datos significa que tanto los consumidores como las empresas pueden trasladar fácilmente sus datos de un sistema a otro. Se asocia generalmente con unos costes de cambio bajos, y por tanto con escasos obstáculos a la entrada, en la economía de los datos. El RGPD otorga a los particulares el derecho a recibir los datos personales facilitados al proveedor de servicios en un formato estructurado, de uso común y lectura mecánica, así como el derecho de transmitirlos a otro proveedor[31].

En lo que respecta a los datos no personales, sin embargo, no existen actualmente obligaciones que garanticen siquiera un nivel mínimo de portabilidad de los datos, ni para servicios en línea tan ampliamente utilizados como el alojamiento en la nube. Esto se debe en parte a que los requisitos para hacer posible la portabilidad de los datos pueden ser técnicamente difíciles y costosos, ya que distintos proveedores de los mismos servicios pueden almacenar los datos de distinta manera.

Una portabilidad de los datos no personales auténtica también habrá de tener en cuenta consideraciones más generales de gobernanza de datos relativas a la transparencia para los usuarios, el acceso gestionado y la interoperabilidad para conectar entre sí distintas plataformas de manera que estimulen la innovación.

5.2. Interoperabilidad

Es frecuente que las consideraciones relativas a la portabilidad de los datos guarden estrecha relación con las cuestiones de interoperabilidad de los datos, que permite que múltiples servicios digitales intercambien datos sin discontinuidades gracias a unas especificaciones técnicas adecuadas. La Directiva sobre la reutilización de la información del sector público y las orientaciones conexas (incluido el Marco Europeo de

[31] Artículo 20.

Interoperabilidad) hace hincapié en la importancia de unos metadatos normalizados y abundantes, que se atengan a vocabularios establecidos, para facilitar la búsqueda y la interoperabilidad. La Directiva sobre la infraestructura de información espacial en la Comunidad Europea (Inspire) y sus reglamentos y orientaciones sobre la interoperabilidad de los datos y los servicios de datos espaciales, incluidos los datos de observación de los sensores, es aplicable actualmente a los datos espaciales del sector público[32].

En el caso de las plataformas en línea, la interoperabilidad de los datos no solo facilita el cambio de proveedor, sino también el uso simultáneo de varias plataformas (el denominado «multi-homing»), así como el intercambio de datos generalizado entre plataformas, que podría potenciar la innovación en la economía digital.

5.3. Normas

Unas políticas de portabilidad eficaces deben estar basadas en las normas técnicas apropiadas para implementar una portabilidad auténtica de forma tecnológicamente neutra. La Comisión se ha comprometido[33] a respaldar las normas apropiadas para mejorar la interoperabilidad, la portabilidad y la seguridad de los servicios en la nube, a través de una mejor integración de la labor de las comunidades de fuente abierta en el proceso de normalización a nivel europeo. Son ejemplos de este planteamiento la especificación TOSCA para aplicaciones en la nube, destinada a mejorar la portabilidad y la gestión operativa de las aplicaciones y servicios en la nube[34], y las especificaciones técnicas y directrices de las normas de desarrollo de Inspire[35].

5.4. Posibles soluciones

Entre las posibles opciones de cara al futuro para abordar los problemas mencionados figuran:

- **Elaborar unas condiciones contractuales recomendadas para facilitar el cambio de proveedor de servicios**: Dado que la portabilidad de los datos y el cambio de proveedor de servicios de datos son interdependientes, podría contemplarse la elaboración de unas cláusulas contractuales tipo que exigieran al prestador de servicios incluir la portabilidad de los datos de un cliente.

- **Desarrollar los derechos a la portabilidad de datos**: Sobre la base del derecho a la portabilidad de los datos previsto en el RGPD y de las normas propuestas en materia de contratos de suministro de contenidos digitales, podrían introducirse nuevos derechos de portabilidad de los datos no personales, en particular referidos a los contextos de empresa a empresa, teniendo debidamente en cuenta

[32] Los datos generados por máquinas son «datos espaciales», ya que los sensores suelen transmitir directa o indirectamente su posición (localización) junto con su medida.

[33] COM(2016) 176 final: Prioridades de normalización en el sector de las TIC para el mercado único digital.

[34] https://www.oasis-open.org/committees/tosca

[35] Legislación de Inspire: http://inspire.ec.europa.eu/inspire-legislation/26

el resultado del control de adecuación en curso sobre elementos clave del Derecho de la UE sobre comercialización y consumidores[36].

- **Experimentos sectoriales sobre normas**: Al objeto de desarrollar un enfoque riguroso en relación con la codificación en normas de las reglas sobre portabilidad, podrían ponerse en marcha enfoques experimentales sectoriales. Dichos enfoques incluirían habitualmente una colaboración de las múltiples partes interesadas, incluidos los organismos de normalización, la industria, la comunidad técnica y las autoridades públicas.

La Comisión consultará a las partes interesadas sobre estos asuntos y determinará sobre esa base si se requieren medidas adicionales, consistentes posiblemente en las acciones mencionadas, ya sea por separado o en combinación.

6. EXPERIMENTACIÓN Y ENSAYO

La experimentación constituye una parte importante de la exploración de las cuestiones novedosas en la economía de los datos. Se estudiará la posibilidad de poner fondos de Horizonte 2020 al servicio de este tipo de ensayos y experimentos.

Antes de llegar a conclusiones sobre la idoneidad de las posibles soluciones en materia de acceso a los datos y responsabilidad, debería organizarse un ensayo específico para analizar estas cuestiones en un entorno realista, en colaboración con las partes interesadas. Resulta necesaria una solución europea, basada en la cooperación y la experimentación entre los Estados miembros.

Podría seleccionarse para esta prueba la movilidad cooperativa, conectada y automatizada[37], dada la dimensión transfronteriza de este sector.

Existen proyectos ya en curso en algunos Estados miembros para desarrollar sistemas cooperativos y niveles de automatización más elevados[38]. Estos proyectos permiten a los vehículos conectarse entre sí y con infraestructuras de la carretera tales como semáforos y señales de tráfico. Además, la Comisión tiene la intención de trabajar con un grupo de Estados miembros interesados para crear un marco jurídico para la realización de experimentos sobre la base de normas armonizadas en materia de acceso a los datos y responsabilidad. A fin de permitir el acceso a un volumen de datos suficientemente elevado, las pruebas deberían basarse en la 5G, coexistiendo sin discontinuidades con tecnologías ya en despliegue y al amparo de un principio de complementariedad[39].

Otra experimentación interesante procederá del sector geoespacial, con la aparición de un nuevo ecosistema de datos en torno a Copernicus, programa de observación de la Tierra de la UE y tercer mayor proveedor de datos del mundo. La Comisión está desarrollando

[36] http://ec.europa.eu/consumers/consumer_rights/review/index_en.htm

[37] Véase COM (2016) 766 de 30.11.2016.

[38] Véase COM (2016) 766: Estrategia europea para unos sistemas de transporte inteligentes cooperativos.

[39] Véase COM (2016) 588: La 5G para Europa: un plan de acción.

soluciones innovadoras para impulsar el desarrollo de aplicaciones basadas en Copernicus y otros datos espaciales, en particular abordando los problemas del acceso a los datos, la interoperabilidad y la previsibilidad.

7. CONCLUSIÓN

Para construir la economía de los datos, la UE necesita un marco político que permita la utilización de los datos en toda la cadena de valor para fines científicos, industriales y sociales. A tal efecto, la Comisión ha puesto en marcha un amplio diálogo con las partes interesadas sobre las cuestiones exploradas en la presente Comunicación. El primer paso en este diálogo será una consulta pública. Los problemas del acceso a los datos y de la responsabilidad también serán objeto de ensayo en un entorno realista en el ámbito de la movilidad cooperativa, conectada y automatizada.

Por lo que atañe a la libre circulación de datos, la Comisión seguirá trabajando en este tema en consonancia con el planteamiento esbozado anteriormente, a fin de aplicar plenamente el principio de libre circulación de datos dentro de la UE, incluso, cuando sea necesario y apropiado, mediante medidas coercitivas priorizadas. La Comisión también continuará informándose y recabando testimonios y, si fuese necesario, podría estudiar otras iniciativas sobre la libre circulación de datos.

Sobre la base de los resultados del diálogo con las partes interesadas, la Comisión decidirá también si se requieren medidas adicionales en relación con los nuevos problemas y propondrá las soluciones que proceda. En este contexto, puede desempeñar un papel importante la experimentación en condiciones realistas.