EUROPEAN DATA PROTECTION SUPERVISOR

Dictamen 4/2015

Hacia una nueva ética digital

Datos, dignidad y tecnología

11 de septiembre de 2015

De conformidad con el artículo 41, apartado 2, del Reglamento 45/2001, el Supervisor Europeo de Protección de Datos (SEPD) es una institución independiente de la UE, que «por lo que respecta al tratamiento de los datos personales... velará por que los derechos y libertades fundamentales de las personas físicas, en particular el derecho de las mismas a la intimidad, sean respetados por las instituciones y los organismos comunitarios», y... «asesorará a las instituciones y a los organismos comunitarios, así como a los interesados, en todas las cuestiones relacionadas con el tratamiento de datos personales.». Su nombramiento tuvo lugar en diciembre de 2014, junto con el Supervisor Adjunto, con la misión específica de ser más constructivo y proactivo. El SEPD publicó en marzo de 2015 una estrategia quinquenal, en la que se establecía cómo pretende llevar a cabo dicha misión y asumir responsabilidades en relación con dicha misión.

Dicho dictamen es consecuencia del anterior dictamen del SEPD en relación con el Reglamento general de protección de datos que tiene por finalidad asistir a las instituciones de la UE en el logro de un consenso sobre el conjunto de normas viables orientadas al futuro que fomenten los derechos y libertades de las personas físicas. Como en el caso del dictamen sobre sanidad móvil de comienzos de 2015, el SEPD analiza el reto al que debe hacer frente la protección de datos en «la era digital», el tercer objetivo de la Estrategia del SEPD, «personalizar los principios existentes de protección de datos para adecuarse a la escena digital mundial», también a la luz de los planes de la UE para el Mercado Único Digital. El dictamen es coherente con el enfoque del Grupo de Trabajo del Artículo 29 sobre los aspectos de la protección de datos asociados al uso de las nuevas tecnologías, como el «Internet de las cosas», al que el SEPD contribuyó en calidad de miembro de pleno derecho del grupo.

Dignity	Dignidad
Future-oriented rules and enforcement	Normas orientadas al futuro y aplicación
Accountable controllers	Responsables del tratamiento que deben rendir cuentas
Empowered individuals	Personas capacitadas
Innovative privacy engineering	Ingeniería de la intimidad innovadora
Ethics	Ética

«La dignidad humana es inviolable. Ha de respetarse y protegerse.»

Artículo 1, Carta de los Derechos Fundamentales de la UE

Los derechos fundamentales a la intimidad y a la protección de los datos personales han cobrado más importancia para la protección de la dignidad humana que en ningún otro momento. Dichos derechos están consagrados en los Tratados de la UE y en la Carta de los Derechos Fundamentales de la UE y permiten a las personas físicas desarrollar sus propias personalidades, llevar vidas independientes, innovar y ejercer otros derechos y libertades. Los principios sobre protección de datos definidos en la Carta de la UE (necesidad, proporcionalidad, imparcialidad, minimización de los datos, limitación a una finalidad específica, consentimiento y transparencia) son aplicables al tratamiento de datos en su integridad, tanto enlo que se refiere a la recopilación como a su uso.

La tecnología no debe dictar los valores y los derechos, pero tampoco debe reducirse su relación a una falsa dicotomía. La revolución digital promete beneficios para la salud, el medio ambiente, el desarrollo internacional y la eficacia económica. En virtud de los planes de la UE relativos a un mercado único digital, la computación en nube, el «Internet de las cosas», los macrodatos y otras tecnologías se consideran esenciales para la competitividad y el crecimiento. Los modelos de negocio están explotando nuevas capacidades para la recopilación masiva, la transmisión instantánea, la combinación y la reutilización de la información personal para fines no previstos, todo ello justificado por prolijas e impenetrables políticas en relación con la intimidad. Como consecuencia, los principios aplicables a la protección de datos se han visto sometidos a nuevas tensiones, lo que a su vez reclama nuevas ideas sobre cómo aplicarlos.

En el entorno digital actual, no basta con respetar la ley sino que es preciso tener en cuenta la dimensión ética del tratamiento de datos. El marco regulador de la UE ya permite la adopción de decisiones y salvaguardas flexibles y específicas en el momento de tratar información personal. La reforma del marco regulador constituirá un avance positivo. Pero subyacen cuestiones más profundas por lo que se refiere a las repercusiones que las tendencias en una sociedad datadirigida pueden tener sobre la dignidad, la libertad individual y el funcionamiento de la democracia.

Estas cuestiones presentan implicaciones jurídicas, éticas, filosóficas, morales y en materia de ingeniería. El presente Dictamen subraya varias tendencias tecnologías principales que podrían implicar un tratamiento no admisible de la información personal o que podrían interferir con el derecho a la intimidad. El Dictamen presenta un «ecosistema de protección de los macrodatos» a cuatro niveles con el fin de responder al desafío digital: un esfuerzo colectivo, reforzado por consideraciones éticas.

(1) Una normativa orientada al futuro del tratamiento de datos y el respeto de los derechos a la intimidad y a la protección de datos.

(2) Obligación de rendir cuentas para los controladores que determinan el tratamiento de información personal.

(3) Productos y servicios para el tratamiento de datos que incorporen una ingeniería y un diseño conscientes de la intimidad.

(4) Personas capacitadas.

El Supervisor Europeo de Protección de Datos desea estimular un debate abierto y documentado dentro y fuera de la UE, en el que participen la sociedad civil, los diseñadores, las empresas, los académicos, las autoridades públicas y las autoridades reguladoras. El nuevo consejo/comité ético en materia de protección de datos que se instaurará en el seno del SEPD contribuirá a definir una nueva ética digital, que permitirá mejorar los beneficios de la tecnología para la sociedad y la economía por vías que refuercen los derechos y las libertades de las personas físicas.

ÍNDICE

1. Los datos están en todas partes: tendencias, oportunidades y desafíos

Cada vez es mayor el volumen de datos personales que están siendo recopilados y tratados de maneras cada vez más opacas y complejas. Con el progresivo despliegue de los ordenadores en las empresas y las administraciones públicas que se llevó a cabo en la década de 1980, existía la impresión generalizada de que las prácticas en materia de tratamiento de datos personales de los potentes empresas y gobiernos estaban reduciendo a las personas a la calidad de meros interesados, lo cual constituía una amenaza para las libertades y los derechos fundamentales. Lo que distingue a la actual ola de tecnología integrada de la información y la comunicación es su ubicuidad y su capacidad.

El año pasado se informó de que existían más dispositivos conectados en el planeta que personas[1]. Los incrementos en la capacidad de los procesadores[2], almacenamiento y ancho de la banda de transmisión implican que cada vez son menos las limitaciones técnicas para el tratamiento de información personal. Se prevé que «Internet de las cosas» y la analítica de macrodatos converjan con la inteligencia artificial, el procesamiento del lenguaje natural y los sistemas biométricos para dotar a las aplicaciones de la capacidad de aprendizaje automático de inteligencia avanzada. Los gobiernos y las empresas pueden trascender la mera «extracción de datos» hasta llegar a la «extracción de realidad», que penetra la experiencia, la comunicación e incluso los pensamientos de cada día[3]. A medida que la sociedad se ajusta a las demandas del comercio digital, se están llevando a cabo renovados esfuerzos por enseñar programación a los niños pequeños[4]. Aprovechar estas tendencias en un sector en el que la UE es un consumidor líder, aunque rezagado respecto de la prestación de servicios, es un leitmotiv de la estrategia de Mercado Único Digital de la Comisión[5].

Estas tendencias y muchos de los conceptos que se utilizan hoy en día, pese a su uso generalizado, son vagos y se yuxtaponen. Con el propósito de estimular el debate, deseamos destacar tendencias específicas que, aunque obviamente no tienen carácter exhaustivo, en nuestra opinión plantean las cuestiones éticas y prácticas más relevantes para la aplicación de los principios que regulan la protección de datos.

1.1 Macrodatos

El término «macrodatos»[6] se refiere a la práctica de combinar grandes volúmenes de información procedentes de fuentes diversas y analizarlos, mediante el uso frecuente de algoritmos autodidactas como método para fundamentar las decisiones. Esta información no siempre tiene carácter personal: los datos generados por sensores para supervisar fenómenos naturales o atmosféricos, como las condiciones meteorológicas o la contaminación, o para supervisar los aspectos tecnológicos de los procedimientos de facturación, no hacen referencia a «una persona física identificada o identificable»[7]. Pero uno de los principales valores de los macrodatos para las empresas y los gobiernos deriva de la supervisión del comportamiento *humano,* a nivel colectivo e individual y reside en su potencial de predicción[8].

Un resultado es la aparición de un modelo de ingresos para las empresas de Internet basado en el seguimiento de la actividad en línea a fin de optimizar el valor económico de las transacciones a los proveedores de servicios, no solo en publicidad dirigida sino también en las condiciones y los porcentajes de políticas de seguros, préstamos y otras relaciones contractuales. En el competitivo mercado por captar la atención de los usuarios, la mayoría de personas no son conscientes del amplio alcance de dicho seguimiento[9]. Dichos «macrodatos»

deberían considerarse personales incluso cuando se han aplicado técnicas de anonimización: cada vez es más sencillo inferir la identidad de una persona combinando datos presuntamente datos «anónimos» con otros conjuntos de datos que incluyen información públicamente disponible, por ejemplo en las redes sociales[10]. En aquellso casos en que los datos se comercialicen, en particular, de forma transfronteriza y entre jurisdicciones, la responsabilidad del tratamiento de la información se diluye y es difícil apreciar o aplicar en virtud de la legislación sobre protección de datos, en particular a falta de otras normas internacionales.

1.2 «Internet de las cosas»

Muchos dispositivos conectados a Internet ya son un elemento habitual, como los teléfonos inteligentes, las tabletas y los cajeros automáticos y las máquinas de registro de embarque de vuelos. Se prevé que en 2020 la conectividad sea una característica estándar, con veinticinco mil millones de objetos conectados (frente a los 4 800 millones de 2015) que van desde la telemedicina hasta los vehículos, desde los contadores inteligentes hasta una amplia gama de nuevos dispositivos fijos y móviles que permiten contar con ciudades inteligentes[11].

Estos sensores proporcionarán información inmediata y pormenorizada que no es accesible para las oficinas de estadísticas y las encuestas, pero que no es necesariamente más exacta y puede inducir potencialmente a error[12]. La cifra estimada de 1 800 millones de conexiones máquina a máquina prevista para 2022 podría reducir los accidentes y la contaminación, aumentar la productividad y la autonomía de las personas mayores y discapacitadas[13]. Las tecnologías denominadas «ponibles» (*wearables*), como la ropa y los relojes tratarán información personal al igual que otros dispositivos conectados. Podrán detectar coágulos sanguíneos y supervisar la condición física y la cicatrización de heridas; los tejidos conectados podrían servir de protección en entornos extremos, como en la lucha contra incendios, por ejemplo. Dichos dispositivos cargarán datos personales directamente en el almacenamiento en nube, asociado a las redes sociales y que posibilita la realización de una transmisión pública, lo cual permite la identificación de usuarios y el seguimiento del comportamiento y los movimientos de personas y del público[14].

El modo en que se gestiona esta información podría afectar a la intimidad no solo de los usuarios de los dispositivos, incluso cuando se utilizan en el lugar de trabajo, sino también a los derechos de otras personas que son observadas y grabadas por el dispositivo. A pesar de que existen pocas pruebas de discriminación real, está claro que el gran volumen de información personal recopilada a través de «Internet de las cosas» resulta de sumo interés para optimizar los recursos mediante una fijación de precios más personalizada, según el comportamiento que ha sido objeto de rastreo, en particular en el sector de los seguros sanitarios[15]. También se cuestionarán otras normas específicas sectoriales, por ejemplo en el caso de que los dispositivos que impliquen el tratamiento de datos relativos a la salud no estén clasificados en la categoría técnica de productos sanitarios y queden fuera del ámbito de regulación[16].

1.3 Computación ambiental

Computación ambiental o invisible se refiere a una tecnología fundamental que subyace al «Internet de las cosas». Una de sus aplicaciones más evidentes son los «hogares inteligentes» y las «oficinas inteligentes» integradas por dispositivos que incorporan una sofisticada capacidad de tratamiento de la información, y que prometen una mayor eficiencia energética,

así como la existencia de un público más informado capaz de influir en su consumo de forma remota (aunque ello dependería del grado de independencia del inquilino respecto al propietario o el administrador del edificio). Deberá especificarse claramente quién es el responsable de la finalidad y de los medios de tratamiento de los datos personales implicados en las aplicaciones de computación ambiental, no solo para proteger los derechos fundamentales de las personas sino también para asignar correctamente la responsabilidad de garantizar el cumplimiento de los requisitos de seguridad del sistema en general.

1.4 Computación en nube

Se conoce como computación en nube a la tecnología facilitadora central tanto para la analítica avanzada, las capacidades de extracción, la recopilación de macrodatos y analítica, como para el flujo de los datos procedentes del «Internet de las cosas», que actualmente es utilizada por aproximadamente una quinta parte de las personas y las empresas de la UE[17]. Dicha tecnología permite la concentración de datos procedentes de la miríada de dispositivos ligados al «Internet de las cosas» y depende de la disponibilidad y la conectividad de enormes volúmenes de datos en sistemas de almacenamiento a gran escala, así como en las instalaciones de tratamiento de todo el mundo[18]. Se estima que una adopción más generalizada de la computación en nube[19] por parte de los sectores público y privado añadiría potencialmente un total de 449 000 millones de euros al PIB de la UE28 (0,71 % del total del PIB de la UE).

El control sobre la información personal a menudo es compartido por el cliente y el proveedor del servicio en nube y no siempre está claro a quién incumbe la responsabilidad de las obligaciones relativas a la protección de datos. Esto puede implicar que, en la práctica, se facilita una protección insuficiente. Dichas obligaciones son independientes de la **ubicación física del almacenamiento de datos. Asimismo,** aunque se trata únicamente de una tecnología de base que apoya las aplicaciones comerciales, la propia infraestructura de computación en nube podrá convertirse en una infraestructura crucial y aumentar los desequilibrios en el poder de mercado; un 30 % de dichas empresas han comunicado recientemente que encuentran dificultades a la hora de cancelar la suscripción o cambiar de proveedores.[20].

1.5 Modelos empresariales dependientes de datos personales

Estas tecnologías han habilitado nuevos modelos empresariales basados en informaciones no solo generadas a partir de la prestación de servicios sino también procedentes de otras fuentes, como la presencia en las redes sociales, a fin de evaluar los riesgos y la solvencia y maximizar los ingresos. En la actualidad, las plataformas que actúan de puente entre vendedores y compradores constituyen un modelo empresarial destacado, facilitando el intercambio y la redistribución de productos, servicios, competencias y activos. Estas plataformas, a las que con frecuencia se denomina como «economía colaborativa», «consumo colaborativo» o plataformas empresariales entre homólogos móviles y en línea,[21] pueden ofrecer eficiencias económicas clásicas, inyectar competitividad a los mercados y reducir residuos. Se estima que su valor global se cuadriplicará de 26 000 a 110 000 millones de dólares estadounidense en los próximos años[22]. Estos modelos empresariales basados en datos ya generan enormes ingresos en el intercambio de vehículos y el alquiler de viviendas, así como en la tecnología financiera y los créditos sociales. Las encuestas indican que los consumidores aprecian su aparentemente mayor asequibilidad y conveniencia[23].

El uso generalizado de dichas plataformas se debe normalmente a la reputación del usuario, las evaluaciones por homólogos y la verificación de la identidad, Esto puede entenderse potencialmente como un refuerzo de la transparencia y la rendición de cuentas pero no necesariamente en relación con el propio proveedor de la plataforma. Los grandes operadores en estos mercados han recibido críticas por retener, presuntamente, datos referentes a la reputación de los usuarios individuales a los que se refiere la información. Es grande el riesgo de que las personas puedan quedar excluidas de los servicios por causa de reputaciones basadas en datos inexactos que no pueden cuestionar o cuya supresión no pueden solicitar. La dependencia de datos procedentes de diversas fuentes también pone en entredicho el principio de minimización de los datos presente en la legislación europea. El alcance del futuro impacto sobre la sociedad y los individuos de estos, y de futuro modelos empresariales facilitados por la tecnología es merecedpr de una cuidadosa reflexión[24].

1.6 Aeronaves no tripuladas y vehículos autónomos

Las aeronaves no tripuladas, o aeronaves semiautónomas, se utilizan principalmente en la actualidad con fines militares, aunque también se están utilizando cada vez más con fines de vigilancia, cartografía, transporte, logística y seguridad pública, así como para combatir incendios forestales[25]. Las fotografías, los vídeos y otros datos personales recogios por los drones pueden intercambiarse en las redes de telecomunicaciones. Su uso plantea riesgos de interferencias graves en la intimidad y un efecto disuasorio en la libertad de expresión. Surge la cuestión sobre cómo pueden regularse su diseño y uso de manera efectiva de forma que los interesados puedan ejercitar sus derechos de acceso a los datos capturados por dichas máquinas.

En tierra, los vehículos autónomos o los vehículos sin conductor cambiarán el modo en que se utilizan y organizan los desplazamientos individuales y pueden difuminar la diferencia entre el transporte público y privado. Se estima que en 2035 habrá doce millones de vehículos completamente autónomos y dieciocho millones de vehículos parcialmente autónomos, siendo Europa uno de los primeros en adoptar esta solución[26]. Los algoritmos que permiten dirigir los coches gobernarán las decisiones que pueden afectar directamente a la integridad física e incluso a la vida o la muerte de las personas, por ejemplo en la elección programada en caso de impacto inevitable. Estas aplicaciones plantean una serie de cuestiones éticas, así como la evidente necesidad de indicar claramente quién es responsable y debe rendir cuentas del control y la seguridad de los datos.

1.7 Tendencias con un impacto a largo plazo potencialmente mayor

Se prevé que en breve **la bioimpresión en 3D** de componentes orgánicos, que utiliza copias de células de pacientes y «vendas biológicas» de colágeno (es decir, datos sensibles en virtud de la legislación de la UE) para crear filas sucesivas de células vivas, sea una realidad[27]. Esta tecnología facilitará el suministro de partes anatómicas humanas personalizadas y será especialmente valiosa en las zonas del mundo más pobres y que salen de un conflicto. La bioimpresión plantea cuestiones obvias en materia de ética médica, salvaguardia de la propiedad intelectual y protección del consumidor, pero también, puesto que está basada en el tratamiento de datos íntimos y sensibles relacionados con la salud de las personas, para la aplicación de las normas sobre protección de datos.

La **inteligencia artificial**, como la robótica, se refiere a un requisito tecnológico para las máquinas autónomas, tanto fijas como móviles. Su evolución brindar un potencial enorme, más allá de su aplicación en la actualidad. Los ordenadores de aprendizaje profundo se

enseñan tareas a sí mismos mediante el procesamiento de grandes conjuntos de datos que utilizan (entre otras cosas) redes neuronales que parecen emular al cerebro humano. Los investigadores y las empresas aspiran a mejorar el aprendizaje no supervisado. Ya existen algoritmos que pueden entender y traducir lenguas, reconocer imágenes, escribir artículos de noticias y analizar datos médicos[28]. Las redes sociales proporcionan grandes cantidades de información personal previamente etiquetada de manera eficaz por las propias personas. Esta podría ser la última de una línea de mejoras cognitivas destinadas a aumentar la capacidad del cerebro humano, como el papel o el ábaco o que se integra en máquinas autónomas, robots, aunque en la actualidad ha llegado el momento de considerar las ramificaciones más amplias para las personas y la sociedad[29].

2. Un gran ecosistema de protección de los macrodatos

En la actualidad, la UE tiene la oportunidad de ser pionera a la hora de demostrar el modo en que los gobiernos, los legisladores, los controladores, los diseñadores, los desarrolladores y los individuos pueden interactuar mejor para reforzar los derechos y orientar, no bloquear, la innovación tecnológica. Las tendencias descritas en la sección dos han «ampliado la brecha entre lo que es posible y lo que está legalmente permitido», según indica uno de los comentaristas[30]. Contrariamente a lo que algunos reivindican, la intimidad y la protección de datos son una plataforma para un entorno digital dinámico y sostenible, no un obstáculo. Las autoridades independientes de protección de datos, como el SEPD, juegan un papel esencial a la hora de disipar dichos mitos y responder a las inquietudes legítimas que suscita en las personas perder el control sobre su información personal[31].

La próxima generación de datos personales podría ser incluso menos accesible para las personas a las que se refieren. La responsabilidad de configurar un mercado único digital sostenible se encuentra necesariamente dispersa, aunque también es interdependiente, como un ecosistema, lo cual exige una interacción eficaz entre desarrolladores, empresas y autoridades reguladoras en la defensa de los intereses de la persona. En la presente sección, se destaca la contribución que pueden efectuar estos cuatro operadores.

2.1 Regulación orientada al futuro

Recientemente, hemos instado a la UE a que aproveche esta oportunidad histórica de aplicar normas más sencillas para gestionar la información personal que seguirá siendo pertinente para una generación[32]. Las negociaciones sobre el Reglamento general de protección de datos y la Directiva de protección de datos en los ámbitos de los cuerpos de policía y la justicia se encuentran en su fase final y, en breve, se prestará atención al futuro de la Directiva sobre la privacidad en las comunicaciones electrónicas («e-Privacy» y el nuevo Reglamento que regula el modo en que las propias instituciones y órganos de la UE tratan los datos personales. Por ser casi insignificante el coste económico de la recopilación y del almacenamiento de datos, quedaría en manos de las autoridades de protección de datos aplicar estas normas de forma coherente, a fin de evitar el «riesgo moral» de excso en el tratamiento de datos[33].

La estrategia de Mercado Único Digital reconoce el vínculo entre el control de grandes volúmenes de datos y el poder del mercado. La estrategia comparte la convicción, ya expresada en nuestro dictamen preliminar de 2014, sobre «Intimidad y competitividad en la era de la obtención de datos masivos», de que es necesaria una mayor coherencia entre los reguladores. La UE ya dispone de las herramientas para corregir los desequilibrios de poder en el mercado digital; por ejemplo, el procedimiento antitrust en marcha de la Comisión

Europea supone el reconocimiento del predominio de los dispositivos móviles para acceder a Internet. Dentro del marco jurídico existente, es posible una aplicación más holística, como a través de una cámara de compensación de la UE para que las autoridades supervisoras consideren si los asuntos individuales pueden plantear cuestiones de cumplimiento de las normas de competencia y protección de los consumidores y los datos. Por ejemplo:

- Exigir una mayor transparencia en el precio, ya sea en efectivo o de otro modo, de un servicio, puede informar y facilitar el análisis de los asuntos relacionados con la competencia[34], y

- Detectar la discriminación de precios desleal sobre la base de una calidad deficiente de los datos y en la elaboración de perfiles y correlaciones injustas[35].

Un diálogo más estrecho entre los reguladores de los diferentes sectores podría implicar una respuesta a las crecientes relaciones de colaboración mundiales que pueden crean unos «bienes comunes» de datos abiertos en los que los datos y las ideas, como las estadísticas y los mapas, pueden fluir y estar disponibles e intercambiarse en interés público, con un menor riesgo de vigilancia, para proporcionar a las personas mayor influencia sobre las decisiones que le conciernan[36].

2.2 Responsables del tratamiento que deben rendir cuentas

La rendición de cuentas exige la aplicación de políticas y sistemas de control internos que garanticen el cumplimiento y proporcionen pruebas pertinentes, en particular, a las autoridades de supervisión independientes.

Somos partidarios de eliminar la burocracia de la legislación sobre protección de datos, mediante la minimización de los requisitos de documentación innecesaria para maximizar el margen de maniobra para iniciativas más responsable por parte de las empresas, con el apoyo de las directrices de las autoridades responsables de la protección de datos. El principio de que los datos personales deberían ser tratados únicamente de manera compatible con el fin específico para el que se hubieran recogido es fundamental a la hora de respetar las expectativas legítimas de las personas físicas. Por ejemplo, los códigos de conducta, auditorías, certificados, auditorías y una nueva generación de cláusulas contractuales y reglas vinculantes para las empresas pueden contribuir a generar una sólida confianza en el mercado digital. Los responsables de la gestión de información personal deben tener una actitud mucho más dinámica y proactiva y alejarse de la tendencia al secreto denominada «Black Box» (caja negra) y de la opacidad de las prácticas empresariales, al tiempo que se exige mayor transparencia por parte de los clientes[37].

2.3 Ingeniería consciente de la intimidad

La innovación humana ha sido siempre producto de actividades de grupos sociales específicos y de contextos específicos, que normalmente reflejan las normas de la sociedad de la época[38]. Sin embargo, las decisiones en materia de diseño tecnológico no deberían dictar nuestras interacciones sociales ni la estructura de nuestras comunidades, sino que deben respaldar nuestros valores y derechos fundamentales.

La UE debe desarrollar y promover técnicas y metodologías de ingeniería que permitan aplicar tecnologías de tratamiento de datos que respeten completamente la dignidad y los derechos de las personas físicas. Los ingenieros de sistemas y de programas informáticos deben entender y aplicar mejor los principios de protección de la intimidad incorporada al

diseño en el caso de nuevos productos y servicios en todas las fases y las tecnologías de diseño. La rendición de cuentas debe apoyarse en una mayor investigación y desarrollo de métodos y herramientas que garanticen auditorías precisas, así como en determinar el cumplimiento de los responsables del tratamiento y de los encargados del tratamiento con las normas, como «etiquetar» cada unidad de datos personales con «metadatos» que describan los requisitos en materia de protección de datos.

Las soluciones de ingeniería deberían capacitar a las personas que deseen preservar su intimidad y su libertad mediante el anonimato. La UE debe promover el diseño y la aplicación de algoritmos que oculten las identidades y los datos agregados a fin de proteger a las personas al tiempo que aprovechan el poder de predicción de los datos[39].

En la actualidad, debemos establecer las bases para abordar estas tareas, reuniendo a los desarrolladores y a los expertos en materia de protección de datos en las distintas áreas de redes amplias, como la Red de Ingeniería de Privacidad de Internet (IPEN), que contribuyen a un intercambio de ideas y de enfoques interdisciplinares provechoso.

2.4 Personas capacitadas

Un entorno de «prosumidores» (productores-consumidores)

Las personas ya no son meros objetos pasivos que exigen la protección de la ley contra la explotación. Las tendencias digitales descritas anteriormente ofrecen positivamente oportunidades para reforzar el papel del individuo. Por ejemplo, hoy en día las personas producen y consumen contenidos y servicios y cada vez podrán ser consideradas más responsables, junto con los proveedores de servicios, por el tratamiento de datos personales, a menos que se destinen para fines meramente «domésticos»[40] (el concepto de «prosumidores» o «productores-consumidores» ha aflorado con el fin de describir esta evolución[41]). Mientras tanto, las monedas virtuales ofrecen anonimato a los usuarios, a la vez que evitan la verificación de las transacciones por parte de terceros y, por consiguiente, reducen los costes de transacción para pagar los productos y servicios transfronterizos. Por otro lado, el anonimato y el carácter transjurisdiccional (o, podría argumentarse *ajurisdiccional*) de dichas monedas virtuales hace vulnerables a las personas frente al fraude y los mercados delictivos difíciles de detectar e investigar. Aparte de las obligaciones de los reguladores, empresas e ingenieros, los ciudadanos también tienen la responsabilidad de ser conscientes, estar atentos, ser críticos y estar informados cuando efectúan elecciones tanto en línea como fuera de línea[42].

Consentimiento

Asimismo, contrariamente al modo de pensar tradicional, no todos los comportamientos humanos pueden explicarse mediante principios económicos que asumen que los seres humanos son totalmente racionales y sensibles a los incentivos económicos[43]. Esto resulta pertinente para el futuro papel del consentimiento de las personas físicas en el tratamiento de información personal que les concierne. En virtud del Derecho europeo, el consentimiento no es el único fundamento legítimo para la mayoría de tratamientos. Incluso en los casos en que el consentimiento juega un papel importante, no exonera a los responsables del tratamiento de su responsabilidad respecto al uso que se hace de los datos, en particular cuando se ha obtenido un consentimiento general para realizar un tratamiento para una amplia gama de finalidades.

Control y «propiedad» de los datos

Las personas deben estar en condiciones de cuestionar los errores y las desviaciones injustas derivadas de la lógica utilizada por los algoritmos para determinar supuestos y predicciones. A modo de ejemplo, en un estudio realizado en los Estados Unidos sobre aproximadamente 3 000 informes de crédito correspondientes a 1 000 consumidores, se consideró que el 26 % presentaban problemas de errores «materiales» lo suficientemente graves como para afectar a las calificaciones crediticias de los consumidores y, por tanto, el coste de obtención de créditos[44].

Los datos suelen ser considerados como un recurso, al igual que el petróleo, que puede comercializarse, en el caso ideal, por las partes que intervienen en la transacción disponiendo de información similar[45]. Los consumidores no son justamente compensados por su información personal comercializada y algunos de ellos se han mostrado partidarios de un modelo de propiedad de los datos. Es difícil garantizar, no obstante, un control absoluto sobre los datos personales, por lo que existirían otras preocupaciones como el interés público y los derechos y las libertades de otras personas. El control es necesario pero no es suficiente[46]. Sin embargo, el respeto de la dignidad humana es una constante y, conforme al Derecho de la UE, la analogía de la propiedad no puede aplicarse como tal a la información personal, la cual está intrínsecamente vinculada a las personalidades individuales. No existe ninguna disposición en la legislación europea sobre protección de datos para que una persona pueda renunciar a este derecho fundamental.

Un método alternativo para proporcionar a las personas un mejor control sobre sus datos, sobre quienes pueden acceder y para qué finalidad, podría ser el uso de depósitos de datos personales o «cajas fuertes de datos»[47]. El concepto de dicho «almacén personal» exige mecanismos de seguridad que garanticen que solo las entidades autorizadas por el interesado puedan acceder a los datos y únicamente a aquellas partes para las que están autorizadas. Los depósitos de datos personales serían más efectivos en los casos en que afectan a la información actual que se actualiza constantemente, como los datos geoespaciales o las señales de vida. Más allá de las salvaguardias técnicas, los interesados se verían obligados a respetar las normas en materia de intercambio y uso de datos. La competencia y la posibilidad de modificar el servicio que se está utilizando es el único poder más eficaz que el consumidor tiene de influir en el mercado de los servicios que posee a su disposición. Garantizar la portabilidad de las conexiones, incluidos los identificadores y la información de contacto, ha demostrado ser una herramienta poderosa para la competencia y ha reducido de manera eficaz los precios para el consumidor, tras la liberalización del mercado de las telecomunicaciones. La portabilidad de datos, que es la posibilidad fáctica y práctica de transferir la mayoría de los datos de una persona desde un proveedor de servicios a otro, es un punto de partida eficaz para crear las condiciones de una verdadera elección del consumidor.

3. La dignidad en el centro de una nueva ética digital

Es necesario que un marco ético respalde los componentes de dicho ecosistema digital. El SEPD considera que un mayor respeto de la dignidad humana y una mayor salvaguardia de la misma podrían servir de contrapeso a la vigilancia generalizada y la asimetría de poder a la que se enfrentan las personas. Debería estar en el centro de una nueva ética digital.

3.1 Dignidad y datos

A raíz de la revolución industrial de los siglos XVIII y XIX, el movimiento en favor de los derechos humanos se esforzó por asegurar el bien social general, mediante la reducción de los obstáculos para el respeto de las personas físicas. En la actualidad, la UE, con la Carta de Derechos Fundamentales, y tras la Declaración Universal de Derechos Humanos y el Convenio Europeo de Derechos Humanos, ha tomado la inviolabilidad de la dignidad humana como punto de referencia. La dignidad de la persona humana no solo es un derecho fundamental en sí misma sino que también constituye la base de las libertades y derechos posteriores, incluidos los derechos a la intimidad y la protección de datos personales[48]. Las violaciones de la dignidad pueden incluir el trato de la persona como objeto, como una herramienta que sirve a los fines de otros[49]. La intimidad es parte integral de la dignidad humana y el derecho a la protección de datos fue concebido originariamente en las décadas de 1970 y 1980 como una forma de compensar la posible erosión de la intimidad y la dignidad a través del tratamiento de datos personales a gran escala. En Alemania, el derecho a la «autodeterminación informativa» se basaba en el derecho a la dignidad personal y el libre desarrollo de la personalidad contemplado en los artículos 1 y 2 de la Constitución alemana[50].

Sin embargo, a comienzos del siglo XXI, a las personas se les exige cada vez más la divulgación de más información personal en Internet con el fin de participar en asuntos sociales, administrativos y comerciales, lo que implica un alcance cada vez menor para la exclusión voluntaria. Con toda esa actividad potencialmente siempre en línea, la noción de consentimiento libre e informado se resiente enormemente. Se van dejando caer «migas digitales» a cada minuto, que se combinan para clasificar a las personas físicas en tiempo real y para crear perfiles múltiples y, en ocasiones, contradictorios. Dichos perfiles pueden circular en microsegundos sin que las personas tengan conocimiento de ello y utilizarse como fundamento para decisiones importantes que les conciernen.

Los perfiles utilizados para predecir la estigmatización de comportamientos de riesgo de las personas, reforzar los estereotipos existentes, la segregación y la exclusión social y cultural[51], en la que dicha «inteligencia colectiva» socava la elección individual y la igualdad de las oportunidades. Dichas «burbujas de filtro» o «cámaras de eco personales» podrían acabar asfixiando la creatividad, la innovación y las libertades de expresión y asociación, que han permitido el florecimiento de las tecnologías digitales.

Mientras tanto se utiliza un estado de excepción continuo por motivos de «seguridad» para justificar las múltiples capas de técnicas intrusivas empleadas para supervisar la actividad de las personas[52]. Para entender este «trinquete de vigilancia» es necesario adoptar una perspectiva a largo plazo sobre los efectos generales de cara a la sociedad y el comportamiento.

Junto con los terceros países, es necesario que la UE examine seriamente cómo garantizar que estos valores no se respetan solo en el papel sino que, de hecho, se ven neutralizados en el ciberespacio. La UE, en particular, dispone ahora de un «período crítico» antes de la masiva adopción de estas tecnologías para incorporar los valores a las estructuras digitales que definirán nuestra sociedad[53]. Esto obliga a evaluar de nuevo si los beneficios potenciales de las nuevas tecnologías realmente dependen de la recopilación y el análisis de la información personal identificable de miles de millones de personas. Dicha evaluación podría suponer un reto para que los desarrolladores diseñen productos que despersonalizan en tiempo real grandes volúmenes de información desorganizada, lo cual complicaría o haría que fuera imposible singularizar a una persona.

Se ha reconocido ya que determinados tratamientos de datos, por ejemplo, de los datos genéticos, no solo deben estar regulados sino que también deben ser sometidos a evaluación en un contexto de inquietudes sociales más amplios, por ejemplo, los comités éticos. Por su propia naturaleza, los datos genéticos no solo hacen referencia a un individuo sino también a su ascendencia y descendencia. Los datos genéticos no solo sirven para identificar las relaciones familiares sino que los componentes localizados en los genes de una persona también pueden facilitar información sobre sus padres e hijos, y conducir a que los responsables del tratamiento adopten resoluciones que influyan en las oportunidades vitales antes incluso de su nacimiento. La posible concentración de datos personales genéticos en manos de unos pocos pero gigantescos operadores en el mercado tiene implicaciones tanto para las economías de mercado como para los interesados. Una creciente dependencia respecto a un sistema global de recogida y análisis de un flujo constante de datos podría hacer que la sociedad y la economía resulten más vulnerables a defectos de seguridad y ataques malintencionados sin precedentes.

El marco existente podría fallar si no adoptamos de cara al futuro un enfoque intelectualmente innovador. Existen una demanda y una necesidad crecientes de considerar a los interesados como personas, no solo como consumidores o usuarios. Las autoridades de protección de datos verdaderamente independientes juegan un papel fundamental a la hora de prevenir que en un futuro las personas físicas estén determinadas por algoritmos y sus continuas variaciones. Es necesario equiparlas para que ejerciten un «deber de diligencia» en relación con las personas físicas y su dignidad en línea. Los conceptos y principios tradicionales de intimidad y protección de datos ya incluyen matices éticos para la protección de la dignidad, como el empleo y la salud. Sin embargo, las tendencias actuales han abierto un capítulo completamente nuevo, y obligan a explorar si los principios son lo suficientemente sólidos para la era digital[54]. La propia noción de datos personales podría cambiar radicalmente a medida que la tecnología permita cada vez más reidentificar a los individuos a partir de datos supuestamente anónimos. Asimismo, el aprendizaje automático y la fusión de la inteligencia humana y la inteligencia artificial socavarán los conceptos de los derechos y la responsabilidad de las personas.

3.2 El Consejo Consultivo de Ética europeo

No se trata de describir una distopia alaramente. En la actualidad ya se están celebrando debates en los ámbitos jurídico, político, económico, social, científico e incluso religioso[55]. Los enfoques simplistas que conceden una ventaja unilateral al beneficio económico o la vigilancia de la seguridad no resultarán probablemente más útiles que una aplicación demasiado restrictiva de las legislaciones existentes que ahogan la innovación y el progreso. En consecuencia, el SEPD propone un análisis en profundidad, amplio y multidisciplinar, que ofrezca recomendaciones y documente el debate a nivel social sobre cómo una sociedad libre y democrática habría de responder al desafío tecnológico.

La estrategia del SEPD [56] que se compromete a desarrollar un enfoque ético de la protección de datos y que reconoce que «factible, útil o provechoso no equivale a sostenible», resalta «la responsabilidad respecto al cumplimiento mecánico con la letra de la ley». Intentamos ir más allá de la comunidad de funcionarios, abogados y especialistas informáticos de la UE para llegar a personas eminentes y equipadas para juzgar las implicaciones a medio y a largo plazo del cambio tecnológico y las respuestas normativas. En los próximos meses, estableceremos en nuestra institución independiente un grupo consultivo externo sobre la dimensión ética de la protección de datos con el fin de explorar las relaciones entre los derechos humanos, la tecnología, los mercados y los modelos empresariales en el siglo XXI.

Nuestro Consejo Consultivo de Ética estará integrado por un selecto grupo de eminentes personalidades en los ámbitos de la ética y la filosofía, la sociología, la psicología, la tecnología y la economía, y contará con el necesario apoyo de expertos adicionales con conocimientos y experiencia en ámbitos como la salud, el transporte y la energía, la interacción social y los medios de comunicación, la economía y finanzas, la gobernanza y la democracia, así como la seguridad y la elaboración de políticas. Se les invitará a considerar las implicaciones éticas más generales de cómo se conciben y utilizan los datos personales, concediendo la máxima transparencia a sus deliberaciones.

4. Conclusión: Tiempo para profundizar en el debate

La intimidad y la protección de datos forman parte de la solución, no del problema. Por el momento, la tecnología está controlada por seres humanos. No es fácil clasificar claramente estas posibles evoluciones como buenas y malas, deseables o dañinas, beneficiosas o perjudiciales, menos aún cuando es preciso tener en cuenta una serie de posibles tendencias en un contexto. Los legisladores, los desarrolladores tecnológicos, los técnicos comerciales y todos nosotros debemos considerar seriamente si queremos y el modo en que queremos influir en el desarrollo de tecnología y en la aplicación de la misma. Pero no es menos importante el hecho de que la UE considere urgentemente la ética y la posición de la dignidad humana en las tecnologías del futuro.

Los principios de protección de datos se han revelado capaces de salvaguardar a las personas físicas y a su intimidad frente a los riesgos derivados de un tratamiento de datos irresponsable. No obstante, las tendencias actuales pueden exigir un enfoque totalmente nuevo, por lo que abriremos un nuevo debate sobre hasta qué punto la aplicación de principios como la imparcialidad y la legitimidad son suficientes. La comunidad de protección de datos podrá jugar un nuevo papel utilizando las herramientas existentes como los controles previos y las autorizaciones, porque ningún otro organismo está equipado para estudiar dichos tratamiento de datos. La tecnología, la innovación a nivel mundial y la interconexión humana se están desarrollando a gran velocidad y ahora tenemos la oportunidad de llamar la atención, generar interés y construir un consenso.

Con el presente dictamen esperamos ofrecer un marco para un debate más amplio y profundo sobre hasta qué punto la UE puede garantizar la integridad de sus valores, al tiempo que acoge los beneficios de las nuevas tecnologías.

Hecho en Bruselas, a 11 de septiembre de 2015

(firma)

Giovanni BUTTARELLI
Supervisor Europeo de Protección de Datos

Notas

[1] Fuente: GSMA Intelligence.

[2] La «ley de Moore» según la cual el número de transistores que pueden aplicarse a un microchip se duplica aproximadamente cada dieciocho meses se ha revelado, por lo general, exacta; Moore, Gordon E. (19-04-1965). «Cramming more components onto integrated circuits», Electronics. 22-08-2011.

[3] Nathan Eagle, Alex (Sandy) Pentland, «Reality mining: sensing complex social systems», *Journal Personal and Ubiquitous Computing*, Volumen 10 nº 4, marzo de 2006, pp. 255–268. Shoshana Zuboff en «Big Other: surveillance capitalism and the prospects of an information civilization», *Journal of Information Technology* (2015) 30, pp. 75-89, escribe «Como resultado de una mediación informática generalizada, se concede una nueva dimensión simbólica a casi cada uno de los aspectos del mundo a medida que los eventos, objetos, procesos y personas se vuelven visibles, conocidos y compartibles de una nueva manera». Zuboff prevé «el auge de una nueva arquitectura universal» que denomina «Big Other» (El Gran otro), «un régimen omnipresente de instituciones vinculadas en red que registra, modifica y mercantiliza la experiencia diaria desde tostadoras a cuerpos, comunicación a pensamiento, con vistas a establecer nuevas vías de monetización y lucros»; pp. 77-81.

[4] «BBC Micro Bit computer's final design revealed» de 7.7.2015, http://www.bbc.com/news/technology-33409311 (acceso de 10.9.2015); «No assembler required: How to teach computer science in nursery school», *The Economist*, 1.8.2015.

[5] Ninguna de las diez empresas líderes en el sector tecnológico por capitalización bursátil está domiciliada en la UE (ocho son empresas estadounidenses, una es china y otra de Taiwán) según PWC Global Top Ten Companies by Market Capitalisation, actualización de 31 de marzo de 2015.

[6] «Macrodatos se refiere al crecimiento exponencial, tanto de la disponibilidad como del uso automático de información: hace referencia a los enormes conjuntos de datos digitales en poder de corporaciones, gobiernos y otras grandes organizaciones, que son posteriormente objeto de un análisis en profundidad (de ahí la denominación de "analítica") mediante el uso de algoritmos informáticos»; Grupo de Trabajo del Artículo 29, Dictamen 3/2013 sobre la limitación a una finalidad específica. Un informe de la Casa Blanca de 2014 describía los macrodatos como «La creciente capacidad tecnológica para capturar, agregar y tratar un volumen, velocidad y variedad de datos cada vez mayor», véase «Big Data: Seizing Opportunities, Preserving Values, Executive Office of the President ("Podesta-report")», mayo de 2014.

[7] En virtud del Derecho de la UE, los «datos personales» se definen como «toda información sobre una persona física identificada o identificable ("interesado"); se considerará identificable a toda persona cuya identidad pueda determinarse directa o indirectamente, en particular mediante un número de identificación o a través de una o varias de sus características individuales físicas, fisiológicas, psicológicas, mentales, económicas, culturales o sociales», artículo 2, letra a), de la Directiva 95/46/CE. Dicha definición puede compararse en líneas generales con la adoptada por el Consejo de Europa en el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personalmente (conocido como Convenio nº 108) y las Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales. Para un análisis en profundidad véase el «Dictamen 4/2007 sobre el concepto de datos personales» del Grupo de Trabajo del Artículo 29, WP136.

[8] Véase por ejemplo el discurso de la Presidenta de la Comisión Federal de Comercio de Estados Unidos en 2014: «La proliferación de dispositivos conectados, el desplome de los costes en concepto de recopilación, almacenamiento y tratamiento de la información, así como la capacidad de los corredores de datos y otros tipos de agentes para combinar datos tanto en línea como no en línea implica que las empresas pueden acumular virtualmente cantidades ilimitadas de información sobre los consumidores y almacenarla indefinidamente». Mediante el uso de análisis predictivos, es

`psobñe conocer una sorprendente cantidad de información sobre cada uno de nosotros a partir de dichos elementos;», Observaciones preliminares de la Presidenta de la CFC, Edith Ramirez, «Big Data: A Tool for Inclusion or Exclusion?», Washington, DC, 15 de septiembre de 2014. Según Sandy Pentland, «La física social es una ciencia social cuantitativa que describe conexiones fiables y matemáticas entre la información y el flujo de ideas, por un lado, y el comportamiento de las personas, por el otro... nos permite predecir la productividad de pequeños grupos, de departamentos dentro de las empresas e incluso de ciudades enteras». Esto «es lo que es necesario para construir mejores sistemas sociales» (pp. 4, 7) y para «permitir (a los funcionarios del Estado, directores de la industria y ciudadanos) el uso de las herramientas de incentivos de redes sociales para *establecer nuevas normas de comportamiento»* (p. 189) (la cursiva es nuestra); Pentland, *Social Physics: How Good Ideas Spread: The Lessons from a New Science*.

[9] El Eurobarómetro especial 431 sobre protección de datos de junio 2015 y la Encuesta del Grupo de expertos de Pew Research de enero de 2014 sobre las percepciones públicas de la intimidad y la seguridad en la época post-Snowden. El promedio de visitas a un único sitio web, de acuerdo con los resultados de un estudio, da origen a 56 casos de recopilación de datos, según Julia Angwin *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, 2012). El informe de la Casa Blanca de 2014 sobre los macrodatos sostiene que «la potencia y la sofisticación informáticas sin precedentes... genera una asimetría de poder entre aquellos que conservan los datos y aquellos que los facilitan de forma intencionada o inadvertida»; «algunos de los desafíos más profundos revelados durante esta revisión afectan al modo en que el análisis de macrodatos puede...crear un entorno de toma de decisiones tan opaco que la autonomía individual se pierde en una serie de algoritmos impenetrable».

[10] Sirviéndose del censo de 1990 sobre uso de los datos anónimos públicos, el 87 % de la población estadounidense podría ser identificada mediante un código postal de cinco dígitos combinado con el sexo y la fecha de nacimiento; véase Paul Ohm «Broken promises of privacy: responding to the surprising failure of anonymisation», *UCLA Law Review* de 2010 y «Record linkage and privacy: issues in creating new federal research and statistical info», abril de 2011. El ADN es único (salvo para los gemelos univitelinos) y estable a lo largo de toda la vida. Contiene información sobre la etnia, las predisposiciones a las enfermedades y permite identificar a otros familiares. En enero de 2013, los investigadores lograron identificar a las personas y a sus familias a partir de datos de ADN anónimos desde bases de datos genealógicos públicamente accesibles; Gymrek, M., McGuire, A. L., Golan, D., Halperin, E. & Erlich, Y. *Science* 339, 321–324 (2013). Véase asimismo «Poorly anonymized logs reveal NYC cab drivers' detailed whereabouts», de 23 de junio de 2014 http://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/ (acceso de 10 de septiembre de 2015). Véase asimismo el Dictamen 4/2007 del Grupo de Trabajo del Artículo 29 sobre el concepto de datos personales; Dictamen 03/2013 del Grupo de Trabajo del Artículo 29 sobre la limitación a una finalidad específica; Dictamen 06/2013 del Grupo de Trabajo del Artículo 29 sobre datos abiertos y reutilización de la información del sector público («ISP»); y Dictamen 05/2014 del Grupo de Trabajo del Artículo 29 sobre técnicas de anonimización.

[11] Fuente: Gartner.

[12] Véase, por ejemplo, el debate de expertos «What is the future of official statistics in the Big Data era?», the Royal Statistical Society, Londres, 19 de enero de 2015; http://www.odi.org/events/4068-future-official-statistics-big-data-era (acceso de 10.9.2015).

[13] *Ten technologies which could change our lives: potential impacts and policy implications* (Diez tecnologías que podrían cambiar nuestras vidas: posibles impactos e implicaciones políticas), Unidad de Previsión Científica, Servicio de Investigación del Parlamento Europeo, enero de 2015.

[14] El Programa de Trabajo 2016-2017 del Horizonte 2020 de la UE apoya estas evoluciones, incluidos los proyectos pilotos a gran escala que analizarán las preocupaciones en materia de ética e intimidad.

[15] El sector de los seguros ha sido descrito como «el modelo empresarial nativo para Internet de las cosas»; en «From fitness trackers to drones, how the 'Internet of Things' is transforming the insurance

industry», *Business Insider*, de 11.6.2015. El concepto de discriminación de precios en el Derecho de la competencia, que deriva del artículo 102 del TFUE, el cual prohíbe a una posición dominante en el mercado «imponer directa o indirectamente precios de compra, de venta u otras condiciones de transacción no equitativas» es muy controvertido; véase por ejemplo Damien Gerardin y Nicolas Petit «Price Discrimination Under EC Competition Law: Another Antitrust Theory in Search of Limiting Principles» (julio de 2005), Documento de trabajo de Global Competition Law Centre, serie nº 07/05. En el caso de los macrodatos y su, según los autores, todavía no materializado potencial de acelerar la indicación de precios personalizada, véase la Oficina Ejecutiva del Presidente de los Estados Unidos, «Big Data and Differential Pricing», febrero de 2015, y un análisis reciente que concluye que la información personalizada sobre precios por lo general implica el tratamiento de datos personales y, por tanto, deberá respetar el principio de transparencia de la legislación sobre protección de datos, la cual exige a las empresas que informen a las personas sobre la finalidad del tratamiento de sus datos personales: las empresas deben indicar si han personalizado los precios. Si una empresa utiliza una cookie para reconocer a alguien, la Directiva sobre la privacidad en las comunicaciones electrónicas exige a la empresa que informen a la persona sobre la finalidad de la cookie; borrador de trabajo de Frederik Borgesius «Online Price Discrimination and Data Protection Law». Disponible en http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2652665 (acceso de 10.9.2015).

[16] Los productos sanitarios se definen en la legislación europea con arreglo a la Directiva 93/42/CEE del Consejo relativa a los productos sanitarios, modificada por la Directiva 2007/47/CE del Parlamento Europeo y del Consejo, de 5 de septiembre de 2007. Sobre las implicaciones de la «sanidad móvil» en materia de protección de datos, véase el Dictamen 1/2015 del SEPD.

[17] Según Eurostat, el 21 % de las personas y el 19 % de las empresas de la UE utilizan servicios de almacenamiento en nube.

[18] «Si Internet mundial fuera un país, sería el doceavo mayor consumidor de electricidad del mundo, ubicándose en algún lugar intermedio entre España e Italia, lo cual representa aproximadamente entre el 1,1 y el 1,5 por ciento del consumo mundial de electricidad (en 2010), y los gases de efecto invernadero generados anualmente por 70 a 90 centrales eléctricas de carbón de gran tamaño (500 megawatios)». Natural Resources Defense Council, Data Centre Efficiency Assessment: Scaling Up Energy Efficiency Across the Data Centre Industry: Evaluating Key Drivers and Barriers 2014.

[19] Informe del estudio «SMART 2013/0043 - Uptake of Cloud in Europe».

[20] Fuente: Eurostat.

[21] La crítica que se ha hecho del término «economía colaborativa» es que induce a error: «The Sharing Economy Isn't About Sharing at All», Giana M. Eckhardt y Fleura Bardhi, *Harvard Business Review*, 28.1.2015.

[22] Rachel Botsman y Roo Rogers, «*What's Mine Is Yours: How Collaborative Consumption is Changing the Way We Live*», 2011.

[23] Fórum sobre el Futuro de la Privacidad (Future of Privacy Forum), «User Reputation: Building Trust and Addressing Privacy Issues in the Sharing Economy», junio de 2015.

[24] Véase el seminario de la Comisión Federal de Comercio de Estados Unidos, de 9 de junio de 2015, titulado «Competition, Consumer Protection, and Economic Issues Raised by the Sharing Economy», https://www.ftc.gov/news-events/events-calendar/2015/06/sharing-economy-issues-facing-platforms-participants-regulators/ (acceso de 10.9.2015).

[25] Sobre las implicaciones de la protección de datos de las aeronaves no tripuladas o de los sistemas de aeronaves pilotadas a distancia, véase el dictamen del SEPD relativo a la Comunicación de la Comisión al Parlamento Europeo y al Consejo «Una nueva era de la aviación - Abrir el mercado de la aviación civil al uso civil de sistemas de aeronaves pilotadas de forma remota de manera segura y sostenible», noviembre de 2014.

[26] Fuente: Boston Consulting Group.

[27] Gartner.

[28] El algoritmo de reconocimiento facial DeepFace de Facebook ha registrado un 97 % de éxito - superando a las personas; DeepFace: Closing the Gap to Human-Level Performance in Face Verification, publicado en el informe de la Conferencia del IEEE sobre visión computacional y reconocimiento de patrones, junio de 2014.

[29] Los robots han sido definidos como «máquinas situadas en el mundo que sienten, piensan y actúan»; Bekey, G, «Current trends in robotics: technology and ethics, in Robot Ethics - The ethical and social implications of robotics», The MIT Press2, 2012, p. 18. Se estima que entre 2013 y 2016 se habrán vendido veintidós millones de robots de servicio, Informe IRF World Robotics, 2013. Sobre inteligencia artificial, véanse Rise of the Machines, Economist de 9.5.15 y Pew Research Centre Internet Project 2014. En 2014, una empresa de inteligencia artificial condicionó su adquisición, por parte de una empresa tecnológica líder, al hecho de que se creara un consejo ético y de seguridad, así como que se prohibiera el uso del trabajo de IA para fines militares o de inteligencia; Forbes, «Inside Google's Mysterious Ethics Board», 3.2.2014.

[30] Pentland, *Social physics*, p. 147.

[31] Véase la nota 9 *supra*. Pentland *Social Physics* p.153: «Son posibles grandes avances en asistencia sanitaria, transporte, energía y seguridad... los principales obstáculos para conseguir estos objetivos son los problemas relacionados con la intimidad y el hecho de que todavía no se ha alcanzado un consenso sobre las posibles compensaciones entre los valores personales y los valores sociales». El debate en torno a la pandemia del ébola de 2014 en África Occidental es un ejemplo de cómo se perfila esta falsa dicotomía entre la intimidad individual y las necesidades de la sociedad. Se ha tendido a dar seguimiento a las enfermedades y medir su ciclo de vida a través de encuestas y censos que fácilmente quedan obsoletos y son difíciles de extrapolar para anticipar dónde se manifestará el próximo brote. Hay algunos ejemplos de uso de los «macrodatos» de seguimiento de los brotes de malaria en Namibia y Kenia y en 2009 para realizar el seguimiento de la eficacia de las advertencias sanitarias del gobierno durante la crisis de la gripe porcina en México. Una fuente de datos son los registros de llamadas desde móviles que muestran la estación de base que gestiona la llamada y que pueden facilitar en tiempo real una aproximación general de la ubicación de las personas y hacia dónde se dirigen. La recopilación de todos estos registros no tiene carácter específico, por lo tanto no permite distinguir entre quienes están y quienes no están infectados por el ébola. Una organización sin ánimo de lucro sueca registró la movilidad de la población en África Occidental pero los datos no fueron utilizados porque los operadores de telefonía móvil no los comunicaban a investigadores externos autorizados, so pretexto de que debían recibir instrucciones de los gobiernos, quienes, a su vez, habían expresado preocupaciones en relación con la intimidad que no podrían garantizarse en virtud de la legislación de la UE http://www.pri.org/stories/2014-10-24/how-big-data-could-help-stop-spread-ebola. (acceso de 10.9.2015)

[32] Dictamen 3/2015 del SEPD.

[33] Un supuesto sobre los macrodatos es que «N=all» se refiere a la observación de todos los puntos de datos, no solo una muestra, Viktor Mayer-Schönberger, y Kenneth Cukier, *The Rise of Big Data: How it's changing the way we think about the world*, 2013 .El Consejo de Lisboa y el Instituto de Política Progresista han comentado que la optimización de la «densidad digital» incrementará la prosperidad, «la cantidad de datos utilizados per cápita en una economía» http://www.lisboncouncil.net/component/downloads/?id=1178 (acceso de 10.9.2015). El Grupo de trabajo internacional sobre protección de datos en las telecomunicaciones (conocido como «el Grupo de Berlín») ha propuesto excepciones a los principios que regulan la protección de datos en relación con los macrodatos; http://www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf. (acceso de 10.9.2015). El Foro Económico Mundial ha solicitado que la atención recaiga en el uso y no en la recopilación, así como

alejarse de la exigencia de consentimiento para la recopilación de datos personales; «Unlocking the Value of Personal Data: From Collection to Usage», 2013.

[34] Véase el Dictamen preliminar del SEPD sobre Intimidad y competitividad en la era de la obtención de datos masivos.

[35] El artículo 21 de la Carta de los Derechos Fundamentales prohíbe «toda discriminación, y en particular la ejercida por razón de sexo, raza, color, orígenes étnicos o sociales, características genéticas, lengua, religión o convicciones, opiniones políticas o de cualquier otro tipo, pertenencia a una minoría nacional, patrimonio, nacimiento, discapacidad, edad u orientación sexual». Para muchas de estas categorías de datos («que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, así como el tratamiento de los datos relativos a la salud o a la vida sexual») se refuerza la protección con arreglo al artículo 8 de la Directiva 95/46/CE.

[36] Respecto a la idea de los bienes comunes digitales, véase «Ambition numérique: Pour une politique française et européenne de la transition numérique», Consejo digital de Francia, junio de 2015 p. 276; Bruce Schneier aboga por la creación de «espacios públicos sin propietario» en Internet, como los parques públicos, *Data and Goliath*, pp. 188-189; Sandy Pentland defiende los «bienes comunes de datos públicos», *Social Physics*, p. 179. Sobre la evaluación de la seguridad de publicar conjuntos de datos agregados como datos abiertos, véase el Dictamen 06/2013 del Grupo de Trabajo del Artículo 29 sobre datos abiertos y reutilización de la información del sector público.

[37] «Während die Einzelnen immer transparenter werden, agieren viele Unternehmen hochgradig intransparent» http://crackedlabs.org/studie-kommerzielle-ueberwachung/info. Sobre la transparencia cualificada, véase, por ejemplo, Frank Pasquale: *The Black Box Society: The Secret Algorithms that Control Money and Information*.

[38] «Behind the technology that affects social relations lie the very same social relations», David Noble, «Social Choice in Machine Design: The Case of Automatically Controlled Machine Tools», en *Case Studies in the Labor Process*, ed. Andrew Zimbalist, 1979. Véase asimismo Judy Wacjman, *Pressed for Time: The Acceleration of Life in Digital Capitalism*, 2014 pp. 89-90; y Zuboff, «Big Other» (citado en la nota 3 *supra*).

[39] Véase el Dictamen 05/2014 sobre técnicas de anonimización, adoptado el 10 de abril de 2014 (WP 216).

[40] Sobre la excepción objeto de interpretación estricta a las normas de protección de datos para fines exclusivamente personales o domésticos, véase la sentencia del TJUE, en el asunto C-212/13 *František Ryneš contra Úřad pro ochranu osobních údajů.*

[41] El término prosumidor (productor-consumidor) fue acuñado por Alvin Toffler en *The Third Wave*, 1980. Respecto de un debate sobre el «entorno de prosumidores» y el modo en que este debería regularse, véase Ian Brown y Chris Marsden, *Regulating Code*, 2013.

[42] Dictamen del Grupo Europeo de Ética de las Ciencias y las Nuevas Tecnologías a la Comisión Europea: Ethics of Security and Surveillance Technologies (Ética de las tecnologías de seguridad y vigilancia), Dictamen nº 28 de 20.5.2015, p. 74 (versión española no disponible).

[43]Véase, por ejemplo, *Homer Economicus: The Simpsons and Economics*, ed. Joshua Hall, 2014.

[44] Con arreglo a la definición de error más conservadora, esto implica que 23 millones de estadounidenses registraron errores materiales en un informe de consumidor. El 5 % de los participantes en el estudio tenían errores que, una vez corregidos, mejoraron su puntuación crediticia de modo que podrían obtener crédito a un precio menor; Comisión Federal de Comercio, «Report To Congress Under Section 319 Of The Fair And Accurate Credit Transactions Act Of 2003», diciembre de 2012; Chris Jay Hoofnagle, «How the Fair Credit Reporting Act Regulates Big Data» (10 de septiembre de 2013). «Future of Privacy Forum Workshop on Big Data and Privacy: Making Ends Meet», 2013. Disponible en SSRN: http://ssrn.com/abstract=2432955.

[45] El Foro Económico Mundial considera los datos como activos valiosos de una persona cuyos derechos de posesión, uso y disposición pueden ser proporcionados a las empresas y los gobiernos como intercambio por los servicios. Véanse asimismo los recientes discursos del Vicepresidente Ansip de la Comisión, por ejemplo de 7.9.2015 en la reunión anual en Bruegel titulado «Productividad, innovación y digitalización: ¿cuáles son los desafíos de la política mundial?»: «Propiedad y gestión de los flujos de datos, uso y reutilización de datos. Gestión y almacenamiento de datos. Estos destacan sectores emergentes importantes como la informática en nube, Internet de las cosas y los macrodatos».

[46] «Así que, ¿quién tiene el derecho a utilizar la información y los datos que no pertenecen verdaderamente a una persona?. Esta es una cuestión que transciende las fronteras del comercio, la ética y la moral, planteando cuestiones de intimidad y protección de la intimidad». Al-Khouri, noviembre de 2012, http://www.academia.edu/6726887/Data_Ownership_Who_Owns_My_Data_036. Véase asimismo Margaret Jane Radin, «Incomplete Commodification in the Computerized World», en *The Commodification of Information 3*, 17, Niva Elkin-Koren & Neil Weinstock Netanel eds. 2002: «Es muy diferente que la intimidad se conciba como un derecho humano, concedido a las personas en virtud del hecho de ser humano, o como un derecho de propiedad, algo que las personas pueden tener como propiedad y pueden controlar. Los derechos humanos son presuntamente inalienables en el mercado, mientras que los derechos de propiedad se presumen alienables en el mercado.».

[47] El proyecto Crosscloud del MIT Computer Science and Artificial Intelligence Lab (Laboratorio de Inteligencia Artificial y de Ciencia de Informática del MIT) que recibió el apoyo de diversas empresas con sede en Europa tiene como objetivo: «a) facilitar el desarrollo de programas informáticos multiusuarios ("sociales") utilizando únicamente el desarrollo de aplicaciones para usuarios y respetando los derechos y la intimidad de los mismos. y 2) permitir a los usuarios la libertad de desplazarse fácilmente entre las aplicaciones, las plataformas de soporte físico y las redes sociales, manteniendo sus datos y las conexiones sociales»; http://openpds.media.mit.edu/#architecture (acceso de 10.9.2015).

[48] Véase la Explicación al artículo 1 de la Carta de los Derechos Fundamentales.

[49] Martha Nussbaum, «Objectification *(Objetualización)*», en *Philosophy and Public Affairs* 24, 4, 1995.

[50] Sentencia de 15 de diciembre de 1983, BVerfGE 65, 1-71, Volkszählung.

[51] Véase el Grupo europeo sobre ética en ciencia y nuevas tecnologías, Dictamen sobre ética y vigilancia, p. 75. Un estudio ha indicado que determinado algoritmo de publicidad dirigida era discriminatorio, ya que las búsquedas devolvían como promedio anuncios de empleos mejor remunerados para los hombres que para las mujeres que visitan las páginas web de empleo; Carnegie Mellon University e International Computer Science Institute Sobre la tendencia de dotar por defecto de voz femenina a los asistentes digitales, véase el ejemplo de Judy Wajcman, «Feminist theories of technology». *Cambridge Journal of Economics*, 34 (1). pp. 143-152, 2010.

[52] Giorgio Agamben, *State of Exeption, 2005.*

[53] Neil Richards, Neil y Jonathan King, «Big Data Ethics» (19 de mayo de 2014), *Wake Forest Law Review*, 2014.

[54] BBC, Information watchdog investigates «charity data sales», 1.9.2015.

[55] Véase la carta de Future of Life Institute. La encíclica papal *Laudato Si* reza: «los medios del mundo digital que, cuando se convierten en omnipresentes, no favorecen el desarrollo de una capacidad de vivir sabiamente, de pensar en profundidad, de amar con generosidad. Los grandes sabios del pasado, en este contexto, correrían el riesgo de apagar su sabiduría en medio del ruido dispersivo de la información. Esto nos exige un esfuerzo para que esos medios se traduzcan en un nuevo desarrollo cultural de la humanidad y no en un deterioro de su riqueza más profunda. La

verdadera sabiduría, producto de la reflexión, del diálogo y del encuentro generoso entre las personas, no se consigue con una mera acumulación de datos que termina saturando y obnubilando, en una especie de contaminación mental. Al mismo tiempo, las relaciones reales con los demás, con todos los desafíos que implican, tienden a verse sustituidas por un tipo de comunicación mediada por Internet. Esto permite seleccionar o eliminar las relaciones conforme a nuestro arbitrio, y de este modo suele generarse un nuevo tipo de emociones artificiales, que tienen que ver más con los dispositivos y las pantallas que con las personas y la naturaleza. Los medios actuales permiten que nos comuniquemos y que compartamos conocimientos y afectos. Sin embargo, a veces también nos impiden tomar contacto directo con la angustia, con el temblor, con la alegría del otro y con la complejidad de su experiencia personal. Por eso debería preocuparnos el hecho de que, junto con las interesantes posibilidades que ofrecen estos medios de comunicación, se desarrolla una profunda y melancólica insatisfacción en las relaciones interpersonales, o un dañino aislamiento.».

[56] Véase la acción nº 4 de la Estrategia 2015-2020 del SEPD titulada «Desarrollar una dimensión ética de la protección de datos».