ECONOMÍA DIGITAL

Una aproximación a la economía de los datos y su regulación

Javier Alonso / Carmen Cuesta Sainz / Santiago Fernández de Lis / David Tuesta

1. Introducción

Los cambios acelerados en la era digital acontecidos en los últimos años han traído consigo la disponibilidad de sistemas de almacenamiento de datos de gran capacidad y nuevas capacidades tecnológicas de procesamiento de información, a precios muy inferiores a los observados a finales del siglo pasado. Al mismo tiempo, el despliegue de las infraestructuras de telecomunicaciones de última generación están ampliando su cobertura por todo el mundo a pasos agigantados, acercando el uso de la tecnología a individuos, empresas y organismos públicos. Su consumo supone la generación de información digital en volúmenes que crecen exponencialmente.

Todo este cúmulo de información generada en diversos canales contiene en gran medida datos considerados de carácter personal, provenientes no sólo de información contextual, o datos pre-procesados y estructurados, sino también de trazas, huellas de conexión y rastros de la navegación por internet del individuo. En la medida que estos datos de carácter personal son útiles tanto para las empresas, al mejorar su propuesta de valor, como para los consumidores, que reciben beneficios directos o indirectos de las innovaciones y customizaciones que su uso proporciona, se va configurando una interacción de alta intensidad con los datos, lo que plantea retos tanto al funcionamiento de los mercados como a su regulación.

Así, los datos de carácter personal que forman parte de la privacidad de los individuos, y las circunstancias en las cuales sus datos son recabados, tratados o cedidos, se encuentran reguladas en prácticamente todas las geografías. Sin embargo, la forma como se ha venido desarrollando la economía digital y los nuevos espacios donde esta información circula y se comparte, han planteado debate respecto a la forma en la que está implementada la regulación y los consecuentes costos-beneficios económicos. Este punto, constituye el eje del presente informe, que tiene como objetivo brindar una visión conceptual -con elementos de la regulación, tecnología y economía- del tratamiento de los datos y su implicación en la privacidad de los individuos.

Tras esta introducción, en el punto 2 resaltamos cómo los datos de carácter personal tienen un potencial valor de intercambio, tanto para las empresas como para los consumidores. En el punto 3, nos aproximamos desde una perspectiva económica a la explotación de la información de carácter personal, intentando identificar las diferentes aristas y retos que plantea su funcionamiento y la regulación. A partir de la perspectiva económica planteada en el punto anterior, discutimos en la sección 4 la regulación vigente, destacando las más representativas en los Estados Unidos y Europa, subrayando algunas líneas de acción que pueden ser relevantes para el futuro. El estudio, finalmente presenta las conclusiones en la sección 5.

Agradecimientos [1]

2. La era digital y el valor de los datos personales

2.1 El valor de los datos personales para las empresas

La información personal referente a preferencias, deseos y necesidades de los consumidores ha sido explotada por las empresas para mejorar sus resultados desde principios de los años 70, cuando comenzaron a desarrollarse con mayor intensidad las estrategias de mercado que acabarían influyendo en todo el proceso productivo. Ya entonces existían diversos factores que permitían a las firmas mejorar sus resultados mediante el uso de la información sobre los hábitos de consumo de sus clientes como un input productivo más. (Bailey, 1998; Biljsma et al, 2014; Dayal, 2001).

La cantidad de información personal disponible en formato digital es sin embargo mucho mayor en la actualidad. Según la consultora IDC (2012) el universo digital se está duplicando cada dos años y se multiplicará por diez entre 2013 y 2020, llegando a 44 billones de gigabytes. Gran parte de este volumen de información contiene datos desagregados de los individuos referentes a sus preferencias, hábitos, características y comportamiento y gracias a las nuevas tecnologías enmarcadas en el concepto de “Big Data”, es posible extraer, procesar, ordenar y clasificar la información necesaria para segmentar a los consumidores por un número ilimitado de variables antes impensables.

El crecimiento exponencial del volumen de información personal en línea se debe en parte a las grandes empresas tecnológicas que han surgido en los últimos años ofreciendo servicios digitales gratuitos a los consumidores finales, tales como, accesos a redes sociales, buscadores online, correo electrónico, almacenamiento de ficheros y fotografías, etc en los que se maneja gran cantidad de información personal. La globalidad con la que operan y el éxito de la simplicidad e innovación en sus servicios, les confiere una cuota de mercado muy elevada y les permite basar su modelo de negocio en ofrecer a terceros el conocimiento de sus usuarios, generalmente a través de espacios publicitarios, construyendo un plan empresarial que puede arrojar grandes beneficios. De esta forma, los datos de carácter personal de los clientes no sólo ayuda a las empresas a mejorar su propia productividad, sino también la de terceros, incrementando así el valor de los datos personales.

Dicho incremento en el valor de los datos personales es aún mayor cuando se comparten y cruzan datos de distintos orígenes, pues permite la aparición de nuevos e innovadores servicios. Así por ejemplo, conociendo la geolocalización de un consumidor a partir de su teléfono móvil y sus hábitos de consumo, se le podría presentar un producto según el consumidor se aproxima a un comercio incluso proponerle una financiación online para su adquisición, si se conoce también su historial crediticio. Según BCG (2012), la construcción de servicios basados en datos personales, puede llegar a aportar beneficios económicos al sector público y privado de hasta 333.000 millones de euros en 2020 (asumiendo una tasa de crecimiento anual del 22%) .

La información personal se convierte así en un bien con un valor transaccional relevante para las empresas ya que (i) ayuda a mejorar su proceso productivo y/o (ii) se convierten en una “materia prima” para construir nuevos productos y servicios.

2.2 El valor de los datos personales para el consumidor

La disponibilidad de la banda ancha fija y móvil a precios cada vez más asequibles, así como la creciente penetración de dispositivos móviles, han permitido que un porcentaje elevado de la población tenga acceso a nuevas fuentes de información, beneficiándose de servicios digitales antes

impensables. Dichos servicios se caracterizan por su inmediatez y su accesibilidad desde cualquier lugar y en cualquier momento y en la mayor parte de las ocasiones, se proporcionan al usuario sin coste directo asociado, más allá de la propia conexión a las redes de telecomunicaciones. Un ejemplo que ilustra este fenómeno son las redes sociales que permiten a los usuarios comunicarse entre sí y compartir todo tipo de información. Facebook tiene más de 800 millones de usuarios que acceden a diario a su perfil en el mundo, 1.280 millones que acceden mensualmente y genera una media de 1.500 actualizaciones por segundo.

Cabe destacar que una gran parte de la información disponible en el mundo digital es aquella que los usuarios comparten sobre sí mismos. Según la consultora IDC (2012), un 68% de la información generada en Internet en 2012 fue creada y consumida por usuarios finales a través de su interacción en redes sociales, correo electrónico, almacenamiento en la nube de fotografías, documentos y vídeos, entre otros. Según los datos de Eurostat, sólo en la UE, el 24 % de la población utiliza Internet para subir información a la red y en algunos países como Portugal y Dinamarca, el porcentaje se eleva hasta casi el 48%

Además de la información de carácter personal que los propios usuarios publican, la red contiene datos que permanecen publicados sine die, tales como aquellos referentes a documentos públicos, prensa digital, comunicaciones, conversaciones y comentarios en foros. Los usuarios dejan rastro también en los sensores de telecomunicaciones y en los navegadores sobre sus visitas y hábitos de navegación. Por otro lado, los servicios digitales manejan, almacenan y procesan también información personal sobre las interactuaciones de los usuarios: accesos, búsquedas, visitas, compras o pagos electrónicos.

Así, dado el grado de conocimiento que se puede obtener de la persona tras cruzar datos de distintos orígenes y dependiendo del uso que se realice de los mismos, los usuarios pueden percibir que su derecho a la intimidad y a la privacidad se ve quebrantado. Al respecto, recientemente se ha generado debate en relación al uso de los datos personales compartidos a través de Facebook, al revelarse que las interacciones de los usuarios hechas en 2012 estuvieron sometidas a experimentos para investigar el contagio de las emociones on line (Kramer et al., 2014). Si bien Facebook ha venido advirtiendo a sus usuarios respecto al aprovechamiento de su información con fines de investigación, y los usuarios supuestamente han dado su consentimiento previamente -quizá la mayoría han aceptado el aviso sin leerlo o sin brindarle mucho interés- los miembros de la comunidad científica de los Estados Unidos enfatizan que cuando se realizan experimentos de comportamiento, la manera de advertir a las personas tiene que ser más personal, detallada y exhaustiva siguiendo lo establecido por los Principios y Guías para la Protección de los Seres Humanos Sujetos a Investigación (The National Commision for the Protection of Human Subject of Biomedical and Behavioral Research, 1979).

Ahora bien, la percepción de una invasión a la privacidad podría tener un elemento de subjetividad y quizá diferir de unos individuos a otros, dándose numerosos casos incongruentes en los que la concienciación en privacidad puede ser muy elevada y sin embargo el individuo expone sus datos sin vacilación (Acquisti et al. 2013; Acquisti et al. 2010; BCG, 2012). Esta situación sostiene la idea de que, en muchas ocasiones, el individuo “vende” su información personal para acceder a un servicio o recibir una compensación, pero no es totalmente consciente del posterior tratamiento de sus datos. Quizá uno de los experimentos recientes más interesantes en el campo académico es de Acquisti et al (2013) en el que se observa la manera como los consumidores ponen un valor monetario al compartir sus datos personales, cuando se les ofrece una cantidad que ellos consideran adecuada. Acquisti (2004) ya adelantaba la idea de la existencia de una preferencia por aceptar la entrega de información personal por parte del individuo para acceder a un servicio o recibir una compensación de forma inmediata, en

contraposición a su disposición a proteger sus datos, que requiere una mayor reflexión. Por su parte, Varian (1996) señalaba también, en los albores de Internet, que las personas tienen diferentes sensibilidades respecto a que se conozcan determinados datos privados. Por ejemplo, menciona que existen aspectos que los individuos no quieren que se hagan públicos (como pueden ser sus datos financieros), mientras quizá tengan mayor tolerancia a que se conozca su número de teléfono o su dirección postal, salvo que como consecuencia de esto último, termine experimentando algún tipo de molestia, como puede ser el hecho que se les "asalte" con información comercial no solicitada. Sobre esto último, el propio Varian (2005) encontraba para los Estados Unidos que esta sensación de molestia debido a asaltos comerciales, variaba dependiendo de las características sociodemográficas de los individuos.

En cualquier caso, consciente o inconscientemente, los datos de carácter personal se pueden terminar convirtiendo en un instrumento de cambio, reportando con ello al individuo diferentes beneficios y/o perjuicios. Acquisti (2010), Goldfarb and Tucker (2011) y Athey (2014) resumen en gran medida estos beneficios netos y los condicionantes a los que se enfrenta el consumidor:

- Si adquiere un producto que ha sido seleccionado y diseñado especialmente para él a partir de su información personal, es muy posible que mejore su utilidad con su uso/consumo, ya que sería aquel que maximizará el valor de sus preferencias.

- La prestación de servicios a la medida, a partir de información personal, mejora la experiencia de usuario. Así por ejemplo, una vez que un servicio de indicación de itinerarios conoce la geo-localización del dispositivo (y por ende del usuario) es capaz de rediseñar la ruta más óptima para llegar a un destino cada vez que nos salimos de la ruta inicial.

- La facilidad con la que recibe la propuesta comercial y su adquisición le puede ahorrar costes de búsqueda, lo que haría aumentar de nuevo su utilidad.

- Por otro lado, la posibilidad de que las empresas pudieran mejorar su discriminación de precio a los clientes en función de su riesgo, en productos como por ejemplo los de seguro, podrían mejorar de nuevo el nivel global del bienestar de los consumidores mediante dos vías alternativas. Así, en el caso de los seguros de automóviles, los conductores más prudentes verían mejorar notablemente el precio de su póliza debido a que las empresas serían capaces de medir mejor su menor nivel de riesgo. Al mismo tiempo, los conductores más infractores, al aumentar el precio de la póliza debido a su perfil de mayor riesgo, se verían desincentivados a seguir manteniendo ese comportamiento, reduciendo tanto su nivel de riesgo, como la del resto de ciudadanos.

- El individuo puede experimentar algún tipo de discriminación en algún mercado por revelaciones de su comportamiento personal (bueno o malo), o algún hecho del pasado que siga circulando, a pesar de haber pasado un tiempo razonable durante el cual la persona pueda haber experimentado un cambio (Mayer-Schönberger, 2011). Este razonamiento estuvo detrás de la decisión del Tribunal de Justicia de la Unión Europea respecto al derecho a que determinada información de carácter personal inadecuada u obsoleta sea retirada de los buscadores y al que se refiere el término "derecho al olvido". (Tribunal de Justicia de la Unión Europea, 2014).

- El individuo puede querer interactuar libremente por internet, pero se ve amenazado por el potencial daño que una filtración de sus datos o un robo de su identidad puede dañar su reputación o intimidad.

- También están las ganancias indirectas que puede tener el individuo a partir del mayor conocimiento de determinadas situaciones que le ayuden a decidir mejor a partir del análisis que otros hagan de datos de carácter personal. Por ejemplo, la explotación de la información personal por parte del periodismo, algún centro de investigación o institución, cuyas conclusiones se hagan publicas.

- En otro extremo, acontecen también situaciones en las que el aprovechamiento de datos personales por parte de las centrales de inteligencia nacionales, para mejorar la seguridad de un país (por ejemplo para evitar un ataque terrorista), podría ser valorado positivamente por una proporción importante de personas y empresas.

En general, siguiendo a Bijlsma et al. (2014) y Varian (1996), ***las personas podrían sentirse cómodas con el tránsito de su información privada en la web, dependiendo del uso que se le dé, el control que tengan sobre ella y los beneficios que puedan obtener*.** Detrás de todos estos aspectos que circunscriben la interacción entre diferentes actores sobre los datos de carácter personal, dos elementos claves son la manera como los agentes económicos interactúan en los mercados, y el marco jurídico y normativo que se conforma. Ambos aspectos se irán abordando en las siguientes secciones.

2.3 Oportunidades que ofrece la explotación de datos de carácter personal en la banca

La banca ha sido uno de los pioneros en la gestión de bases de datos de clientes con el fin de proporcionar servicios financieros tanto de ahorro y crédito. 30 años atrás, un visionario de la industria bancaria señalaba que “la banca era sólo bits and bytes” (Skinner, 2014). Los datos personales proporcionados por los clientes para la obtención de determinados servicios financieros ha sido en gran medida la base para conformar los historiales de crédito, para evaluar de la idoneidad del cliente financiero de acuerdo a los estándares regulatorios de blanqueo de capital, así como para generar la oferta de nuevos productos. En esta era digital, la gestión de la información de los clientes se toma un valor central de cara a hacer más eficientes los servicios en favor de los diferentes actores que actúan en el ecosistema financiero. A continuación mencionamos, a modo de ejemplo, dos áreas que podrían beneficiarse de un mayor uso de la información de clientes.

Procesos de rating y scoring

Los procesos de evaluación de la solvencia, previos a la concesión de un crédito, pueden verse mejorados al incorporar variables nuevas provenientes de Internet relacionados con la reputación social (de un individuo o de una empresa) o la información pública ofrecida por los Estados (concesiones, resoluciones, etc).

Atendiendo variables cualitativas es posible ofrecer otra visión del riesgo. Datos como el número de conexiones en LinkedIn o de contactos en otras redes sociales- en el caso de individuos- o el número de visitas a una Web, el número de “me gusta”, las referencias positivas, etc. - en el caso de un comercio electrónico- parecen destinados a convertirse en nuevos indicadores a introducir en los modelos de riesgo. Con ello, no se trata de sustituir los modelos analíticos tradicionales basados en la información histórica del comportamiento crediticio del cliente sino más bien de completarlos con variables de información puramente digital que complementen al perfil de riesgo del sujeto.

No obstante, es preciso señalar que a pesar de la accesibilidad de los datos obtenidos de las redes públicas, estos pueden ser fácilmente falsificables, y por tanto no ofrecer una alta garantía. Lo cierto es que esta información digital se torna más útil cuando se aplica a sujetos de los que apenas se tiene información cualitativa relacionada con su historial de crédito. De hecho, existen ya instituciones de crédito pioneras en la utilización de datos sociales digitales para la evaluación del riesgo como Neo

Finance (Palo Alto, California) o Lenddo (Hong Kong), Kreditech (Alemania, operando también en Polonia y España) o MovenBank.

Sin embargo, existe cierta controversia al aplicar estas técnicas a individuos físicos, ya que algunos sectores interpretan que estas actividades pueden transgredir la privacidad de los individuos. A mediados del año 2012, la Schufa, entidad encargada de recoger el historial de crédito de los residentes alemanes, tuvo que abortar el proyecto encargado al Instituto Hasso Plattner de evaluar en qué medida la información pública de la red puede contribuir a mejorar la solvencia de los consumidores. Las presiones de las asociaciones de consumidores apoyadas en la legislación alemana en temas de privacidad fueron determinantes.

Lucha contra el fraude

Otro proceso bancario que se ve beneficiado por el impulso de Big Data es el de la gestión del fraude. Las técnicas de prevención y lucha contra el fraude tienen dos ópticas: (i) a través de protocolos de identificación y autenticación para validar la identidad del cliente (ii) mediante el monitoreo de las operaciones del mismo para identificar movimientos ilícitos.

La monitorización de movimientos y operaciones realizadas a través de tarjetas financieras es una actividad ya muy extendida en la que se utilizan técnicas de Data Mining y sistemas de inteligencia artificial basadas en redes neuronales que aprenden de datos históricos para el reconocimiento de patrones de fraude. El aumento de capacidad de procesamiento que ofrecen los servicios de cloud y las nuevas tecnologías de Big Data permite incorporar a la monitorización un número mayor de variables que enriquecen el sistema ofreciendo mejores estimaciones de la probabilidad de que una operación es fraudulenta.

Por otro lado, mediciones sobre la velocidad de tecleo, los hábitos de acceso a determinadas páginas Web como horarios o dispositivos desde los que se conecta el individuo, incluso cómo maneja el ratón o cómo interactúa con un dispositivo móvil, conforman un patrón que permite autenticar a un individuo de forma muy poco intrusiva ofreciendo una experiencia al usuario más amigable.

3. La teoría económica, la privacidad de los datos y la interacción de los agentes

Beneficios del mercado de datos de carácter personal

Algunos de los experimentos comentados, como el de Acquisti (2013), parecen confirmar el valor transaccional de los datos de carácter personal. Los consumidores pueden obtener beneficios directos e indirectos por su entrega, mientras que las empresas cuentan con ello para incrementar valor a la actividad de la firma. Sin embargo, una aproximación económica a los mercados, donde los datos de carácter personal circulan por diferentes vías, nos indica que existen varias dimensiones de análisis que intentaremos abordar.

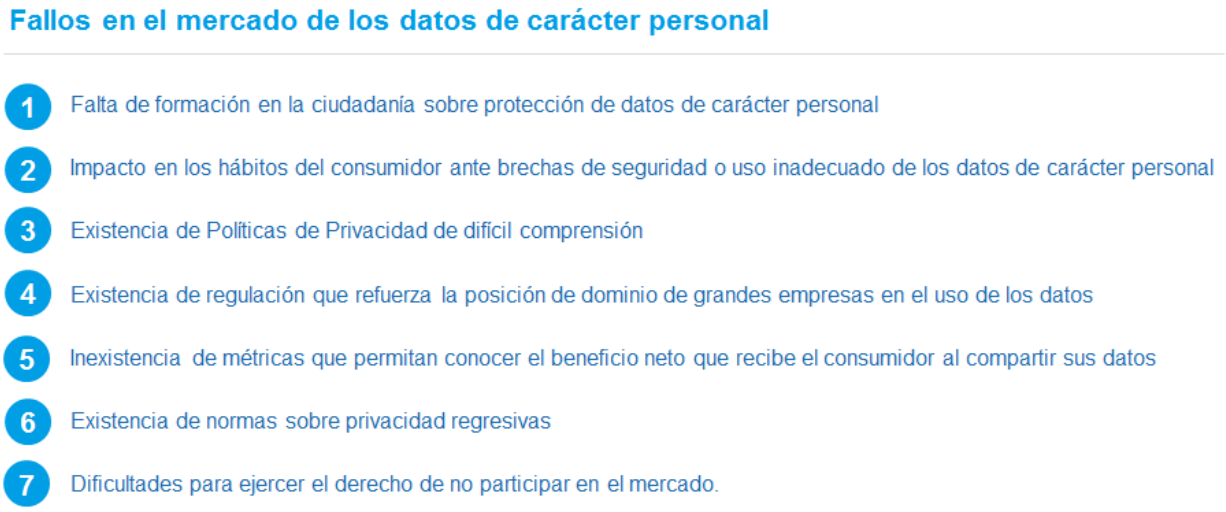
En la medida en que los datos de carácter personal tengan un valor económico para las empresas, estos pueden ser transaccionados en un mercado organizado y regulado. La teoría económica nos muestra que el mercado de competencia perfecta es aquel en el que se maximiza el denominado “excedente” del productor y del consumidor, siendo esta solución de equilibrio eficiente y pareto óptima. Si el bien llamado “datos de carácter personal” fuera transaccionado en un mercado primario en competencia perfecta, se entiende que se alcanzaría este equilibrio en tanto ofertantes y

demandantes maximicen su bienestar. En el caso de este hipotético mercado de datos de carácter personal, la oferta estaría representada por los ciudadanos, mientras que la demanda estaría representada por las empresas.

Más allá de los beneficios individuales en un mercado de competencia, existiría un elemento distintivo como consecuencia de compartir masivamente los datos de carácter personal en el mercado, lo cual incrementa más aún el bienestar de las personas y la sociedad. Es lo que se conoce en la teoría económica como externalidad de redes, entendida como el incremento en la utilidad derivada del uso de un producto cuando aumenta el número de gente que usa este producto. Es decir, cada usuario adicional confiere un beneficio extra a los ya existentes (Economides, 1996; Shapiro y Varian, 1999; Liebowitz, 2002; entre otros). Los beneficios directos se derivan de la interacción entre usuarios mientras que los indirectos son los derivados de los productores quienes, movidos por los efectos de escala, tienen el incentivo a desarrollar nuevos bienes y servicios compatibles con dicha tecnología. En la era digital, es justamente este fenómeno económico el que explica los beneficios de una mayor participación en la web, donde se comparte información que las personas encuentran útil, siendo quizá las redes sociales tales como Facebook o Twitter uno de sus principales referentes. En estas redes sociales, además de informarse de manera directa entre unos y otros, existen algoritmos generados por estas empresas que brindan una mejor selección o recomendación de servicios y productos de acuerdo a sus preferencias, lo que amplía la experiencia de la personas y por tanto lo lleva a alcanzar una mayor satisfacción. Y el tema de las externalidades de redes no queda solamente en las redes sociales, pues es justamente esta mayor participación de las personas con sus datos personales lo que viene permitiendo grandes desarrollos en diferentes campos e industrias, y mencionábamos anteriormente cómo nuevos actores financieros han podido ampliar la oferta de créditos a nuevos segmentos de la población en base al análisis de esta ingente cantidad de datos personales, brindándoles mayores oportunidades de crecimiento.

Fallos en el mercado de datos de carácter personal

Independientemente de los beneficios que un mercado de datos de carácter personal puede aportar a la sociedad, existen numerosos elementos que provocan la existencia de fallos de mercado que lo alejan de un funcionamiento de competencia perfecta.



Falta de formación en la ciudadanía sobre protección de datos de carácter personal

Por ejemplo, muchos consumidores no están suficientemente informados respecto a cómo proteger sus datos de carácter personal y no logran entender los riesgos y beneficios de las políticas de privacidad, y condiciones de uso existentes en el mercado (Athey , 2014). Más aún, McDonald y Cranor (2008) estiman que un usuario americano de internet medio gastaría 201 horas al año sólo leyendo las Políticas y Avisos de privacidad antes de dar su consentimiento. Esta situación se complica más con la existencia de múltiple regulación sectorial y local, dependiendo del ámbito geográfico o que aplique, lo que genera que, el público general e incluso los más expertos, no puedan entender cómo los gobiernos y otras entidades hacen uso de los datos. Cuando los escándalos de pérdida o uso ilícito de la información se publican en la prensa, los usuarios no tienen claro si las organizaciones involucradas están siguiendo las mejores prácticas ni si cumplen la regulación vigente en toda su extensión, dado que esta información no suele ser de carácter público. Esto puede generar una indefensión en el consumidor

Impacto en los hábitos del consumidor ante brechas de seguridad o uso inadecuado de los datos de carácter personal

Otro factor que resaltan Goldfarb y Tucker (2011), Tsai et al. (2011), Athey (2014) y Acquisti (2013), es la reacción que en la práctica tiene el consumidor en el mercado cuando se producen escándalos revelados en prensa respecto a una inadecuada gestión de los datos de carácter personal. Es decir, es difícil conocer sus percepciones en el corto y mucho más aún en el largo plazo, donde se requerirían realizar experimentos longitudinales. Algunas pistas se han observado con el trabajo de Goldfarb y Tucker (2011), que han encontrado una reacción de “retirada” o de comportamientos más cautos en la web, por parte de los usuarios cuando se conocen casos de fugas de información. Lamentablemente, esto no permite captar hipótesis relacionadas con los cambios de percepción entre generaciones.

Existencia de Políticas de Privacidad de difícil comprensión

Una interesante puntualización de las fallas de mercado en el mundo de los datos de carácter personal lo señala Athey (2014) al hacer gráfico que muchos de los mercados de productos tecnológicos son altamente concentrados y los consumidores no terminan de comprender claramente las diferencias entre las distintas políticas de privacidad de servicios equivalentes. Por ejemplo, las formas en que se comunican las Políticas de Privacidad, así como las cláusulas de información y consentimiento al usuario no pueden ser fácilmente valorables si no existe una alternativa comparable en otro producto. Además, advierte la investigadora, si el usuario ha invertido mucho tiempo en aprender y familiarizarse con una aplicación, se le hace luego difícil moverse a otro servicio cuando la Política de Privacidad del producto que usa ha cambiado; y es más, no tiene cómo enterarse de que la Política de Privacidad del servicio alternativo/competidor ha cambiado también. Por tanto, el incentivo para el consumidor de penalizar a la firma por su inadecuada Política de Privacidad es muy bajo.

Existencia de regulación que refuerza la posición de dominio de grandes empresas en el uso de los datos de carácter personal

Respecto al punto anterior, algunas posiciones afirman que es la propia regulación la que termina distorsionando más el mercado. Athey (2014) muestra que las Políticas de Privacidad pueden limitar el desarrollo de nuevos “ventures” en el mercado y con ello limitar la competencia. En línea similar, Campbell et al (2013) afirma que la regulación actual podría estar reforzando la posición de dominio de

las grandes empresas que utilizan datos de carácter personal, dificultando la incorporación de nuevos actores en el mercado.

Inexistencia de métricas que permitan conocer el beneficio neto que recibe el consumidor al compartir sus datos

Es casi imposible, en la vida real, calcular cuál es el beneficio neto del consumidor por compartir o no los datos de carácter personal. En el caso de las Políticas de Privacidad, por ejemplo, no se podría saber ni medir de una manera coherente los supuestos beneficios que generan las mismas. Como señala Athey (2014), es imposible medir algo que el consumidor no entiende; es más, se observan situaciones que llaman la atención cuando algunas afirmaciones desde diferentes ámbitos, advierten de la incomodidad que manifiestan las personas ante la presencia de avisos comerciales personalizados en base a su información del correo, pero al mismo tiempo estas compañías siguen incrementando sus ganancias por el uso de estas prácticas. Veíamos en la sección 2 que los trabajos de Acquisti (2013) y Varian (2005) encontraban que la percepción de los mayores o menores beneficios por parte del consumidor del uso de sus datos personales era dependiente del contexto. Por tanto, esta situación hace también muy complicado plantear políticas de regulación de aplicación homogénea.

Existencia de normas sobre privacidad regresivas

Relacionado también con el punto anterior, es interesante llamar la atención de que las regulaciones sobre privacidad pueden llegar a ser regresivas. Athey (2014) encuentra que en muchos casos la regulación sobre los avisos comerciales on-line afectan a la publicidad de los llamados productos de acceso libre (o gratuitos), que son justamente aquellos más apreciados por las personas de bajos ingresos, por los estudiantes y por los pequeños negocios. En un ejemplo, Miller y Tucker (2011) encuentran que en el caso de los estados de los Estados Unidos que adoptaron las Políticas de Privacidad más estrictas, redujeron la adopción de los sistemas de registros electrónicos médicos, lo que trajo como consecuencia el incremento de la mortalidad infantil, especialmente en los grupos de menores ingresos, y sobre todo en las mujeres. Un claro ejemplo de políticas que persiguen buenas intenciones pero que traen malos resultados.

Dificultades para ejercer el derecho de no participar en el mercado

Es necesario garantizar el derecho de cualquier ciudadano a no participar en el mercado si dentro de sus preferencias está el no hacerlo, es decir, no debe haber barreras de entrada ni de salida del mercado. Como veíamos anteriormente, en Internet se asocia por ejemplo al “derecho al olvido” que recientemente ha producido una sentencia en Estrasburgo contra Google (Tribunal de Justicia de la Unión Europea, 2014) que asegura a los ciudadanos la posibilidad de exigir la eliminación de cierta información personal obsoleta y/o no apropiada susceptible de ser rastreada por el buscador.

En general, se puede observar que las fallas existentes en los mercados de uso de datos de carácter personal lleva a soluciones que no son las mejores para los agentes que interactúan en ellos, alterando los beneficios netos que se podrían esperar para la sociedad de un uso idealmente correcto. Hemos visto también que estos hechos, que justifican claramente la intervención del regulador, sobre todo teniendo en cuenta que el derecho a la intimidad y a la privacidad es un derecho universal, lleva a soluciones que no son las mejores; ¿Qué contenidos tiene la regulación actual? ¿Qué vías de mejora se pueden observar? Discutimos esto en el siguiente apartado.

4. La regulación en materia de privacidad

4.1 Elementos característicos de la regulación relevante en derecho a la intimidad y protección de datos de carácter personal

La Privacidad está considerada en el artículo 12 de la Declaración Universal de Derechos Humanos (1948), en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (1966), además de otros muchos tratados internacionales y regionales de Derechos Humanos. Prácticamente todos los países en el mundo incluyen el derecho de privacidad en su Constitución, regulando la relación entre los Estados, los organismos públicos o privados, y los ciudadanos con respecto a su derecho a la privacidad y protección de datos de carácter personal.

Si bien la preocupación de la privacidad tiene un largo recorrido histórico, fue a finales de los 80, principios de los 90, ante los primeros avances en el despliegue de las nuevas tecnologías informáticas, cuando la sociedad se puso en alerta sobre la exposición de su privacidad. Las redes de comunicación favorecían la transmisión de información entre lugares alejados y las grandes computadoras eran capaces de procesar grandes volúmenes de información. Hoy en día, la evolución tecnológica ha aumentado exponencialmente las capacidades de interconexión de información lo cual puede redundar en la posibilidad de configurar un perfil exhaustivo de la persona.

Europa

Europa es la región que más ha desarrollado la regulación en materia de privacidad de la información y protección de los datos de carácter personal de sus ciudadanos, respetando de forma íntegra los principios de la OCDE (1980). En 1995 se publicó en Europa la "Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los datos" con el objetivo de armonizar las regulaciones nacionales y establecer unos principios comunes que facilitaban la creación del Mercado Único europeo. Se permitían así los flujos de información entre los países miembros en un contexto de protección de los derechos de los consumidores, impidiendo esta circulación hacia países donde no se cumplían los requisitos de protección adecuados. La Directiva y las guías de la OCDE han sido también fuente de inspiración para regulaciones en otros continentes. De esta forma, otras geografías obtienen un nivel equiparable de protección, asimilable al Europeo, bajo la cual se permite la transferencia de datos desde Europa, no obstaculizando así, el comercio entre distintas áreas geográficas.

Estados Unidos

Los reguladores de la Unión Europea y los de los Estados Unidos han mantenido posturas muy distintas en el desarrollo del marco jurídico en materia de protección de los datos de carácter personal de sus ciudadanos y privacidad. Mientras que en Europa se ha puesto el foco en arbitrar todos los supuestos en los que se traten datos de carácter personal, en los Estados Unidos existen numerosas normas estatales y nacionales que afectan sectorialmente a las industrias que tratan datos más sensibles, como los financieros, los de salud o los relativos a menores.

En el caso de EEUU, y a pesar del impacto que supuso la implementación de la Directiva europea para las empresas estadounidenses con presencia en Europa, las iniciativas de implementar una regulación similar se vieron descartadas a favor de fomentar la innovación en un mundo cada vez más digital y en el que los datos personales son el insumo sobre el que giran los nuevos negocios. Gracias, en parte, a la libertad con la que las empresas estadounidenses nacieron y han ido desarrollando la utilización de

los datos de sus clientes, han aparecido grandes empresas tecnológicas como Google, Facebook, YouTube, Twitter o Groupon que basan su modelo de negocio en la publicidad online a partir del perfilado que obtienen de sus usuarios. Ahora bien, esta aproximación únicamente sectorial ha coadyuvado a la creación de espacios en el sistema que permite a nuevas empresas digitales, facilitar servicios y aplicaciones propios de otras industrias, que por su naturaleza jurídica sí están sujetas a los preceptos de la legislación, hecho que implica un contraste entre las realidades regulatorias de ambas regiones en el mundo.

4.2 Vías de mejoras de la regulación en una perspectiva global

Conceptualmente la regulación que se establezca sobre la privacidad y la protección de los datos de carácter personal debería reunir una serie aspectos que cumpla con las expectativas de los agentes económicos. Por un lado, algunos consumidores desean poner en valor su información y que esta sea bien gestionada y salvaguardada. Por otro lado, las empresas desearían utilizar dicha información para su proceso productivo con las menores fricciones, en un contexto regulatorio equilibrado para consumidores y firmas, que les permita contribuir con el proceso de innovación. Es decir, la regulación debería articularse para poder alcanzar un entorno de tipo más competitivo en el que tanto consumidores como productores maximicen conjuntamente su utilidad y beneficio, lo que redunde en una ganancia para la sociedad.

Vías de mejora de la regulación en materia de protección de datos

1. Actualización permanente de la regulación
2. Políticas de Privacidad estandarizadas y simplificadas. Hacia la segmentación del mercado de datos
3. Procesos de autorización adecuados
4. Consideración de datos pseudónimos
5. Mejor balanceo del "accountability" entre los generadores de datos y los usuarios de los mismos
6. Certificaciones de buenas prácticas en el uso de datos de carácter personal
7. Colaboración internacional

La actualización permanente de la regulación

La velocidad de cambio en el procesamiento de información es tal que las aproximaciones regulatorias en materia de privacidad y protección de datos personales se están quedando obsoletas. Se trata de diversas normas nacionales y locales que no están preparadas para afrontar un ecosistema en el que la información fluye entre diferentes regiones y continentes. Los servicios accesibles desde cualquier lugar o en cualquier momento, cada vez más demandados, proliferan de forma proporcional al acceso a las redes ultrarrápidas y de comunicación móvil, que permiten el acceso a un mundo digital en el que los participantes (usuarios y organizaciones) pueden estar sujetos a leyes muy distintas entre sí.

Por ejemplo, en este contexto podría darse en el tiempo un escenario muy probable en el que se produzcan los siguientes hechos en simultáneo: (1) un aumento de la demanda de información por datos de carácter personal, (2) un cambio en la percepción de los usuarios de las nuevas generaciones que sean más proclives a ceder/vender un mayor volumen de datos personales (cambio de percepción respecto a la privacidad); y (3) un marco regulatorio que sigue manteniendo la misma posición regulatoria, respecto al bienestar de las personas. Esta combinación de efectos podría producir una pérdida de eficiencia y bienestar que una regulación adecuadamente dinámica debería evitar.

Políticas de Privacidad estandarizadas y simplificadas: Hacia la segmentación del mercado de datos

Una manera de favorecer el alcanzar un mercado competitivo es el de segmentarlo en sub-mercados que aproximen la demanda a las características de la oferta, de manera que sea más fácil el ajuste al mercado competitivo. En este caso, los ciudadanos podrían ofrecer o restringir su información en función de sus preferencias para usos diversos y diferentes a los del mercado normal, y percibir por ello un precio/servicio diferenciado por parte de la demanda. El hecho de que la regulación permita que la oferta tenga control sobre su propia segmentación favorece la aproximación a un escenario de competencia, que en teoría generaría mayor bienestar.

Lo anterior requiere fundamentalmente una regulación que estandarice y simplifique las Políticas de Privacidad para su correcto entendimiento, y que se incorporen incentivos de mercado para que el usuario tenga la posibilidad de comparar estas políticas y decidir sobre ellas, y con ello surjan espacios para incentivar al usuario o sancionar en su caso por este atributo; aunque, como señalamos previamente, una buena política de privacidad, no es lo único que observa el usuario, sino también, por ejemplo, el costo que significa renunciar al tiempo invertido y familiaridad ganada con un servicio/producto. La vía de los mercados segmentados es buena, pero se tiene que tomar en cuenta estos otros aspectos que algunos usuarios pueden valorar más y que pueden restar el efecto de la política de regulación planteada.

Procesos de autorización adecuados

Los formatos actuales de aceptación y consentimiento del uso de datos de carácter personal tienen un alto coste de lectura y comprensión por parte de los usuarios. Por ello se puede dar la circunstancia de que los usuarios pueden estar aceptando por defecto las condiciones que le impone el proveedor. Más tarde, dicho consumidor observa las implicaciones que conlleva dicho acto (por ejemplo, la recepción de publicidad no adecuada a sus gustos; o enterarse del uso de sus datos del cual no era consciente) lo que le lleva a desconfiar del sistema.

La regulación debería permitir confeccionar formularios de aceptación de uso de datos personales que sea sencilla, ágil y de fácil comprensión. Desde una perspectiva teórica, Campbell et al (2013) proponen que se pueda crear un perfil de aceptación de uso de datos personales que se realice sólo la primera vez y que sirva para cualquier empresa o aplicación informática del mundo, reduciendo el coste de transacción de los agentes económicos de tener que autorizar cada vez que se solicita una acceso. Otra aproximación podría ser el permitir un mayor control sobre los datos al propio individuo, a través de mecanismos que le permitan a él decidir el tratamiento que se realice sobre sus datos, durante todo el transcurso de la relación contractual, lo que añadiría una mayor transparencia y podría generar confianza. Al margen de las bondades que cada una de estas aproximaciones pueda llegar a tener, el reto central sigue siendo el incrementar la probabilidad de que el usuario realmente lea, se informe y tome conciencia de lo que sucede.

Los datos pseudónimos

Otro aspecto importante a tener en cuenta es la consideración de cierta información personal o pseudopersonal que identifica a la persona y es por ende objeto de protección bajo las regulaciones actuales. Si bien es cierto que con las nuevas tecnologías es posible llegar a identificar a la persona física a partir de datos a priori no personales como las trazas de navegación, o reconociendo los dispositivos desde los que se navega, la generación de perfiles y patrones de comportamiento y su explotación desligada de los identificadores personales continúa generando un gran valor para las empresas y en última instancia para la sociedad. La introducción del concepto de datos pseudónimos por el Parlamento Europeo en su revisión del nuevo Reglamento de Privacidad (aún pendiente de aprobación) y la rebaja de la carga regulatoria sobre estos datos, se presenta como una iniciativa acorde con la necesidad de permitir una mayor flexibilidad en el tratamiento de los datos a las empresas sin obviar los derechos fundamentales de los individuos.

Mejor balanceo del "accountability" entre los generadores de datos y los usuarios de los datos

Señalábamos que uno de los principales problemas era que los individuos muchas veces no somos conscientes de las autorizaciones que damos al uso de los datos de carácter personal. Los recuadros de avisos y advertencias que aparecen frecuentemente cuando se interactúa en la web, son muchas veces ignorados, aceptándolos rápidamente para continuar con la navegación. Muchos expertos consideran que esto se debe a la longitud y complejidad de los textos, pero algunos anticipan que una simplificación de los mismos tampoco aseguraría que una proporción importante de la población asumiera mayor consciencia y buscara informarse. Este problema es más complejo si cabe en la era del Big Data, siendo difícil explicarle a las personas el uso exacto que se hará de la información, así como la complejidad que envuelven los experimentos y consecuencias de los mismos sobre su bienestar futuro.

Teniendo en cuenta lo anterior, muchos expertos recomiendan un mejor balance respecto a la responsabilidad de uso de los datos de carácter personal, de tal manera que no se le cargue todo el peso de la responsabilidad a las personas. Mayer-Schönberer y Cukier (2013) y The Centre for Information Policy Leadership (2009), por ejemplo, plantean que ese "accountability" debe recaer también sobre los que explotan esta información. Es decir, "notificar" a las personas y "esperar su consentimiento" parece no ser suficiente en la era del Big Data. En cierta medida, parece tener sentido trasladar mayor responsabilidad a los usuarios de la información dado que ellos conocen mucho más que cualquiera -y con seguridad más que el consumidor o regulador- cuál es su intención con el uso de los datos. En las recomendaciones que los expertos dan sobre esta mayor carga de responsabilidad sobre los analistas de los datos, es que se les pida que hagan un análisis de riesgo del uso de los datos, no sólo como consecuencia del primer uso sino de usos ulteriores. Si bien para algunos esto puede ser costoso, esto se podría mitigar si el regulador señala qué tipos de datos o situaciones requieren este análisis de riesgos. Si este análisis de riesgos está bien hecho, las empresas podrían ahorrarse los costos de estar pidiendo consentimiento cada vez que se quiera usar estos datos, pues los mismos ya habrían sido estudiados previamente.

No sólo protección ex-ante sino ex-post: regulando el riesgo de que las predicciones a partir de los datos personales sean determinantes para las personas

Los problemas del uso de los datos de carácter personal no sólo deben ser controlados ex-ante sino también ex-post. De acuerdo a Mayer-Schönberger (2011) y, Mayer-Schönberger y Cukier (2013), en la era del Big Data y las predicciones que arrojan sus complicados algoritmos, el mundo está tendiendo

poco a poco a utilizarlos como elementos determinísticos. En varias situaciones el uso de los escenarios probabilísticos que arroja la explotación de los datos de carácter personal dentro de un esquema de Big Data, ha podido ayudar por ejemplo a reducir el crimen en determinadas ciudades.Hoy más del cincuenta por ciento de los consejos de libertad condicional en los Estados Unidos utilizan predictores basados en técnicas de Big Data como un factor decisorio respecto a dejar libre a una persona o no.

La explotación de los datos de carácter personal plantea situaciones desde el punto de vista ético y de reflexión respecto a las condiciones del ser humano, que requerirán evoluciones importante en la las futuras regulaciones.

Los "Algorithmistas" y los certificadores de buenas prácticas en el uso de los datos de carácter personal

Los fundamentos que están detrás de los algoritmos que son utilizados en la explotación de los datos de carácter personal son de una elevada complejidad que las personas nunca podrán entender las consecuencias amplias que se pueden derivar de ello. En ese sentido Mayer-Schönberger (2010) y, Mayer-Schönberger y Cukier (2013) discuten la posibilidad de la existencia de incorporar la figura del "algoritmista", o científicos que realicen auditoría de algoritmos, en la definición de las regulaciones y en el diseño de una supervisión de los datos de carácter personal que permita un balance de justicia para las personas y eficiencia para la sociedad en cuanto al uso de la información.

En ese contexto estos expertos plantean que la sociedad cuente con este clase de especialistas que certifiquen la manera como estos datos son utilizados. Los algorithmistas podrían ser expertos en las áreas de ciencias de la computación, matemáticas y estadísticas y actuarían como auditores de los análisis y predicciones del Big Data. Ellos tomarían una posición imparcial y de confidencialidad en sus labores, de la misma manera que los contadores y otras profesiones lo hacen ahora. Siguiendo a Mayer-Schönberger y Cukier (2013), los algoritmistas evaluarían la selección de la fuente de datos, la elección de las herramientas analíticas y predictivas, incluyendo algoritmos y modelos, así como la interpretación de sus resultados. La función del algoritmista podría ser clave en brindar una solución equilibrada de mercado para todos los agentes económicos, en lugar de esquemas regulatorios excesivamente intrusivos. Para ello, se podría fijar los roles de los algoritmistas externos e internos. Así, los algoritmistas externos, estarían atentos a atender solicitudes de los gobiernos en situaciones que se requiera revisar o validar predicciones de Big Data. Podrían también conformarse empresas certificadoras, cuyos veredictos puedan ser aceptados por reguladores y supervisores.Así mismo, podría pensarse en la generación de colegiaturas profesionales de algorimistas que al igual que los médicos, abogados, arquitectos y otras profesiones, se sometan a estrictos códigos de conducta y ética en sus actos.

Así mismo, podrían instituirse algoritmistas internos dentro de las organizaciones para monitorear in situ las actividades que se realizan con datos de carácter personal, velando sobre todo los intereses de las personas que pudieran verse afectadas. Esto sería una especie ombudsman algorítmico, que asegure que todo el proceso del manejo de datos desde su obtención hasta los outputs finales estén enmarcados dentro de las buenas prácticas éticas y científicas. Evidentemente, todo este tipo de acciones requerirían ser proporcionales, para evitar que se conviertan en procesos costosos que limitan el avance tecnológico.

Colaboración internacional en la regulación de la protección de datos de carácter personal.

En el contexto global y universal de la era digital, es necesario que exista una mayor aproximación

entre reguladores internacionales para que se definan unas reglas de juego básicas y comunes en el tratamiento de los datos personales, permitiendo el flujo de los mismos, pero salvaguardando el derecho de los individuos a su privacidad. Una buena aproximación a este respecto es el trabajo que se está desarrollando en Europa para disponer de un reglamento que afecte por igual a todos los países miembros así como una única entidad supervisora central para todos ellos. Los beneficios estimados por la Comisión Europea de esta integración ascienden a 2,3 miles de millones de euros anuales.

Pero un mercado global, va mucho más allá de lo que suceda en determinadas geografías. La interacción de los mercados y el circuito de los datos suceden en todo el orbe y vemos en la actualidad a compañías digitales de todo tamaño nacidas en un lado del Atlántico o del Pacífico, brindando sus servicios hacia las orillas contrarias. Teniendo en cuenta este elemento global en el mundo digital, la regulación evidentemente tiene un camino muy largo que recorrer para consolidarse.

5. Conclusiones

En la actual era digital, donde los datos juegan un papel central en avance tecnológico de la sociedad, su potencial valor transaccional y la regulación que la circunscribe son determinantes. Parece evidente que si se lograra alcanzar un equilibrio donde los intereses de consumidores, firmas y principios regulatorios estuviesen alineados, las ganancias para la economía y el impulso innovador serían importantes. No obstante, lo que observamos es un mundo donde las fallas de mercados predominan y donde el rol de regulador, a veces muy paternalista, puede terminar generando soluciones ineficientes.

Es cierto que los principios universales que consagran los derechos a la intimidad y a la privacidad es un elemento que debe ser respetado y defendido innegociablemente. El punto quizá, puede centrarse en esa frontera no suficiente clara entre lo que cada persona puede considerar como privado, y los costos de oportunidad que para ellos mismos puede tener contar con una regulación que permita dar a todos un margen de elección, sin renunciar a los principios de la buena salvaguarda de nuestros datos de carácter personal.

Hemos abordado estos aspectos, presentando la problemática económica de los datos de carácter personal, el marco regulatorio y sus interacciones, para luego aproximarnos al contexto real de los mercados con todas sus imperfecciones. Hemos visto que existen muchos problemas para que el dueño de los datos tenga real conocimiento de la manera como estos son usados tanto por gobiernos e instituciones. También hemos visto las dificultades para plantear políticas de privacidad sobre las que los usuarios tengan interés en leer, comprender y elegir. Existen múltiples evidencias de que las personas no se toman el tiempo suficiente para leer y entender avisos muy sencillos, y que es simplemente la confianza de un servicio del cual obtiene valor y en el que han invertido mucho tiempo para familiarizarse, lo que termina teniendo más peso en su decisión. Y esto mismo, sumado a la posición de dominio de algunos proveedores de estos servicios lo que termina elevando las barreras de entrada de nuevos players, lo que a su vez hace difícil que las personas puedan escoger, premiar o penalizar a quien tenga las mejores/peores prácticas de políticas de privacidad.

Estas circunstancias, evidentemente, establecen un caso para la intervención del regulador. El problema está que en muchos casos, la regulación es incapaz de medir los efectos netos sobre el bienestar de las personas y, peor aún, discernir quién se beneficia y quién no. Más aún sus intervenciones pueden mellar los beneficios que el compartir los datos de carácter personal pueden traer a la sociedad, como consecuencia de las externalidades de redes generadas. Hemos también

ilustrado algunos de las situaciones paradójicas que se producen como consecuencia de las buenas intenciones de las regulaciones y, lamentablemente, sus malos resultados, generando perjuicios en muchos casos a los segmentos más vulnerables. También se ha observado cómo algunas prácticas de protección de los datos, sin proponérselo, terminan incrementando el poder de mercado de las ahora grandes compañías que entraron primero, en perjuicio de los ventures.

Nadie ha dicho que regular este mercado sea fácil, pero ello no implica que no se deba hacer nada. La regulación se enfrenta a un escenario, nuevo y complejo, con muchas dinámicas en varios frentes. Quizá el más interesante sea el factor generacional, que puede llevar a un cambio de percepción de los límites de lo que es privado o no. Estos cambios pueden derivar en que la regulación tal como está ahora, hacia el futuro, deba de adaptarse a los nuevos tiempos, como lo hacen regulaciones en otros campos. La adaptabilidad y flexibilidad deberá ser quizá un camino a ir explorando con el paso de los años. Y dentro de estas tendencias, no se debe olvidar un elemento clave de nuestras economías y sociedades: el factor global. La era digital, plantea hoy más que nunca, un escenario de integración, donde las fronteras y geografías casi desaparecen en el intercambio. Seguir persistiendo con regulaciones fragmentadas, hacen poco favor al avance tecnológico y sus efectos positivos sobre la sociedad.

Referencias

Acquisti, Alessandro (2010) “The Economics of Personal Data and the Economics of Privacy”. Working Paper. Carnegie Mellon University.

Acquisti, Alessandro, Leslie John, George Loewenstein (2013) “What is Privacy Worth?” The Journal of Legal Studies. Vol. 42, Nº 2. June. pp. 249-274. The University of Chicago Press

Acquisti, A. (2004) “The Economics of Privacy”,. Carnegie Mellon University, Software Engineering Institute. Febrero.

Athey, Susan (2014) “Information, Privacy and the Intenet: An Economic Perspective”. June 2014. CPB Netherlands Bureau for Economic Policy Analysis.

Bartelsman, E. J. (2013) “ICT, Reallocation and Productivity” Economic Papers 486, April 2013 European Economy. European Commission.Directorate-General for Economic and Financial Affairs. Bruselas.

Bailey, J.P (1998) Internet price discrimination: Self-regulation, public policy, and global electronic commerce. Technical report, The Robert H. Smith School of Business, University of Maryland, 1998.

BCG-The Boston Consulting Group (2012) “The Value of our digital Identity”, Ed. Liberty Global-Policy Series.
(http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf)

Bijlsma, Michiel, Bas Straathof and Gijsbert Zwart (2014) “Choosing Privacy: How to Improve the Market for Personal Data” CPB Policy Brief | 2014/04. CPB Netherlands Bureau for Economic Policy Analysis.

Campbell, James David and Goldfarb, Avi and Tucker, Catherine, Privacy Regulation and Market Structure (2013). Disponible en at SSRN: http://ssrn.com/abstract=1729405

Dayal,S. Landesberg H. y Zeisser M. (2001) “Building trust on line”. McKinsey Quarterly, 4, 2001.

Economides, N. The economics of networks, International Journal of Industrial Organization 14 (6) (1996) 673–699.

Goldfarb, A. y C. Tucker (2011) “Privacy Regulation and Online Advertising,” Management Science, Vol. 57 No. 1, January 2011, pp. 57-71.

IDC Consulting (2012) The Digital Universe in 2020: Big Dta, Bigger Digital Shadows and Biggest Growth in the Far East.
(http://www.emc.com/collateral/analyst-reports/idc-digital-universe-united-states.pdf)

Kramer, Adam, Jamie E. Guillory and Jeffrey T. Hancock (2014) “Experimental Evidence of Massive Scale Emotional Contagion Through Social Network” Proceedings of the National Academy of Science. Core Data Science Team, Facebook, Inc., Menlo Park, CA 94025; and Departments of Communication and Information Science, Cornell University, Ithaca, NY 14853. Edited by Susan T. Fiske, Princeton University, Princeton, NJ, and approved March 25, 2014 (received for review October 23, 2013).

Liebowitz, S. Re-thinking the Network Economy: The True Forces that Drive the Digital Marketplace, AMACOM, New York, NY, 2002.

Mayer-Schönberger, Viktor y Kenneth Cukier (2013) “Big Data: A Revolution That Will Transform How We Live, Work and Think” Eamon Dolan Book-Houghton MIfflin Harcourt. Boston and New York.

Mayer-Schönberger, Viktor (2011) “Delete: The Virtue of Forgetting in the Digital Age” Princeton University Press.

McDonald, A. M. and L. F. Cranor (2008). The cost of reading privacy policies. Journal of Law and Policy for the Information Society 4 (3)

Miller, Amalia R. and Tucker, C. (2009) “Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records· NET Institute Working Paper No. 07-16. (http://ssrn.com/abstract=960233)

Shapiro, C. H.R. Varian, Information Rules: A Strategic Guide to the Network Economy, Harvard Business School Presss, Boston, MA, 1999.

Skinner, Chris (2014) “Digital Bank: Strategies to Launch or Become a Digital Bank” Marshall Cavendis International, Singapore.

The National Commission for the Protection of Human Subject of Biomedical and Behavioral Research (1979) “Ethical Principles and Guidelines for the Protection of Human Subject to Research”. The Belmont Report. U.S. Department of Health and Human Services .

The Centre for Information Policy Leadership (2009) “Data Protection Accountability: The Essential Elements” Document for Discussion. October.

(http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf)

Tribunal de Justicia de la Unión Europea (2014) “El gestor de un motor de búsqueda en Internet es responsable del tratamiento que aplique a los datos de carácter personal que aparecen en las páginas web publicadas por terceros”. Comunicado de Prensa Nº 70/14. Luxemburgo, a 13 de mayo de 2014. Sentencia en el asunto C-131/12 - Google Spain, S.L., Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González.

Tsai, J, S. Egelman, I.Cranor, A. Acquisti (2011) “The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study”. Information System Research, 22, 254-268, 2011.

Varian, Hal (1996) “Economic Aspects of Personal Privacy” University of Berkeley. December 6, 1996. http://people.ischool.berkeley.edu/~hal/Papers/privacy/

Varian, Hal (2005) “Demographics of the Do-Not-Call List” IEEE Security and Privacy. Jan/Feb. 2005

Vu, Khuong M. (2011) “ICT as a Source of Economic Growth in the Information Age: Empirical Evidence from the 1996-2005 Period (March 1, 2011)” Telecommunications Policy, Vol. 35, No. 4, pp. 357-372, 2011; Lee Kuan Yew School of Public Policy Research Paper No. PP 11-02

Notas

1. Queremos agradecer los comentarios y sugerencias ofrecidos por las áreas de Cumplimiento Normativo, Servicios Jurídicos e IT Compliance de BBVA. En especial las aportaciones de Miguel Ángel Cañete, Miguel Marqués, Juan Manuel Matalobos y Jesús Alonso