REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 7 NÚM. 2 (2018) • PÁGS. 45-80 • DOI 10.5354/0719-2584.2018.50578
RECIBIDO: 15/7/2018 • APROBADO: 22/10/2018 • PUBLICADO: 30/12/2018

DOCTRINA

Mecanismos de regulación de datos personales: Una mirada desde el análisis económico del derecho

Personal data regulation mechanisms: A law and economics perspective

Catalina Frigerio Dattwyler

Abogada, Chile

RESUMEN El presente artículo busca analizar diversos mecanismos de regulación del mercado de datos personales desde la perspectiva del análisis económico del derecho. En él, se describe el mercado y sus particularidades, se identifican las fallas existentes y se analiza el derecho a la privacidad y protección de datos personales como bien económico y las implicancias que ello conlleva. Luego, se examinan los mecanismos que mejor abordan estas fallas de mercado, como la regulación del consentimiento, la creación de incentivos para la valoración de la reputación, la aplicación de impuestos, la implementación de cambios estructurales, la responsabilidad civil y la aplicación de normas de libre competencia.

PALABRAS CLAVE Regulación, privacidad, datos personales, análisis económico del derecho.

ABSTRACT The present work offers an analysis of diverse regulation mechanisms for the personal data market, from a law and economics perspective. It describes the market and its particularities, identifies market failures and analyzes the right to privacy and protection of personal data as an economic good, and the implications that this entails. Then it examines which are the mechanisms that best address such market failures, among others, consent regulation, creation of incentives for the valuation of reputation, tax application, the implementation of structural changes, liabilities and the applicability of free competition rules.

KEYWORDS Regulation, privacy, personal data, law and economics.

Introducción

El creciente desarrollo y la masificación de internet y de las nuevas tecnologías han traído cambios dramáticos en la forma en que los individuos y las empresas interactúan y en cómo se llevan a cabo las transacciones. Vivimos en una economía digital en la que personas y objetos se comunican de manera constante gracias a la rápida interconexión existente, situación que permite la emisión y recepción de enormes cantidades de información a un costo muy bajo. Esto ha posibilitado que las empresas exploten datos a gran escala, lo que genera valor agregado e innova de maneras que antaño parecían impensables.[1]

En este contexto, los datos personales, es decir, la información relacionada con una persona natural identificada o identificable, es uno de los activos más polémicos, ya que permite a las empresas mejorar sus servicios, pero a la vez también utilizar dicha información de formas que potencialmente pueden entrar en conflicto con el derecho humano a la privacidad, protegido en numerosos tratados internacionales y consagrado en el artículo 19 numeral 4 de la Constitución Política de la República de Chile.[2] El principal problema es que, a medida que la tecnología mejora y se extiende de forma exponencial, la dinámica del mercado cambia continuamente, lo que crea incertidumbre y hace complejo el establecimiento de mecanismos eficientes para regular el procesamiento de datos personales y, al mismo tiempo, dar garantía a la protección del derecho a la privacidad de sus titulares.

La regulación de datos personales es actualmente un tema candente en el debate internacional, una materia sujeta a múltiples enmiendas en todo el mundo y que cuenta con la propuesta regulatoria más audaz en la reciente regulación de la Unión Europea, el Reglamento General de Protección de Datos, en vigor desde mayo de 2018. Dicha normativa extiende su esfera de aplicación incluso a empresas fuera de la Unión Europea siempre que procesen datos personales pertenecientes a residentes de la Unión Europea para la oferta de bienes o servicios (no se requiere pago) o monitoreen su comportamiento dentro de dicho territorio.

Chile no se encuentra exento de dicho debate. El 16 de junio 2018 se publicó la Ley 21.096, la cual elevó la protección de datos personales a la categoría de garantía constitucional.[3] A ello se suma el actual proyecto de ley que consiste en un texto refundido

1. «The new personal data landscape», Ctrl-Shift, 22 de noviembre de 2011, disponible en http://bit.ly/2ESYf5u.

2. Pedro Huichalaf Roa, «Hacia la unificación de criterios sobre seguridad y protección de datos en internet», declaración de Chile para el Observatorio Iberoamericano de Protección de Datos, presentada en Santiago en el Seminario de Datos Personales organizado por la Facultad de Derecho de la Universidad de Chile, en colaboración con la ONG META, disponible en http://bit.ly/2PcgEyJ.

3. El articulo 19 numeral 4 de la Carta Fundamental señala: «La Constitución asegura a todas las personas el respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la

que pretende modificar sustancialmente la Ley 19.628 y que, entre otras materias, crea la Agencia de Protección de Datos Personales (Boletín 11.144-07).

Ante este escenario, este artículo busca analizar diversos mecanismos de regulación de la protección de datos personales desde el punto de vista del análisis económico del derecho.[4] Para ello, primero se determinará si el derecho a la privacidad —y como corolario de ello, a la protección de los datos personales— es renunciable o no por el interesado y, de ser así, bajo qué condiciones. Si se concluye que dicho derecho es alienable, se determinará si derechos de propiedad deben reconocerse sobre el mismo para permitir que los interesados obtengan beneficios pecuniarios con su información personal. Si se acepta que el derecho no es completamente disponible, ya que existe un interés público con respecto al mismo, el siguiente paso será identificar mecanismos regulatorios, desde la perspectiva del análisis económico del derecho, que equilibren de mejor manera el crecimiento económico en la era digital junto con la adecuada protección del derecho a la privacidad y la protección de los datos personales, teniendo en cuenta que estas herramientas acarrean consecuencias tanto para el individuo como para la sociedad.

Dentro de dicho contexto, el objetivo de este artículo es demostrar que restringir el análisis al otorgamiento del consentimiento individual no es un criterio suficiente para subsanar las fallas del mercado existentes. De esta forma, el presente trabajo de investigación describirá el mercado en líneas generales y qué lo hace especial, definirá lo que se entiende por datos personales, señalará cómo se utilizan, quiénes son los participantes de dicho mercado y cuál es el producto o servicio relevante que se brinda a su respecto. Luego, individualizará las fallas de mercado existentes con el objeto de comprender cuáles son los flancos que el regulador debe tener a la vista a la hora de regular. A continuación, estudiará el derecho a la privacidad desde una perspectiva económica, para analizar cómo considerarse como un bien cuasi privado o un bien público y las implicancias que ello conlleva, lo que lo hace un interés jurídico complejo de proteger. Finalmente, examinará algunos de los mecanismos que abordan dichas fallas de mercado, con una distinción entre mecanismos *ex ante* y *ex*

protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley».

4. El análisis económico del derecho (economical analysis of law o law and economics) es una escuela económica y jurídica nacida en Estados Unidos que aplica conceptos propios de la ciencia económica a la regulación para predecir el efecto de las normas jurídicas, con el objetivo de determinar cuáles son económicamente más eficientes en variados ámbitos de aplicación (contratos, derecho de propiedad, responsabilidad extracontractual, derecho procesal, entre otros). En su enfoque positivo, dicha escuela estudia las consecuencias de las normas y, en base a ello, logra predecir el efecto producido mediante su adopción; en su enfoque normativo, establece recomendaciones específicas sobre qué norma es más eficiente basándose en las consecuencias económicas que derivan de la aplicación de un determinado curso de acción.

post dependiendo de si el daño causado por la divulgación de información personal se ha generado o no.

Por una parte, se concluirá que, a largo plazo, la intervención que más adecuadamente se ocupa de las fallas de mercado existentes es la creación de cambios estructurales con mecanismos tecnológicos, en que el objetivo es que el modelo de negocios se encuentre centrado en el usuario como generador, controlador y partícipe de los beneficios. Por otra, se inferirá que, a corto plazo, las propuestas *ex ante* se muestran más eficientes que las *ex post*, en particular, la creación de impuestos junto con la implementación de mecanismos que apunten a la importancia de la reputación, pues son ellos los que mejor mitigan las externalidades negativas y las asimetrías de información.

El mercado de datos personales

¿Qué son los datos personales?

En su artículo 2 letra f), la Ley 19.628 define datos de carácter personal o datos personales como «los relativos a cualquier información concerniente a personas naturales, identificadas o identificables». Dicha definición es concordante con la adoptada por la OCDE en sus Directrices sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales de 2013, además del Reglamento General de Protección de Datos, que los definen como «toda información sobre una persona física identificada o identificable». Por lo tanto, el concepto de datos personales debe entenderse como opuesto al de los datos anónimos, esto es, información no relacionada con una persona identificada o identificable.[5]

Los datos personales pueden obtenerse de diferentes maneras y el Foro Económico Mundial hace una distinción entre datos voluntarios, observados e inferidos: los primeros se refieren a datos explícitamente compartidos por los individuos, los segundos aluden a datos capturados por las actividades de registro de los usuarios y los terceros se relacionan a datos basados en el análisis de otros datos personales (WEF, 2011: 13).

A su vez, en atención a su naturaleza, los datos personales pueden ser o no sensibles. La Ley 19.628 define en su artículo 2 letra g) a los primeros como

> aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, como los

5. Por su parte, los datos anónimos podrían encontrar protección jurídica como secretos empresariales bajo el amparo de los artículos 86, 87 y 88 de la Ley 19.039 (Ley de Propiedad Industrial), siempre que constituyan un conocimiento sobre productos o procedimientos industriales, cuyo mantenimiento en reserva proporciona a su poseedor una mejora, avance o ventaja competitiva.

hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

Este tipo de datos son particularmente propensos a lesionar derechos fundamentales de sus titulares, razón por la cual se les otorga un nivel de protección jurídica especial. En particular, la Ley 19.628 señala en su artículo 10 que ellos no pueden ser objeto de tratamiento salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

El concepto de datos personales es de particular importancia, ya que determina el alcance de las reglas de protección a su respecto, es decir, su aplicación e interpretación. Claramente, el concepto debe ser lo suficientemente amplio, flexible y dinámico como para poder subsumir la aparición de nuevas situaciones imprevistas que surgen en la actual realidad tecnológica que cambia rápidamente (Purtova, 2018).

En un dictamen no vinculante para la Unión Europea —pero altamente respetado por sus países miembros— emitido en 2007,[6] el artículo 29 del Grupo de Trabajo[7] analizó el concepto de datos personales y distinguió sus cuatro componentes principales: i) «cualquier información»; ii) «relacionada con»; iii) «una persona natural»; iv) «identificada o identificable».

«Cualquier información» se refiere a datos que pueden ser objetivos —por ejemplo, tipo de sangre—, subjetivos —por ejemplo, una opinión—, no necesariamente verdaderos o probados —en cuyo caso el individuo tiene derecho a rectificación—y relacionados con la vida privada y familiar o cualquier tipo de actividad del individuo. En cuanto al formato en que están contenidos, el concepto incluye información disponible en cualquier forma, ya sea alfabética, numérica, gráfica, fotográfica o acústica.

La expresión «relacionada con» requiere un elemento de «contenido» o de un elemento de «propósito» o un elemento de «resultado». El elemento «contenido» está presente cuando la información es sobre esa persona, independientemente de cualquier propósito por parte del procesador de datos o de un tercero, o del impacto de esa información en el sujeto titular de datos; el elemento de «propósito» existe cuando los datos se utilizan o serán probablemente utilizados con el propósito de evaluar,

6. Article 29 Data Protection Working Party, «Opinion 4/2007 on the concept of personal data», sitio web de la Comisión Europea, 01248/07/EN, disponible en http://bit.ly/2PtGYnv.

7. Article 29 Data Protection Working Party era un órgano consultivo de la Unión Europea creado en 1996 dentro del marco de la Directiva 95/46/EC, sobre la protección de personas físicas en lo respectivo al tratamiento de datos personales y a la libre circulación de estos datos, regulación previa al actual Reglamento General de Protección de Datos. Estaba compuesto por un representante de la autoridad de protección de datos de cada Estado miembro, el supervisor europeo de protección de datos y la Comisión Europea. El Consejo Europeo de Protección de Datos lo reemplazó en virtud del Reglamento.

tratar de cierta manera o influenciar el estado o el comportamiento de un individuo; y el elemento «resultado» surge cuando el uso de datos puede tener impacto en los derechos e intereses de una persona determinada.

El término «personas naturales» se refiere, en principio, a individuos vivos identificados o identificables. Se dejan de lado los casos especiales de personas fallecidas,[8] niños por nacer y personas jurídicas, ya que escapan al alcance de este estudio.

Finalmente, se indica que una persona natural puede considerarse «identificada» cuando, dentro de un grupo de personas, se la distingue de todos los demás miembros del grupo, e «identificable» cuando, si bien la persona todavía no ha sido identificada, ello podría hacerse directamente (por el nombre) o indirectamente (mediante una combinación de criterios significativos que le permitan ser reconocido). Este último caso se da cuando los identificadores iniciales disponibles no permiten la identificación directa de una persona en particular, pero no obstante esa persona aún podría ser «identificable», porque esa información combinada con otros datos permitiría que el individuo se distinga de los demás. Cabe hacer presente que el actual proyecto de ley expresamente señala en la definición de «dato personal» consagrada en su artículo 2 letra f) que

> se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante información combinada con otros datos, en particular mediante un identificador, como el número de cédula de identidad, el análisis de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

¿Cómo se pueden usar los datos personales? ¿Por qué es importante protegerlos?

Las tecnologías han evolucionado exponencialmente durante las últimas décadas y la información disponible en formato digital ha aumentado de forma dramática. Las computadoras, los televisores, los teléfonos celulares, las tabletas y muchos otros dispositivos digitales forman parte de nuestra vida cotidiana, nos brindan acceso continuo a internet y producen grandes cantidades de información. El desarrollo y la masificación de la tecnología no solo ha cambiado la infraestructura de los mercados, sino también la forma en que se efectúan las transacciones y en que se llevan a cabo las relaciones comerciales.

Dado este escenario, cantidades impresionantes de información son creadas y contenidas en conjuntos de datos de una magnitud tan alta que los métodos tradicio-

8. El proyecto de ley contempla expresamente en su artículo 4 que «en caso de fallecimiento del titular de datos, los derechos que reconoce esta ley pueden ser ejercidos por sus herederos».

nales de análisis no son adecuados para manejarlos. Esto es lo que se ha denominado «big data», un conjunto de información tan voluminoso y complejo que escapa al concepto de procesamiento de datos tradicional.[9] Actualmente, todas las empresas más importantes de internet, como Facebook, Google, Ebay, Microsoft y Amazon, entre otras, participan en *big data*. La idea detrás es simple: los datos son información y ello proporciona una ventaja competitiva que se transforma en ingresos. Entre más datos, más ganancias. Una parte importante de esta información se refiere a las preferencias, los hábitos, las características y el comportamiento de personas identificadas o identificables. Así, a través del análisis computarizado de datos, las compañías generan perfiles de usuarios que actualmente se extienden a cada aspecto y fase de la vida individual y social de las personas. Esta información tiene una gran importancia económica, ya que se utiliza para crear valor agregado e innovación en la economía digital actual.

Una de las formas más comunes en que los datos personales se usan para crear valor es mediante la predicción de comportamientos con fines de *marketing*. El acceso a esta gran cantidad de información permite a los proveedores organizarla, procesarla y clasificarla de tal forma que permite segmentar a los consumidores según diferentes tipos de criterios. La información sobre preferencias y necesidades de los usuarios se recopila, ordena y analiza para crear estrategias de mercado que influyan y mejoren todo el proceso de producción. Mediante el uso de datos personales, los motores de recomendación crean valor para los clientes al reducir los costos de búsqueda y evaluación de los productos, lo que hace que los resultados sean más personalizados y eficientes.

Además, cuando los datos personales son cruzados entre diferentes fuentes, se pueden crear servicios nuevos e innovadores que aumentan aún más su valor, base para crear nuevos y mejores productos y servicios.[10] Por ejemplo, al hacer referencias cruzadas entre registros de salud de instituciones públicas, es posible realizar investigaciones que den como resultado hallazgos importantes, como descubrir patrones específicos de síntomas producto del uso de dos fármacos combinados, que por separado son inocuos y no producen el efecto observado. Esto puede dar como resultado importantes iniciativas de políticas públicas relacionadas con la atención médica.[11] O

9. «Big data: Why companies collect and store personal data?», blog de Le VPN, 21 de septiembre de 2018, disponible en http://bit.ly/2Dg6VRQ.

10. Javier Alonso, David Tuesta, Carmen Cuesta y Santiago Fernández de Lis, «Digital economy: An approach to the economy of personal data and its regulation», BBVA Research. Economic Watch, 17 de septiembre de 2014, página 2, disponible en http://bit.ly/2yTCKMh.

11. Los datos personales de salud se encuentran regulados en la Ley 20.584, que «Regula los derechos y deberes de las personas en relación con acciones vinculadas a la salud», y son considerados como datos sensibles, por lo que gozan de mayor protección jurídica. Asimismo, los datos personales médicos también tienen la categoría de sensibles, en virtud de lo señalado en el artículo 127 del Código Sanitario.

la gestión del tráfico, en la que se analizan los datos personales relativos a la ubicación para la toma de decisiones que impliquen la construcción de carreteras y la mitigación de la congestión del tráfico.

Desde la perspectiva del consumidor, la masificación actual de la tecnología les permite una experiencia más personalizada, sin un costo directo (monetario) asociado. El acceso a su información personalizada reduce los costos de transacción y les permite recibir beneficios indirectos, con lo que logran una interacción más eficiente en el mercado. Por ejemplo, los bancos e instituciones financieras generalmente tienen un patrón de compra específico asociado a cada titular de las tarjetas de crédito, información que se utiliza para evitar transacciones fraudulentas cuando los movimientos no calzan con dicha pauta.

Dentro de dicho contexto, las empresas están obteniendo importantes beneficios pecuniarios al utilizar los datos personales como *commodity* y, por lo tanto, son altamente valorados en el mercado. No obstante, los titulares no reciben una remuneración directa por su uso y tienen poco conocimiento sobre cómo son utilizados, a pesar de que existe consenso en que tienen derecho a al menos cierto nivel de control, ya que este tipo de información está protegida por una garantía constitucional. En la actualidad, la protección de dicho derecho ha estado enfocada en el otorgamiento del consentimiento a la recopilación y tratamiento de los datos, uno de los pocos momentos en los que los usuarios tienen una opción explícita de escoger entre compartir la información o proteger su privacidad, pero que, en la práctica, no es una opción real en absoluto. Además, hay poca conciencia de las consecuencias negativas que el mal uso de dicha información puede acarrear, tanto para el individuo en particular como para la sociedad en general. Por lo tanto, aun cuando las actividades que utilizan datos personales como *commodity* crean valor agregado y servicios innovadores, su obtención y tratamiento debe ser regulado, ya que dicha información puede caer en manos equivocadas o incompetentes o incluso ser utilizada por la empresa autorizada de una manera perjudicial, lo que traería riesgos asociados con la posible violación del derecho a la privacidad, especialmente en el caso de datos personales sensibles.

Una de las cuestiones que plantea esta problemática es que cuando se afirma que la privacidad debe protegerse, no existe un concepto único de la misma, lo que dificulta al regulador expresar los límites de dicho derecho y la posibilidad de determinar *ex ante* el daño que la infracción puede generar, ya que hay una gran variedad de situaciones que caben dentro de dicha categoría (Solove, 2002).[12] Por consiguiente, aun cuando no es posible llegar a un acuerdo y establecer un concepto unitario de

12. El autor distingue entre ellas: i) el derecho de no estar expuesto; ii) limitado acceso al yo; iii) secreto; iv) control de información personal; v) identidad; y vi) intimidad. Sobre un análisis de la privacidad como bien económico, véase Posner (1978).

privacidad que sea inmutable ante diversas situaciones, para efectos de este análisis en particular se da por supuesto que las violaciones de privacidad implican una variedad de tipos de actividades dañinas o problemáticas, y se asume que los individuos cuentan con cierto grado de protección al hecho de reservarse o no hacer pública su información personal, a lo cual se refiere precisamente el derecho a la protección de datos personales (Solove, 2006).[13] Por ende, el enfoque se da al análisis económico del concepto de privacidad y protección de datos personales, tanto como bien cuasi privado como bien público.

Descripción del mercado

En términos simples, los datos personales constituyen la materia prima a partir de la cual se crea el mercado de datos personales. A través de la gran cantidad de dispositivos y sensores que actualmente están conectados por redes digitales, se generan, comunican, comparten y transmiten datos personales. Así, aquella información que cumple los requisitos individualizados en la sección precedente es el insumo básico que se procesa en relación con diferentes tipos de objetivos y a través de una amplia variedad de mecanismos.

A diferencia de la normativa chilena, en el Reglamento General de Protección de Datos es posible distinguir al agente que controla el propósito y la manera en que se procesa la información, del agente que solo realiza la operación de procesamiento técnico (aun cuando ambos podrían ser la misma entidad). El primero se conoce como el «controlador de datos», mientras que el segundo como «procesador de datos». Dicha distinción, basada en el grado de control sobre el contenido de los datos personales, es importante para determinar las responsabilidades cuando las transacciones no funcionan correctamente.

Con el resultado de tales acciones se obtiene un producto final: información personal estructurada y organizada que se demanda para la creación de valor o la innovación en una industria en particular. Este esquema funciona en muchos sectores, como finanzas y banca, servicios de salud e instituciones gubernamentales, entre otros.

En concordancia con lo anterior, la clave para comprender la importancia del mercado es el concepto de tratamiento de datos personales, pues son dichas acciones las que generan el valor agregado y determinan la aplicabilidad de la Ley. Este concepto se encuentra definido en el artículo 2 letra o) de la Ley 19.628 como

> cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar,

13. Se adopta el concepto de privacidad como el derecho que cierta información no sea revelada en contraposición a el derecho a ser dejado solo (Bullard, 1998).

> elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

A su vez, el artículo 4, numeral 2 del Reglamento define el mismo concepto como

> cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Básicamente, la definición es tan amplia que el procesamiento o tratamiento de datos personales significa cualquier actividad que se haga con datos personales, lo que nos hace inferir que lo que caracteriza al mercado es la particularidad de la materia prima en sí.

La demanda la constituyen tanto organizaciones públicas como pequeñas, medianas y grandes empresas privadas dedicadas al tratamiento de datos. En consecuencia, los datos personales deben considerarse como la materia prima, pero también como un producto semielaborado que forma parte de una relación compleja, dado que las relaciones de los agentes involucrados en su oferta y demanda en el mercado (titular de datos, procesador de datos y terceros demandando dicha información con valor agregado para la provisión de un producto o servicio específico) puede ser unidireccional o bidireccional.[14] Este último caso surge cuando el interesado disfruta de un producto del tercero que utiliza sus datos.

A partir de este simple esquema, es posible observar que lo que hace que esta «materia» sea peculiar es que su producción está protegida por una garantía fundamental. Como se señaló previamente, en un primer nivel, cabe preguntarse hasta qué punto el derecho a la privacidad y la protección de datos personales es renunciable. Asumiendo que es posible disponer de este derecho, una siguiente pregunta es si debería existir un sistema que permita a las personas obtener beneficios pecuniarios por ello, en cuyo caso se reconocería un derecho de propiedad sobre el mismo con el objetivo de facilitar la determinación de su valor monetario. Esta última alternativa podría resultar problemática, ya que implicaría ponerle un precio a un derecho fundamental. Desde un punto de vista doctrinario, se han defendido principalmente dos posturas en este sentido: aquéllos que defienden la existencia de un derecho de propiedad sobre la información personal, y aquéllos que defienden la prohibición

14. Arnold Roosendaal, Marc van Lieshout y Anne Fleur van Veenstra, «Personal data markets», TNO Report, 2 de noviembre de 2014, disponible en http://bit.ly/2PifphS.

del comercio de datos personales y avocan por la restricción de su libre disposición (Purtova, 2017).

Como se expondrá en las siguientes secciones, la adopción de derechos de propiedad sobre datos personales aumenta las fallas existentes en el mercado —como la existencia de asimetrías de información—, plantea problemas para controlar el uso secundario de la información y para determinar el valor monetario de los mismos, fija un precio sobre valores protegidos por un derecho fundamental, lo que excluye a las personas que no tienen la situación económica para optar por su protección, y deja de lado las problemáticas relacionadas con la privacidad y protección de datos personales como bien público.

Fallas de mercado de datos personales

Una vez identificadas las principales características del mercado de datos personales, corresponde ahora abordar sus fallas de mercado más importantes, impedimentos existentes para el adecuado equilibrio entre la protección del derecho a la privacidad y la protección de datos, y la existencia de incentivos para la creación de valor agregado e innovación por flujos de información personal. Por lo tanto, su existencia exige un enfoque especial para el regulador.

Racionalidad limitada

Una de las suposiciones centrales de la economía neoclásica es que los individuos son racionales, lo que significa que son conscientes de la cantidad y calidad de opciones que enfrentan, pueden clasificarlas de acuerdo con preferencias estables, desean maximizar su utilidad y toman decisiones en concordancia con dicho objetivo. Bajo el modelo neoclásico, la racionalidad de la decisión no depende ni de factores psicológicos ni de procesos cognitivos.

Estas suposiciones fueron criticadas por Simon (1970) durante los años setenta, quien propuso que al momento de analizar la racionalidad de una decisión, también deben considerarse las restricciones informativas y cognitivas de la misma, para lo que adoptó el término de «racionalidad limitada» o *bounded rationality*. Al tomar en cuenta dichos elementos, un comportamiento es procedimentalmente racional —en oposición a sustancialmente racional— cuando es el resultado de una deliberación apropiada, si tenemos en cuenta el acceso y procesamiento limitado de la información disponible y la percepción que el individuo tiene al momento de elegir. El concepto de racionalidad limitada nos hace inferir que las decisiones sustantivamente racionales generalmente no son posibles y el regulador debe tener dichas restricciones en consideración al momento de determinar cuál es la política pública más apropiada.

Con respecto a la privacidad y la protección de datos personales, la regulación

actual se ha enfocado en crear mecanismos que permitan a las personas administrar sus intercambios de privacidad y usarlos en su mejor interés, asumiendo que los individuos son racionales y enfatizando la importancia de la naturaleza del consentimiento y la forma en que se otorga en las políticas de privacidad de las plataformas en línea. Pero los estudios teóricos y empíricos demuestran que los individuos están dispuestos a intercambiar privacidad por conveniencia o negociar la divulgación de información personal a cambio de recompensas relativamente pequeñas, y que rara vez están dispuestos a adoptar tecnologías de protección de privacidad (Acquisiti y Grossklags, 2005: 1). Esto también va acompañado de una falta de conocimiento sobre las formas tecnológicas o legales de protección de la privacidad.[15]

Los autores identifican tres formas en que el individuo que toma una decisión con respecto a su privacidad se aleja del agente racional asumido en el modelo neoclásico: i) mediante la existencia de información incompleta disponible en la toma de decisión; ii) por la limitada capacidad cognitiva para procesar la información disponible, y iii) por la tendencia continua a desviaciones sistemáticas de dicho modelo. En línea con estas ideas, se debe considerar que, dado el escenario complejo y dinámico de la economía digital, hacer un análisis de costo-beneficio para el individuo no resulta simple, ya que hay una tendencia a subestimar las consecuencias de los problemas de privacidad, pues los agentes no están completamente al tanto de cuán poderosa puede ser esa información. En consecuencia, a pesar de proporcionar a los titulares de datos personales información completa sobre la actividad de las empresas, es altamente probable que no la procesen de manera adecuada. Esto es lo que ocurre cuando se descarga una aplicación que tiene una política de privacidad que debe ser aceptada para poder ser utilizada, como Facebook o Whatsapp: los usuarios simplemente aceptan los términos y condiciones sin siquiera leer y conocer las implicaciones que tal consentimiento podría tener en el presente o el futuro, para ellos y para la sociedad.

Por lo tanto, desde un punto de vista regulatorio, es necesario tener en cuenta que los individuos no siempre tendrán como objetivo maximizar su utilidad, que tienen información incompleta sobre las alternativas disponibles y las consecuencias de sus acciones y que tomarán decisiones de acuerdo con lo que perciben, basados en su experiencia personal previa. Por consiguiente, una política apropiada debe proveer un adecuado acceso a la información sobre los datos personales, pero también tener en cuenta que su disponibilidad no siempre es procesada por los individuos de la manera que mejor proteja sus intereses.

15. Los autores hicieron un estudio con una muestra educada estadounidense, de la cual más del 70% no pudo nombrar ni describir una actividad o tecnología para navegar por internet de forma anónima con el fin de evitar que otros identifiquen su dirección IP.

Asimetrías de información

Además de las limitaciones planteadas respecto de la capacidad de los consumidores para decidir sobre su información personal, claramente existe una situación de asimetría de información en las transacciones en que se proporcionan datos personales, pues el procesador de datos tiene más o mejor información sobre el uso que se les dará y las implicaciones que ello conlleva.

Dada la gran cantidad de información compleja y técnica provista en las políticas de privacidad o la existente en regulaciones que prescriben estándares mínimos sobre su contenido y que los individuos no tienen otra opción real si quieren utilizar el servicio prestado —pues se enfrentan a una situación de «tómalo o déjalo»—, la ignorancia o la falta de comprensión simplemente llevan a la aceptación de cualquier condición, beneficiosa o no —o incluso nociva— para el interés del usuario. Por ejemplo, al ingresar a un sitio web y completar un formulario con datos personales, puede ocurrir que muchas más compañías tengan acceso a ellos, ya sea con fines analíticos o publicitarios, y que el usuario desconozca por completo la situación de dicho acceso a su información. Además, habitualmente los sitios web se reservan el derecho de cambiar sus políticas de privacidad, lo que teóricamente podría dar lugar a que las personas tengan que revisarlas constantemente para proteger sus intereses, algo que en la práctica rara vez ocurre.

Estas situaciones nos hacen inferir que las personas carecen de suficiente comprensión sobre varios asuntos importantes relacionados con la computación en la nube, la seguridad en línea y el comercio de datos para la información personal en línea (Bashir y otros, 2015). Lo anterior se conoce como la «paradoja de la transparencia», ya que entre más información se comparte mediante declaraciones de aviso, menos entendibles se vuelven para el otorgamiento de un consentimiento auténtico e informado del usuario.

Además, esta situación podría traer el problema del «mercado de limones», individualizado por Akerlof (1970): en presencia de asimetría de información sobre la calidad de los productos o servicios ofrecidos, el consumidor podría no ser capaz de distinguir una buena calidad de una baja y, por lo tanto, su disposición a pagar —que, debido a la incertidumbre, se equiparará con el precio de baja calidad— saca del mercado los productos o servicios de alta calidad. Esto conlleva un problema de selección adversa y, por lo tanto, ningún vendedor tiene un incentivo para ofrecer términos más favorables (mejor protección a la privacidad) para el procesamiento de datos.

Por lo tanto, aunque el uso potencial de datos personales sigue siendo incierto debido al creciente desarrollo de nuevas tecnologías, parece razonable imponer una mayor responsabilidad sobre aquéllos que usan la información extraída. Es el controlador de datos el que puede prevenir a un menor costo los riesgos de violación de privacidad y definir quién debe asumir el riesgo de la actividad.

Costos de transacción

De acuerdo con el teorema de Coase (1960), en lo que respecta a la forma más eficiente de utilizar los recursos, la asignación inicial de derechos (*legal entitlements*)[16] resulta irrelevante siempre que los costos de transacción sean inexistentes. Expuesto de otra forma, independiente de la titularidad de los derechos iniciales, si las partes interesadas no incurren en costos de transacción para negociar el resultado que mejor satisfaga su interés, necesariamente se producirá un resultado eficiente,[17] es decir, la actividad será realizada por la parte que la valore más. Aun cuando dicha aseveración ha sido objeto de numerosas críticas, es innegable el aporte que la propuesta generó al examinar la existencia de costos de transacción como impedimentos al logro de soluciones cooperativas.

Los costos de transacción son aquéllos en que se incurre para iniciar, ejecutar y hacer cumplir un acuerdo cuando dos o más partes hacen un intercambio voluntario. En otras palabras, son impedimentos para negociar y lograr una solución cooperativa. Siguiendo a Cooter y Ulen (2016), dichos costos pueden ser de búsqueda, incurridos al localizar un bien que no es fungible o cuando no está claro quién es la parte que tiene la titularidad del derecho; de negociación, costos necesarios para llegar a un acuerdo aceptable con la otra parte de la transacción y que son más altos cuando hay menor información pública sobre el tema: cuanto mayor es la asimetría de información, mayores son los costos de negociación, pues una de las partes puede tener más información sobre el valor del acuerdo de cooperación o las amenazas de no ingresar al mismo; y de monitoreo, costos incurridos para observar y verificar que la otra parte haya cumplido el acuerdo o para hacer cumplir un acuerdo que ha sido violado ante tribunales.

Con respecto al mercado de datos personales, entre los costos de búsqueda se reconoce el tiempo y los costos incurridos para identificar a todos los procesadores de datos y para coordinar a todos los sujetos afectados por la política de privacidad de las plataformas. Entre los costos de negociación, está la manera en que los procesadores manejan la información y los beneficios que se obtienen al hacerlo; y entre los costos de ejecución o monitoreo, se encuentra la capacidad de detectar el problema respecto a un procesamiento inadecuado o ilegal de datos personales, identificar a todas las partes responsables involucradas, así como todos los costos incurridos si se

16. Cabe señalar que el concepto de derecho se refiere aquí a una acepción económica más amplia, que alude a la legitimación para hacer algo o para que cierto estado sea respetado. En el clásico ejemplo del agricultor y el ganadero en «el problema del costo social» de Coase, si es el agricultor quien tiene derecho a que los animales no pasten en su territorio, él tendrá la asignación del derecho (entitlement).

17. No obstante, si bien el resultado de la negociación será eficiente, la determinación de los derechos de propiedad es relevante para efectos de determinar los incentivos existentes para las partes en la negociación, así como también para determinar la manera en que se distribuyen los beneficios.

desea penalizar a la parte infractora (notificar a la institución especializada, asistir a los tribunales, etcétera).

De particular importancia son los costos de ejecución, ya que las violaciones a las declaraciones de privacidad —y, por lo tanto, el incumplimiento de este tipo de contratos— no son evidentes ni siquiera para una persona experta en el tema. En primer lugar, las filtraciones de información son muy difíciles de rastrear. Además, muchos de los actores relevantes no son parte del acuerdo concreto con el individuo e incluso pueden tener políticas de privacidad en conflicto con el proveedor que aparece directamente ante el consumidor. Aún más: en principio, el procesamiento de datos podría realizarse en un contexto transnacional, en una jurisdicción desconocida para el usuario. A lo anterior, se suma que las violaciones de los acuerdos de privacidad no son reversibles, lo que significa que una vez que la información se ha filtrado, no se puede recuperar su estatus de privada, ya que se mueve rápidamente a través de medios digitales. Esto resulta relevante en la efectividad de los mecanismos de regulación *ex post*. Finalmente, también se debe considerar que una vez que los usuarios han invertido un tiempo significativo en familiarizarse con una aplicación o plataforma, les resulta difícil migrar a otro proveedor cuando se modifica la política de privacidad y que, además, el consumidor no tiene forma de saber si la empresa competidora los cambió también. En consecuencia, el incentivo para que los consumidores penalicen a una empresa por una mala política de privacidad es bajo (Athey, 2014).

Externalidades

Las externalidades negativas son costos impuestos a terceras partes[18] que no forman parte de la transacción y, por lo tanto, no se ven reflejados en los precios del mercado generando ineficiencias, pues se genera una sobreproducción o sobreoferta del producto o servicio.[19]

Con respecto al intercambio de datos personales, al momento de compartir dicha información se hace posible que terceras partes que acceden a ella puedan saber más o de mejor manera sobre los demás que eligen no compartir los suyos (Choi, Doh-Shin y Byung-Cheol, 2018: 2). Así, dada la interconexión que se enfrenta hoy en día, la privacidad de un usuario individual se verá necesariamente afectada por las

18. Las externalidades positivas son beneficios conferidos a terceras partes que no forman parte de la transacción.

19. El clásico ejemplo para entenderlas es la actividad de una fábrica que genera polución: los vecinos de alrededor que se ven perjudicados por tener aire contaminado no forman parte de la transacción (venta del producto producido que genera la contaminación) y se ven perjudicados por la actividad de la empresa. Ello es una externalidad negativa que, en principio, no se ve reflejada en el precio del producto ofrecido por la empresa contaminante.

decisiones de los demás, lo que da lugar al fenómeno conocido como «privacidad interdependiente» (Biczok y Hui Chia, 2013: 1). Este concepto se refiere principalmente a las externalidades generadas por decisiones individuales, ya que la protección de la privacidad depende no solo de las decisiones de uno, sino también de amigos, parientes, personas con las que tenemos una relación e incluso extraños con quienes compartimos los mismos patrones. Por ejemplo, incluso si un «tipo» de consumidor no utiliza un servicio en particular, el hecho de que haya varios consumidores similares a él que usan el servicio puede permitir cierta inferencia acerca de sus usos. En este sentido, cuando contribuimos publicando información sobre nosotros mismos, la falta de privacidad generada por los efectos indirectos de tales acciones podría considerarse como un mal público y no como un bien público, en el entendido de que los bienes públicos y los males públicos son dos caras del mismo problema (Fairfield y Engel, 2015: 423), idea que será desarrollada en la sección siguiente.

Regulación del mercado de datos personales

El derecho a la privacidad y la protección de datos personales como bien económico

Como se indicó en la sección anterior, lo que hace que este mercado sea peculiar es que la materia de su producción está protegida por una garantía fundamental respecto de la cual no existe consenso acerca de su definición. Teniendo aquello presente, a continuación, se analizará el derecho a la privacidad y la protección de datos personales como bien económico.

En principio, un bien económico puede ser un bien escaso tangible o intangible con valor económico. Para que el bien sea económico, debe haber agentes que estén dispuestos a pagarlo porque tiene la capacidad de satisfacer sus necesidades. Dos son las principales características que determinan la naturaleza de un bien económico: primero, su *rivalidad,* es decir, si su consumo por parte de un consumidor impide el consumo simultáneo de otros consumidores; y segundo, su *excludibilidad*, dependiendo de si es posible o no evitar que otras personas que no lo hayan pagado tengan acceso al mismo. De acuerdo con estos atributos, inicialmente se pueden distinguir cuatro categorías de bienes económicos: bienes privados (rivales y excluibles), bienes públicos (no rivales y no excluyentes), bienes cuasi públicos (bienes comunes, no excluibles y rivales) y cuasi privados (bienes de club, excluibles, pero no rivales) (Jervis, 2006: 27).

Derecho a la privacidad como bien cuasiprivado (bienes de club)

Un bien cuasiprivado se distingue por ser no rival y excluible. Dado que cuando se protegen los datos personales se exceptúa a otros de la posibilidad de disponer

de la información protegida por dicho derecho, podría decirse que el mismo es un bien excluible: al negarse el titular a que procesen sus datos, «consume» su derecho a la privacidad y la protección de datos personales y a la vez excluye a otros de la posibilidad de utilizarlos. Por su parte, dado que es posible proteger el derecho a la privacidad y datos y, al mismo tiempo, permitir que otros individuos disfruten del consumo del mismo derecho, el bien tendría una naturaleza de bien cuasi privado: el sujeto puede negarse a que procesen sus datos personales y nuevamente está «consumiendo» su derecho a la privacidad y protección de datos, pero ello no obsta a que terceros disfruten de su consumo simultáneo. Sin embargo, una clasificación como ésta no resulta simple, pues el derecho a la privacidad y protección de datos personales guarda relación con la protección o no de información, la que tiene naturaleza de activo intangible y que, por lo mismo, puede ser consumida simultáneamente por muchas personas.

En consecuencia, desde la perspectiva de bien económico cuasiprivado, la privacidad y la protección de los datos personales se relacionan con el derecho a usar, controlar y transferir información sobre uno mismo, y es la regulación más adecuada aquélla que da énfasis en informar y empoderar a los titulares. Por tanto, bajo esta premisa, el enfoque de la regulación debe basarse en la creación de incentivos adecuados para que las empresas creen herramientas para alcanzar tales objetivos. El sujeto es quien debe ser centro de atención y que tiene el control para restringir los flujos de información personal, pero que también soporta la carga y el costo de los mismos. Esto está en línea con el reconocimiento de la privacidad como un derecho a la autodeterminación informativa que busca que el tratamiento de datos se realice a partir de una decisión libre y voluntaria de las personas. Por ende, la suposición es que, en principio, solo el individuo tiene un interés en el límite de lo que constituye privacidad o no y que, como regla general, el derecho a la privacidad y la protección de datos es alienable (Regan, 2002).

La crítica estándar con respecto al procesamiento de datos personales desde este punto de vista es que los consumidores no están suficientemente informados sobre lo que se hace con su información (Sholtz, 2001).[20] En línea con estas ideas, si la privacidad y la protección de datos se centran en el individuo y el control que éste puede ejercer y el ejercicio de dicho control es un derecho alienable, sería razonable otorgar a las personas derechos de propiedad sobre su información personal y permitirles vender esos derechos libremente a fin de poner la información en su uso más valioso. En tal caso, las personas que deseen vender sus datos personales

20. Sholtz reconoce como problemas para la propietarización de datos personales la incapacidad de los consumidores para contratar con empresas sobre la recopilación y el uso de su información personal, dada la imposición de políticas de privacidad y no de un contrato; y también, la existencia de enormes asimetrías de información entre el titular y las empresas.

podrían hacerlo y existiría un mercado explícito, pero también, ello tendría como consecuencia la creación de un mercado diferenciado y quienes valoren más su privacidad tendrían que pagar un costo mayor por protegerla. Aun cuando los datos personales son utilizados como bien económico, bajo las condiciones actuales de dicho mercado, todavía no es posible que las compañías discriminen los precios, ya que las empresas no pueden distinguir entre aquéllas que valoran más su privacidad que otras. Investigadores de diversas disciplinas han intentado estimar empíricamente el valor que los individuos asignan a la privacidad y sus datos personales, pero los resultados de sus hallazgos demuestran que las valoraciones de privacidad dependen especialmente del contexto (Acquisiti, 2010). Bajo la dinámica actual, a los consumidores solo les queda una decisión binaria: o permiten o prohíben la recopilación de sus datos personales. Por lo tanto, actualmente, un consumidor que prefiere tener sus datos personales protegidos no tiene que pagar un precio extra por no revelar su información personal.

Pensar en un mercado en el que el derecho a la privacidad puede ser total y libremente alienable presenta algunos problemas: primero, prohibiría al titular limitar a otra parte en el uso o transferencia de datos (un individuo podría estar dispuesto a vender sus datos por un propósito «a», pero podría no estarlo para uno «b» a un tercero interesado); a ello se suma lo difícil que resulta estimar un precio apropiado para el uso secundario de datos personales, pues los adquirentes posteriores pueden valorarlos más y ello debiera verse reflejado en el precio. Además, de permitirse la libre alienación, se generaría un mercado diferenciado en cuanto a la valoración de la privacidad, lo que abriría paso a que aquellas personas de menores recursos que valoren mayormente su privacidad no puedan costear la protección de la misma, lo que derivaría en una desventaja que podría tornar en discriminación y, por tanto, el derecho a la privacidad perdería en dicho contexto su naturaleza de derecho fundamental. Por último, debe tenerse en cuenta que la privacidad cuenta con características de bien público y al establecer derechos de propiedad sobre los mismos, se generarían incentivos para el *free riding*, así como una situación análoga a aquélla conocida como «tragedia de los comunes», ideas que serán desarrolladas en la siguiente sección (Schwartz, 2004: 2.091).

Derecho a la privacidad como bien público

Desde otra perspectiva, el derecho a la privacidad debe ser considerado un bien público, esto es, no excluible y no rival, lo que proporcionaría un beneficio social que todos pueden compartir por igual, sea mediante la contribución al mismo o no, como ocurre con el aire limpio o la defensa nacional. En esta línea, si la privacidad y la protección de datos personales implican el anonimato, una vez que se crea la privacidad para uno, es difícil excluir a otros de los beneficios colectivos obtenidos de tenerla,

aun cuando otros titulares decidan revelar su información (no excluibilidad). Asimismo, cuando la información personal de un titular en particular está protegida, nadie más puede disfrutar del derecho a la privacidad de la misma (no rivalidad). Esta perspectiva incorpora entonces la existencia de las externalidades informacionales señaladas anteriormente. Si ese es el caso, se podría hacer una analogía con el ejemplo de Hardin sobre la tragedia de los comunes, ya que la racionalidad individual no es igual a la racionalidad colectiva: al decidir, los individuos actuarán de una manera que sea beneficiosa para ellos mismos aunque, de considerarse colectivamente, tal acción sea perjudicial para la sociedad en su conjunto y, en consecuencia, para ellos en el futuro. Por lo tanto, siempre que el beneficio inmediato de la divulgación de sus datos exceda el riesgo a largo plazo para su privacidad, los individuos optarán por regalar sus datos (Fairfield y Engel, 2015).

Analizar la privacidad y la protección de datos como un bien público es entendido de mejor manera como no tener privacidad como un mal público. Esto queda claro cuando se considera el caso de unirse a una red social como Facebook, situación en la que los usuarios saben que pagarán indirectamente poniendo su información personal a disposición. Un usuario en particular no percibirá el intercambio individual de su información personal como un riesgo suficiente para abstenerse de los beneficios inmediatos y personales que le aporta unirse a la red. Sin embargo, si se considera la suma del daño potencial resultante de la divulgación de todos los demás usuarios, puede inferirse que nadie querría unirse a la red social si la empresa permite la divulgación de datos personales. Bajo tal idea, el caso reciente de Cambridge Analytica proporciona un ejemplo de este riesgo: se alega que la recopilación de datos personales de hasta 87 millones de usuarios de Facebook se utilizó para influir en la opinión de los votantes en nombre de los políticos que contrataron a la consultora.[21] Al usar la red social, no hubo una reflexión por parte cada usuario acerca de las consecuencias futuras de permitir que Facebook acceda y procese sus datos personales, ya que la decisión de utilizar la red social fue tomada desconociendo el perjuicio que la suma de cada revelación podría causar en el futuro.

Dicho lo anterior, el otorgamiento de derechos de propiedad sobre este tipo de bienes acarrea el problema de *free riding:* cuando se ve afectada una multitud de partes por un bien público, es poco probable que ellas lleguen a un acuerdo para una asignación adecuada de los costos del suministro del mismo, ya que cada parte afectada sabrá que soportar todos los costos o una parte de ellos en medida desproporcionada —en este caso, de aquellos costos incurridos para proteger la privacidad y proteger los datos personales— no tiene mucho sentido si los beneficios se compartirán igualmente con todas las otras partes afectadas. Por tanto, como todos tendrán tendencia

21. Nicholas Confessore, «Cambridge Analytica and Facebook: The scandal and the fallout so far», The New York Times, 4 de abril de 2018, disponible en https://nyti.ms/2QfEDJQ.

a pensar de esta forma, nadie tomará ninguna medida. Esto refleja un problema de incentivos y de coordinación grupal.

En consecuencia, se requiere de mecanismos institucionales, en una combinación de regulación y autogobierno, para resolver este problema de cooperación, ya que si solo se informa y empodera a los individuos, ello no resulta suficiente para resolver el dilema social, pues incluso con individuos perfectamente informados y facultados para controlar sus datos, ellos no pueden influir en la gran cantidad de información a partir de la cual funcionan los algoritmos del *big data* (Fairfield y Engel, 2015: 411).

Mecanismos regulatorios *ex ante*

Consentimiento

El otorgamiento del consentimiento es de suma importancia, ya que es el mecanismo a través del cual se manifiesta la aceptación o rechazo del uso de los datos personales del individuo.[22] Ya sea analizando la privacidad como un bien cuasiprivado o bien público, dicho acto unilateral es la unidad básica de análisis en cualquier política pública, puesto que el regulador debe aspirar a que el mismo refleje la libre voluntad del sujeto, pero, al mismo tiempo, de considerarse —como ocurre en el presente artículo— que el derecho a la privacidad tiene el carácter de bien público, y que el mismo se otorgue con la ayuda de incentivos y mecanismos institucionales que resuelvan los problemas de coordinación derivados de la racionalidad grupal.

Hay consenso generalizado sobre los actos básicos que requieren la manifestación del interesado: en primer lugar, debe exigirse cuando existe la intención de procesar los datos personales del sujeto por primera vez para un propósito específico; y también, cuando el objetivo del procesamiento es diferente al originalmente acordado —en concordancia con el principio de finalidad—.[23] Por otra parte, dado que los costos de requerir consentimiento no son altos, debería ser obligatorio siempre que el procesamiento de datos sea realizado por un agente diferente al acordado inicialmente, individualizándolo e informando al interesado para reducir los costos de búsqueda, incluso si el propósito es el mismo. Esto también reduce los costos de monitoreo.

22. Para un interesante análisis de la reciente jurisprudencia chilena sobre el carácter contractual de este tipo de autorizaciones, véase De la Maza y Momberg (2017).

23. Cabe señalar que el proyecto de ley establece en su artículo 3 los principios que regirán la nueva legislación, entre los cuales expresamente reconoce en su letra b) el principio de finalidad, al especificar que «en aplicación de este principio, no se pueden tratar los datos personales con fines distintos a los informados al momento de la recolección, salvo que el tratamiento sea para fines compatibles con los autorizados originalmente; exista una relación contractual o precontractual entre el titular y el responsable que justifique el tratamiento de los datos con una finalidad distinta; el titular otorgue nuevamente su consentimiento; los datos provengan de fuentes de acceso público, y cuando lo disponga la ley».

Además de ser libre y específico, el consentimiento también debe ser informado y no ambiguo para tratar las asimetrías de información.[24] Teniendo como límites los antecedentes educativos y la conciencia de la racionalidad limitada de los agentes económicos, como regulador es posible mejorar las asimetrías de información existentes facilitando el acceso y seleccionando y priorizando el tipo de información que se debe comunicar. No obstante, como se señaló anteriormente respecto de la paradoja de la transparencia, se ha demostrado que los consumidores no leen la información contenida en las políticas de privacidad y que incluso en el caso excepcional de que lo hagan, no las entienden, por lo que es posible concluir que simplemente hacer clic en un cuadrado aceptándolas no es suficiente. Por tanto, resultan necesaria la aplicación de otros mecanismos más simples y efectivos para tratar de abordar estos problemas (Fairfield y Engel, 2015).

En este sentido, la implementación de una política que adopte una calificación de servicio de acuerdo con estándares objetivos podría ser una alternativa útil (Martin, 2013). La idea detrás de esta propuesta es similar al mecanismo adoptado en Chile[25] y otros países para la industria alimenticia, con el objetivo de subsanar las asimetrías de información existentes en la población respecto de los componentes nutricionales: criterios específicos de privacidad considerados relevantes podrían seleccionarse, clasificarse y clasificarse según diferentes categorías —por ejemplo, utilizar el rojo para sitios que tengan una política de privacidad muy baja, amarillo para una intermedia y verde para una alta—. Así, cuando se dé una situación que requiera consentimiento podría exigirse la manifestación de una característica clara y notable —como se señaló, podría ser un color, pero también un número— que notifique al sujeto la clasificación de la política de privacidad.

Cabe preguntarse si esta clasificación debiera hacerse según un procedimiento gubernamental, lo que implicaría un alto nivel de información por parte de la agencia pública, o si se debiera requerir que su implementación sea obligatoria pero permitir a los usuarios clasificar las políticas de privacidad por sí mismos, lo que promovería un mecanismo regulatorio de autocontrol. Dado que la privatización y otorgamiento de derechos de propiedad para el funcionamiento de un libre mercado de datos personales conllevan los problemas ya descritos en la sección anterior, y puesto que la intervención pública requeriría un alto nivel de conocimiento, la autorregulación se presenta como una alternativa adecuada. Como señaló Ostrom (1990), cuando surge el problema de coordinación de la tragedia de los comunes, la intervención estatal requiere un alto nivel de información por parte de la agencia reguladora, tanto para identificar a los infractores como para aplicar el castigo a la acción correcta. Por ende, al momento de calcularse los costos y beneficios de implementar regulación públi-

24. La Ley 19.628 señala que la autorización debe ser expresa y escrita.

25. Como hace la Ley 20.606, «Sobre composición nutricional de los alimentos y su publicidad».

ca, dichas probabilidades deben también tenerse en consideración.[26] Además, dicha alternativa implicaría mayores costos para la creación de una institución adecuada a cargo de la vigilancia (costos de promulgar una ley que cree la institución, los recursos utilizados para implementarla, además de todo el tiempo que ello implicaría, entre otros). Por tanto, teniendo en cuenta la interacción del mercado digital, en que el anonimato es fácilmente factible y las tecnologías dejan un importante espacio de incertidumbre, la brecha informativa para una agencia reguladora sería demasiado alta. Por ende, la implementación de un mecanismo de autorregulación en el que los mismos participantes en la industria puedan ser monitoreados por los usuarios parece ser una solución más efectiva. Un mecanismo como éste permitiría a los participantes identificarse y comunicarse entre sí, lo que aumentaría la cooperación en situaciones de dilema de bien público. Según esta lógica, hacer obligatorios para los procesadores de datos la utilización de un mecanismo estandarizado que los evalúe crearía un incentivo para que tengan mejores políticas de privacidad.

Aunque pareciera existir una contradicción entre la identificación y la comunicación entre los usuarios y la provisión de privacidad como bien público, la clave estaría en asegurar que la evaluación (o la existencia de comentarios) sea confiable sin divulgar información sobre la identidad de los participantes en el mundo real. Por lo tanto, los agentes capaces de evaluar el sistema y comunicar su opinión deberían poder hacerlo utilizando seudónimos bajo un sistema de encriptación. De esa manera, la «comunidad de usuarios» podría construir reputaciones y relaciones estables y comunicarse entre sí y al mismo tiempo limitar la información del mundo real que deseen revelar. En esta línea, aun cuando éste sea un mecanismo de autocontrol, sería necesario por parte de las autoridades regulatorias la creación y provisión de un sistema de verificación que permita la creación de seudónimos de los participantes —sin perder privacidad— y que haga imposible que las mismas empresas pertenecientes a la industria creen software u otro tipo de trucos para tener una mejor clasificación.[27] La adopción de un mecanismo con estas características haría posible atacar el problema del «mercado de los limones», ya que el sistema de calificación permitiría discriminar la calidad entre los proveedores. De esta forma, cuando se otorgara el consentimiento, el usuario podría tomar una decisión mejor y más informada o, al menos, una decisión tomando en consideración la voluntad del resto de la comunidad que utiliza los servicios y se ve afectada por el procesamiento de datos.

26. De esta forma, desde la perspectiva del potencial infractor, al calcular las posibles ganancias o beneficios de cada acción, debe restarse el costo incurrido por la aplicación de la sanción o multa, multiplicado por la probabilidad de que sea efectivamente impuesta.

27. Por ejemplo, esto es lo que hace el complemento de navegador Terms of Service; Didn't Read (disponible en http://tosdr.org), que analiza las políticas de privacidad de los servicios en línea y resume el análisis en una calificación.

Finalmente, además de ser informado, el consentimiento también debiera ser inequívoco, lo que significa que debe darse por una acción afirmativa en la que el sujeto de datos acepte claramente el procesamiento.[28] Así, a pesar de que no se requiera que este sea necesariamente explícito, la acción por parte del interesado no debe dejar lugar a dudas sobre su concesión. Este requisito también auxilia en la existencia de asimetrías de información, ya que constituye una garantía legal de notificación al interesado.

Reputación

En línea con la idea anterior, de particular importancia resulta potenciar mecanismos institucionales que permitan desarrollar el autogobierno. La reputación —según la Real Academia Española, «opinión o consideración que se tiene a alguien o algo»— es una de las herramientas más fuertes que puede ser influenciada por el regulador. Una buena reputación comercial, dada por las creencias que la comunidad tiene sobre un proveedor específico, brinda a los proveedores una ventaja competitiva frente a los demás participantes de la misma industria. La imagen proyectada determina la lealtad del consumidor, influye en la capacidad de expansión del negocio, abre oportunidades de crecimiento y tiene muchas implicaciones en la dinámica del mercado. La forma en que se manifiesta dicha reputación es a través del *goodwill* asociado a una marca particular, es decir, a la representación gráfica que identifica en el mercado un producto o servicio, con la que los consumidores pueden relacionar origen, fuente y calidad del producto o servicio ofrecido.[29]

Siguiendo a Choi, Doh-Shin y Byung-Cheol (2018: 2), el regulador puede incentivar decisiones basadas en la reputación al fijar el precio cuando se debe autorizar la integración de datos personales entre dos plataformas. Su modelo asume que las plataformas no pueden comprometerse a usar información personal solo para mejorar el bienestar de los usuarios, y que una plataforma con buena reputación es aquélla que proporciona un mayor excedente de bienestar para los consumidores cuanto más comparten su información personal. En otras palabras, una plataforma de buena reputación es la que mejor protege la privacidad de sus usuarios, al ofrecer más protección contra acciones que puedan infringir el derecho a la privacidad a un menor

28. El artículo 2 letra o) del proyecto de ley define «consentimiento» como «toda manifestación de voluntad libre, específica, inequívoca e informada, mediante la cual el titular de datos, su representante legal o mandatario, según corresponda, autoriza el tratamiento de los datos personales que le conciernen».

29. El artículo 19 de la Ley 19.039 (Ley de Propiedad Industrial), define marca comercial como «un signo que sea susceptible de representación gráfica capaz de distinguir en el mercado productos, servicios o establecimientos industriales o comerciales, pudiendo consistir en palabras, incluidos los nombres de personas, letras, números, elementos figurativos como imágenes, gráficos, símbolos, combinaciones de colores, así como también cualquier combinación de estos signos».

costo. La lógica es la siguiente: si un consumidor tiene la opción de decidir si permite la transferencia o integración de datos (*opt in*) o no (*opt out*) entre dos compañías al mismo precio, solo autorizará a aquellas empresas que tengan una buena reputación. Pero si existen dos precios diferentes (es decir, las plataformas con menor protección tienen un menor costo y viceversa), esto puede llevar a que la plataforma de mala reputación induzca un equilibrio indeseable, lo que llevaría a los consumidores a una peor situación, debido a las externalidades negativas de la información: los consumidores preferirán la plataforma de precio más bajo y dicha decisión afectará a otros consumidores debido a la interconectividad de la información. Sin embargo, al regular el precio, el usuario autorizará a la plataforma de buena reputación para integrar sus datos personales, lo que funciona como un incentivo para otorgar la autorización siempre que el procesador de datos tenga una buena reputación respecto de sus políticas de privacidad. Esto implica que una posible solución sería crear un mecanismo en el que no exista diferencia de precio entre la opción de aceptar la integración o no, lo que implicaría que incluso los usuarios que opten por no aceptarla deberían poder utilizar igualmente los servicios de la plataforma sin ser excluidos del mercado. En consecuencia, si una empresa que tiene autorización para procesar los datos de un titular desea integrar dicha información con una nueva —como ocurrió con Whatsapp en Facebook— y el precio de permitirlo o no para el usuario es el mismo, este último solo aceptará la integración —y el consecutivo tratamiento— si la reputación respecto a la privacidad es buena.

Para que la reputación influya efectivamente en la decisión a tomar en una transacción, debe ser posible identificar la existencia de comportamientos oportunistas o fraudulentos y debe tratarse de transacciones repetidas, ya que ellas permiten construir la reputación a lo largo del tiempo y dan la oportunidad de modificar comportamientos según el precio o la calidad deseada (Martin, 2013). Cuanto más frecuentes sean las transacciones, más eficientes son los efectos de reputación, así como los incentivos para invertir en ellos (Williamson, 2005). Además, las personas deben tener la oportunidad de señalar sus preferencias en cuanto a precio y calidad. Si tenemos en cuenta dichas características, otra posible solución sería la creación de una aplicación o página web en la que los usuarios puedan calificar las políticas de privacidad, como la que actualmente se utiliza para clasificar los restaurantes y sus servicios. Esto debiera ser acompañado de una campaña de marketing que promueva y fomente su uso. Tal mecanismo permitiría a los mismos usuarios identificar las marcas que no cumplen con los estándares requeridos. Cabe notar que, respecto de esta propuesta, también surge la necesidad de crear un sistema de verificación que permita la privacidad del usuario y que evite la manipulación de los resultados por parte de los agentes de la industria.

Dicho lo anterior, se debe tener presente que para que este mecanismo resulte se requeriría que los usuarios sean conscientes de las consecuencias de la disminuida

protección de su privacidad, lo que, como se ha señalado, no ocurre en la práctica. No obstante, existe convicción en cuanto al poder de la publicidad que brindan las redes sociales e internet, el que, de todos modos, resulta una herramienta útil para auxiliar con un problema tan complejo, especialmente en lo que respecta a la privacidad como bien público.

Impuestos

Una vez identificada la existencia de externalidades negativas en un mercado, los impuestos son una de las posibles soluciones para corregir ineficiencias. A través de lo que se conoce como «impuestos pigouvianos», el costo social de una actividad que no está cubierto por su costo privado es internalizado por su productor. De lo contrario, el resultado del mercado no es eficiente y puede generar un consumo excesivo del servicio o producto, lo que produce externalidades negativas. Por lo tanto, una alternativa sería gravar a las compañías que obtienen beneficios del tratamiento de datos personales para evitar su sobreexplotación. El principal problema en la creación de un impuesto al tratamiento de datos consiste en determinar el valor monetario generado por la actividad, ya que ello es complejo y depende en gran medida del contexto y de la información provista. Esto está relacionado con la determinación de cuál es el evento imponible (OCDE, 2018).

Una alternativa sería gravar las ventas o los ingresos generados en los sitios de publicidad en línea, ya que su principal valor es creado por el tratamiento de datos personales y esto tiene un precio de mercado. Otra forma en que el valor es observable y negociable, y en que podría eventualmente aplicarse un impuesto, es en la industria de corretaje de datos (*data brokage*). Los corredores de datos son empresas que recopilan y agregan información del consumidor de una amplia gama de fuentes para crear perfiles detallados de personas.[30] Por lo general, dichas compañías no interactúan directamente con las personas y recopilan información de una amplia variedad de fuentes (registros públicos, redes sociales o acuerdos de cooperación). Venden la información compilada a otras compañías, agencias gubernamentales o personas, la cambian de forma gratuita bajo un acuerdo de cooperación o la proporcionan sin costo, pues ganan dinero a través de publicidad o referencias. Este tipo de transacciones podría ser más fácilmente gravado, ya que el valor de los datos personales es explícito.

La idea de gravar el tratamiento de datos personales en la actualidad está siendo arduamente debatida en la escena internacional. La naturaleza de la economía digital presenta nuevos desafíos para los recaudadores de impuestos, entre los cuales está la

30. «Data brokers and "people search" sites», Privacy Rights Clearinghouse, 4 de junio de 2018, disponible en http://bit.ly/2qsaPic.

dificultad para identificar puntos específicos de estabilidad sobre los que aplicar un impuesto, y la práctica de disociar el lugar de establecimiento de la empresa proveedora del servicio con el lugar de consumo por el usuario. El 16 de marzo de 2018, la OCDE publicó su informe provisional «Retos impositivos derivados de la digitalización», en el que reconoce que los nuevos procesos de creación de valor tienen una serie de características, entre ellas, el uso de escalas masivas de datos personales, valor que no es totalmente capturado bajo las políticas fiscales actuales. No obstante, el informe muestra una falta de consenso sobre la regulación de este tema a nivel internacional. Un par de días después, el 21 de marzo de 2018, la Comisión Europea propuso nuevas reglas para garantizar que las actividades comerciales digitales se graven de manera justa y favorable al crecimiento en la Unión Europea. En dicho documento, que tiene como una prioridad importante el desarrollo de una economía digital, la Comisión propuso una reforma fiscal a largo plazo y la creación de un impuesto interino a corto plazo (con lo cual apuntan a las brechas y vacíos más urgentes en la tributación de las actividades digitales). Este último sería aplicado a los ingresos creados por la venta de espacios publicitarios en línea, a ingresos creados a partir de actividades intermediarias en el entorno digital que permiten a los usuarios interactuar con otros usuarios y que facilitan la venta de bienes y servicios, y a aquellos ingresos creados por de la venta de datos generados a partir de información proporcionada por usuarios (OCDE, 2018). Dicho documento se encuentra actualmente en discusión.

Al pensar en determinar el hecho imponible, se podría considerar la aplicación de diferentes instrumentos tributarios para que el nivel de recopilación y tratamiento de datos se efectúe de manera eficiente, considerando también las externalidades negativas. Un interesante modelo crearon Bloch y Demange (2018), quienes estudiaron los efectos en el nivel de recopilación y explotación de datos personales de diversos instrumentos tributarios, en particular, de los efectos de: i) un impuesto sobre los ingresos monetarios de la plataforma; ii) un impuesto aplicado por usuario ingresado a la plataforma; iii) un sistema tributario sobre ingresos diferenciados, el cual distingue entre los ingresos por acceso a la plataforma —es decir, el valor generado por un usuario independientemente de la recopilación de datos— y los ingresos generados por la explotación de datos; y iv) un impuesto aplicado a cada usuario por acceder a la plataforma. En su modelo, las ganancias de la plataforma son directas o inmediatas (aquéllas generadas por el ingreso a la plataforma o por publicidad, a través de motores de búsqueda o redes sociales digitales) o indirectas (las generadas por la venta de datos o por ganancias publicitarias futuras). A diferencia de las primeras, estas últimas solo se obtienen mediante el tratamiento de datos personales. Por su parte, los usuarios se diferencian a través de su costo de privacidad: aquéllos que se preocupan más por su privacidad tienen un mayor costo de privacidad y viceversa. El beneficio para los usuarios está compuesto por un componente fijo, determinado por el mero

acceso a la plataforma, y un componente variable, provisto por las ventajas de tener sus datos recopilados y procesados (valor agregado por el cual la plataforma no cobra extra). Bajo tales supuestos, la plataforma monopólica que proporciona el servicio en línea debe elegir un grado de explotación (tratamiento) de datos que equilibre el aumento de valor por su uso (a través de publicidad o precios específicos) y la posibilidad de que los usuarios no accedan a la plataforma debido a los altos costos de privacidad que ello implica, teniendo en consideración que su decisión estará basada en los beneficios generados por el uso de la plataforma menos los costos de la privacidad. Los autores concluyen que el único impuesto que permite corregir la excesiva recopilación de datos es un impuesto sobre los ingresos que trata diferencialmente los ingresos de la plataforma derivados del uso único, (como los ingresos generados por subastas de productos) y los ingresos vinculados a la recopilación de datos (como la reventa de datos a los intermediarios). Por ende, concluyen que si las autoridades fiscales cobraran un mayor nivel de impuestos sobre la reventa de datos que sobre los ingresos de la subasta, ello impediría que la plataforma explote los datos de manera ineficiente, lo que corregiría las externalidades negativas generadas con la sobreexplotación (Bloch y Demange, 2018).

Cabe señalar que dicho modelo supone la existencia de un mercado diferenciado en cuanto al costo de la protección de la privacidad, lo que, como se indicó anteriormente, no ocurre en la actualidad. Así, de seguirse este modelo y sus conclusiones sobre los diversos tipos de impuestos, debe tenerse en cuenta que para que la aplicación de estos impuestos cumpla el objetivo de un impuesto pigoviano, se requeriría que exista diferenciación entre los usuarios que valoran más su privacidad y los que no, lo que, como ya se señaló, acarrearía las problemáticas individualizadas respecto de la imposición de un precio sobre un derecho fundamental.

Mecanismos tecnológicos con cambios estructurales

Una propuesta más radical y a largo plazo sería la generación de un cambio fundamental en la gestión de datos personales, lo que viraría el centro de análisis desde un mundo donde son las organizaciones las que recopilan y utilizan información sobre sus clientes para sus propios fines, a una economía en que sean los individuos quienes manejan su propia información para los fines que les resulten convenientes, con los titulares compartiendo parte de esta información con proveedores para lograr beneficios conjuntos, utilizando mecanismos tecnológicos que garanticen el adecuado resguardo al derecho de privacidad de protección de datos (Bass y Symons, 2017: 49). En esta línea, la Unión Europea actualmente estudia y desarrolla un enfoque interesante, que busca anticiparse a los avances en la tecnología más que reaccionar ante los mismos, bajo un proyecto denominado DECODE (DEcentralised Citizen Owned Data Ecosystem o Ecosistema de Datos de Propiedad Ciudadana Descentralizado),

cuyo objetivo es cambiar los modelos comerciales actuales en que son las empresas quienes ofrecen sus servicios en internet a uno más «usuario céntrico», en el que las personas puedan agrupar sus datos. Con dicho objetivo, bajo DECODE, actualmente se están implementando proyectos piloto que incluyen talleres en colaboración con ciudadanos y comunidades, en los que, mediante el uso de técnicas criptográficas sofisticadas, es posible explorar cómo construir una economía digital centrada en los usuarios, en la que los datos son generados y recopilados por los ciudadanos, el internet de las cosas y redes de sensores, lo cual los hace disponibles para un uso comunal más amplio y genera conjuntos de «datos comunes» que cuenten con protecciones de privacidad adecuadas.

A largo plazo, la idea es que, bajo el enfoque más radical, se creen cooperativas de datos comunes como comunidades autónomas con reglas acordadas de forma colectiva y democrática y que ellas prioricen el valor social de esta información por encima de su valor económico. Para lograrlo, se requeriría adoptar el principio de reciprocidad en su gobernanza: los terceros interesados que usan los datos debieran devolver algo a estos conjuntos de datos generados como bienes comunes —como podría ser, espacio de almacenamiento, horas donadas por los trabajadores o simplemente recursos económicos—. El objetivo es que los titulares de los datos tengan control sobre cómo se accede y utiliza su información a través de la implementación de la tecnología *blockchain* basada en criptografía.[31] Ello permitiría utilizar la información para la creación de valor y la innovación sin que el derecho a la privacidad se vea menoscabado.

Una solución como ésta, aplicada a escala masiva, cambiaría completamente la estructura económica del mercado de los datos personales y sus ineficiencias. No obstante, dados los intereses económicos y el poder oligopólico ejercido por las grandes compañías que manejan las más importantes cantidades de *big data* —como Facebook, Google, Amazon y otros—, se ve como una realidad lejana, aunque deseable. Cabe notar también que, a pesar de que se han creado métodos de desidentificación de datos anonimizados, se ha demostrado que por lo general se puede volver a identificar y asociar con entidades específicas (Tene y Polonetsky, 2013: 257). Por lo tanto, la utilización de este mecanismo debería garantizar la seguridad de los datos y el principio de rendición de cuentas.

31. Básicamente, blockchain es un medio para procesar una transacción en línea sin la necesidad de un intermediario. Cada vez que ocurre una transacción, la información sobre la misma se agrega a la «cadena». Estas unidades de información se conocen como bloques, los que, una vez agregados, no se pueden modificar (son un registro permanente e inmutable). Para más información, véase «Blockchain: A technical primer», Deloitte Insights, 6 de febrero de 2018, disponible en http://bit.ly/2Qi8fXd.

Mecanismos *ex post*

Responsabilidad civil por filtración de datos

La filtración de datos puede ser entendida en términos generales como la divulgación no autorizada o ilegitima de información personal por parte de una organización (Acquisti, Hoffman y Romanosky, 2013: 125). El reconocimiento de responsabilidad por filtración de datos es un mecanismo *ex post*, ya que resulta aplicable una vez que los datos personales dejan de estar protegidos. Al determinar la existencia de responsabilidad por parte del procesador de datos, no solo el regulador asigna el riesgo en la organización, sino que también proporciona incentivos para que se tomen estándares de cuidado, especialmente en lo que se refiere al control de seguridad.[32] En consecuencia, la responsabilidad *ex post* sirve como elemento de disuasión para las empresas, pues aumenta los costos en la participación de actividades que puedan ser potencialmente perjudiciales. Por lo tanto, a medida que la probabilidad de ser considerado responsable por los daños aumenta, la cantidad de pérdidas del consumidor internalizada por la empresa también aumenta (Acquisiti y Romanosky, 2009).

Actualmente, quienes vean su derecho a la privacidad o la protección de datos perjudicado en Chile pueden recurrir ante la Corte de Apelaciones de su domicilio e interponer una acción de protección con el objetivo de que se tomen medidas para poner fin al acto u omisión arbitraria o ilegal, que signifique una privación, perturbación o amenaza a sus derechos y garantías constitucionales (Viollier, 2017: 27). Además, la Ley 19.628 cuenta con lo que en doctrina se conoce como *habeas data,* que busca resguardar los derechos de la persona afectada en sus derechos respecto del tratamiento de sus datos personales.[33] No obstante, dichas acciones no compensan los daños ocurridos por una filtración, razón por la cual, según las reglas generales, eventualmente sería posible entablar una demanda por indemnización de perjuicios, sea por vía contractual o extracontractual,[34] si se tiene en cuenta que por parte de la empresa tratante existe el deber de proteger la información del afectado y que ello es procedente si dicha obligación fue incumplida, con los consecuentes daños ciertos, reales y determinados.

Sin embargo, esta alternativa se enfrenta al desafío de que el daño —y, en consecuencia, los perjuicios— suelen ser inciertos y difíciles de probar, situación que

32. El proyecto de ley reconoce en sus artículos 14 quater y artículo 14 quinquies el deber de adoptar medidas de seguridad y el deber de reportar las vulneraciones de las mismas a la Agencia de Protección de Datos Personales.

33. El proyecto de ley establece dos procedimientos: de tipo administrativo (tutela de datos y de infracción de ley) y uno posterior, de tipo judicial (de reclamación).

34. Para efectos de este artículo, se deja de lado la discusión sobre la naturaleza jurídica de la acción. Se remite nuevamente al análisis que hacen De la Maza y Momberg (2017).

disminuye las probabilidades de ganar un juicio, lo que genera un desincentivo para entablar este tipo de acciones (Solove, 2008: 125). Las filtraciones de datos generalmente conllevan una cantidad importante de daños directos intangibles —por ejemplo, vergüenza asociada con tener partes de la vida privada expuestas al público—, situación que da lugar a incertidumbre, a la cual los tribunales son especialmente reacios. Por parte de la empresa realizando el tratamiento, los costos asociados con estas infracciones son altamente especulativos y, por lo tanto, probabilísticos, como la probabilidad de que la información personal caiga en manos equivocadas.[35] A lo anterior se suma que es muy difícil para la parte afectada probar la causalidad, ya que debido a la existencia de asimetrías de información, la víctima puede no ser consciente de la filtración de datos o no ser capaz de darse cuenta del daño que ha creado la misma. Esto eventualmente se contrarresta con la existencia de obligaciones de reporte cuando existe un riesgo razonable de que con ocasión de vulneraciones a las medidas de seguridad se genere daño.[36]

Para que tales mecanismos realmente funcionen, se requiere un comportamiento racional del consumidor, que entienda los riesgos implicados y qué medidas sea adecuado tomar, situación que en realidad no ocurre debido a sesgos de racionalidad limitada y a los altos costos de transacción. Aún más, es posible que de aumentar los reportes en los medios acerca de infracciones de seguridad que involucren desprotección de datos personales, se pueda crear un efecto de habituación psicológica, que insensibiliza tanto a los consumidores como a las empresas de sus efectos y, por lo tanto, minimiza el impacto deseado de las notificaciones (Acquisiti y Romanosky, 2009: 1.094).

Además, como la violación de datos implica la circulación de información, podría ocurrir que el daño real ocurra mucho después de que la situación que causó el incumplimiento y ya no sea posible reclamar las pérdidas a la empresa que incurrió en la responsabilidad. En una investigación con datos pertenecientes a infracciones de datos en Estados Unidos, Acquisti y Romanosky (2013: 131) concluyeron que entre todos los tipos de información personalmente identificable que requieren mayor protección, solo aquélla que comprometía datos financieros se correlaciona significativamente con la probabilidad de juicio. Esto tiene sentido, ya que en el mercado financiero es donde es más probable que ocurra un daño real y que se pruebe más fácilmente.

35. Vale la pena señalar que el artículo 82 del Reglamento reconoce explícitamente el derecho del interesado a recibir una compensación por el daño material o moral sufrido como resultado de una infracción.

36. Particularmente, al potencial daño acaecido debido a la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos personales tratados o la comunicación o acceso no autorizados de los mismos.

Los problemas que presenta la responsabilidad civil por filtración de datos guardan estrecha relación con el tipo de regla adoptada para la adecuada protección en la asignación de derechos. Siguiendo a Calabresi y Melamed (1972), estos últimos pueden ser protegidos por reglas de propiedad,[37] responsabilidad e inalienabilidad (o más de una a la vez). En la primera, quien desee obtener la asignación del derecho deberá negociar el precio *ex ante* con su titular. Dicha norma debiera ser utilizada cuando los costos de transacción son bajos, o bien, cuando siendo altos existe claridad sobre quién es el titular que a un menor precio puede evitar dichos costos (*least cost avoider*). En la segunda, la asignación puede tomarse del titular inicial pagando un precio objetivo, determinado por el mercado (ya sea por un tribunal o por una ley). En la tercera, la transferencia de la asignación está prohibida, aun cuando haya disposición de ambas partes a realizar la transacción.

Dado el valor subjetivo de la privacidad, el reconocimiento de que es alienable pero que su valor debe ser negociado *ex ante* por su titular —y no *ex post* por los tribunales de justicia o la ley mediante una compensación—, que los titulares son quienes valoran más su privacidad y protección de datos que quienes los tratan, y que la protección mediante reglas de propiedad protege el derecho de elegir por sobre la transferibilidad, se infiere que esta última es más eficiente (Jervis Ortiz, 2006: 250). Es por ello que las reglas de responsabilidad no resuelven las fallas existentes en el mercado.

Dicho lo anterior, vale la pena notar que el establecimiento de responsabilidad trata con la protección de la privacidad como un bien cuasi privado, pero deja de lado su protección como un bien público. En este sentido, una potencial alternativa sería crear acciones de clase para situaciones de violación de datos, ya que las mismas son eficientes cuando los reclamos individuales pueden no justificar un litigio individual. Esto no solo ayudaría con los costos de transacción, sino que también funcionaría en la protección de la privacidad como un bien público.[38]

Abuso de posición dominante

Como se ha señalado a lo largo de este artículo, los datos personales son de gran valor porque proporcionan a los participantes del mercado un activo importante para

37. El concepto de propiedad utilizado por el análisis económico del derecho no debe entenderse en el sentido del artículo 582 del Código Civil, sino que en una acepción más amplia que da importancia a la forma en que se protege la titularidad de un derecho. No obstante, generalmente los derechos de propiedad en sentido jurídico caben dentro de las asignaciones protegidas por las reglas de propiedad en el sentido expuesto por Calabresi y Melamed.

38. El actual proyecto de ley no contempla este tipo de acciones para entablar demandas por indemnización de perjuicios. Por su parte, el articulo 80 del Reglamento, si bien no la llama acción de clase pero sigue la misma lógica, otorga al interesado el derecho de ordenar a una entidad, organización o asociación sin fines de lucro que presente la queja en su nombre.

construir ventajas competitivas, como el conocimiento sobre el comportamiento de los usuarios y las preferencias de los consumidores, lo que permite el direccionamiento de productos y publicidad. Teniendo esto en cuenta, el uso indebido de datos personales también podría eventualmente subsumirse en la normativa que regula conductas que atenten contra la libre competencia del Decreto Ley 211, especialmente en lo que se refiere al abuso de posición dominante. La idea detrás de este argumento es que los mercados en línea —y en particular de las redes sociales— se encuentran altamente concentrados, lo que da un alto poder de mercado a sus participantes, quienes a través de conductas abusivas generarían una disminución de las posibilidades de que los usuarios controlen sus datos personales. En consecuencia, la aplicación estricta de las normas que regulan la libre competencia podría ser necesaria para que realmente exista una elección por parte del consumidor.

En esta línea, el año 2016 la autoridad de competencia alemana (*Bundeskartellamt*) fue pionera en Europa al iniciar un proceso contra Facebook Alemania por abuso de posición dominante en el mercado de redes sociales al infringir las normas de protección de datos.[39] Esto sentó un precedente en Europa, puesto que la recopilación de datos personales siempre había sido analizada y sancionada solo por las autoridades de protección de datos y no por las de competencia.[40] El argumento del *Bundeskartellamt* es que al condicionar Facebook a la aceptación de sus términos y condiciones respecto de las políticas de privacidad, los usuarios no tienen forma de optar a que sus datos personales no sean tratados por terceros asociados a las plataformas (como Whatsapp o Instragram), por lo que están sujetas a publicidad dirigida con el uso de esta información, lo que genera un efecto de bloqueo (*lock-in effect*). Por lo tanto, se argumenta que el consentimiento obtenido por el proveedor que tiene una posición dominante en el mercado bajo estas condiciones no es voluntario.

Otro ejemplo de cómo se relacionan estas dos áreas se refleja en el caso europeo de fusión de Facebook con Whatsapp. En 2014, la Comisión Europea autorizó la fusión de estas dos empresas, dado que Facebook argumentó que no sería posible

39. Charlotte Ducuing, «When competition law and data protection law embrace: The German Competition Authority investigates Facebook», CITIP Blog, 9 de enero de 2018, disponible en http://bit.ly/2Qk7xZw.

40. Como ocurrió en las decisiones de fusión de Google con Double Click y Facebook con Whatsapp, en las que la Comisión Europea declaró explícitamente que las preocupaciones relacionadas con la privacidad derivadas de la mayor concentración de datos no entran dentro del ámbito de las leyes de competencia de la Unión Europea, sino dentro del ámbito de la reglas de protección de datos de la Unión Europea. Para Google con Double Click, véase «Mergers: Commission clears proposed acquisition of DoubleClick by Google», European Commision Press Release Databse, 11 de marzo de 2008, disponible en http://bit.ly/2Qht1Gk. Para Facebook con Whatsapp, véase «Mergers: Commission approves acquisition of Whatsapp by Facebook», European Commision Press Release Databse, 3 de octubre de 2014, disponible en http://bit.ly/2QfZDAl.

combinar sus cuentas con las de los usuarios de Whatsapp. En agosto de 2016, una vez autorizada la fusión de ambas compañías, las nuevas políticas de privacidad de Whatsapp efectivamente incluyeron la posibilidad de vincular el número de teléfono del usuario con las identidades de los usuarios de Facebook. La Comisión multó a Facebook por 110 millones de euros por proporcionar información engañosa sobre la adquisición de Whatsapp. Como es posible apreciar, este caso está relacionado con el modelo propuesto por Choi, Doh-Shin y Byung-Cheol (2018), que busca promover el desarrollo de una buena reputación entre los competidores al fijar el precio cuando ocurre la integración de datos, abogando por la existencia de una opción para que los usuarios puedan efectivamente elegir. Así, la política de fomento de la reputación solo funcionaría si realmente hay una opción de elegir otra plataforma y ello ocurriría solo si la libre competencia está garantizada.

En consecuencia, mientras suficientes consumidores consideren la privacidad y la protección de sus datos a la hora de decidir qué servicio que trate sus datos utilizar y, a su vez, los proveedores ofrezcan diferentes grados de privacidad en sus servicios, un mercado competitivo podría garantizar mejor la protección de los datos personales. Bajo tales premisas, las reglas de competencia están estrechamente relacionadas con la protección de datos, ya que los datos personales y su uso crean nuevos mecanismos que permiten el abuso por parte de los proveedores. Por ende, a pesar de no tener como objetivo principal la protección de datos personales, dichas normas protegen indirectamente el derecho a la privacidad y la protección de los datos.

Cabe señalar que la lógica detrás de este argumento se refiere a la privacidad y la protección de datos como un bien cuasi privado, es decir, enfatiza el control del individuo sobre sus datos personales, pero no proporciona una solución directa a los problemas que surgen de la privacidad como bien público, como ineficiencias de coordinación bajo la racionalidad colectiva. No obstante, garantizar que los consumidores puedan elegir su privacidad constituye el primer paso para hacer frente a las ineficiencias del mercado: primero, el regulador debe ofrecer la posibilidad de elegir y luego crear un mecanismo que coordine las decisiones.

Conclusión

Dada la naturaleza del derecho a la privacidad como bien económico público, se concluye que centrarse únicamente en fortalecer el consentimiento del interesado —como lo han venido haciendo las tendencias regulatorias actuales— no es suficiente para abordar todas las fallas en el mercado de datos personales.

Aunque no existe una definición precisa del derecho a la privacidad y la protección de los datos personales, se reconoce que el mismo es renunciable, pero que, hasta el momento, no es recomendable establecer derechos de propiedad sobre su utilización para la creación de un libre mercado, ya que ello acarrearía consecuen-

cias indeseables, como sería la dificultad de control sobre la información y la difusa valoración de usos secundarios de la misma, la potencial discriminación contra las personas con capacidad económica restringida y la falta de solución a los problemas de incentivos y coordinación de la privacidad como bien público, en el que la racionalidad individual no es suficiente para resolver el dilema social generado.

Por ende, se concluye que dadas las características de la economía digital en la que nos encontramos inmersos, a largo plazo el mecanismo más eficiente y que mejor se ocupa de las fallas del mercado es la creación de cambios estructurales con aplicación de mecanismos tecnológicos, que centran el modelo de negocios en el usuario y crean conjuntos de datos como bienes públicos, de generación voluntaria y segura con adecuadas protecciones de privacidad.

En el corto plazo, los mecanismos *ex ante* resultan ser más eficientes que los *ex post*. En particular, la creación de impuestos junto con la implementación de mecanismos que apunten a la importancia de la buena reputación son los que mitigan mejor las externalidades de información y las asimetrías de información.

Referencias

Acquisiti, Alessandro (2010). «The economics of personal data and the economics of privacy». En OCDE Privacy Guidelines, WPISP-WPIE Roundtable. Disponible en http://bit.ly/2yO03Hq.

Acquisiti, Alessandro y Jean Grossklags (2005). «Privacy and rationality in individual decision making». *IEEE Security & Privacy Magazine*, 3 (1): 26-33. DOI: 10.1109/MSP.2005.22.

Acquisti, Alessandro, David Hoffman y Sasha Romanosky (2013). «Empirical analysis of data breach litigation». *Journal of Empirical Legal Studies*, 30: 1-31. DOI: 10.2139/ssrn.1986461.

Acquisiti, Alessandro y Sasha Romanosky (2009). «Privacy costs and personal data protection: Economic and legal perspectives». *Berkeley Technology Law Journal*, 24 (3): 1.061-1.102. DOI: 10.15779/Z38SD7D.

Akerlof, George (1970). «The market for "lemons": Quality uncertainty and the market mechanism». *The Quarterly Journal of Economics*, 84 (3): 488-500.

Athey, Susan (2014). «Information, privacy, and the internet: An economic perspective». reporte por encargo del CPB Netherlands Bureau for Economic Policy Analysis. Disponible en http://bit.ly/2CZTJQ9.

Bashir, Masooda, Carol Hayes, April Lambert y Jay Kesan (2015). «Online privacy and informed consent: The dilemma of information asymmetry». *Journal of Proceedings of the Association for Information Science and Technology.* 52 (1): 1-10. DOI: 10.1002/pra2.2015.145052010043.

Bass, Theo y Tom Symons (2017). *Me, my data and I: The future of the personal data economy*. Londres: DECODE. Disponible en http://bit.ly/2PLRgja.

Biczok, Gergely y Pern Hui Chia (2013). «Interdependent privacy: Let me share your data». En Ahmad-Reza Sadeghi (editor), *Financial cryptography and data security* (pp. 338-353). Heidelberg: Springer. DOI: 10.1007/978-3-642-39884-1_29.

Bloch, Francis y Gabriel Demange (2018). «Taxation and privacy protection on Internet platforms». *Journal of Public Economic Theory*, 20 (1): 52–66. DOI: 10.1111/jpet.12243.

Bullard, Alfredo (1998). «No se lo digas a nadie: ¿Se puede vender el derecho a la privacidad en el mercado?». *Ius et Veritas,* 17: 166-180. Disponible en http://bit.ly/2QpUKVD.

Calabresi, Guido y Douglas Melamed (1972). «Property rules, liability rules, and inalienability: One view of the cathedral». *Harvard Law Review*, 85 (6): 1.089-1.128. DOI: 10.1002/9780470752135.ch3.

—. (1960). «The problem of social cost». *The Journal of Law & Economics*, 3: 1-44. DOI: 10.1086/466560.

Choi, Jay Pil, Jeon Doh-Shin y Kim Byung-Cheol (2018). «Privacy and personal data collection with information externalities». *Social Science Research Network*, 8: 1-34. DOI: 10.2139/ssrn.3115049.

Cooter, Robert y Thomas Ulen (2016). *Law and economics*. Berkeley: Berkeley Law.

De la Maza, Iñigo y Rodrigo Momberg (2017). «Términos y condiciones: Acerca del supuesto carácter contractual de las autorizaciones para el tratamiento de datos personales en sitios web». *Revista Chilena de Derecho y Tecnología,* 6 (2): 25-55. DOI: 10.5354/0719-2584.2017.46226.

Fairfield, Joshua y Christoph Engel (2015). «Privacy as a public good». *Duke Law Journal*, 65 (3): 385-457. Disponible en http://bit.ly/2PfOG5t.

OCDE, Organización de Cooperación y Desarrollo Económicos (2018). *Tax challenges arising from digitalisation: Interim report 2018*. París. DOI: 10.1787/9789264293083-en.

Ostrom, Elionor (1990). *Governing the commons: The evolution of institutions for collective action*. Cambridge: Cambridge University Press.

Jervis Ortiz, Paula (2006). «La regulación del mercado de datos personales en Chile». Tesis para optar al grado de Magíster en Derecho, Universidad de Chile.

Martin, Kirsten (2013). «Transaction costs, privacy, and trust: The laudable goals and ultimate failure of notice and choice to respect privacy online». *Peer-Reviewed Journal on the Internet*, 18 (12). Disponible en http://bit.ly/2PcGNxr.

Posner, Richard (1978). «John A. Sibley lecture: The right of privacy». *Georgia Law Review*, 12 (3): 393-422. Disponible en http://bit.ly/2JOqocV.

Purtova, Nadezhda (2017). «Do property rights in personal data make sense after

the big data turn? Individual control and transparency». *Journal of Law and Economic Regulation,* 21: 1-27. Disponible en https://ssrn.com/abstract=3070228.

—. (2018). «The law of everything: Broad concept of personal data and future of EU data protection law». *Law, Innovation and Technology*, 10 (1): 40-81. DOI: 10.1080/17579961.2018.1452176.

Regan, Priscilla (2002). «Privacy as a common good in the digital world». *Information, Communication & Society*, 5 (3): 382-405. DOI: 10.1080/13691180210159328.

Rubinstein, Ira (2013). «Big data: The end of privacy or a new beginning?». *Journal of International Data Privacy Law*, 3 (2): 74-87. DOI: 10.1093/idpl/ips036.

Schwartz, Paul (2004). «Property, privacy, and personal data». *Harvard Law Review*, 117 (7): 2.056-2.128. Disponible en http://bit.ly/2PcJZZX.

Sholtz, Paul (2001). «Transaction costs and the social costs of online privacy». *First Monday, Peer Reviewed Journal on the Internet*, 6 (5). DOI: 10.5210/fm.v6i5.859.

Simon, Herbert (1970). «From substantive rationality to procedural rationality». En Spiro Latsis (editor), *Methods and appraisal in economics* (pp. 129-148). Cambridge: Cambridge University Press. DOI: 10.1017/CBO9780511572203.006.

Solove, Daniel (2002). «Conceptualizing privacy». *California Law Review*, 90 (4): 1.087-1.155. DOI: 10.15779/Z382H8Q.

—. (2006). «A taxonomy of privacy». *University of Pennsylvania Law Review*, 154 (3): 477-560. Disponible en http://bit.ly/2PcxZrF.

—. (2008). «The new vulnerability: Data security and personal information». En Anupam Chander, Lauren Gelman y Margaret Jane Radin (editores), *Securing privacy in the internet age*. Palo Alto: Stanford University Press.

Tene, Omer y Jules Polonetsky (2013). «Big data for all: Privacy and user control in the age of analytics». *Northwestern Journal of Technology and Intellectual Property*, 11 (5): 239-273. Disponible en http://bit.ly/2Pdq0Je.

Williamson, Oliver (2005). «The economics of governance». *The American Economic Review*, 95 (2):1-18. Disponible en http://www.jstor.org/stable/4132783.

WEF, World Economic Forum (2011). *Personal data: The emergence of a new asset class*. Ginebra. Disponible en http://bit.ly/2RD01sP.

Viollier, Pablo (2017). *El estado de la protección de datos personales en Chile*. Santiago: Derechos Digitales. Disponible en http://bit.ly/2APoeqk.

Sobre la autora

Catalina Frigerio Dattwyler es abogada. Licenciada en Ciencias Jurídicas y Sociales por la Universidad de Chile, magíster en Análisis Económico del Derecho, Eramus Mundus Master Programme, Universidad de Bolonia, Italia, Universidad de Gante, Bélgica, e Indira Gandhi Institute of Development Research, India. Su correo electrónico es catalina.frigerio@emle.eu.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista de Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

EDITOR GENERAL

Daniel Álvarez Valenzuela
(dalvarez@derecho.uchile.cl)

SITIO WEB

rchdt.uchile.cl

CORREO ELECTRÓNICO

rchdt@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.cl).