REVISTA CHILENA DE DERECHO Y TECNOLOGÍA
CENTRO DE ESTUDIOS EN DERECHO INFORMÁTICO • UNIVERSIDAD DE CHILE
ISSN 0719-2576 • VOL. 2 NÚM. 2 (2013) • PÁGS. 11-47 • DOI 10.5354/0719-2584.2013.30308

La autogestión de la privacidad y el dilema del consentimiento

Privacy self-management and the consent dilemma

DANIEL J. SOLOVE
George Washington University Law School

RESUMEN El enfoque normativo vigente para la protección de la privacidad implica lo que denomino «autogestión de la privacidad»: la ley entrega a las personas un conjunto de derechos que les permiten ponderar los costos y beneficios de la recolección, uso o divulgación de su información. El consentimiento legitima casi cualquier tipo de recolección, uso o divulgación de datos personales. Aunque la autogestión de la privacidad es ciertamente un componente necesario de cualquier régimen regulatorio, en este artículo considero que las expectativas puestas en este régimen se encuentran fuera de sus posibilidades. La autogestión de la privacidad no entrega a las personas un control significativo sobre sus datos. Por otra parte, la gente puede no autogestionar su privacidad apropiadamente debido a una serie de problemas estructurales. Existen demasiadas entidades recolectando y utilizando datos personales como para que sea factible que las personas administren su privacidad en forma separada con cada entidad. Es virtualmente imposible para la gente ponderar los costos y beneficios de revelar información o permitir su uso o transferencias sin un entendimiento de los potenciales usos posteriores, lo que limita aún más la efectividad de la autogestión de la privacidad. Para avanzar, la legislación y las políticas de privacidad deben enfrentar un complejo y confuso dilema sobre el consentimiento. En este artículo,

propongo varias maneras en que las leyes de privacidad pueden lidiar con el dilema del consentimiento y dejar de confiar demasiado en la autogestión de la privacidad.

PALABRAS CLAVE Privacidad, protección de datos personales, autogestión de la privacidad, consentimiento.

ABSTRACT The current regulatory approach for protecting privacy involves what I refer to as «privacy self-management» — the law provides people with a set of rights to enable them to decide how to weigh the costs and benefits of the collection, use, or disclosure of their information. People's consent legitimizes nearly any form of collection, use, and disclosure of personal data. Although privacy self-management is certainly a necessary component of any regulatory regime, I contend in this article that it is being asked to do work beyond its capabilities. Privacy self-management does not provide meaningful control. Moreover, people cannot appropriately self-manage their privacy due to a series of structural problems. There are too many entities collecting and using personal data to make it feasible for people to manage their privacy separately with each entity. It is virtually impossible for people to weigh the costs and benefits of revealing information or permitting its use or transfer without an understanding of the potential downstream uses, further limiting the effectiveness of the privacy self-management framework. In order to advance, privacy law and policy must confront a complex and confounding dilemma with consent. In this article, I propose several ways privacy law can grapple with the consent dilemma and move beyond relying too heavily on privacy self-management.

KEYWORDS Privacy, personal data protection, privacy self-management, consent.

INTRODUCCIÓN

Durante la década pasada, los problemas que involucran a la privacidad de la información —el advenimiento del *big data*[1] y los centros de

1. *Big data*: datos de gran tamaño, al punto que su tratamiento presenta retos logísticos significativos; también la rama de la computación dedicada a estos datos. (*N. del T.*)

intercambio de información, el tsunami de violaciones de seguridad de datos, el advenimiento de la web 2.0, el crecimiento del *marketing* por comportamiento y la proliferación de las tecnologías de rastreo— se han vuelto más complejos. Las autoridades han propuesto y aprobado significativas nuevas regulaciones en los Estados Unidos y el extranjero, sin embargo la forma básica de enfrentar la protección de la privacidad se ha mantenido prácticamente inalterada desde la década de 1970. Bajo el paradigma actual, la ley entrega a las personas un conjunto de derechos que les permiten tomar decisiones respecto a cómo gestionar sus datos. Estos derechos consisten básicamente en derechos de notificación, acceso y consentimiento, respecto a la recolección, uso y divulgación de datos personales. El objetivo de este conjunto de derechos es entregar a las personas el control respecto de sus datos personales, para que a través de este control puedan decidir por ellas mismas cómo determinar los costos y los beneficios de la recolección, uso y divulgación de su información. Me referiré a esta aproximación a la regulación de la privacidad como «autogestión de la privacidad».

La autogestión de la privacidad se basa en el consentimiento: trata de ser neutral respecto al fondo —si determinadas formas de recopilar, usar o divulgar datos personales son buenas o malas— y se centra en si la gente autoriza determinadas prácticas respecto de su privacidad. El consentimiento legitima casi cualquier tipo de colección, uso o divulgación de datos personales.

Aunque la autogestión de la privacidad es ciertamente un componente necesario y deseable de cualquier régimen regulatorio, considero que las expectativas puestas en este régimen se encuentran fuera de sus posibilidades. La autogestión de la privacidad no entrega a las personas un control significativo sobre sus datos. En primer lugar, investigaciones empíricas y de ciencias sociales han demostrado que existen severos problemas cognitivos que socavan la autogestión de la privacidad. Estos problemas cognitivos debilitan la capacidad de los individuos para realizar elecciones informadas y racionales respecto de los costos y beneficios de consentir en la recolección, uso y divulgación de sus datos personales.

En segundo lugar, y más problemático, incluso los individuos racionales y bien informados se encuentran impedidos de autogestionar su privacidad debido a varios problemas estructurales. Existen demasiadas entidades recolectando y utilizando datos personales como para que sea

factible que las personas administren su privacidad en forma separada con cada entidad. Además, muchos daños a la privacidad se producen como resultado de una agregación de distintos datos a través de un período de tiempo, por parte de diferentes entidades. Es virtualmente imposible para la gente ponderar los costos y beneficios de revelar información o permitir su uso o transferencias sin conocer los potenciales usos posteriores, lo que limita aún más la efectividad de la autogestión de la privacidad.

Adicionalmente, la autogestión de la privacidad trata este derecho en una serie de transacciones aisladas, guiadas por individuos particulares. Sin embargo, los costos y beneficios asociados a la privacidad son mejor evaluados cumulativa y holísticamente, no meramente a nivel del individuo. Como lo demuestran varios artículos de este Simposio,[2] la privacidad tiene un impacto social enorme. El profesor Neil Richards argumenta que la privacidad salvaguarda las actividades intelectuales, existiendo un valor social más amplio al proteger robusta y explícitamente la lectura, el discurso y la exploración de ideas (Richards, 2013: 1945-52). La profesora Julie Cohen argumenta que la innovación depende de la privacidad, la cual se encuentra cada vez más amenazada, a medida que el *big data* recolecta información de los individuos y los proveedores de contenidos rastrean el consumo de ideas de la gente a través de la tecnología (Cohen, 2013: 1904, 1918-27). Además, en varios casos, como sostiene el profesor Lior Strahilevitz, la protección de la privacidad tiene efectos distributivos; beneficia a algunas personas y daña a otras (Strahilevitz, 2013: 2010). La privacidad, entonces, hace más que proteger a personas individualmente consideradas. Promueve un cierto tipo de sociedad, ya que las decisiones de las personas sobre su propia privacidad afectan a toda la sociedad, y no sólo a ellas. Debido a que las decisiones individuales sobre consentir en la recolección, uso y divulgación de los datos puede que no conlleve el resultado social más deseable, la autogestión de la privacidad con frecuencia fracasa en abordar estos valores sociales más amplios.

Sin embargo, ante cada signo de fracaso por parte de la autogestión de la privacidad, la respuesta típica por parte de legisladores, académi-

2. El presente artículo fue inicialmente presentado en el Simposio sobre Privacidad y Tecnología de *Harvard Law Review*, en mayo de 2013. (*N. del T.*)

cos y otros, es pedir más y mejor autogestión de la privacidad. En este artículo argumento que, para avanzar, las leyes y políticas sobre privacidad deben enfrentar el problema que supone la autogestión de la privacidad y comenzar a concebir una nueva orientación.

Cualquier solución debe confrontar el complejo dilema del consentimiento. El consentimiento para utilizar y divulgar datos personales no suele ser significativo, y la solución más evidente —medidas paternalistas— niega a las personas, incluso de forma más directa, la libertad para tomar decisiones voluntarias sobre sus datos. Este paternalismo podría resultar fácil de justificar si muchos de los usos de los datos generasen pocos beneficios, o fuesen dañinos para las personas o la sociedad. Pero muchos de los usos de los datos tienen beneficios además de costos, y los individuos podrían llegar a conclusiones opuestas respecto a si los beneficios son mayores que los costos. Realizar esta elección por los individuos limita la autonomía de su voluntad. Consecuentemente, en la medida en que las soluciones legales sigan un camino que se aleje de la autogestión de la privacidad, hacia una alternativa más paternalista, probablemente se limitará la voluntad. Una vía de escape a este dilema sigue siendo elusiva.

Hasta que la regulación reconozca la verdadera profundidad de las dificultades que presenta la autogestión de la privacidad y confronte el dilema del consentimiento, las leyes sobre privacidad no serán capaces de avanzar mucho más. En este artículo propondré varias formas a través de las cuales las regulaciones pueden hacerle frente al dilema del consentimiento sin depender demasiado de la autogestión de la privacidad.

I. AUTOGESTIÓN DE LA PRIVACIDAD

La autogestión de privacidad tiene sus orígenes en las *Fair Information Practices,*[3] las cuales son comúnmente conocidas como las *Fair Information Practices Principles* (FIPP) (Gellman, 2013: 9-10). Las FIPP aparecieron oficialmente en un reporte del año 1973 emanado del *U.S.*

3. Principios Justos de Información. Véase Federal Trade Commission, «Fair Information Practice Principles», disponible en <http://www.ftc.gov/reports/privacy3/fairinfo.shtm>. (*N. del T.*)

Department of Health, Education, and Welfare (HEW)[4] con el fin de abordar las preocupaciones existentes respecto a la creciente digitalización de datos. Los principios incluían: 1) transparencia respecto a los sistemas de registro de datos personales, 2) el derecho a notificación respecto de dichos sistema de registro, 3) el derecho a impedir que los datos personales fuesen utilizados para nuevos fines sin consentimiento, 4) el derecho a corregir o enmendar los registros sobre información propia, y 5) la responsabilidad de los tenedores de datos para prevenir su mal uso.[5] Estos principios se encontraban plasmados selectivamente en varios estatutos en los Estados Unidos, y ayudaron a dar forma a las Directrices de Privacidad de la OCDE de 1980 y a la Norma Marco sobre Privacidad de la APEC de 2004.[6]

Casi todos los ejemplos de los FIPP no especifican qué datos pueden ser recolectados o cómo pueden ser utilizados. En cambio, la mayoría de las formas de recolección, uso y divulgación de datos son permisibles bajo los FIPP si las personas tienen la oportunidad de autogestionar su privacidad, esto es, si son notificadas y entregan su consentimiento.

La autogestión de la privacidad es tan ampliamente aceptada, que incluso profundas disputas sobre la protección de la privacidad se convierten en diferentes interpretaciones y aplicaciones de ella. En el año 2012, por ejemplo, la *Federal Trade Commission* (FTC) y la Casa Blanca, insatisfechas con el enfoque normativo actual, emitieron importantes nuevos marcos para la protección de la privacidad. En el núcleo de ambos, sin embargo, se encuentra el mismo viejo modelo de autogestión de la privacidad. El marco de la FTC apunta a «hacer que la recolección y usos de la información sean transparentes» y entregar a la gente la «capacidad de tomar decisiones sobre sus datos en momentos y contextos relevantes».[7] La pieza central de la propuesta hecha por la Casa Blanca

4. Departamento de Salud, Educación y Bienestar de los Estados Unidos de América. (*N. del T.*)

5. Secretary's Advisory Committee on Automated Personal Data Systems, *Records, computers and the rights of citizens*, U.S. Dep't. of Health, Education and Welfare, pp. 41-2.

6. Organisation for Economic Co-operation and Development, *OECD Guidelines on the protection of privacy and transborder flows of personal data*; Asia-Pacific Economic Cooperation, *Apec privacy framework*. Véase Gellman (2013: 7).

7. Federal Trade Commission, *Protecting consumer privacy in an era of rapid chan-*

en la *Consumer Bill of Rights*[8] es el derecho de los consumidores a ejercer un «control apropiado» sobre sus datos personales y a tomar «elecciones claras y simples, presentadas de tiempo en tiempo, y de maneras que permitan a los consumidores tomar decisiones significativas sobre la recolección, uso y divulgación de datos».[9]

Como expondré en esta parte, sin embargo, la autogestión de la privacidad enfrenta una serie de problemas que en conjunto demuestran que este paradigma, por sí mismo, no puede servir de núcleo para un régimen regulatorio viable de privacidad. En general analizaré dos tipos de problemas: 1) problemas cognitivos, referidos a los retos que se producen por la forma en que los seres humanos toman decisiones, y 2) problemas estructurales, referidos a los retos que surgen por la forma en que están diseñadas las decisiones sobre privacidad.

A) PROBLEMAS COGNITIVOS

Un número de problemas cognitivos plagan la autogestión de la privacidad. La autogestión de la privacidad supone una persona racional e informada que toma decisiones apropiadas respecto a consentir o no en las múltiples formas de recolección, uso y divulgación de datos personales. Pero tanto evidencia empírica como estudios en ciencias sociales muestran que la capacidad de las personas para tomar estas decisiones informadas y racionales ni siquiera se acercan a la visión contemplada por la autogestión de la privacidad.

1) *El problema del individuo desinformado*. Dos de los componentes más importantes de la autogestión de la privacidad son informar a los individuos sobre los datos que son recolectados y utilizados (notificación) y permitirles decidir si aceptan o no tal recolección y uso (elección). Estos componentes son ampliamente aceptados en los Estados Unidos

ge. Recommendations for businesses and policymakers, disponible en <http://ftc.gov/os/2012/03/120326privacyreport.pdf>.

8. Proyecto de Ley de Derechos del Consumidor. (*N. del T.*)

9. The White House, *Consumer data privacy in a networked world a framework for protecting: Privacy and promoting innovation in the global digital economy*, disponible en <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

(Brill, 2010), en un enfoque denominado «notificación y elección». Las entidades han normalizado la práctica de proveer notificación y elección al ofrecer notificaciones de privacidad y la posibilidad de *opt-out*[10] de algunas de las formas de recolección y utilización de datos descritas en las notificaciones.

La FTC ha intervenido para servir como una especie de ente coercitivo de las notificaciones de privacidad. Desde 1998, la FTC ha mantenido que quebrantar promesas hechas en una notificación de privacidad es constitutivo de «actos o prácticas desleales o engañosas en el comercio o que afectan el comercio» lo que constituye una vulneración del *Federal Trade Commission Act*.[11] Cuando encuentra una vulneración de esta naturaleza, la FTC puede interponer acciones civiles y solicitar medidas cautelares.[12] El enfoque de notificación y elección también se ha plasmado en el centro de la legislación en materia de privacidad. La ley Gramm-Leach-Bliley[13] requiere, por ejemplo, que las instituciones financieras provean a sus clientes notificaciones de privacidad, permitiéndoles a sus clientes la posibilidad de *opt-out* respecto de los datos compartidos con terceros.[14]

A pesar de la adopción de la notificación y elección, la gente no parece estar muy involucrada en la autogestión de su privacidad. Regularmente, la mayoría de las personas no lee las notificaciones de privacidad.[15] Res-

---

10. Elegir no participar en algo. (*N. del T.*)

11. Ley de la Comisión Federal de Comercio. (*N. del T.*) 15 U.S.C. § 45(a)(1) (2006). Para más antecedentes sobre la aplicación de las políticas en materia de privacidad realizadas por la FTC, véase Solove y Schwartz (2011: 820-31).

12. 15 U.S.C. § 45(l)-(m).

13. También conocida como Ley de Modernización de los Servicios Financieros (Financial Services Modernization Act). (*N. del T.*) Gramm-Leach-Bliley Act de 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codificada en secciones repartidas entre los títulos 12 y 15 del U.S.C.).

14. 15 U.S.C. § 6802(a)-(b) (2006).

15. Véase Nissenbaum (2010: 105), quien analiza un estudio del año 2006 que mostraba que «la mayor parte del tiempo» sólo un 20 % de la gente leía las notificaciones de privacidad (citando, TRUSTe y TNS, «Consumers have a false sense of security about online privacy: Actions inconsistent with attitudes», *PR Newswire*, 6 de diciembre de 2012, disponible en <http://www.prnewswire.com/news-releases/consumers-have-false-sense-of-security-about-online-privacy---actions-inconsistent-with-attitudes-55969467.html>). Cate (2006: 343, 361-2), Milne y Culnan (2004: 15, 20-1) encontraron que

pecto a las otras clases de notificaciones, tales como acuerdos de licencia de usuario final y contratos de adhesión, los estudios muestran que sólo un minúsculo porcentaje de gente los lee.[16] Más aún, poca gente ejerce su derecho de *opt-out* respecto de la recolección, uso o divulgación de sus datos, cuando se les presenta la oportunidad de hacerlo.[17] La mayoría de la gente ni siquiera se molesta en cambiar la configuración preestablecida de los sitios de Internet (Acquisti y Grossklags, 2008: 363, 369). Como el director de la FTC, Jon Leibowitz, ha concluido: «inicialmente, las políticas de privacidad parecían una buena idea. Pero en la práctica, dejan mucho que desear. En muchos casos, los consumidores no notan, leen o entienden las políticas de privacidad» (Leibowitz, 2007).

¿Por qué hay tan pocas personas involucradas en la autogestión de la privacidad? Una explicación posible es que las notificaciones de privacidad son largas y difíciles de comprender.[18] Han existido muchas propuestas para acortar y simplificar las políticas de privacidad, aunque este tipo de medidas no ha mostrado una mejora significativa en su comprensión.[19] Por ejemplo, el profesor M. Ryan Calo sugiere que la «notificación visceral» puede resucitar el enfoque de notificación, al intentar hacer que la gente experimente las notificaciones de forma más directa y emocional (Calo, 2012: 1034-35). Como ejemplo, Calo hace referencia al esfuerzo de la FDA de requerir advertencias gráficas, incluyendo imágenes de muerte, en los cigarrillos (2012: 1069-70). Aunque algunas advertencias antitabaco pueden ser efectivas, por cuanto el cáncer y la

---

sólo el 4,5 % de los encuestados dijeron que siempre leían los avisos de privacidad de las páginas de Internet y 14,1 % los leía frecuentemente.

16. Véase, por ejemplo, Ben-Shahar y Schneider (2011: 647, 665-78), Marotta-Wurgler (2011: 165, 178), quienes comentan un estudio que revelaba que las personas accedían a la sección donde se encontraban los contratos de adhesión menos del 1 % de las veces.

17. Véase Janger y Schwartz (2002: 1219, 1230), quienes señalan que de acuerdo a un estudio «sólo un 0,5 % de los clientes bancarios había hecho valer sus derechos de *opt out*».

18. Véase Anton y otros (2004: 36, 42-4), Janger y Schwartz (2002: 1230-2) y Sherman (2008).

19. «Los estudios sólo muestran una mejora marginal en el entendimiento de los consumidores cuando las políticas de privacidad son expresadas como tablas, íconos o etiquetas, asumiendo que el consumidor ni siquiera las lee» (Calo, 2012: 1027, 1033).

muerte son consecuencias bien terribles y concretas, las advertencias de privacidad pueden ser más difíciles de traducir en términos viscerales debido a que sus consecuencias son mucho más abstractas.

Existe un problema aún más difícil con las propuestas para mejorar las notificaciones, ya sean simplificadas o viscerales. Tales propuestas no toman en consideración un dilema fundamental de las notificaciones: hacerlas simples y fáciles de entender entra en conflicto con la finalidad de informar a las personas, en los términos más completos posibles, sobre las consecuencias de entregar información, consecuencias que pueden resultar bastante complejas si se explican con suficientes detalles como para que valga la pena. La gente necesita un entendimiento y antecedentes más profundos para tomar decisiones informadas. Sin embargo, muchas notificaciones de privacidad son vagas sobre los futuros usos de los datos.

Además, como señala Strahilevitz en este Simposio, las elecciones sobre la privacidad son frecuentemente de orden binario, como sucede con el Do Not Call Registry[20] que permite a las personas ejercer un *opt-out* respecto de ofrecimientos a través de *telemarketing* (Strahilevitz, 2013: 2038). Muchas personas pueden desear mayor nivel de decisión, pero esto implicaría añadir mayor complejidad, creando mayores riesgos de confusión.

Agravando las dificultades asociadas a la notificación y elección, se encuentra el hecho de que la gente opera bajo supuestos incorrectos sobre cómo su privacidad es protegida. Un estudio encontró que las personas sólo respondieron correctamente un 30 % de las preguntas acerca de la privacidad de sus transacciones en línea (Turow y otros, 2009: 20-1). Otro estudio encontró que el 64 % (de las personas encuestadas) no sabían que un supermercado está autorizado para vender a otras compañías la información sobre lo que compraban y que el 75 % falsamente creía que cuando «un sitio de Internet tenía una política de privacidad, significaba que el sitio no podía compartir mi información con otros sitios o compañías» (Turow, Feldman y Meltzer, 2005).

Hasta ahora, en la mayoría de las situaciones la gente no se involucra

20. Registro nacional a través del cual una persona puede elegir no recibir llamadas con fines de *telemarketing*. Véase Federal Trade Commission, «National Do Not Call Registry», disponible en <https://www.donotcall.gov/>. (*N. del T.*)

en actividades de autogestión de privacidad. La evidencia sugiere que las personas no están bien informadas sobre materias de privacidad. Los esfuerzos para mejorar la educación en esta materia son ciertamente loables, como también lo son los esfuerzos para hacer las notificaciones de privacidad más comprensibles. Pero tales esfuerzos fracasan en afrontar un problema más profundo: la privacidad es bastante complicada. Este hecho lleva a la disyuntiva entre proveer una notificación que sea significativa o entregar una simple y corta.

2) *El problema de la toma de decisiones sesgada*. Incluso si la mayoría de las personas leyeran habitualmente las políticas de privacidad, la mayoría de ellas carece de la pericia suficiente para sopesar las consecuencias de autorizar determinados usos o divulgaciones de sus datos. Las personas entregan rutinariamente sus datos a cambio de beneficios bastante menores (Acquisti y Grossklags, 2006: 15, 16). Algunos concluyen de esta circunstancia que los consumidores no dan gran valor a su privacidad (Goldman, 2002). Algunos han sugerido que puede haber un cambio generacional en las normas de privacidad, en donde la gente joven ya no esté interesada en la privacidad (Nussbaum, 2004). Pero en los estudios la gente habitualmente declara lo importante que les resulta su privacidad, y la actitud hacia la privacidad, tanto en adultos como en jóvenes, es bastante similar (Hoofnagle y otros, 2010).

Existe entonces una clara incoherencia entre el alto valor que se señala que tendría la privacidad y la conducta de las personas, la cual indica que se le asigna un valor muy bajo. ¿Esto significa que a las personas no les importa la privacidad? Los estudios existentes en ciencias sociales indican que esta desconexión provendría de ciertos impedimentos para tomar decisiones racionales.

Los trabajos en ciencias sociales —que definiré en términos amplios incluyendo la economía conductual, la psicología y estudios empíricos de otras áreas— muestran que muchas de nuestras suposiciones más preciadas sobre la forma en que las personas toman decisiones respecto a su privacidad son erradas. Como señalan los profesores Richard Thaler y Cass Sunstein, la «presunción es que casi todas las personas, casi todo el tiempo, toman decisiones que favorecen sus intereses, en el peor de los casos, mejores que las que tomaría un tercero en su lugar» (Thaler y Sunstein, 2008: 9). Estudios realizados por los profesores Daniel Kah-

neman, Amos Tversky y otros, demuestran la falsedad del modelo tradicional de agente racional en la toma de decisiones, por cuanto muchas veces las personas toman sus decisiones basadas en la heurística y en la forma en que las alternativas son presentadas (Kahneman, 2011: 411).[21]

Las personas tienen una «racionalidad limitada» —luchan por aplicar su conocimiento a situaciones complejas— con respecto a la privacidad (Acquisti y Grossklags, 2006: 25-6). Como observan los profesores Alessandri Acquisti y Jens Grossklags, «nuestra racionalidad limitada innata limita nuestra habilidad para adquirir, memorizar y procesar toda la información relevante, y nos hace confiar en modelos mentales simplificados, estrategias aproximadas y la heurística» (2008: 369). La evaluación del riesgo también se encuentra sesgada por la «disponibilidad heurística», donde las personas evalúan peligros conocidos como más riesgosos, que aquellos desconocidos (Thaler y Sunstein, 2008: 25).

Las ciencias sociales también revelan que las preferencias de privacidad no se desarrollan abstractamente, sino que dentro de un contexto. La forma en que las elecciones son presentadas, y muchos otros factores, tienden a sesgar las preferencias de privacidad (Acquisti y Loewenstein, 2009). Las personas también se encuentran más dispuestas a compartir información personal cuando se sienten en una situación controlada, sin importar si tal control es real o ilusorio. Generalmente, «las personas están más dispuestas a tomar riesgos y juzgarlos como menos severos, cuando se sienten en control» (Brandimarte, Acquisti y Loewenstein, 2013: 3).

Las personas también tienden a cometer ciertos errores de juicio de forma consistente (Ariely, 2008: 240-1). En esta época, empresas, políticos y otros, que buscan influenciar decisiones, están recién comenzando a aprovechar los conocimientos provenientes de las ciencias sociales y hasta ahora utilizan medios de persuasión para nada científicos y más bien anecdóticos. Cuando quienes buscan influenciar decisiones lo hagan basados en técnicas entregadas por las ciencias sociales (las que irónicamente han podido surgir gracias a la siempre creciente cantidad de datos sobre individuos y sus comportamientos), las elecciones de las personas podrán ser controladas como nunca antes (las cuales irónica-

21. Véase, en general, Kahneman y Tversky (2000) y Kahneman, Slovic y Tversky (1982).

mente, podrán ser estructuradas para hacer creer que son las personas quienes toman las decisiones).

El resultado final de este problema es que las decisiones sobre privacidad son particularmente susceptibles de problemas como la racionalidad limitada, la disponibilidad de la heurística y los «efectos de encuadre» debido a lo complejo, contextual y difícil de conceptualizar de la privacidad.

Los problemas cognitivos señalados presentan entonces numerosos obstáculos a la autogestión de la privacidad: 1) la gente no lee las políticas de privacidad; 2) si las leen, no las entienden; 3) si las leen y las entienden, usualmente carecen de los conocimientos y pericia necesarios para tomar una decisión informada; y 4) si las leen, entienden y pueden tomar una decisión informada, su decisión puede verse sesgada por varias dificultades producidas en el proceso de toma de decisiones. La situación se asemeja a aquella enfrentada por el protagonista del relato de Franz Kafka «Ante la ley», en donde la entrada es resguardada por un conjunto infinito de guardianes, cada uno más poderoso que el anterior (Kafka, 1998: 215).

B) PROBLEMAS ESTRUCTURALES

Incluso si asumimos que las personas son racionales, que están plenamente informadas, que existe una forma de impedir que su toma de decisiones sea sesgada y una forma de capturar sus preferencias de forma precisa, la autogestión de la privacidad enfrenta además serios problemas estructurales. Estos problemas estructurales impiden evaluar adecuadamente los costos y beneficios de consentir las diversas formas de recolección, uso y divulgación de información personal. La estructuración de decisiones en materia de privacidad resulta ser una tarea inmensamente difícil.

1) *El problema de escala*. Una persona puede ser capaz de administrar su privacidad con varias entidades, pero la autogestión de privacidad no funciona tan bien a medida que la necesidad de utilizarla aumenta. Incluso si cada entidad proveyera a las personas una forma fácil y clara de administrar su privacidad, son simplemente demasiadas las entidades que recolectan, utilizan y dan a conocer los datos de una persona, como

para que ésta pueda manejarlo. En particular, el americano promedio visita alrededor de cien páginas de Internet al mes, y realiza negocios en línea con innumerables compañías (servicios, seguros, tecnologías, viajes, financieros, etcétera).[22] Las personas no sólo tendrán dificultades para administrar su privacidad con entidades que conocen, ya que además existen innumerables entidades que tratan datos personales sin que la gente se dé cuenta. Las personas no pueden administrar su privacidad respecto a estos extensos «depósitos» de datos a menos que conozcan su existencia y puedan identificar a las entidades que las mantienen (Citron, 2007: 241, 243-51).

Este problema nos recuerda al desafortunado estudiante cuyos profesores colectivamente le asignan demasiadas lecturas cada noche. De la perspectiva de cada profesor, la extensión del texto parece razonable para una tarde. Pero cuando simultáneamente cinco o seis profesores asignan lecturas para una tarde, el volumen en conjunto se vuelve excesivo. Entonces, incluso si todas las compañías proveyeran notificaciones de privacidad e instancias de decisión adecuadas, este problema de administración de datos persistiría; la persona promedio simplemente no posee el tiempo suficiente o los recursos necesarios para administrar su privacidad en todas las entidades que tienen sus datos. Un estudio ha estimado que costaría alrededor de $781 billones de dólares en productividad perdida, si cada persona leyera cada política de privacidad de los sitios que visitasen en el período de un año (McDonald y Cranor, 2008: 543, 564). Y muchas entidades modifican frecuentemente sus condiciones de privacidad, por lo que leerlas sólo una vez al año no bastaría. El problema se produce tanto con políticas de privacidad *opt-in*,[23] como *opt-out*.

Muchas entidades quieren hacer lo correcto y ser transparentes respecto a sus prácticas de privacidad y sobre cómo serán utilizados los datos de las personas. Sin embargo, incluso con políticas de privacidad simples, visibles y entendibles, el problema de escala persistiría.

---

22. Véase The Nielsen Company, «August 2011. Top US Web Brands», *Nielsen Wire*, 30 de septiembre, disponible en <http://blog.nielsen.com/nielsenwire/online_mobile/august-2011-top-us-web-brands/>.

23. Elegir participar en algo. (*N. del T.*)

2) *El problema de agregación.* Otro problema es que incluso si las personas toman decisiones racionales sobre compartir fragmentos aislados de datos, resulta difícil poder analizar cómo serán utilizados esos datos en el futuro. Supongamos que en una oportunidad una persona entrega un dato bastante inofensivo, pensando que no está revelando nada sensible. Más adelante esta persona entrega otro dato igual de inofensivo. Sin pensarlo, esta información puede ser combinada y analizada para revelar hechos bastante sensibles sobre esta persona, la que nunca dio a conocer esta información sensible, ni anticipó que ésta sería descubierta. El problema fue que entregó demasiadas pistas. El análisis moderno de datos, que también es denominado como minería de datos o *big data,* puede deducir bastante información sobre una persona a partir de estas pistas. En otras palabras, pequeños pedacitos de información pueden decir mucho cuando son combinados.[24] Me he referido a esto como el «efecto de agregación» (Solove, 2004: 44-7).

El problema con el efecto de agregación es que vuelve prácticamente imposible cualquier manejo de datos. Las clases de nueva información que pueden ser obtenidas a partir del análisis de información existente y las predicciones que pueden ser realizadas a partir de estos datos son demasiado vastas y complejas, y evolucionan demasiado rápido como para que las personas puedan evaluar completamente los riesgos y beneficios involucrados. Este escenario hace muy difícil evaluar si entregar cualquier tipo de información permitirá más tarde revelar información sensible de una persona al combinarse con otros datos.

Los costos y beneficios de cada situación dependen del conjunto de decisiones sobre la entrega de información, tomadas previamente. En la época 1, puede que haya tenido sentido para una persona revelar el hecho 1. En la época 2, la persona puede decidir revelar el hecho 2. Lo que es difícil determinar es si en la época 3, los hechos 1 y 2 podrían ser combinados para revelar el hecho 3 y si esta persona podría verse dañada por el hecho de que se dé a conocer o se use el hecho 3. Incluso, en la época de revelar el hecho 1 y el hecho 2, la persona podría no tener idea que el hecho 1 más el hecho 2 den como resultado el hecho 3.

24. Además de obtener nueva información a partir de la combinación de trozos de información, el análisis de datos puede realizar predicciones sobre comportamientos futuros. El *big data* puede saber algo sobre alguien, incluso antes que esa persona.

En el mundo real no tenemos unos pocos hechos, sino que miles de datos. Supongamos que durante el transcurso de la década pasada una persona entrega 50.000 datos. La persona no se ha visto negativamente afectada por revelarlos. Un día, la persona revela el 50.001, un hecho relativamente inocuo que combinado con otros datos que la persona entregó muchos años antes revelan el hecho 50.002. Deducido a través de un algoritmo creado recientemente, este hecho prueba ser dañino para la persona.

Por supuesto, el hecho 50.002 podría resultar ser beneficioso para la persona, o para la sociedad en su conjunto; quizás revela que esa persona se encuentra en riesgo de contraer una enfermedad altamente contagiosa y letal. El punto es que es virtualmente imposible para una persona realizar juicios sustantivos sobre los costos y beneficios de revelar cierta información. Por lo tanto, en muchas situaciones se desconoce demasiado como para tomar una decisión relevante sobre costos y beneficios al momento en que se le pide a una persona que administre su privacidad.

Para permitir que una persona tome una decisión racional sobre compartir datos, esa persona tendría que tener un entendimiento del rango de posibles daños y beneficios, como para poder hacer un análisis de costo-beneficio. Claro, las personas toman decisiones todo el tiempo en escenarios inciertos, pero cuando lo hacen tienden a hacerlo bastante mal. Como lo ha señalado el psicólogo Daniel Gilbert, las predicciones de las personas acerca de cómo varios eventos pueden afectar su felicidad futura son notablemente erróneos (Gilbert, 2006: 24-5).

Otro reto es que la agregación altera la posibilidad de identificar otros datos. La normativa sobre privacidad tiene típicamente su ámbito de aplicación sobre «información personal identificable» (o PII, del inglés «personally identifiable information»), definida en términos generales como información que permite la identificación de un individuo. Típicamente, las leyes de privacidad regulan sólo cuando existe PII involucrada (Schwartz y Solove, 2011: 1814, 1816). Un problema con la PII es que, como se ha discutido más arriba, no es estática: la posibilidad de identificar a través de datos depende del contexto (2011: 1890). Una búsqueda en Internet, por ejemplo, no es inherentemente identificable. Su capacidad de identificación dependerá de la información disponible en línea. Tal como el caso de los famosos resultados anónimos de búsqueda de AOL, que fueron dados a conocer y que permitieron a un reportero

identificar a una persona basado en las búsquedas que realizó (Barbaro y Zeller, 2006: i). A medida que se agregan datos, la información que no es identificable puede convertirse en identificable.

3) *El problema con evaluar el daño*. Agravando estos problemas, se encuentra el hecho de que las personas usualmente se inclinan por los beneficios inmediatos incluso cuando pueden existir detrimentos futuros (Acquisti y Grossklags, 2006: 372). El efecto de agregación muestra que la privacidad es un asunto de manejo de información a largo plazo, mientras que la mayoría de las decisiones para consentir en la recolección, uso o divulgación de información, se encuentran vinculados a beneficios de corto plazo.

La autogestión de la privacidad le pide a la gente que evalúe de forma temprana el daño potencial que pueden inferirse, generalmente cuando los datos son inicialmente recolectados. Sin embargo, por un número de razones, la gente encontrará inmensamente difícil realizar este análisis de costo-beneficio. Primero, como ya fue discutido, muchos daños a la privacidad son cumulativos por naturaleza: las personas acceden a muchas formas de recolección, uso y divulgación de datos a través de un largo período, y los efectos dañinos pueden sólo emerger de los usos de los datos a través del tiempo.

Los daños a la privacidad, mientras tanto, son usualmente pequeños y dispersos. Por supuesto que revelar fotografías de desnudos o datos altamente vergonzosos o que causen descréditos, pueden generar gran angustia emocional. La mayoría de las violaciones a la privacidad probablemente sólo causarán una picadura. A pesar de este hecho, sería incorrecto concluir que debieran ser ignoradas. Una picadura de abeja puede ser un asunto de baja importancia, pero un centenar o un millar pueden ser letales. Los daños provenientes de las violaciones a la privacidad pueden desarrollarse gradualmente a través del tiempo, pero las decisiones sobre privacidad pueden ser hechas de forma individual y con bastante anticipación.

Adicionalmente, la autogestión de la privacidad no toma en cuenta el impacto social que tienen las decisiones individuales sobre privacidad. La privacidad de las personas tiene varias funciones sociales. Se ha reconocido que la privacidad es un «componente» de la sociedad (Janger y Schwartz, 2002: 1247). La profesora Priscilla Regan demues-

tra la necesidad de entender la privacidad en cuanto a sus beneficios sociales (Regan, 1995: 212-4). El profesor Joel Reidenberg sostiene que «la sociedad en su conjunto tiene un interés importante en los contornos de la protección de la información personal» (Reidenberg, 2003: 877, 882-3). El profesor Spiros Simitis reconoce que «las consideraciones de privacidad ya no surgen de problemas individuales determinados, sino que expresan conflictos que afectan a todos» (Spiros Simitis, 1987: 707, 709). El entonces profesor Robert Post afirmaba que la protección de la privacidad «garantiza reglas de civilidad que, en forma significativa son elementos constitutivos tanto de los individuos, como de la comunidad» (Post, 1989: 957, 959). El profesor Paul Schwartz ha desarrollado la teoría de la privacidad constitutiva, argumentando a favor de la importancia de la privacidad en la sociedad civil (Schwartz, 1999: 1609, 1613). Schwartz se centra en la forma en que la protección de la privacidad informativa puede favorecer el autogobierno y la democracia en Internet (1999: 1613-4).

Según Cohen, la protección de la privacidad «conserva una zona de autonomía informativa para las personas» (Cohen, 2000: 1373, 1428). La privacidad es esencial no sólo para nuestro desarrollo individual, sino también para nuestro desarrollo cultural. Nuestro desarrollo intelectual depende de la creatividad de otros, y nuestra creatividad, a su vez, da forma al crecimiento intelectual de aquéllos. Estas fuerzas interactúan para desarrollar una cultura rica. Atrofiar la creatividad individual y el desarrollo intelectual empobrecen a la sociedad en su conjunto (Cohen, 2013: 1918).

El concepto de «privacidad intelectual» de Richards también reconoce la importancia de la privacidad desde un punto de vista social más amplio (Richards, 2008: 387). Richards afirma que «las nuevas ideas se desarrollan mejor lejos del intenso escrutinio de la exposición pública» y que la privacidad es esencial para promover la libertad intelectual (Richards, 2013: 1946). También sostiene que la privacidad intelectual «debe ser tutelada tanto respecto de agentes privados, como del Estado», porque «estamos limitados en nuestras acciones tanto por la presión del grupo, como por el Estado» (2013: 1951).

La autogestión de la privacidad cede a los individuos, en forma sustancial, la responsabilidad de preservar la privacidad, y asume que el principal daño que debe remediar es la recolección, uso o divulgación de

datos sin consentimiento. Aunque ir en contra del consentimiento constituye un daño susceptible de ser remediado, las acciones colectivas de las personas respecto a la privacidad pueden involucrar valores sociales más amplios. La autogestión de la privacidad no previene, remedia, ni siquiera considera las infracciones a esos valores sociales.

Hay un valor social compensatorio en ciertos usos de datos, como cuando son usados con fines investigativos, lo que podría justificar el no requerimiento de consentimientos individuales. Como hemos dicho Schwartz y yo en otro trabajo, el análisis de datos ha llevado a tratamientos médicos nuevos y mejorados, así como también a respuestas más eficaces a las violaciones a sistemas de seguridad de datos (Schwartz y Solove, 2011: 1866-8). Hay, pues, valores sociales tanto a favor como en contra de la privacidad que no se reflejan adecuadamente en la autogestión de la privacidad, que se centra exclusivamente en el consentimiento.

A menudo, la autogestión de la privacidad pide a la gente tomar decisiones en un punto temprano en el tiempo (cuando se recolecta la información) y en una serie de casos aislados. Pero las verdaderas consecuencias para las personas por el uso de esa información no pueden ser conocidas cuando se toman estas decisiones. Además, las consecuencias son acumulativas, y no pueden ser evaluadas adecuadamente en una serie de operaciones aisladas. La estructura misma de la autogestión de la privacidad impide lograr su objetivo de dar a la gente el control efectivo sobre sus propios datos. Además, su enfoque centrado en individuos deja de lado las amplias dimensiones sociales de la privacidad.

II. MÁS ALLÁ DE LA AUTOGESTIÓN DE LA PRIVACIDAD

¿Dónde debe apuntar la regulación de la privacidad a partir de ahora? Aferrarse con más fuerza a la autogestión de la privacidad no es la respuesta. Tampoco es el abandono de este paradigma o abrazar la regulación paternalista. En esta parte, propongo una guía para la dirección futura de la regulación de la privacidad. Aunque estoy lejos de proponer una solución final, puedo señalar, con razonable confianza, qué caminos son fructíferos y cuáles no lo son.

A) NAVEGANDO EL DILEMA DEL CONSENTIMIENTO

A través de la autogestión de la privacidad, la ley busca dar a las personas el control sobre sus datos. El núcleo de este control implica dar a la gente la facultad para decidir y dar su consentimiento para la recopilación, uso y divulgación de sus datos. Como he demostrado, en muchas situaciones las personas no son capaces de dar un consentimiento verdaderamente válido.

La alternativa más obvia sería que la ley regule y establezca ciertas decisiones sobre privacidad. Sin embargo, la regulación de la privacidad correría el riesgo de ser demasiado paternalista. La norma que deje de lado el consentimiento negará a las personas la libertad de elección. El resultado final sería que las personas tomen elecciones que no dan un control real, o que se les niegue por completo la facultad de elegir. Irónicamente, la regulación paternalista podría limitar la libertad para decidir de las personas, en el nombre de salvaguardar su autonomía. A este problema lo llamo el «dilema del consentimiento». Los académicos dedicados a la privacidad deben identificar una concepción del consentimiento que proteja la privacidad y evite el paternalismo.

1) *Repensando el consentimiento y el paternalismo*. El consentimiento es un concepto insuficientemente estudiado, y es crucial para la privacidad y para muchas otras áreas del derecho. El consentimiento cumple una enorme cantidad de funciones. Actividades que de otro modo serían ilegítimas, se hacen legítimas a través del consentimiento. Por ejemplo, una persona puede convenir en mantener la confidencialidad de cierta información como una condición para un determinado empleo. La persona normalmente sería libre para hablar acerca de esta información en virtud del derecho a la libertad de expresión establecido en la Primera Enmienda, pero en cambio ha accedido a renunciar a este derecho (Solove y Richards, 2009: 1650, 1676). De hecho, muchos de los derechos constitucionales pueden ser renunciados con el consentimiento, incluidos algunos que implican temas de privacidad, tales como los derechos a la libertad de expresión y de asociación de la Primera Enmienda; el derecho a la protección contra registros e incautaciones irrazonables de la Cuarta Enmienda; el derecho a la protección contra la autoincrimi-

nación de la Quinta Enmienda;[25] y el derecho a la privacidad de la información (Solove y Richards, 2009: 1653). Además de renunciar a sus derechos constitucionales, las personas pueden dar su consentimiento a una amplia gama de otras incursiones en su privacidad, como la vigilancia de las comunicaciones y las pruebas de drogas.[26]

Como he demostrado anteriormente, las personas no pueden manejar adecuadamente su propia privacidad, y el consentimiento no da un control significativo en muchos contextos relacionados con la privacidad. La primera alternativa regulatoria, avalada por varios académicos, es que la ley debe regular la privacidad de una manera más paternalista. Por ejemplo, la profesora Anita Allen sostiene que la privacidad es un «bien humano fundacional», esencial para una sociedad libre y democrática (Allen, 2011: 13). Sostiene que, en ciertos casos, la privacidad debe imponerse: «en aras de bienes humanos fundacionales, las sociedades liberales limitan adecuadamente tanto la coerción del Estado como la elección individual...» (2011: 13).

Cohen critica la noción de privacidad como algo que siempre puede ser «intercambiado por otros bienes» (Cohen, 2012: 148). Bajo su punto de vista, las personas no debieran poder renunciar a la privacidad en una serie de circunstancias. La renuncia a la privacidad puede conducir a una menor creatividad e incidir en el desarrollo de la individualidad. En su contribución a este simposio, Cohen sostiene que la privacidad «es una característica estructural indispensable de los sistemas políticos democráticos liberales» (2013: 1905). La implicancia es que la ley debe reemplazar el consentimiento individual en ciertos casos.

El llamado a aumentar el paternalismo se deriva en parte del hecho de que las personas parecen estar compartiendo datos con mayor frecuencia y magnitud. La mayoría de las personas no están haciendo uso de sus derechos de *opt-out* a medida que las empresas reúnen y utilizan sus datos. Están exponiendo los pormenores íntimos de sus vidas en sitios como Facebook y Twitter. Este aumento de la difusión de datos persona-

25. Véase Mazzone (2003: 801-2). Algunos derechos, sin embargo, no pueden ser renunciados con el consentimiento, como por ejemplo el derecho a voto.

26. Jennings v. Minco Tech. Labs, Inc. (1989), 765 S.W.2d 497, 502 (Tex. App.). Se sostuvo que dar a elegir a los empleados entre tomarse una prueba de drogas o ser despedidos fue suficiente para tener consenso sobre la prueba de drogas.

les no es el resultado de las puras preferencias de las personas. Su exposición es, en parte, consecuencia del hecho de que muchos sitios web están diseñados para estimular la exposición de las personas, minimizando la toma de conciencia de los riesgos. Este problema se hace aún más agudo por el hecho de que muchos de los usuarios de estos sitios son adolescentes y su capacidad para tomar decisiones no es completamente madura.

En términos más generales, a causa de los problemas cognitivos y estructurales de la autogestión de la privacidad, la gente consiente la recopilación, uso y divulgación de sus datos personales cuando no necesariamente favorece sus propios intereses. Esta tendencia da sustento a aquellos que defienden la regulación paternalista.

A pesar de los múltiples problemas de la autogestión de la privacidad, hay dos argumentos que van contra el paternalismo. En primer lugar, las decisiones correctas respecto a la privacidad y el uso de datos no siempre son claras. Por ejemplo, a pesar de que una amplia autoexposición puede tener consecuencias desastrosas, muchas personas utilizan los medios sociales con éxito y de forma productiva. Supongamos que una persona que sufre de bulimia quiere compartir sus experiencias e información médica con el mundo. Ella está dispuesta a sufrir la pérdida de su privacidad porque encuentra que compartir sus experiencias es catártico y la empodera. Ella también desea ayudar a otras personas que sufren de la enfermedad, y el hacerlo le da una sensación gratificante de propósito en su vida. Escribe con pasión sobre ella, dejando al descubierto detalles que más tarde podrían ser vistos por empleadores u otras personas que potencialmente resultarían en una pérdida de oportunidades de empleo. ¿Puede la ley prohibirle compartir su historia? Si la ley pone restricciones a su divulgación, entonces estaría limitando su libertad y autonomía, irónicamente en nombre de preservar su libertad y autonomía. Otro problema con el enfoque paternalista es que el análisis de costo-beneficio, por lo menos en esta hipótesis, no aconseja claramente oponerse a la divulgación. De hecho, los beneficios podrían superar con creces los costos. Podría, por ejemplo, usar su exposición para escribir un libro comenzando una exitosa carrera como escritora y como activista contra la bulimia.

Del mismo modo, algunas personas quieren *marketing* dirigido. Ellos quieren compartir sus datos. Quieren que les envíen catálogos a sus casas. Quieren ser rastreados. Que se hagan perfiles de ellos. Quieren que

las empresas utilicen su información personal para que les recomienden productos y servicios. Estas personas no deben ser clasificadas como ignorantes o tontas, ya que no está claro si los costos para ellas son mayores que los beneficios.

En segundo lugar, y en términos más generales, existen beneficios sociales vinculados al análisis de datos. Como señalan los profesores Omer Tene y Jules Polonetsky, la recopilación, uso y divulgación de datos personales —incluso sin consentimiento— puede conducir a grandes beneficios para los individuos y la sociedad (Tene y Polonetsky, 2013: 6-12).[27] Por ejemplo, muchas empresas de Internet ofrecen contenidos de manera gratuita, usando el análisis o la venta de datos personales como su principal fuente de ingresos (Whittington y Hoofnagle, 2012: 1327, 1328-9). Si muchas personas se niegan a dar su consentimiento para el uso de sus datos, estos modelos de negocio fracasarían. Por lo tanto, estructuralmente, uno de los beneficios de la recolección, uso y divulgación de datos es que paga por los contenidos en línea. Hay problemas de fondo con este tipo de situaciones, por cuanto las personas, por lo general, no están plenamente conscientes de que están pagando con sus datos personales los contenidos en línea (2012: 1327, 1328-9), pero establecer restricciones legales a este tipo de modelo de negocios les parecería a muchos demasiado paternalista.

La ley, en términos generales, restringe la capacidad de las personas para dar su consentimiento cuando los daños, individuales o sociales, que podrían producirse con su consentimiento, claramente sobrepasan los beneficios. Los costos y beneficios sociales globales de la renuncia de una persona a su derecho a la privacidad son difíciles de calcular. Como Strahilevitz observa en este simposio, varias restricciones a la recolección, uso y divulgación de datos personales conducen a beneficios para algunas personas y perjuicios para otras (Strahilevitz, 2013: 2022). La privacidad tiene efectos distributivos, y este hecho hace que sea aún más complicado el poder determinar qué opción es la correcta (2013: 2027).

Por otro lado, la ley generalmente no busca anular el consentimiento, incluso en casos de actividades potencialmente peligrosas. Las personas pueden dar su consentimiento para fumar cigarrillos y beber alcohol, a

27. Schwartz y yo planteamos ejemplos adicionales en otros lugares. Véase Schwartz y Solove (2011: 1866-8).

pesar de que esas actividades son peligrosas. Lo mismo es cierto para jugar al fútbol o dedicarse a oficios como la minería del carbón o la extinción de incendios. En cambio, otras actividades voluntarias están prohibidas, como la prostitución y el consumo de ciertas drogas; estas actividades son evaluadas con poco valor social. Si bien estas actividades pueden ser distinguibles de las legales sólo por razones históricas y morales, se encuentran entre las pocas actividades consensuales que están prohibidas por la ley. La decisión de renunciar a la privacidad no parece afectada por las consideraciones morales o de seguridad inherentes a este pequeño grupo de actividades voluntarias prohibidas.

En términos generales, la ley se abstiene de restringir transacciones que parecen ser consensuales, y tolera una cantidad importante de manipulación e incluso de coacción, antes de que considere una transacción como no consensual. El derecho contractual no cuestiona cada acuerdo, aunque sean asimétricos y alguna de las partes no le haya ido muy bien. Las personas adoptan todo el tiempo decisiones que no están de acuerdo a sus intereses. Las personas renuncian a derechos y toman riesgos, y la ley en la mayoría de los casos no las detiene.

Como señaló Schwartz en este simposio, la Unión Europea tiene un enfoque más paternalista respecto del procesamiento de datos (Schwartz, 2013: 1966, 1971-6, 1992-2001). Sus leyes de privacidad tienen un componente de autogestión, pero requieren de una forma mucho más estricta y explícita de consentimiento que la que encontramos en la regulación de privacidad de Estados Unidos.[28] Por otra parte, la legislación europea es más restrictiva respecto de la recopilación, uso y divulgación: se requiere un fundamento legal antes de que los datos personales puedan ser procesados, mientras que en Estados Unidos generalmente se pueden procesar «a menos que una ley lo prohíba específicamente» (Schwartz, 2013: 1976).

A pesar de estas diferencias, los requisitos de consentimiento más explícitos de la Unión Europea no conducen necesariamente a que las personas efectúen un análisis de costo-beneficio más significativo con

28. El profesor Fred Cate señala que, aunque algunos funcionarios de la Unión Europea subestiman el grado en que la Directiva de Protección de Datos de la UE depende de la notificación y del consentimiento, la Directiva lo hace «claramente», ya que, «muchas de las protecciones sustantivas pueden ser modificadas sin el consentimiento» (Cate, 2006: 360).

respecto a la recolección y uso de sus datos. En la Unión Europea, el consentimiento es sin duda más difícil y costoso de obtener, a veces hasta el punto de que puede impedir el flujo de información beneficiosa. Por otra parte, su regulación puede ser formalista, puesto que a menudo establece restricciones sin un nexo causal con el daño. La regulación puede, por tanto, obstaculizar el procesamiento que no causa daño, y que incluso podría ser beneficioso. En cambio, la ley de Estados Unidos generalmente permite el tratamiento de datos a menos que cause un problema (2013: 1976). La dificultad con el enfoque de la Unión Europea es que la recopilación, el uso y la divulgación de datos, rara vez es intrínsecamente buena o mala. Los costos y beneficios dependen de las consecuencias. El paternalismo es mucho más fácil de justificar cuando las consecuencias son claramente malas.

2) *El fracaso del sistema de consentimiento opt-in*. Hay quienes sostienen que la respuesta a muchos de los problemas del consentimiento es pasar a un método más explícito y afirmativo para procurar el consentimiento: un régimen *opt-in* en vez de uno de *opt-out*. Como ha dicho el Comisionado de la FTC, Jon Leibowitz, «las empresas deben pasar a un modelo en el que los consumidores puedan hacer un *opt-in* cuando se trate de recolectar información, sobre todo cuando se trata de compartir información del consumidor con terceros a través de diversos servicios que funcionan en Internet» (Leibowitz, 2007: 6).

A pesar de mi optimismo inicial acerca del *opt-in*, ahora pienso que fracasará. Una de las razones es que muchas organizaciones tendrán la sofisticación y la motivación para encontrar maneras de generar alta tasas de *opt-in*. Pueden hacerlo de forma sencilla por medio del condicionamiento de productos, servicios o accesos al realizar el *opt-in*. Como Schwartz ha señalado acertadamente, «es probable que muchas organizaciones tratadoras de datos sean buenas para obtener el consentimiento de sus términos, independientemente de que si por defecto se requiere que los consumidores autoricen o impidan el intercambio de información» (Schwartz, 2005: 1269, 1274).[29]

29. Véase también Cate (2006: 366-7). «Si se requiere el consentimiento como condición para la apertura de una cuenta o la obtención de un servicio, siempre se puede obtener una tasa de respuesta alta» (2006: 366).

Por otra parte, «es probable que los consumidores sean mucho más sensibles a las cláusulas de precio, como el costo de una cuenta corriente, que a otros términos como las políticas y prácticas de privacidad de una institución financiera» (2005: 1274). En efecto, aceptar contratos de adhesión *online* y acuerdos de licencia de usuario final es a menudo un requisito previo para obtener acceso a un sitio web o para utilizar un producto o servicio. Considere el acuerdo de licencia de usuario final de la tienda iTunes de Apple.[30] Periódicamente, este acuerdo aparece en pantalla y las personas están obligadas a aceptar. En un iPhone, el texto de este acuerdo a menudo se extiende a más de medio centenar de pantallas. Si las personas quieren descargar aplicaciones desde la tienda, no tienen más remedio que aceptar. Este requisito es similar a un sistema *opt-in*: se busca el consentimiento afirmativo. Pero no se produce casi ninguna forma de negociación o elección durante este proceso. Por lo tanto, a pesar de las buenas intenciones de los reguladores, un sistema *opt-in* o un requisito de consentimiento afirmativo para la mayoría de nuevos usos de los datos, va a significar hacer más clics y firmar más formas, pero no una protección más significativa de la privacidad.

Exigirle a las empresas que obtengan consentimiento afirmativo para muchos de los nuevos usos de los datos puede ser innecesariamente costoso y obstaculizar usos socialmente beneficiosos (Cate, 2006: 364-5). Volver al consentimiento en algo engorroso y costoso de obtener puede tener el efecto de restringir ciertos usos, no porque la gente niegue su consentimiento, sino porque los costos de adquisición del mismo pueden impedir que las empresas puedan realizar aquellos usos. El resultado sería impedir ciertos usos de datos por razones formales que no distinguen entre usos beneficiosos y dañinos. Algunos podrían decir que menos recopilación, uso y divulgación de datos es siempre una victoria, pero ¿debe ganar la privacidad cuando los beneficios de determinados usos de datos son mayores que los costos? ¿O cuando los individuos desean que sus datos sean usados, pero no se les preguntó porque pedir el consentimiento sería demasiado costoso?

Algunos podrían apoyar el sistema *opt-in* porque los consumidores se verían obligados a prestar atención a las notificaciones acerca de cómo

30. Véase Apple, «iTunes Store. Terms and Conditions», disponible en <http://www.apple.com/legal/itunes/us/terms.html>.

se usarán y comunicarán sus datos; con un sistema de *opt-out*, en cambio, los consumidores tienen menos probabilidades de conocer estas notificaciones. A pesar de esta ventaja del *opt-in*, hay un costo. En los regímenes *opt-in* la gente indica afirmativamente su consentimiento para la recopilación e intercambio de sus datos. Con este consentimiento claro y legítimo, las empresas podrían sentirse con derecho para utilizar y divulgar los datos más ampliamente. Por el contrario, con la opción del *opt-out*, el consentimiento adquirido es menos legítimo que con un régimen de *opt-in*. Esta disparidad no hace que el consentimiento del *opt-out* sea ilegítimo, pero es ciertamente ambiguo, dado que el consentimiento del *opt-out* podría ser el producto de la mera inercia o la falta de conciencia de la opción de *opt-out*.

En el largo plazo, el régimen de *opt-in* puede incluso no conducir a que menos personas compartan sus datos. Si las empresas deben obtener el consentimiento de modo *opt-in,* podrían también ser más agresivas en cuanto a la cantidad de datos que solicitan (Lundblad y Masiello, 2010: 155, 162). Los recolectores de datos pueden intentar definir posibles usos futuros de manera más amplia y vaga, con el fin de evitar tener que obtener un nuevo consentimiento en el futuro. Al final, el *opt-in* es sólo otra versión de la autogestión de la privacidad y sufre de los mismos problemas de fondo.

3) *¿Debe ser abandonada la autogestión de privacidad?* A pesar de sus defectos, la autogestión de la privacidad no debe ser abandonada. Proveer notificaciones, acceso y la capacidad de controlar sus datos a las personas es clave para facilitar una cierta autonomía en un mundo donde cada vez más se toman decisiones sobre ellos con el uso de sus datos personales, procesos automatizados y raciocinios clandestinos, y donde las personas tienen pocas facultades para hacer algo respecto a estas decisiones. Un mundo sin autogestión de privacidad sería claramente problemático, ya que las personas deben tener el derecho a saber cómo se utiliza su información para también poder tomar decisiones acerca de esos usos.

Adicionalmente, los esfuerzos para mejorar la autogestión de la privacidad a través de más educación a los consumidores, más avisos destacados y más instancias para manifestar el consentimiento, son sin duda loables e importantes. Tales esfuerzos han sido una importante meta legal y política. En esencia, este trabajo apuesta por la autogestión.

Irónicamente, tal vez el gran impacto práctico que ha tenido la autogestión de la privacidad no está en informar a las personas y mejorar su gestión de la privacidad, sino que en informar a las empresas que recogen y usan los datos y en mejorar la gestión de la privacidad por parte de éstas.[31] El proceso de creación de avisos de privacidad obliga a cambios internos dentro de una empresa y a aumentar la conciencia sobre la recolección y uso de datos. Los *Chief Privacy Officers*[32] enseñan al personal a ser conscientes de la privacidad e influyen para que el *software*, los productos y el diseño de servicios, sean más respetuosos de la privacidad. La autogestión de la privacidad, por lo tanto, tiene el efecto positivo de generar protecciones estructurales para la privacidad y responsabilidades dentro de las instituciones (Bamberger y Mulligan, 2011: 247).

Tampoco debe ser abandonada la autogestión de la privacidad porque hay momentos en que la gente quiere manejar su privacidad, y la negación de esta facultad puede desempoderar a las personas y restringirles su libertad. Por ejemplo, algunas personas tienen mucho cuidado para ajustar la privacidad de sus perfiles de redes sociales. Algunos quieren que sus perfiles estén expuestos al mundo. Otros quieren que sus perfiles sólo estén disponibles a sus amigos. La gente de cada grupo podrá cuidar mucho de su configuración de privacidad en una determinada red social, y pueden, sin embargo, no molestarse en mirar las políticas de privacidad de otros sitios que utilizan.

Por lo tanto, la autogestión de la privacidad no debe ser abandonada, y, del otro extremo, las soluciones paternalistas son preocupantes. No existe una solución mágica, por lo que debemos continuar participando de la elaborada danza que produce la tensión entre la autogestión y el paternalismo.

---

31. Véase Swire (2002: 1263, 1316), «uno de los principales efectos de las notificaciones ha sido el de exigir a las instituciones financieras que inspeccionen sus propias prácticas.... Con el fin de redactar las notificaciones, muchas instituciones financieras llevaron a cabo un extenso proceso, a menudo por primera vez, para saber hasta qué punto los datos se comparten o no, entre las diferentes partes de la organización y con terceros».

32. Funcionario responsable de la protección de la privacidad dentro de una institución. (*N. del T.*)

B) FUTURAS DIRECCIONES

Aunque no debemos rechazar la autogestión de la privacidad, actualmente se pide que sostenga mucho más peso del que puede soportar. Entonces, ¿qué se puede hacer?

1) *Repensando el consentimiento y empleo de nudges*.[33] Para que la regulación de la privacidad pueda avanzar, la ley requiere un mejor y más coherente enfoque del consentimiento con respecto a la privacidad. De hecho, en muchas áreas del derecho, el consentimiento juega un papel fundamental, sin embargo, lo que constituye un consentimiento válido varía enormemente entre las distintas ramas del derecho. Hasta el momento, pocos han tratado de analizar sistemáticamente lo que implica el consentimiento para así desarrollar un enfoque más coherente de él.

Actualmente, el derecho no ha tratado suficientemente lo que las ciencias sociales han dicho acerca de las complejidades y desafíos involucrados en la toma de decisiones humana. ¿Qué significa realmente el consentir en algo?, ¿qué debe reconocer la ley como un consentimiento válido? Muchas transacciones se realizan con algún tipo de asimetría de conocimiento y de poder, ¿cuándo estas asimetrías son tan trascendentes como para ser coercitivas? La visión actual de la ley sobre el consentimiento es incoherente, y lo trata como un binario simple (es decir, que existe o no). El consentimiento tiene muchos más matices, y la regulación de la privacidad necesita un nuevo enfoque que los tenga en cuenta sin ser demasiado compleja en su aplicación.

También hay fórmulas prometedoras para combinar el consentimiento con el paternalismo. Por ejemplo, Thaler y Sunstein proponen formas de «paternalismo libertario», a las que se refieren como *nudges*, que buscan estructurar decisiones a fin de cambiar «el comportamiento de la gente en una forma predecible sin prohibir las decisiones ni cambiar significativamente sus incentivos económicos» (Thaler y Sunstein, 2008: 5-6). Los *nudges* son paternalistas, pero no en la forma restrictiva y ab-

33. *Nudge* es un concepto de las ciencias de la conducta, que hace referencia al intento de influenciar las motivaciones, incentivos y decisiones a través de estímulos positivos, sugerencias indirectas y una cuidadosa selección y presentación de las opciones que se le entregan a una persona o grupo. (*N. del T.*)

soluta de la regulación paternalista más tradicional. En algunos casos, los *nudges* podrían ser un término medio efectivo entre la autogestión de la privacidad y el paternalismo.

2) *Desarrollando una autogestión de la privacidad parcial*. En el fondo, lo que mucha gente quiere sobre su privacidad es que sus datos sean recogidos, utilizados y difundidos de manera que ellos, o la sociedad, sean beneficiados sin recibir daños. Si la gente tiene objeciones a determinados usos de sus datos, quieren tener el derecho a decir que no. Pero muchas personas no quieren microgestión de su privacidad, y en cambio quieren tener a alguien que vele por su privacidad y les proteja de usos dañinos.

Como los alimentos que comemos y los automóviles que conducimos, tenemos muchas opciones para elegir qué comprar, y confiamos en que estos productos estarán dentro de ciertos parámetros razonables de seguridad. No tenemos que ser expertos en automóviles o leche, y la gente no necesariamente quiere llegar a ser experta en privacidad tampoco. A veces las personas quieren controlar su privacidad en una situación particular, y debieran ser capaces de hacerlo. Pero globalmente, con todas las entidades que reúnen datos, la gente probablemente encontrará que la autogestión será una tarea casi imposible. La gente quiere un poco de autogestión de la privacidad, pero no demasiada. La regulación de la privacidad necesita encontrar una manera de ofrecer una autogestión de la privacidad morigerada o parcial.

Una posible respuesta podría ser encontrar formas para que la gente maneje su privacidad a nivel mundial sobre todas las entidades, en lugar de una a la vez. Pero unificar dicha gestión puede ser un reto, ya que será difícil encontrar un conjunto uniforme de opciones de privacidad que sea aplicable a todas las entidades, y las consecuencias de la recolección, uso o divulgación de los datos pueden diferir dependiendo de qué entidades estén involucradas.

3) *Ajustando el momento de aplicación y el enfoque de la privacidad*. El momento de aplicación de la regulación de la privacidad necesita ser ajustado. La autogestión de la privacidad y la ley se centran en gran medida en el momento de la recogida inicial de datos; y, a menudo, en cada transacción en que se intercambian datos. Pero es muy difícil que en el

momento de la recolección de datos la persona pueda hacer un juicio correcto sobre las futuras implicancias de la privacidad, porque estas consecuencias son a menudo desconocidas.

Por lo tanto, el enfoque debe centrarse más en los usos aguas abajo, en lugar del momento de la recolección inicial de los datos. En muchos casos, los beneficios pueden no ser evidentes en el momento de la recogida de los datos. Nuevas ideas para combinar datos, nuevos descubrimientos en la agregación y análisis de datos, y las nuevas técnicas y tecnologías de análisis de datos pueden cambiar los costos y beneficios de la situación. Las normas que requieran obtener nuevamente el consentimiento para nuevos usos de los datos podrían demostrar ser prohibitivamente demasiado costosas, y servir como una barrera *de facto* a estos nuevos usos. Tal resultado podría no ser socialmente deseable, y puede que no sea el resultado querido por la mayoría de las personas cuyos datos son tratados. Por otro lado, un consentimiento en blanco, que permite una variedad casi ilimitada de nuevos usos puede ser indeseable, por cuanto los datos pueden ser potencialmente utilizados en alguna forma dañina que la gente no pueda anticipar o entender.

Adicionalmente, la medición de los costos de ciertas formas de recopilación, uso y divulgación de los datos personales es extremadamente difícil debido a que los daños a la privacidad son difíciles de definir. En definitiva, dado el dinamismo de esta área, la evaluación de costos y beneficios requiere un alto grado de especulación sobre el futuro. Probablemente las personas no serán capaces de tomar tales decisiones muy bien de antemano, pero tampoco la ley.

Tales decisiones se hacen mejor en el momento en que se llevan a cabo los usos particulares de los datos. Lo que se necesita es que la ley evalúe y entregue lineamientos sobre los nuevos tipos de usos en el momento en que éstos se propongan. Tal vez algunos nuevos usos deban ser restringidos absolutamente; algunos deban ser limitados; otros deban necesitar una nueva manifestación de consentimiento; algunos deban ser permitidos, pero con el derecho a revocar el consentimiento; y algunos deban ser permitidos sin una nueva autorización. Quizás sea necesario que una agencia deba revisar las propuestas de nuevos usos que puedan surgir.

4) *Avanzando hacia el fondo por sobre la neutralidad*. Cualquier avance requerirá que la ley tome difíciles decisiones sobre el fondo. La autoges-

tión de la privacidad intenta permanecer neutral en cuanto a las cualidades de determinadas formas de recolección, uso o divulgación de datos, y se fija más en la existencia o no de consentimiento. Bajo la autogestión de la privacidad, la mayoría de los formas de recolección, uso o divulgación de datos son aceptables si son consensuales. El consentimiento a menudo se convierte en una forma muy cómoda de lograr resultados sin confrontar los importantes valores en juego. Para avanzar, no se puede seguir sosteniendo este tipo de neutralidad.

La ley debe desarrollar y codificar normas básicas de privacidad. Esta codificación no debiera ser excesivamente paternalista; puede tener la forma del Código Uniforme de Comercio (UCC, del inglés «Uniform Commercial Code»), donde ciertas normas supletorias pueden ser renunciadas. Las normas de la UCC han logrado arraigarse bien y son a menudo seguidas. Las desviaciones de estas normas son bastante notorias. La regulación de la privacidad ha dicho muy poco sobre las formas adecuadas de recolección, uso y divulgación de los datos. No estoy sugiriendo un régimen paternalista, donde la ley prohíba una amplia gama de recopilaciones, usos o divulgaciones de datos; sólo en los casos extremos la ley debe prohibir. La ley debe tomar una postura más firme sobre el fondo del asunto.

Normas más sustantivas sobre la recopilación, uso y divulgación de los datos podrían estar formadas de limitaciones que bloqueen prácticas particularmente problemáticas, así como también de normas supletorias que puedan ser negociadas. Las reglas supletorias pueden ser redactadas de una forma que modulen la facilidad con que las partes pueden negociar sobre ellas. Con normas más sustantivas que establezcan un conjunto básico de normas sobre la privacidad, será más fácil que la gente entienda cómo está protegida su privacidad. Las desviaciones de estas normas serán más llamativas. La disonancia entre los diferentes enfoques de la privacidad será menor.

CONCLUSIÓN

Durante demasiado tiempo la regulación de la privacidad se ha basado en la autogestión de la privacidad. Sin embargo, esta forma regulatoria no puede alcanzar los objetivos que se le exigen y ha sido llevada más allá de sus límites. Así y todo, la autogestión no debe ser abandonada,

puesto que las alternativas a este sistema corren el riesgo de volverse demasiado paternalistas.

El fondo de muchos problemas de privacidad es el dilema del consentimiento, lo que muy a menudo es ignorado por el derecho, la política y la educación. Para seguir avanzando: 1) se debe desarrollar un enfoque coherente del consentimiento, que dé cuenta de los conocimientos que las ciencias sociales tienen que aportar sobre cómo las personas toman decisiones acerca de sus datos personales; 2) se debe reconocer que la gente puede participar en la autogestión de su privacidad sólo en determinados casos; 3) debe ajustarse el momento en que se aplique la privacidad, centrándose en los usos posteriores; y 4) se deben desarrollar normas de privacidad más de fondo. Éstos son retos enormes, pero deben ser abordados. De lo contrario, la regulación de la privacidad seguirá siendo insuficiente, mientras que los problemas a los que debe hacer frente crecen sin forma de controlarlos.

REFERENCIAS

Acquisti, Alessandro y Jens Grossklags (2006). «Privacy and rationality: A survey». En Katherine J. Strandburg y Daniela Stan Raicu (editoras), *Privacy and technologies of identity*. Nueva York: Springer.

—. (2008). «What can behavioral economics teach us about privacy?». En Alessandro Acquisti y otros (editores), *Digital privacy*. Boca Ratón (Estados Unidos): Auerbach Publications.

Allen, Anita L. (2011). *Unpopular privacy: What must we hide?* Nueva York: Oxford University Press.

Anton, Annie I. y otros (2004). «Financial privacy policies and the need for standardization». *IEEE Security & Privacy*, 2.

Ariely, Dan (2008). *Predictably irrational*. Nueva York: HarperCollins Publishers.

Bamberger, Kenneth A. y Deirdre K. Mulligan (2011). «Privacy on the books and on the ground». *Stanford Law Review*, 63 (2).

Barbaro, Michael y Tom Zeller (2006). «Jr., A face is exposed for AOL searcher 4417749», *New York Times*, 9 de agosto, sec. Technology. Disponible en <http://select.nytimes.com/gst/abstract.html?res=F10612FC345B0C7A8CDDA10894DE404482>.

Ben-Shahar, Omri y Carl E. Schneider (2011). «The failure of mandated disclosure». *University of Pennsylvania Law Revie*w, 159.

Brandimarte, Laura, Alessandro Acquisti y George Loewenstein (2013). «Misplaced confidences: Privacy and the control paradox». *Social Psychological and Personality Science*, 4 (3). Disponible en <http://www.heinz.cmu.edu/~acquisti/papers/acquisti-spps.pdf>.

Brill, Julie (2010). «Remarks by commissioner Julie Brill. United States Federal Trade Commission» (Trabajo presentado en la Conference of Western Attorneys General Annual Meeting, Privacy 3.0 Panel, Nuevo México, Santa Fe, 20 de julio), disponible en <http://www.ftc.gov/speeches/brill/100720cwagtranscription.pdf>.

Calo, M. Ryan (2012). «Against notice skepticism in privacy (and elsewhere)». *Notre Dame Law Review*, 87.

Cate, Fred H. (2006). «The failure of fair information practice principles». En Jane K. Winn (editor), *Consumer potection in the age of the 'information economy'*. Bodmin (Inglaterra): Ashgate Publishing.

Citron, Danielle Keats (2007). «Reservoirs of danger: The evolution of public and private law at the dawn of the information age». *Southern California Law Review*, 80.

Cohen, Julie E. (2000). «Examined lives: Informational privacy and the subject as object». *Stanford Law Review*, 52.

—. (2012). *Configuring the networked self*. New Haven: Yale University Press.

—. (2013). «What privacy is for». *Harvard Law Review*, 126.

Gellman, Robert (2013). «Fair information practices: A basic history». Disponible en <http://bobgellman.com/rg-docs/rg-FIPShistory.pdf>.

Gilbert, Daniel (2006). *Stumbling on happiness*. Nueva York: Vintage.

Goldman, Eric (2002). «The privacy hoax». *Forbes*, 14 de octubre. Disponible en <http://www.forbes.com/forbes/2002/1014/042.html>.

Hoofnagle, Chris Jay y otros (2010). «How different are young adults from oder adults when it comes to information privacy attitudes & policies?». *Social Science Research Network*. Disponible en <http://ssrn.com/abstract=1589864>. Manuscrito inédito.

Janger, Edward J. y Paul M. Schwartz (2002). «The gramm-leach-bliley act, information privacy, and the limits of default rules». *Minnesota Law Review*, 86.

John, Leslie K., Alessandro Acquisti y George Loewenstein (2009). «The best of strangers: Context dependent willingness to divulge personal information». *Social Science Research Network*. Disponible en <http://ssrn.com/abstract=1430482>. Manuscrito inédito.

Kafka, Franz (1998). *The trial*. Traducido por Breon Mitchell. Nueva York: Schocken Books.

Kahneman, Daniel (2011). *Thinking, fast and slow*. Nueva York: Farrar, Straus and Giroux.

Kahneman, Daniel, Paul Slovic y Amos Tversky (eds.) (1982). *Judgment under uncertainty: Heuristics and biases*. Nueva York: Cambridge University Press.

Kahneman, Daniel y Amos Tversky (eds.) (2000). *Choices, values, and frames*. Nueva York: Cambridge University Press.

Leibowitz, Jon (2007). «So private, so public: Individuals, the internet and the paradox of behavioral marketing» (Trabajo presentado en la FTC Town Hall Meeting on «Behavioral advertising: Tracking, targeting, and technology», 1 de noviembre). Disponible en <http://www.ftc.gov/speeches/leibowitz/071031ehavior.pdf>.

Lundblad, Nicklas y Betsy Masiello (2010). «Opt-in dystopias». *SCRIPTed*, 7 (1). Disponible en <http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.pdf>.

Marotta-Wurgler, Florencia (2011). «Will increased disclosure help? Evaluating the recommendations of the ALI's 'Principles of the law of software contracts'». *University of Chicago Law Review*, 78.

Mazzone, Jason (2003). «The waiver paradox». *Northwestern University Law Review*, 97.

McDonald, Aleecia M. y Lorrie Faith Cranor (2008). «The cost of reading privacy policies». *I/S: A Journal of Law and Policy for the Information Society*, 4.

Milne, George R. y Mary J. Culnan (2004). «Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices». *Journal of Interactive Marketing*, 18.

Nissenbaum, Helen (2010). *Privacy in context*. Palo Alto: Stanford University Press.

Nussbaum, Emily (2004). «My so-called blog», *New York Times*, 11 de enero, sec. Magazine. Disponible en <http://www.nytimes.com/2004/01/11/magazine/11blog.html>.

POST, Robert C. (1989). «The social foundations of privacy: Community and self in the common law tort». *California Law Review*, 77.

REGAN, Priscilla M. (1995). *Legislating privacy: Technology, social values and public policy*. Chapel Hill: The University of North Carolina Press.

REIDENBERG, Joel R. (2003). «Privacy wrongs in search of remedies». *Hastings Law Journal*, 54.

RICHARDS, Neil M. (2008). «Intellectual privacy». *Texas Law Review*, 87.

—. (2013). «The dangers of surveillance». *Harvard Law Review*, 126.

SCHWARTZ, Paul M. (1999). «Privacy and democracy in cyberspace». *Vanderbilt Law Review*, 52.

—. (2005). «Privacy inalienability and the regulation of spyware». *Berkeley Technology Law Journal*, 20.

—. (2013). «The EU–U.S. privacy collision: A turn to institutions and procedures». *Harvard Law Review*, 126.

SCHWARTZ, Paul M. y Daniel J. SOLOVE (2011). «The PII problem: Privacy and a new concept of personally identifiable information». *New York University Law Review*, 86.

SHERMAN, Erik (2008). «Privacy policies are great-for PhDs». *CBS News*, 4 de septiembre de 2008, sec. MoneyWatch. Disponible en <http://www.cbsnews.com/news/privacy-policies-are-great-for-phds/>.

SIMITIS, Spiros (1987). «Reviewing privacy in an information society». *University of Pennsylvania Law Review*, 135.

SOLOVE, Daniel J. (2004). *The digital person: Technology and privacy in the information age*. Nueva York: New York University.

SOLOVE, Daniel J. y Neil M. RICHARDS (2009). «Rethinking free speech and civil liability». *Columbia Law Review*, 109.

SOLOVE, Daniel J. y Paul M. SCHWARTZ (2011). *Information privacy law*. 4.ª ed. Nueva York: Aspen Publishers.

STRAHILEVITZ, Lior Jacob (2013). «Toward a positive theory of privacy law». *Harvard Law Review*, 126.

SWIRE, Peter P. (2002). «The surprising virtues of the new financial privacy law». *Minnesota Law Review*, 86.

THALER, Richard H. y Cass R. SUNSTEIN (2008). *Nudge*. New Haven: Yale 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.

Turow, Joseph, Lauren Feldman y Kimberly Meltzer (2005). *Open to Exploitation: American Shoppers Online and Offline*. Annenberg Public Policy Center of the University of Pennsylvania. Disponible en <http://www.annenbergpublicpolicycenter.org/downloads/information_and_society/turow_appc_report_web_final.pdf>.

Turow, Joseph y otros (2009). «Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It». *Social Science Research Network*. Disponible en <http://ssrn.com/paper=1478214>. Manuscrito inédito.

Whittington, Jan y Chris Jay Hoofnagle (2012). «Unpacking privacy's price». *North Carolina Law Review*, 90.

SOBRE EL AUTOR

Daniel J. Solove es John Marshall Harlan Research Professor of Law de la George Washington University Law School de Estados Unidos. El autor agradece a su asistente de investigación, Rachel Kleinpeter, por sus investigaciones para este artículo; agradece también a Danielle Citron, Julie Cohen, Deven Desai, Woodrow Hartzog, Chris Hoofnagle, Orin Kerr, Harriet Pearson y Paul M. Schwartz, por sus comentarios al manuscrito.

Este artículo fue publicado originalmente en *Harvard Law Review* 126 (2013): 1880-1903, con el título «Introduction: Privacy self-management and the consent dilemma», y fue traducido al castellano por Juan Pablo Hernández Hellriegel y Sebastián Molina Necul, ayudantes del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, conforme a la expresa autorización del autor.