Hacia una Internet libre de censura

Propuestas para América Latina

Eduardo Bertoni
COMPILADOR

Facultad de Derecho
Centro de Estudios en Libertad de Expresión y Acceso a la Información

CELE

UP
Universidad de Palermo

Hacia una Internet libre de censura

Propuestas para América Latina

Eduardo Bertoni
COMPILADOR

Facultad de Derecho
Centro de Estudios en Libertad de Expresión y Acceso a la Información

Hacia una internet libre de censura : propuestas para América Latina / compilado por Eduardo Andrés Bertoni. - 1a ed. - Buenos Aires : Universidad de Palermo - UP, 2012.
352 p. ; 23x16 cm.

ISBN 978-987-1716-54-8

1. Políticas Públicas. 2. Internet. I. Bertoni, Eduardo Andrés, comp.
CDD 320.6

Compilador:
Eduardo Bertoni

Diseño grá co:
Patricia Fiuza

Diseño original de tapa:
Departamento de Diseño Institucional - Universidad de Palermo

Corrección:
Julieta Botto

Editado por la Universidad de Palermo, enero de 2012, Buenos Aires, Argentina

ISBN: 978-987-1716-54-8

Hecho el depósito que marca la ley 11.723

Esta edición, de 500 ejemplares, se terminó de imprimir en el mes de enero de 2012 en BRAPACK Industria Gráfica, Saraza 1354, Ciudad de Buenos Aires.

Impreso en la Argentina / Printed in Argentina

Universidad de Palermo
Rector
Ing. Ricardo H. Popovsky

Facultad de Derecho
Decano
Roberto Saba

Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE)
Director
Eduardo Bertoni

Mario Bravo 1050
(C1175ABW) Ciudad de Buenos Aires
Argentina
Tel.: (54 11) 5199-4500 | Fax: (54 11) 4963-1560
cele@palermo.edu | www.palermo.edu/cele

Este libro se publica gracias al apoyo financiero de la Fundación Open Society Institute.

Índice

Capítulo cuatro

Protección de datos personales y prestación de servicios en línea en América Latina[1]

Alberto J. Cerda Silva

Introducción

Cuando el Gobierno de Chile anunció que monitorearía las redes sociales que operan en línea, tales como MySpace y Twitter, generó tan amplio rechazo ciudadano que se vio obligado a desechar la iniciativa. Desde el momento en el que Facebook modificó unilateralmente sus políticas de privacidad, con lo que dejaba al descubierto la participación de ciudadanos iraníes en grupos antigubernamentales, organismos de seguridad del Gobierno adoptaron medidas represivas contra esos usuarios y sus familiares. A partir de que el Gobierno de Venezuela publicó en Internet el listado de adherentes a una solicitud de referendo nacional, generó persecución cruzada entre sus partidarios y opositores. Con sus bemoles, cada uno de los casos recién reseñados deja en evidencia cómo la adecuada protección de los datos personales es una garantía para el ejercicio de la libertad de expresión y demás derechos fundamentales, así como el rol crítico que Internet tiene hoy en la preservación de esos derechos.

1. Este ensayo recoge con cierta coherencia la intervención del autor en el taller Libertad de Expresión e Internet: aspectos de regulación en América Latina, organizado por el Centro de Estudios en Libertad de Expresión y Acceso a la Información de la Facultad de Derecho de la Universidad de Palermo, que tuvo lugar en la ciudad de Buenos Aires los días 12 y 13 de septiembre de 2011. El autor desea expresar su profundo agradecimiento por la invitación extendida para ser parte de dicho evento.

La protección de los datos personales satisface fines de interés público inherentes a una sociedad democrática. Dicha protección no solo evacúa la necesidad individual de quien quiere excluirse de la vida social, sino que también actúa como salvaguarda para el libre ejercicio de sus derechos. Así, por ejemplo, al imponer limitaciones al tratamiento de datos relativos a nuestras opciones políticas, religiosas o sexuales, se fortalece el libre ejercicio del derecho de asociación, de la libertad de pensamiento y de la autodeterminación sexual, entre otros. En verdad, la posibilidad de excluirse de la sociedad en sus diversas vertientes jurídicas –llámese inviolabilidad del hogar y de las comunicaciones, derecho a la vida privada, derecho a la protección de los datos personales e, incluso, el derecho al voto secreto– preserva un espacio para la libre expresión y la plena realización de la personalidad, un objetivo propio del orden democrático.

Recientemente, una serie de argumentos han sido esbozados con el propósito de erosionar el derecho a la protección de los datos personales. Se ha sostenido que tal preservación debería estar circunscrita únicamente a la información que reviste carácter privado. Se ha dicho que el concepto de dato personal es excesivamente amplio, lo que genera incertidumbre jurídica. Se ha afirmado, también, que el simple consentimiento de las personas es suficiente para legitimar el procesamiento de información que les concierne, sin más. Para ser franco, dichos argumentos no son resultado de una preocupación en torno a la libertad de expresión, sino del afán de disponer de un entorno legal más proclive al tráfico inmune e impune de la información personal.

Los argumentos tendentes a socavar una protección adecuada a los datos personales han sido especialmente oficiosos cuando se los aplica a Internet; de hecho, han sido enarbolados con el propósito de brindar mayor flexibilidad a la prestación de servicios en línea; basta traer a colación algunos casos de los años recientes, tales como la publicidad contextual y las vistas callejeras de Google, los sistemas de localización geográfica de Apple, la modificación unilateral de políticas de privacidad de Facebook y el pasaporte de identificación en línea de Microsoft. Frente a ellos, las autoridades europeas en materia de protección de datos han reaccionado enérgicamente y, como era previsible, la progresiva adopción de medidas similares en América Latina suscita preocupación entre los prestadores de servicios en línea.

Este ensayo controvierte las líneas de argumentación por medio de las cuales se intenta mermar la obtención de un adecuado nivel de resguardo al derecho a la protección de los datos personales. La primera sección

se extiende sobre la verdadera naturaleza del bien jurídico protegido, rechazando que este sea solamente el derecho a la vida privada. La segunda sección impugna la acusación de que la legislación latinoamericana en la materia sea excesivamente proteccionista al conceptualizar qué es un dato personal. La tercera sección enfatiza acerca de que el simple consentimiento no es suficiente a los efectos de legitimar el tratamiento de información personal. La cuarta sección intenta develar el propósito ulterior de dichos argumentos y, en contrapartida, expresa su preocupación por el rol que los prestadores de servicios en línea tienen en la retención de datos en América Latina. Unos breves comentarios y conclusiones ponen fin al texto.

I. La protección de los datos personales como derecho autónomo

La legislación sobre protección de los datos personales se desarrolla a partir de la década de los setenta, como una reacción al creciente poder que las tecnologías proveen para procesar información personal y, consiguientemente, emplear esta para fines ilegítimos de control social por el Gobierno. Progresivamente, el ámbito de aplicación de dicha normativa se extendió a efectos de brindar una protección integral. Así, para evitar la elusión de la ley, en especial en áreas sensibles como el tratamiento de datos en el sector de la salud, renuente a la automatización y afincado en la cultura del papel, el ámbito de aplicación se extendió también al tratamiento manual de datos. Del mismo modo, a medida que las tecnologías estuvieron disponibles no solo para servicios gubernamentales, sino, también, para empresas y entidades del sector privado, la legislación extendió la protección de las personas al tratamiento de datos efectuados por estas. Así, hoy tenemos una legislación comprensiva, que brinda protección a las personas en relación con el tratamiento de sus datos, ya sea por medios manuales o automatizados, por el sector público y privado.

La legislación sobre protección de datos se articuló inicialmente en torno al derecho a la vida privada como bien jurídico. En parte, porque la preocupación central era resguardar la información personal, especialmente aquella sensible atinente a una esfera íntima, frente a su potencial mal uso. Y en parte, porque el desarrollo conceptual no encontraba otro bien jurídico más apropiado para sustentar la protección. Así, tal como en la obra de Warren y Brandeis, el derecho de propiedad sirvió de fundamento al derecho a la vida privada, este lo fue del derecho a la protección de los datos personales. Sin embargo, en la tradición del derecho continental de

la cual América Latina es parte, tanto el derecho a la vida privada como el derecho a la protección de los datos personales son categorías jurídicas claramente diferenciadas.

El derecho a la protección de los datos personales cobró autonomía propia a comienzos de la década de los ochenta. En 1983, el Tribunal Constitucional Federal Alemán, el cual ha sido especialmente acucioso en el control de las leyes que confieren poder al Gobierno para tratar información personal, declaró la inconstitucionalidad de la Ley de Censo, sosteniendo que «...el derecho general de la personalidad... abarca... la facultad del individuo, derivada de la idea de autodeterminación, de decidir, básicamente por sí mismo, cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida». Lo propio fue reconocido también por el Tribunal Constitucional de España en 1998, cuando identificó «un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona..., pertenezcan o no al ámbito más estricto de la intimidad, para, así, preservar el pleno ejercicio de sus derechos». Entonces, este derecho, conocido en doctrina como *autodeterminación informativa* o *libertad informativa*, faculta a las personas para controlar la información que les concierne, siendo irrelevante a efectos de su protección si dicha información es privada o pública.

En Europa, el derecho a la protección de los datos personales también ha tenido recepción normativa. De hecho, diversas cartas constitucionales han reconocido aquel como un derecho diferenciado del derecho a la vida privada. Todavía más, la Carta de Derechos Fundamentales de la Unión Europea, adoptada el 7 de diciembre de 2000, hace un claro distingo. Así, tras reconocer en su artículo 7 el derecho a la vida privada, su artículo 8 reconoce que «toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan», y luego fija las exigencias mínimas impuestas al adecuado respecto de este derecho desde la perspectiva de los derechos humanos.

En América Latina, el derecho a la protección de los datos personales también ha tenido reconocimiento constitucional. En general, las constituciones de la región reconocen no solo el derecho a la vida privada, sino, también, el denominado *habeas data*, que no es más que el derecho a la protección de los datos personales. Esto último acontece, con diferentes matices, en las constituciones de la Argentina, Brasil, Colombia, México, el Perú, y Venezuela. Incluso en aquellos países en que la confusión conceptual aún persiste en el texto constitucional, esta ha sido superada por sus cortes constitucionales, las cuales reconocen el derecho a controlar la información

personal; así, recientemente, el Tribunal Constitucional de Chile reconoció expresamente el derecho a la autodeterminación informativa, pese a no estar explícito en la Constitución, al declarar la inconstitucionalidad de la ley que obligaba a los cibercafés a llevar registro de sus usuarios para fines de persecución penal.

Comparativamente, el constitucionalismo latinoamericano ha sido más eficiente en la salvaguarda del derecho a la protección de los datos personales. Primero, reconociéndolo como un derecho autónomo. Segundo, proveyéndolo de acciones constitucionales para su protección, ya sea a través de la *acción de amparo* –conocida como *acción de tutela* en Colombia; *recurso de protección* en Chile; y *mandado de segurança* en Brasil–, o bien, de una acción específica también denominada de *habeas data.* Tercero, a diferencia del constitucionalismo estadounidense y con mayor énfasis que el europeo, las cartas magnas de América Latina reconocen derechos y establecen procedimientos judiciales para su protección, no solo respecto del sector público, sino, también, respecto del sector privado. Así, pese a carecer de leyes especiales en la materia en diversos países de la región, el derecho a la protección de los datos personales ha tenido lugar en la sede constitucional, tanto cuando el Gobierno trata información personal como cuando empresas de telecomunicaciones o prestadores de servicio de reportes crediticios tratan datos personales con infracción a los derechos fundamentales reconocidos por la Constitución.

Sin embargo, la normativa constitucional no ha sido suficiente para garantizar un adecuado nivel de protección de los datos personales en América Latina. Esto sucede porque dicho resguardo se verifica preferentemente en sede judicial y ello trae aparejado una serie de limitaciones, tales como sus altos costos transaccionales; su ineficacia para prevenir infracciones y su falta de experiencia en temas que, en ocasiones, resultan altamente técnicos. Además, como en los demás países depositarios de la tradición del derecho civil, en los países latinoamericanos, los precedentes judiciales carecen de fuerza obligatoria en casos futuros, salvo limitadísimas excepciones. Así, en la práctica, ello obliga a (re)iniciar acciones judiciales individuales a cada uno de los titulares de datos personales afectados por un ilegítimo tratamiento de esos, efectuados, por ejemplo, por Equifax o algunas de sus filiales locales al emitir reportes de crédito.

Los preceptos constitucionales resultan aún demasiado generales y admiten un amplio margen de interpretación. En efecto, siguiendo a Robert Alexy, las disposiciones constitucionales establecen principios cuya aplicación al caso concreto puede redundar en reglas equívocas

o ambiguas. Así ha sucedido con el denominado *derecho al olvido*, en relación con el tratamiento de datos personales relativo a deudas incluso después de verificado su pago. Mientras para las Cortes Supremas de la Argentina y Costa Rica el tratamiento de datos sobre deudas pagadas infringe los derechos fundamentales, la Corte Suprema de El Salvador, frente a análogos preceptos constitucionales, ha determinado exactamente lo contrario. Esto pone en evidencia que la protección basada en puros preceptos constitucionales resulta en ocasiones insuficiente e introduce incertidumbre jurídica, tanto entre los titulares de datos personales como entre quienes los tratan.

América Latina está adoptando leyes que reglamentan el tratamiento de datos personales de un modo integral, esto es, en las que sea comprendido el procesamiento de información tanto por el sector público como por el privado. Diversas razones explican este fenómeno: los nuevos bríos democráticos, que invitan a brindar adecuada protección a los derechos de las personas; el afán de minimizar la incertidumbre de un modelo de protección basado solo en disposiciones constitucionales; pero más significativamente, la aspiración de transformarse en un país que brinda un nivel de protección adecuado, de acuerdo con los estándares promovidos por la Unión Europea, a efectos de acceder a la transferencia de datos personales desde esta y, con ello, facilitar la inversión en aquellos nichos de mercado que suponen tratamiento de datos provenientes de aquella. Así, al temprano reconocimiento de la Argentina como país seguro, se suma el inminente de Uruguay; en tanto, Colombia, Costa Rica, México y el Perú han modificado recientemente su legislación interna para tales efectos; mientras, Brasil y Chile cuentan ya con iniciativas legislativas en la materia.

El modelo latinoamericano de protección de datos personales está en un estadio de transición. Años atrás, se verificaba a través de disposiciones constitucionales, a las cuales se incorporaba un mayor o menor número de leyes, lo que hacía de ella una regulación fragmentaria y, en ocasiones, inconsistente. Hoy, en las principales economías de la región, esta protección constitucional se traslapa con una norma general que reglamenta el tratamiento de la información personal, sea o no privada. Como resultado de esa superposición de medidas constitucionales y legales, la protección de los datos personales aparece robustecida en América Latina, si bien aún resta fortalecer el efectivo cumplimiento de la ley.

Limitar la protección de los datos personales a aquellos que conciernen a la vida privada es, entonces, un error en lo tocante a la determinación del

bien jurídico protegido. Sostener que la protección de los datos personales debe limitarse a la información privada implica un desconocimiento del desarrollo histórico del amparo, con un argumento que retrotrae el desarrollo doctrinario y jurisprudencial más de treinta años. Además, introduce serias dificultades para fijar los límites de la protección, dada la multiplicidad de teorías respecto de qué se entiende por privado, un tópico sobre el cual se ha escrito bastante y cuyo análisis excede los propósitos de este ensayo. Pero aún más, limitar hoy la protección a la vida privada, junto con precarizar la protección de las personas, generaría un enorme retroceso en la armonización normativa internacional, un costo bastante elevado de cara a los efectos de la globalización. En cambio, el derecho a la protección de los datos personales garantiza a las personas el control sobre la información que les concierne, independientemente de su conexión con la vida privada, aspecto que, de hecho, se soslaya.

Naturalmente, sostener que el derecho a la protección de los datos personales resguarda más que la vida privada no obsta brindar un plus de protección a aquella información que devela aspectos particularmente íntimos de las personas. Precisamente, esto se logra por medio del establecimiento de una protección reforzada para los denominados *datos sensible*. Estos son aquellos datos que revelan información merecedora de especial resguardo por el mayor peligro que su tratamiento implica para las libertades y derechos ciudadanos. De acuerdo con los *Principios rectores para la reglamentación de los cheros computarizados de datos personales,* adoptados por las Naciones Unidas (1990), estos datos pueden originar una discriminación ilícita o arbitraria. Entre estos se cuentan los datos relativos al origen racial o étnico de una persona, su color, vida sexual, opiniones políticas, convicciones religiosas, filosóficas o de otro tipo, así como sobre la participación en una asociación o la afiliación a un sindicato. Algunos países, según su propia experiencia, agregan la información genética, la afiliación política u otros datos a este listado. Todos los países latinoamericanos que disponen de leyes en esta materia fijan normas que brindan una protección reforzada a los datos sensibles.

En suma, aun cuando existe algún traslape entre el derecho a la vida privada y el derecho a la protección de los datos personales, este último tiene una entidad autónoma, mediante el cual se garantiza a toda persona el derecho a controlar la información que le concierne, independientemente de si es pública o privada. Sostener lo contrario implica un serio retroceso en materia de derechos fundamentales en general y de protección de datos en particular.

II. La apropiada extensión del concepto *dato personal*

Una segunda línea de argumentación que intenta mermar la protección de los datos personales en América Latina asegura que aquellos países que han adoptado leyes sobre la materia yerran al extender de forma excesiva la protección no solo a los datos relativos a personas identificadas, sino, también, a aquellas que resulten identificables. Esto implica que no solamente quedan afectos a la ley el tratamiento de los datos asociados a una persona inequívocamente individualizada, sino, también, el de aquellos datos correspondientes a una persona no identificada pero susceptible de serlo. Este sería el caso, por ejemplo, de los datos personales asociados al rol único tributario en Chile; del número de seguridad social en Estados Unidos; del número de identificación fiscal en España o de las huellas dactilares de su titular. En todos estos casos, por medio de un procedimiento posterior, es posible llegar a identificar la persona a la que corresponden los datos.

En realidad, la protección de los datos personales se extiende a personas identificadas o identificables en todos los instrumentos internacionales y las legislaciones locales. En efecto, desde las *Directrices sobre protección de la privacidad y ujos transfronterizos de datos personales*, adoptadas en 1980 por la Organización para la Cooperación y el Desarrollo Económico (OCDE), pasando por la *Directiva sobre Protección de Datos Personales* de la Unión Europea de 1995, hasta el más reciente *APEC Privacy Framework,* adoptado en 2005 por el Foro de Cooperación Económica Asia-Pacífico, todos y cada uno de los instrumentos internacionales relativos al tema extienden su protección a personas identificadas e identificables. Lo propio acontece con la legislación comparada, inclusive la latinoamericana. Por consiguiente, sustentar que este es un equívoco de los países de América Latina es, por decir lo menos, errado.

La extensión del derecho a la protección de los datos personales a datos correspondientes a personas identificables apunta a garantizar la integridad de dicho acto. Se evita, así, que el propósito de la ley sea burlado mediante un subterfugio técnico que desvincule en apariencia los datos respecto de la persona a quien conciernen. Si esta es potencialmente identificable, tal como acontece en cada una de las hipótesis arriba mencionadas, la ley es aplicable, el titular goza de derechos, la entidad que trata los datos debe cumplir con sus obligaciones y queda ligada a las responsabilidades previstas por la ley. La protección es, pues, también efectiva sobre datos respecto de personas identificables.

La protección sobre datos correspondientes a personas identificables garantiza la adecuación de la ley al desarrollo de la tecnología. De este modo, las personas no quedan desamparadas de la ley por los progresos técnicos que permiten la asociación de ellas con determinados datos. Así, en la medida que sea posible correlacionar datos con personas –de acuerdo con el estado del arte de disciplinas como la dactiloscopia, la biometría, la genética o el simple cruce de bases de datos–, permitiendo su eventual identificación, dicho tratamiento de datos queda vinculado a cumplir con la ley sobre datos personales. Esto nos lleva a la raíz de este problema, al menos para los prestadores de servicio en línea: los números IP.

Un número IP es un identificador numérico mediante el cual se identifica un dispositivo conectado a Internet. Él es parte esencial del protocolo de comunicaciones en Internet, tal como un número telefónico lo es para las comunicaciones telefónicas. Sin embargo, a diferencia de este último, por lo general, un número IP no está asignado a un abonado en particular, sino que le es adjudicado al usuario cada vez que se conecta a la red por la empresa que le brinda la conexión de entre el conjunto de números que esta administra. Esto le permite al prestador correlacionar los números IP que asigna con el listado de sus abonados y, eventualmente, identificar al usuario que se ha conectado a la red. Consiguientemente, siendo un dato susceptible de vincularse a una persona determinable, su tratamiento debe cumplir con la ley sobre datos personales.

Los prestadores de servicio en línea sostienen que los números IP no constituyen propiamente datos personales y deberían ser excluidos de la aplicación de la ley. De acuerdo con ellos, los números IP no están concebidos para identificar usuarios, sino dispositivos; por ende, un número IP permite precisar desde qué equipo se verificó una comunicación, pero no establece la identidad de quién empleó dicho equipo.

Las autoridades europeas en materia de protección de datos personales, en cambio, sostienen que el tratamiento de números IP queda sujeto a las leyes sobre datos personales. En verdad, incluso si el propósito inicial de los números IP fuese tan solo facilitar técnicamente la comunicación en Internet, ello no es un impedimento para su empleo en la eventual identificación de ciertos usuarios; es tan cierto esto, que en diversos países se han adoptado normas especiales concernientes a la retención de datos de tráfico, incluyendo los números IP, a efectos de la persecución criminal, pues facilitan la labor de identificación del supuesto infractor. Este es el caso de la *Directiva sobre Retención de Datos* adoptada por la Unión Europea, de la Convención sobre Cibercrimen del Consejo de Europa, y hasta de la Digital Millenium Copyright Act de los Estados Unidos.

Con los nuevos estándares de comunicación sobre Internet, el potencial riesgo para las personas asociado al tratamiento de los números IP se incrementará. El actual protocolo IPv4 dispone de una limitada secuencia de números, lo que hace prácticamente obligatorio que su uso sea compartido entre los usuarios y administrado por el prestador de servicio de Internet. Sin embargo, el protocolo IPv6, que ya ha comenzado a ser implementado en varios países, ha incrementado exponencialmente el número de dichas secuencias. Esto permitirá que próximamente no solo nuestra computadora, así como, también, nuestros teléfonos celulares y GPS estén conectados a Internet, sino que, además, lo estarán nuestros vehículos, dispositivos de seguridad domiciliaria y hasta ciertos electrodomésticos. IPv6 permitirá la conexión continua a Internet y, con ello, un mayor tratamiento de datos personales de los usuarios de dispositivos conectados.

En suma, las legislaciones nacionales adoptadas en América Latina han hecho bien en conceptualizar los datos personales como aquellos concernientes a personas identificadas o identificables. Dicha noción garantiza la compatibilidad normativa con la legislación de otras latitudes; otorga una protección integral al derecho de toda persona de controlar su información personal; y permite la adecuación de la ley a los progresos de la ciencia y la tecnología, particularmente respecto de la identificación de los usuarios en Internet.

III. El consentimiento como legitimación para el tratamiento de datos

El derecho a la protección de los datos personales confiere a su titular la posibilidad de registrar la información que le concierne. Es ella quien determina a quién, cuándo y cómo suministra sus datos. Aún más, es ella quien define cuándo y cómo ejercer alguna de las facultades que le brinda la ley, tal como acceder a ellos, solicitar su modificación, eliminación o bloqueo, según los casos. Así, salvo las excepciones previstas legalmente, el tratamiento de datos personales puede verificarse solo cuando la persona a quien ellos se refieren lo ha autorizado. De hecho, aun habiendo autorización, el titular puede revocarla, lo que impediría el procesamiento ulterior de sus datos. Entonces, el consentimiento es esencial para el tratamiento legítimo de los datos personales.

Sin embargo, en ocasiones, el consentimiento no resulta suficiente para validar el uso de datos personales. Así, la aquiescencia de un empleado para

con su empleador en relación con que este acceda a su correo electrónico o de un consumidor respecto de su proveedor para con la transferencia de sus datos a terceros, aparece condicionada por la relación misma que tiene lugar. El consentimiento allí obtenido, cualquiera sea la fórmula contractual que revista, está constreñido. Esto ha llevado a diversos países a la adopción de reglas especiales que protegen a empleados y consumidores en relación con el tratamiento de la información personal que les conciernen por parte de sus empleadores y proveedores.

El permiso para tratar datos personales resulta aún más problemático en relación con Internet y la prestación de servicios en línea, particularmente cuando la validez de aquel descansa en haber sido entregado libre e informadamente. Es discutible el grado de información del que dispone un usuario promedio en relación con el opaco funcionamiento de las tecnologías de la información. Incluso es discutible la voluntad de un usuario avezado, si se considera la asimetría de información que media entre él y su proveedor de servicios. Otro tanto cabe agregar respecto de la libertad con que dicho consentimiento es brindado cuando la prestación de servicios no tiene carácter competitivo; en la mayor parte de la región, el mismo acceso a Internet es una prestación monopólica y, en el mejor de los casos, oligopólica. Esto pone al consumidor en el poco dichoso dilema de consentir al tratamiento de sus datos para acceder a Internet o resguardarlos y permanecer desconectado.

Las redes sociales en línea presentan problemas específicos en torno a cuán efectivo es el permiso brindado por sus usuarios. Este dilema se explica con las denominadas *economías en red,* ya que en ellas no es necesariamente el mejor prestador de servicios el que prevalece, sino aquel capaz de aglutinar una masa crítica de la demanda por servicios y proveer acceso no solo a este, sino a su red. Así, por ejemplo, un usuario puesto ante la disyuntiva de escoger un proveedor de telefonía, entre oferentes con igualdad de condiciones económicas, elegirá a aquel que le brinda acceso preferencial a una más amplia red de abonados o que le otorga servicios adicionales. Este ha sido el caso de los usuarios del paquete de ofimática de Microsoft, de los servicios de mensajería instantánea de Gmail o de los aplicativos de dispositivos Apple. En Chile, este es el caso de Facebook, la red social que congrega al 50% de los chilenos; naturalmente, los nuevos usuarios del país tienden a escoger dicho servicio por la ventaja comparativa de acceder a una red tan amplia de usuarios, haciendo caso omiso de la política de privacidad de la compañía.

Dado que el consentimiento brinda una limitada protección al titular de los datos personales, se han adoptado ciertos correctivos. Una de estas medidas es que el tratamiento de la información personal debe verificarse de

acuerdo con la finalidad que justificó su colecta, aquella que en su momento fue informada al titular y respecto de la cual este consintió. Así, el uso de datos personales en un proceso de reclutamiento laboral debe extenderse a información pertinente, a efectos de establecer la idoneidad laboral del candidato; requerir datos que excedan dicha finalidad, aun cuando sea consentido, implica un tratamiento ilícito de datos personales. Parafraseando las ya mencionadas recomendaciones de las Naciones Unidas en la materia, el tratamiento de datos personales debe ser adecuado, pertinente y no excesivo en relación con una finalidad legítima. Esto plantea preocupación respecto de ciertas prácticas de tratamiento de información personal en línea, tales como la publicidad contextual de Google o el reconocimiento facial de usuarios de Facebook.

Adicionalmente, la aspiración a reconducir toda la legitimidad del tratamiento de información personal a los términos de un contrato evade la responsabilidad pública en el resguardo de los derechos fundamentales de los usuarios. El costo transaccional de hacer cumplir la ley en un caso individual es altísimo, y dejar librado el respecto de los derechos del titular a las leyes del mercado es abandonarlo a su suerte. Esto es particularmente funesto si se ven forzados contractualmente a resolver cualquier conflicto con su proveedor de servicio ante jurisdicciones ajenas. Es precisamente la necesidad de enfatizar la protección que requieren las personas en relación con sus datos personales lo que ha llevado a la mayor parte de los países desarrollados, y progresivamente a los de América Latina, a establecer una autoridad pública que supervisa el cumplimiento de la ley.

En suma, salvo las excepciones previstas en la ley, el consentimiento de la persona concernida por la información es necesario para su tratamiento legítimo, pero no es suficiente. El tratamiento de datos personales debe cumplir con los demás preceptos de la ley sobre su protección, pero especialmente debe ser adecuado, pertinente y no excesivo en relación con una finalidad legítima.

IV. El riesgo del tratamiento de datos personales por prestadores de servicio en línea

La intención de reducir la protección que se brinda a los datos personales sobre la base de limitarla solo a los privados, concernientes a personas identificadas y sujetos a meras disposiciones contractuales, no es infundada. Por medio de dichos argumentos, los prestadores de servicios en línea

procuran disponer de un entorno legal más favorable para su prestación, removiendo los obstáculos jurídicos que pesan sobre el funcionamiento de Internet. Es, en ciertos casos, el entorno de que han dispuesto en su país de origen: los Estados Unidos. Con el afán de promover la extensión de Internet, en su día, el legislador estadounidense garantizó inmunidad a los prestadores de servicio en relación con los contenidos provistos por terceros, a excepción de aquellos que infringen la propiedad intelectual. En la práctica, este hecho ha conferido no solo inmunidad, sino, también, impunidad a los prestadores de servicio en relación con toda infracción cometida por terceros, incluso si dicho prestador está al corriente de ella. El derecho a la privacidad y el derecho a la protección de la información personal han resultado seriamente menoscabados como consecuencia de dicha política.

Las características de Internet sugieren que es necesario adoptar algunas reglas específicas respecto del tratamiento de datos personales que tiene lugar en la red. La colecta automatizada de información inherente al funcionamiento técnico de Internet hace necesario cierto tratamiento de esa, así como en el caso de números IP y *cookies*. El alojamiento de contenidos por terceros suscita dudas en cuanto a la responsabilidad que, eventualmente, cabe a quien provee servicios de almacenamiento para dicha información. La expresión de consentimiento, la individualización de usuarios, la adopción de normas especiales en protección de la infancia, entre otros, requieren del establecimiento de reglas certeras para el entorno en línea.

Sin embargo, la adopción de normas específicas en relación con el procesamiento de datos personales en Internet no implica derogar el derecho a su protección. En ciertos casos, será necesaria la introducción de flexibilidades, salvaguardias o limitaciones. Por ejemplo, ya hemos aludido al *derecho al olvido*, que supone que se prescinda del tratamiento de información personal en determinados casos, tales como sanciones criminales y administrativas ya cumplidas o deudas ya pagadas. En aquellos casos, su uso estaba fundado en una finalidad legítima, el cobro de un crédito o la imposición de una pena; sin embargo, una vez que se ha cumplido, los datos deben ser eliminados o bloqueados, según la opción legislativa que se adopte. Dicha eliminación o bloqueo también debería tener lugar en Internet. Sin embargo, el reconocimiento del *derecho al olvido* debe dejar a salvo ciertas excepciones, tales como aquellas resultantes del tratamiento de información personal para fines de investigación periodística y científica. Mediante esas flexibilidades, salvaguardias o limitaciones, el derecho a la protección de datos personales queda a resguardo, pero reconociendo ciertas excepciones a los efectos de cumplir con fines de interés público.

El establecimiento de reglas específicas en lo que concierne al tratamiento de datos personales en Internet, como se ha sugerido, también requiere precisar la responsabilidad a la que está sujeto un prestador de servicio en línea ante infracciones cometidas en la red. Dicha responsabilidad resulta relativamente clara cuando es el propio prestador de servicios quien realiza un uso indebido de datos personales, por ejemplo, al colectar datos de sus usuarios subrepticiamente. Algo más complicada es la hipótesis cuando se trata de escindir responsabilidad entre dicho prestador y quien provee los contenidos; garantizar inmunidad absoluta es repulsivo para el reguardo de los derechos de terceros, tanto como forzar a los prestadores a censurar contenidos críticos a simple requerimiento de quien es objeto de los reproches, sin siquiera poseer orden judicial. Sin embargo, en América Latina, un problema más serio parece ser el relativo a la retención de datos personales por los prestadores de servicios en línea y el posterior uso que se hace de dichos datos.

A diferencia de la normativa sobre protección de datos, en América Latina existe menos progreso en lo relativo a la reglamentación de la retención de datos por los prestadores de servicio en la red, es decir, a la colecta y preservación de datos relativos al uso de Internet por sus usuarios, tales como los números IP asignados, fecha y hora de conexión, entre otros. Aunque varios proveedores se han visto forzados a procesar dicha información a los efectos de la tarificación y el control de acceso a sus servicios, otros solo lo hacen como resultado de obligaciones impuestas por la ley a efecto de facilitar la eventual identificación de usuarios.

Desafortunadamente, en América Latina, esta reglamentación no es uniforme; de hecho, no existe en todos los países, y en aquellos en los que existe, obedece a distintos impulsos legislativos. Así, por ejemplo, en la Argentina, se carece de regulación, tras la decisión de la Corte Suprema de Justicia, en el bullado caso *Halabi,* de declarar inconstitucional la ley y reglamentación adoptadas en la materia. Naturalmente, tanto las disposiciones constitucionales como las normas sobre protección de datos resultan aplicables en la materia, pero ellas son esquivas para la completa y acertada regulación de la retención de datos. En México, es la ley federal de telecomunicaciones la que reglamenta la materia. En Chile, en cambio, el código procesal penal fija normas al respecto, en el contexto de la individualización de responsables por delitos de pornografía infantil y otros crímenes. Este distingo en el impulso legislativo no es baladí, pues él incide obviamente en el mayor o menor celo del legislador al reglamentar.

Uno de los aspectos críticos al legislar sobre retención de datos por los prestadores de servicios en línea es la adopción de medidas de resguardo para los derechos fundamentales de las personas concernidas por la información. No solo es necesario precisar qué tipo de prestador de servicios es el obligado a retener, sino, también, qué información, cómo y por cuánto tiempo debe retener dicha información. Es igualmente crítico establecer a quién y bajo qué condiciones suministra dicha información. Establecer una apropiada normativa no es una tarea fácil; de hecho, los cuestionamientos a la constitucionalidad de la regulación son frecuentes. A la reciente declaración de inconstitucionalidad formulada por el Tribunal Constitucional Federal Alemán respecto de varias leyes que reglamentaban la materia, cabe agregar la ya mencionada decisión de la Corte Suprema de Justicia de la Argentina en el caso *Halabi*, y el también reciente fallo del Tribunal Constitucional de Chile en el que se resuelve la inconstitucionalidad de un sistema de registro de usuarios de cibercafés, el cual pretendía servir de complemento a la obligación legal de los prestadores de servicio de Internet de retener datos de sus usuarios. Todos ellos enfatizan la necesidad de resguardar apropiadamente los derechos de las personas atañidas por la información, a la hora de imponer en los prestadores de servicio la obligación de reservar datos personales de sus usuarios.

En los años venideros, los países de América Latina, especialmente aquellos que han suscrito tratados de libre comercio, se verán forzados a adoptar normas especiales sobre retención de datos personales a efectos de hacer cumplir las leyes sobre propiedad intelectual. De hecho, Chile ya ha implementado dicho compromiso, conduciendo a la inconsistente decisión de que la retención de datos tiene lugar para fines de persecución criminal de delitos graves y de infracciones a la ley de derechos de autor cualquiera sea su entidad. En Colombia, el denominado proyecto de Ley Lleras, a través del cual se intenta implementar dichas normas, ha suscitado un fuerte rechazo ciudadano, lo que obligó al Gobierno a su reformulación y dilación legislativa. Lo propio deberá tener lugar en otros países de la región, que han adoptado tratados de libre comercio (*e.g.*, Perú, República Dominicana y el Salvador) o consideran su adhesión a nuevos instrumentos en materia de protección a la propiedad intelectual (*e.g.*, México).

En suma, el tratamiento de datos en Internet plantea serios desafíos no solo a los prestadores de servicio de Internet, sino, también, a los Poderes Legislativos de la región, en orden a adoptar prácticas y normas que satisfagan legítimos fines de interés público y el adecuado respecto del derecho a la protección de los datos personales. La reglamentación de la retención de dichos datos sea, quizá, el más crítico en los próximos años.

V. Conclusiones

El derecho a la protección de los datos personales satisface más que simplemente la aspiración individual de una persona a excluirse de la vida social, por medio de su protección se salvaguarda el interés público envuelto tanto en el respeto de los derechos fundamentales de las personas, como en la preservación de condiciones de desarrollo inherentes a una sociedad democrática.

Los países de América Latina han hecho significativos avances en materia de protección a los datos personales, transitando progresivamente desde un modelo de protección preferentemente constitucional a un modelo que es complementado por legislación comprensiva. Este proceso ha brindado una protección más integral, con lo que se incrementa la certidumbre jurídica y avanza en la armonización normativa internacional.

Internet plantea nuevos desafíos para la protección de los datos personales en el entorno en línea. La adopción de normas especiales parece necesaria. En este contexto, se ha sugerido que la protección debería limitarse a los datos privados, referentes a personas identificadas, y dar preeminencia a soluciones contractuales. En este ensayo, hemos discutido cada una de dichas sugerencias, que, en vez de instar a la adopción de normas de adecuación al entorno en línea, limitarían ostensiblemente el derecho a la protección de los datos personales, sacrificando cada uno de los logros habidos hasta la fecha en la materia.

Dentro de los múltiples temas de relevancia, en los próximos años será crítico para los países latinoamericanos el acogimiento de leyes referidas a la retención de datos por los prestadores de servicio en línea, por medio de las cuales se procura la identificación de los usuarios. Sin embargo, cualquiera sea el interés que empuje dicha regulación, no debe omitirse la adopción de medidas de resguardo apropiado para las personas referidas por la información. Incrementar la eficacia de la ley no puede hacerse a cualquier precio. El derecho a la protección de los datos personales no puede ser sacrificado, pues su menoscabo afecta no solo a la persona a quien la información refiere, sino a la pervivencia de los derechos humanos y a los supuestos mismos del sistema democrático.