Ley de protección de datos personales y función notarial

Néstor D. Lamber

RESUMEN

Se analiza la incidencia de la Ley 24326 de Protección de Datos Personales en ciertos aspectos de la actividad notarial, ante la mayor exposición de estos datos privados en la esfera pública, desde su incorporación a bases digitales, su tratamiento y su *viralización*. En un primer aspecto, partiendo del instituto de *habeas data* referido a los tradicionales ficheros o registros guardados en soporte papel, se analiza la incidencia que ya tenía la dispensa de consentimiento para su uso en la propia ley y su decreto reglamentario. En un segundo aspecto, ya más relacionado con los soportes electrónicos de datos digitalizados, se analiza la distinción entre cesión y transferencia de datos a la hora de calificar el consentimiento del titular en la gestión de documentos notariales digitales y el almacenamiento y guarda en servidores de prestadores *clouding* de la información obtenida para la función notarial.

PALABRAS CLAVE

Protección de datos personales; datos sensibles; tratamiento de datos; cesión de datos; transferencia de datos; bases de datos; archivos de datos; registro de datos; bancos de datos.

Recibido: 31/7/2020
Aceptado: 14/8/2020
Publicado online: 9/12/2020

Sumario: ***1.*** *Concepto de datos personales y sensibles.* ***1.1.*** *Fundamento de la protección de datos personales y la acción de habeas data. Identidad digital. Derecho al olvido.* ***1.2.*** *Datos protegidos. Conceptualización jurídica de determinación e identificación.* ***2.*** *La función notarial en la protección de datos personales.* ***2.1.*** *Derecho de acceso del titular del dato en el documento notarial y el secreto profesional: exhibición del protocolo.* ***2.2.*** *Principio de calidad del dato: realidad tangible y certeza de su representación.* ***2.3.*** *Datos sensibles: actas de constatación de contenido de chats, WhatsApp, e-mail, correspondencia epistolar.* ***2.4.*** *Transferencia y cesión de datos personales: almacenamientos en servicios cloud computing.* ***3.*** *Conclusión.* ***4.*** *Bibliografía.*

1. Concepto de datos personales y sensibles

1.1. Fundamento de la protección de datos personales y la acción de habeas data. Identidad digital. Derecho al olvido

La Ley 25326 de Protección de Datos Personales (LPDP) y su Decreto reglamentario 1558/2001 regulan la operatividad de la acción de *habeas data*, establecida en el tercer párrafo del artículo 43 de la Constitución Nacional como un derecho humano fundamental, cuyo objeto es la protección de la identidad de la persona humana y de la jurídica. En su concepción inicial, dicha acción estuvo ligada más al derecho público de evitar la discriminación de la persona por el tratamiento de datos personales, incluyéndola en categorías sospechosas, como ha sostenido la jurisprudencia norteamericana.[1] Posteriormente, su interpretación evolucionó con especial incidencia de la cultura digital, donde la fácil conversión de datos privados en públicos, a través de nuevas tecnologías que facilitan exponencialmente la captura, almacenamiento, transferencia y tratamiento de la información, permite la construcción, reconstrucción o modificación por terceros de la reputación en las redes –y en el mundo digital en general–, de la identidad de la persona, especialmente estableciendo perfiles que afectan no solo su intimidad sino su relación con el resto de la comunidad, sus consumos, sus relaciones de trabajo y afectivas y sus expresiones políticas.

El primer aspecto del concepto de protección de datos personales se explica plenamente en una de sus categorías: los "datos sensibles", de conformidad con el artículo 7 LPDP, y definidos por el artículo 2 LPDP como aquellos "datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual". Si bien se puede argumentar se apunta a la protección de la esfera íntima de la persona, la finalidad que determina el interés jurídico protegido, tal como expresamente establece el artículo 43 de la Constitución Nacional, es la de prevenir la discriminación de la persona. Al respecto, Peyrano explica:

> El comportamiento del ser humano ha demostrado a través del transcurso de la historia, que determinadas creencias, inclinaciones, preferencias, situaciones, padecimientos, etc., se han constituido en una fuente recurrente de discrepancias, enfrentamientos, dominaciones, en los distintos Estados y sociedades, como igualmente y a causa de ello en fuente u origen de tratos diferenciales y discriminatorios […] Del mismo modo, otros aspectos de las personalidades y condiciones humanas tales como sus inclinaciones sexuales, situación socioeconómica, estado de salud (fundamentalmente, por

1. La Corte Suprema de los Estados Unidos de Norteamérica, en autos "Kaorematsu v. United States" (18/12/1944), se ha valido del concepto de categoría sospechosa, entendido como la agrupación de individuos según criterios generales que llevan, por su implicancia o significado en el medio social del país, a presumir finalidades por las que se le debe aplicar un tratamiento injustificadamente desigualitario en relación a los demás individuos no pertenecientes a las categorías en cuestión; y, en base a esa presunción social o legal, resolvió invalidar las normas consecuentes. Este criterio, propio del derecho público y la organización democrática, es el que predominaba al momento de la inclusión del instituto de *habeas data* en el art. 43 de la Constitución Nacional en 1995 y que subyacía en las primeras interpretaciones judiciales, con un entendimiento más limitado que el que impuso la realidad de "mundos virtuales" en este siglo. [*N. del E.*: ver aquí; fuente: https://www.courtlistener.com/; última consulta: 28/8/2020].

> padecerse ciertas enfermedades o afecciones), etc., también comparten esa potencialidad "discriminatoria", por prejuicios históricos, culturales y sociales, o, en algunos casos, por ignorancia o superstición.[2]

Y concluye –en opinión que compartimos– que

> El parámetro detonante entonces, de caracterización de los "datos personales" como "datos sensibles", finca en la posibilidad de generar, por la trascendencia de su contenido, esto es, por las connotaciones que implican en el medio social las realidades que representan, actitudes discriminatorias respecto de sus titulares, y no por esa supuesta voluntad de "reserva", que cierto es por lo general los acompaña (aunque, como se ha visto, puede perfectamente encontrarse ausente).[3]

El segundo aspecto de la protección apunta a la de todo dato personal, conceptualizando el dato como el vehículo para llegar al conocimiento de la persona y de las circunstancias que determinan su existencia como tal, su identidad. Este conocimiento se logra a través de representaciones documentales en todo tipo de soportes –no solo electrónicos, como analizamos en este trabajo–, que pueden almacenarse tanto en ficheros analógicos como en registros, archivos o bases de datos informáticas. Así, el dato es la representación parcializada de acceso al conocimiento de una parte de la personalidad y la identidad. En ese aspecto, la razón de la protección del dato es la intimidad, la esfera de reserva que merece la persona para mantener su dignidad y autonomía respecto de sus actos privados; y también la reputación digital, entendida como la construcción de una identidad virtual, donde la finalidad del interés jurídico protegido es la enunciada en el artículo 43 CN, de tender a evitar la falsedad del dato, en su concepto amplio de no limitarse solo a la veracidad de lo representado sino que el mismo sea actualizado con la situación presente de la persona, que se plasma en el denominado derecho al olvido, receptado, entre otras normas, en los arts. 16 (inc. 7) y 26 (inc. 4) de la LPDP, al establecer que los datos deben ser conservados por un plazo determinado previamente y luego suprimidos.

La Corte Suprema de Justicia de la Nación, con posterioridad a la sanción de la LPDP, ha sostenido:

> Cabe revocar la sentencia que rechazó la acción de habeas data deducida contra el Banco Central de la República Argentina y la entidad bancaria que le comunicó la información adversa relativa a su condición de deudor incobrable, con el objeto de que ésta última brinde adecuada información acerca de los datos que envía a aquélla entidad en relación con la Central de Deudores del Sistema Financiero y que se elimine la información de morosidad, fundando el pedido en el artículo 43 de la Constitución Nacional y artículo 26, inciso 4º, de la ley 25326, pues la ley ha consagrado el derecho del afectado a exigir que –transcurrido cierto tiempo– los datos significativos para evaluar su solvencia económica-financiera no sean mantenidos en las bases de datos ni difundidos, con el

2. Peyrano, Guillermo F., "Datos sensibles: perfiles y regulaciones. El impacto del desarrollo tecnológico" [online], en AA.VV., *Dossier: habeas data. Selección de jurisprudencia y doctrina*, Buenos Aires, Sistema Argentino de Información Jurídica - Ministerio de Justicia y Derechos Humanos, 2020, p. 474; en http://www.saij.gob.ar/docs-f/dossier-f/habeas_data.pdf; última consulta: 31/7/2020. (El artículo citado fue originalmente publicado en *El Derecho*, Buenos Aires, Universidad Católica Argentina, boletín Nº 10651, 13/12/2002).

3. Ibídem.

> objeto de que el individuo no quede sujeto indefinidamente a una indagación sobre su pasado.[4]

Molina Quiroga nos señala la ampliación de este aspecto de la protección de los datos personales al decir que

> La fundamentación jurídica del derecho a la protección de datos personales, sin duda puede y debe relacionarse con el tradicional derecho a la intimidad, pero lo excede ya que también alcanza a datos públicos, incide en otros derechos personalísimos como el honor, la imagen o la identidad, y lo que es más decisivo para nuestra hipótesis, es que no solo se vincula con personas físicas, sino también con personas jurídicas. Por ello el control de la información personal está relacionado con el concepto de autonomía individual para decidir, hasta cierto límite, cuándo y qué información referida a su persona, puede ser objeto de procesamiento (automatizado o no), por lo que también se ha denominado a la protección del dato personal, autodeterminación informativa, e incluso libertad informática.[5]

Y aclara:

> El derecho a la autodeterminación informativa consiste en la posibilidad que tiene el titular de los datos personales de controlar quiénes serán destinatarios de dicha información y qué uso le darán, y se ejercita a través de los derechos de acceso, rectificación y cancelación.[6]

La actual era digital nos impone a los operadores del derecho –en especial del privado– tener en mira esta concepción de protección de los datos personales. Hemos citado la jurisprudencia de la Corte Suprema de Justicia del año 2011, por su relevancia en los tribunales del país, en la que ha dejado de fundar la protección solo en los casos de comprobada falsedad previa –como antes de la sanción de la LPDP[7]–, admitiendo la protección jurídica de la actualización de los datos personales almacenados, su corrección o supresión, dando así lugar a que no se limita a acreditar falsedad, ni su intención o no, dolo, negligencia o error en la recolección, conservación, tratamiento o transferencia, sino que reconoce, además, el derecho a su supresión por el mero paso

4. Sumario de CSJN, 8/11/2011, "Catania, Américo Marcial c/ BCRA-(base de datos) y otro s/ habeas data" C.1380. XLII (*Fallos*, 334:1276), en AA.VV., ob. cit. (cfr. nota 2), pp. 9, 31 y 35 (sumario catalogado como SAIJ A0072438). [*N. del E.:* ver fallo completo aquí; fuente: CSJN; última consulta: 28/8/2020]. Ver también CSJN, 8/11/2011, "Napoli, Carlos Alberto c/ Citibank N.A. y otro s/ habeas data" N.112.XLII (*Fallos*, 334:1327), en AA.VV., ob. cit. (cfr. nota 2), pp. 10, 33 y 77 (sumarios catalogados como SAIJ A0072441). [*N. del E.:* ver fallo completo aquí; fuente: CSJN; última consulta: 28/8/2020].

5. Molina Quiroga, Eduardo, "Protección de datos personales como derecho autónomo. Principios rectores. Informes de solvencia crediticia. Uso arbitrario. Daño moral y material" [online], en AA.VV., ob. cit. (cfr. nota 2), p. 347; en http://www.saij.gob.ar/docs-f/dossier-f/habeas_data.pdf; última consulta: 31/7/2020. El autor inicia diciendo: "El llamado 'Habeas data' tutela un derecho especial, que podemos denominar 'autodeterminación informativa' o derecho a la protección de datos personales. Es necesario independizar conceptualmente este interés jurídicamente tutelable de otros derechos personalísimos, tales como el derecho a la intimidad, el derecho al honor o el derecho a la imagen, y aún el derecho a la identidad, sin desconocer que tienen puntos de confluencia" (p. 345).

6. Ibídem.

7. Ver CSJN, 6/3/2001, "Lascano Quintana, Guillermo Víctor c/ Veraz SA s/ habeas data" L.215.XXXV (*Fallos*, 324:567), en AA.VV., ob. cit. (cfr. nota 2), p. 14 (sumario catalogado como SAIJ A0059215): "El art. 43 de la Constitución Nacional prevé la supresión de datos de los registros, ante actos de ilegalidad o arbitrariedad manifiesta, sólo para los casos de falsedad o discriminación". El cambio del criterio del máximo tribunal consagra la nueva visión dinámica del derecho, donde la norma del Congreso de la Nación permite, en su interpretación, hacer operativa la garantía constitucional y el derecho humano aplicable por la convencionalidad de los tratados internacionales que los reconocen. [*N. del E.:* ver fallo completo aquí; fuente: CSJN; última consulta: 28/8/2020].

del tiempo, haciendo patente el derecho al olvido. Este es concebido como aquel por el que nadie puede ser perseguido indefinidamente por su pasado –ser su esclavo–, en congruencia con el principio del derecho informático de la caducidad temporal de todo registro, licencia, firma digital, etc. Se trata de un aspecto de los derechos humanos y constitucionales que tiene efecto directo en la publicitación del derecho privado y en la actividad notarial, en aspectos que se analizarán más adelante en el presente trabajo.

La protección de los datos personales en la reforma constitucional de 1994 se fundaba esencialmente en evitar la discriminación (exclusivamente respecto de los datos sensibles) y evitar la falsedad del dato con realidad tangible que permite parcialmente conocer (persona e identidad), pero el desarrollo de la nuevas tecnologías de información y el conocimiento impone su razón en la protección de la dignidad humana en la construcción de su identidad o reputación digital (autodeterminación informativa).

1.1.1. Derechos humanos y autodeterminación informativa

Ante la consagración legislativa de la constitucionalización del derecho privado y la primacía en derechos humanos en el artículo 1 del Código Civil y Comercial (CCyC), Masciotra explica que

> Los datos personales se hallan estrechamente vinculados a la existencia de la persona, no sólo por cuanto a través de ellos la identificamos, sino que los mismos resultan imprescindibles para el ejercicio de sus derechos y la satisfacción de sus obligaciones. Sin datos que individualicen e identifiquen a las personas, es materialmente imposible conformar una sociedad humana que respete los derechos fundamentales que hacen a la identidad, la libertad, la intimidad, la imagen, el honor, la propiedad, el ejercicio de derechos civiles y políticos, etc. A través de los datos se individualiza a la persona y ésta se inserta dentro del mundo jurídico; toda nuestra existencia se halla registrada, desde el nacimiento hasta nuestra muerte, e incluso después de ella, con motivo de la tramitación del juicio sucesorio; y todos los datos que surgen de la vida cultural, social, profesional, laboral, económica, financiera, etc., son objeto de su pertinente tratamiento. Esta íntima e imprescindible relación entre los datos personales y la identidad misma de la persona, acredita su vital relevancia, como de su obtención, conservación, almacenamiento, adaptación o modificación, extracción, consulta, cotejo o interconexión, limitación, evaluación, bloqueo, supresión, destrucción, difusión, y cesión a terceros.[8]

1.2. Datos protegidos. Conceptualización jurídica de determinación e identificación

El titular del dato personal goza del derecho a acceder al archivo, registro o base de datos que contiene su información personal, a ser informado del mismo, su finalidad, exactitud, actualización y supresión, y de su tratamiento, en principio, con su consentimiento

8. Masciotra, Mario, "Protección de datos personales y su integración en el marco de los derechos humanos" [online], en AA.VV., *Dossier: habeas data. Selección de jurisprudencia y doctrina*, Buenos Aires, Sistema Argentino de Información Jurídica - Ministerio de Justicia y Derechos Humanos, 2020, p. 141; en http://www.saij.gob.ar/docs-f/dossier-f/habeas_data.pdf; última consulta: 31/7/2020. (El artículo citado fue originalmente publicado en www.saij.gob.ar, el 10/12/2018).

informado. La operatividad de este derecho requiere que el dato sea atribuible a la persona titular determinada o determinable, como lo plasma, *a contrario sensu*, el artículo 28 LPDP al admitir su tratamiento si la persona no es determinable merced a un proceso técnico de disociación que impide relacionar el dato personal con la misma, como sucede en esta "anonimación" para fines estadísticos, de salud, entre otros.

El Reglamento (UE) 2018/1725,[9] en su considerando Nº 16, dice:

> Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesario para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto, los principios de protección de datos no deben aplicarse a la información anónima, es decir, información que no guarda relación con una persona física identificada o identificable o datos convertidos en anónimos de forma que el interesado no sea identificable o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, ni siquiera con fines estadísticos o de investigación.

El dato será considerado personal para su protección en tanto en cuanto sea atribuible a una persona determinada o determinable; no importa ello identificar o individualizar al titular del dato en la formalización del acto en que se obtiene el mismo, a diferencia de la valoración del juicio de identidad y discernimiento que hace el notario cuando acepta un requerimiento. El dato referido a una persona será objeto de protección únicamente si es vinculable a ella, sin importar su identificación concreta al momento del almacenamiento, tratamiento, transmisión o cesión, operaciones que pueden ser íntegramente despersonalizadas. En cambio, se requerirá la identificación de la misma al momento de valorar la prestación de su consentimiento informado, aun cuando sea por la modalidad de adhesión a la propuesta predeterminada por un algoritmo en los términos de una contratación a distancia y de consumo. En este caso, se deben valorar el discernimiento y la identidad en base a datos de individualización o previo conocimiento, como manda a los notarios el artículo 306 CCyC, lo cual importa llegar a un juicio de valor, una valoración personal del agente que ejerce una función pública.

Por el artículo 20 LPDP (inc. 1), se prevé que toda resolución administrativa o judicial que importe una juicio valor, valoración o ponderación personal del agente no se puede resolver solo valiéndose de datos personales almacenados y tratados entre sí; requiere de un juicio humano (no de inteligencia artificial exclusivamente). El acto público notarial, que en el caso importa un juicio de valoración del notario, se asimila a

9. Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) 45/2001 y la Decisión 1247/2002/CE.

la resolución del acto administrativo sobre bases de datos personales, que, al implicar la apreciación o valoración de conductas humanas, en especial en cuanto al discernimiento, previo conocimiento o conductas corroborantes y complementarias de la exhibición del documento de identidad para arribar al juicio de identificación, no puede tener como único fundamento el resultado del tratamiento informatizado de los datos personales que suministren una definición del perfil o personalidad del interesado o se limiten a su identidad digital.

2. La función notarial en la protección de datos personales

La protección de datos personales en la actividad notarial se relaciona con la manda constitucional y el derecho humano a la autodeterminación informativa, donde la LPDP es un parámetro de analogía para el ejercicio de la función con el resguardo de este interés jurídico protegido. El notario no está comprendido en la tipología legal de ser usuario o administrador de una base de datos de conformidad con lo establecido por esta ley ni debe inscribirse como tal en la Dirección Nacional de Protección de Datos Personales (art. 3 LPDP). El registro de datos que hace el notario no tiene como función la elaboración de informes o perfiles de personas en base a sus datos dirigidos a terceros; por el contrario, su actuación está limitada en su publicidad por el deber de secreto profesional y la exhibición de documentación solo a las personas legitimadas por la ley o a solicitud judicial.

El traslado de los actos notariales genéricos a terceros no se produce por informes del notario sino por la publicidad cartular, cuyo soporte documental (testimonio papel o electrónico) está en poder del interviniente, y es este quien autoriza su divulgación o conocimiento cuando entrega al documento (cartular papel o electrónico). En los casos en que la ley establece su publicidad *erga omnes*, impone la obligación de inscribir en registros públicos, que son los que brindan informes o certificados a terceros –y no el notario–, como ocurre con el registro de la propiedad inmueble, el registro de testamentos, el registro de actos de autoprotección y los registros societarios, entre otros. La publicidad del acto notarial se limita a la denominada cartular, que se cumple por la decisión de quien obtuvo el testimonio del documento notarial (papel o electrónico) y lo exhibe a terceros; en ese momento, está prestando el consentimiento a que esos terceros conozcan el contenido de los datos personales. Esto sucede también en la verificación de folios notariales digitales de los documentos notariales digitales de la Provincia de Buenos Aires y la Ciudad Autónoma de Buenos Aires, a la que no se puede acceder si no se cuenta con la clave de seguridad (CVS) o código QR informáticos que surgen del propio documento, por lo cual solo puede proceder a tal verificación aquel a quien se le haya entregado el documento digitalizado, por ejemplo, remitiéndoselo por un servicio de chat, e-mail, etc.

En cuanto al objeto, la función notarial no está destinada al almacenamiento y tratamiento de datos personales, sino que suele referirse a actos de contenido patrimonial, donde los datos personales son necesarios pero accesorios al contenido del acto notarial y se los recaba y trata con esa finalidad. El uso de datos personales en la

escritura pública u otra intervención notarial está exento del consentimiento expreso del titular del dato, como veremos de conformidad con el artículo 5 LPDP.

En esta sección abordaremos la incidencia de la protección de los datos personales que se incorporan en los documentos notariales en relación con la LPDP, pero con las lógicas prevenciones de la analogía y la interpretación de las finalidades del orden jurídico, y en modo alguno incluyendo al notario en la figura tipificada de usuario o administrador, ni al protocolo o libro de requerimientos notariales en el supuesto de archivo o base de datos incluidos en la LPDP.

2.1. Derecho de acceso del titular del dato en el documento notarial y el secreto profesional: exhibición del protocolo

Los documentos notariales en soporte papel o electrónico, si bien pueden constituir un registro público de actos, son de conocimiento limitado por el público en general, solo accesibles para las personas legalmente legitimadas en atención a los fines admitidos por la ley que impone la forma derivada de la actuación notarial. En resguardo de esta limitación de la información al público en general, se estable el derecho-deber de secreto profesional del notario en las leyes de organización del notariado (art. 35 inc. 6 Decreto-ley 9020/1978 en la Provincia de Buenos Aires y art. 29 inc. j Ley 404 en la Ciudad Autónoma de Buenos Aires).

El Decreto-ley 9020 bonaerense limita la exhibición del protocolo a requerimiento del juez o de quien tenga interés legítimo con relación al documento, enumerando a los otorgantes y sus representantes o sucesores universales o singulares (art. 150), extendiendo la limitación en los casos que el notario considere secretos (art. 151). Asimismo, prevé que el notario "adoptará las providencias que estime pertinentes para que la exhibición no contraríe sus deberes fundamentales o las garantías de los interesados" (art. 152). Su Decreto reglamentario 3887/98 prevé la exhibición del protocolo para el supuesto del denominado estudio de títulos, en que la autoriza cuando lo requiera otro notario para el cumplimiento de sus funciones (art. 105), que podrá hacerlo por sí o por su mandatario o referencista. En este supuesto, se respeta acabadamente el artículo 4 LPDP, en cuanto dispone que los datos personales sean exhibidos o tratados de conformidad a la finalidad para la cual fueron recogidos y en cumplimiento de mandas legales. En términos similares, la Ley 404 de la Ciudad Autónoma de Buenos Aires establece el deber de exhibición a requerimiento judicial (art. 73 inc. a) o de quienes tuvieren interés legítimo en relación con el documento, enunciando como tales a los sujetos instrumentales y negociales, sus sucesores o representantes, los profesionales que justifiquen tareas de estudios de títulos, el otorgante de actos de última voluntad y el hijo reconocido (inc. b), siendo clara y congruente con la normativa en análisis al regular que "la exhibición no resulte incompatible con su finalidad" (art. 29 inc. j, parte final).

Si bien el protocolo notarial y el libro de requerimientos de firmas e impresiones digitales no están comprendidos en la normativa de necesaria inscripción como registro de bases de datos, las normas citadas muestran la análoga facultad y derecho de acceso del titular del dato –a la vez interviniente del acto documentado– con la solicitud y previa acreditación de su identidad (art. 14 inc. 1 LPDP). Lo mismo sucede en la generación de

documentos notariales digitales, cuyo contenido no resulta de acceso público si no es con el permiso derivado del acceso al código QR o CVS de los mismos.

Esta exhibición y el uso de estos datos en el destino del documento (p.ej., la rogación del acto titularizado en el registro de la propiedad inmueble) que puede importar su tratamiento no requieren consentimiento ni prevención alguna de ello por separado o en una cláusula escrituraria, de conformidad con el artículo 5, inciso 2, apartado b, de la LPDP, al decir este que no se requiere cuando "se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal", como, por ejemplo, los exigidos por el artículo 305 CCyC. Para mayor abundamiento, en general, los datos personales recabados son de fuentes de acceso público o se limitan a nombre y apellido, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio, supuestos expresamente eximidos del consentimiento para su tratamiento en los apartados a y c del inciso 2 del artículo 5 LPDP.

La armonía de las normas de ejercicio de la función notarial con la LPDP es lo que ha creado la conciencia en el notariado de su no aplicación a su actividad, por la simple razón de que, desde antes de la vigencia de la ley, ya cumplía con lo que ella posteriormente ha regulado, en especial en la dimensión papel. El advenimiento de la cultura digital incide en la actividad notarial al expandirse las esferas íntimas y privadas a un ámbito potencialmente de mayor publicidad en el mundo virtual, pero esto no modifica las conclusiones previas.

2.2. Principio de calidad del dato: realidad tangible y certeza de su representación

Los datos personales deben ser obtenidos por medios lícitos y reunir los requisitos de calidad determinados por su certeza y finalidad de almacenamiento y uso (art. 4 LPDP). El dato será cierto cuando sea exacto o congruente con la realidad que representa; en el caso de los datos digitalizados, con la realidad tangible o analógica.

En ciertos actos que determinan su eficacia jurídica según la relación de los datos que lo integran, esa exactitud no puede ser librada al mero interés de los propios interesados en el negocio, fundado en el principio de derecho de determinar incompatibilidades a fin de evitar el abuso o aprovechamiento de la posición en el acto; por ejemplo, la prohibición del beneficiario de un testamento de ser testigo del mismo; del juez, de celebrar contratos sobre los bienes en litigio que debe resolver; de los notarios, sus parientes hasta el cuarto grado de consanguinidad o segundo de afinidad, de autorizar actos notariales en que estén comprometidos sus intereses. Las incompatibilidades en derecho tienden también a garantizar la calidad del datos, y, si bien en la mayoría de los casos basta con su almacenamiento, conservación, tratamiento o cesión sin restricción según el interés personal de los sujetos que desarrollan estas actividades, en los más importantes se exige la intervención de un tercero imparcial, a quien el Estado le ha conferido la competencia pública de hacerlo por la trascendencia frente a terceros.

Esto fue notorio en el inconveniente presentado en la pretendida registración de boletos inmobiliarios instrumentados en documentos electrónicos o digitalizados, a los que se quiso dar publicidad con el solo control de certeza de uno de los interesados, que

aplicaba su firma digital –hoy derogado en la Provincia de Buenos Aires[10]–. Ello era altamente disvalioso, por el riesgo de falta de certeza o exactitud, entre otros elementos, de los datos personales, el conferir los especiales efectos frente a terceros del artículo 1170 CCyC sin cumplir con la certificación de firma por notario o autoridad competente (art. 3 Ley 17801), lo que permite el ejercicio de un mínimo control de legalidad de los aspectos subjetivos del acto, certeza y valoración que le confieren carácter de auténtico al dato personal cierto registrable. El registro de la propiedad debe recibir datos ciertos para incluirlos en su base, formada por los asientos que reflejen la realidad extrarregistral, y para ello se debe propender a la debida calidad de los datos fundantes de dichos asientos, entre otros medios, por el control de legalidad de los datos personales, contando con finalidad y certeza garantizadas por un funcionario público imparcial. Si se va a afectar el derecho de propiedad de dos personas, al menos sus datos personales e identidades deben tener calidad suficiente y adecuada al destino del negocio jurídico documentado.[11]

La calidad del dato estará determinada no solo por su certeza sino también por el destino o finalidad para el que es recogido o almacenado. Todo dato cierto se obtiene con un fin lícito; de lo contrario, debe permanecer en la esfera íntima de la persona, en respeto de su autonomía informativa, que afecta derechos personalísimos como la imagen, la voz, el honor, la intimidad o la identidad. Su alteración o cambio pueden afectar la dignidad, que se construye en base a estos derechos, entre otros. El artículo 4 LPDP es claro al enunciar que el dato debe ser "adecuado, pertinente y no excesivo en relación al ámbito y finalidad para los que se hubieren obtenido" (inc. 1), con la consecuente prohibición de utilizarlo para "finalidades distintas o incompatibles con aquellas que motivaron su obtención" (inc. 3); y también es claro al enunciar la obligación de su destrucción "cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados" (inc. 7).

Va de suyo que los datos personales conservados por los notarios en sus actuaciones notariales tienen un destino o finalidad en principio perpetua. Esta no cesa en virtud del paso del tiempo, por lo cual el titular no puede pedir su supresión por extinción de la finalidad del acto, ya que justamente el ordenamiento jurídico ha instituido la función notarial con la intención, entre otras, de preservar, guardar o conservar, indefinidamente o por largo tiempo, ciertos actos o hechos jurídicos que así lo ameritan. El Estado requiere la formalidad de ciertos actos para asegurar su eficacia en el transcurso del tiempo, por lo que no pueden caducar sino que, por el contrario, deben sostenerse por más de una generación. Lo que los documentos notariales digitales hacen en la era digital es brindar certeza al contenido del acto, que se prioriza en situaciones o

10. La Disposición técnico registral 6/2019 del Registro de la Propiedad, que implementó el "Registro Especial de Boletos de Compraventa de Unidades Futuras", fue derogada por la Disposición técnico registral 4/2020.

11. Similar recorrido han tenido las normas administrativas de la constitución de sociedades por acciones en la Inspección General de Justicia de la Capital Federal, la que, a través de la Resolución general 17/2020, derogó el art. 2 de la Resolución general 8/2017, que admitía la toma de razón de la constitución de este tipo societario en soporte electrónico, con la firma electrónica de los socios, bastando que solo uno aplicara al final su firma digital, e impuso el plazo de noventa días para su subsanación mediante la presentación de su ratificación en instrumento privado con las firmas de sus otorgantes certificadas por escribano público, funcionario bancario autorizado, funcionario Judicial autorizado o funcionario de la Inspección General de Justicia autorizado, quienes deberán digitalizar el instrumento y firmarlo digitalmente (por remisión al art. 7 inc. 2 del anexo de la Resolución general 6/2017). E impuso la no inscripción de otros actos si no se cumple previa o simultáneamente con esta subsanación.

relaciones jurídicas que requieren una representación documental por largos períodos de tiempo, como la vivienda familiar, el estatuto patrimonial del matrimonio, la programación sucesoria, entre otros, mientras que en muchos de los actos propios de la cultura digital es el principio de caducidad el que se impone.

La calidad del dato personal impone un concepto dinámico que asegura y protege el derecho de acceso de su titular a las bases de datos en que aquel se registre o almacene, lo que se garantiza en las leyes de organización del notariado a través del derecho del otorgante a que le sea exhibido el documento notarial y a obtener copias y, en su caso, testimonios del mismo. También se le asegura y confiere acción para su rectificación cuando ha variado el contenido representado o han mutado las circunstancias que modifican su sentido o la finalidad de su recolección, como reconoce el propio artículo 26 inciso 4 LPDP al limitar a las prestadoras de servicios de información crediticia los informes de datos personales solo a los significativos para evaluar la solvencia económico-financiera de los últimos cinco años (reducibles a dos años cuando el deudor cancele o de otro modo extinga la obligación).

En el ámbito de nuestra profesión, no aparecen muchos casos que obliguen a la rectificación de datos personales en los actos notariales, donde se busca la estratificación de ellos en un momento determinado: la fecha del acto. Se está ante datos históricos, que no dan lugar al derecho a su rectificación, salvo error o falta de certeza, como quien dijo ser de estado civil soltero cuando era casado y lo acredita con la respectiva partida de matrimonio. Las rectificaciones de datos personales en lo notarial no se limitan al interés del titular del dato, sino que su corrección y requisitos se deben armonizar con los derechos de terceros. La rectificación del estado civil del adquirente de un inmueble que dijo ser casado y luego dice ser soltero importa que su declaración jurada creó la apariencia de ganancialidad del bien registrable con su consecuente responsabilidad y destino en caso de indivisión postcomunitaria, que amerita la mayor prevención y requisitos que llevan a la acreditación judicial de tales extremos, y no basta que el notario rectifique el dato personal oportunamente almacenado.

El carácter histórico de la guarda documental notarial determina la prohibición de supresión material mediante borrado, tapadura u ocultamiento de cualquier modo; debe existir constancia documental de tal supresión, de relevancia jurídica, como cuando se exige la constancia de puño y letra del notario respecto de lo testado previo a la firma de la escritura, o la rectificación de datos por error u otra causa, por una nueva escritura pública, para insertar anotación al margen de la aclaración o rectificación, o excepcionalmente la nota marginal que dé cuenta de la rectificación por constatación directa del notario de otros documentos públicos. En cualquier caso, no se puede ocultar lo modificado por ninguna causa. Incluso respecto del cambio de género por reconocimiento de la identidad sexual autopercibida, una vez cumplido el trámite de la Ley 26743 de Identidad de Género en el registro civil, del que resulta una nueva partida de nacimiento que no da cuenta del género anterior, con la manda de reserva íntima y no divulgación del género previo en ningún ámbito y su registro bajo absoluta reserva, no se puede tapar, borrar o modificar sin dejar rastro del antecedente, sino que se requiere la confección de una escritura rectificatoria, otorgada por el titular del dato, con la sola restricción de que no se podrá explicitar la causa de cambio de

género ni conservar agregada al protocolo la documentación que dé cuenta de esta opción legal.

El documento notarial captura la situación o relación jurídica en un tiempo determinado, con la información relativa a la persona en ese momento. Por eso, es siempre un archivo histórico que el orden jurídico pretende preservar. Ese es uno de los fundamentos de la guarda notarial, de aquellos que trascienden el presente y requieren de su certero recuerdo en el futuro.

2.3. Datos sensibles: actas de constatación de contenido de chats, WhatsApp, e-mail, correspondencia epistolar

La protección de los datos sensibles en general y derechos del paciente en especial se relaciona con el artículo 318 CCyC, que establece que los datos o información confidencial destinada a la prueba contenida "no puede ser utilizada sin el consentimiento del remitente", lo cual también puede extenderse a datos de terceros allí mencionados. El propio artículo aclara que se refiere a la correspondencia, cualquiera sea el medio y soporte en que se realice, sea en papel o electrónica, por correo postal, entrega en mano, chat, mensajería, e-mail, entre otros. Recepta el principio de equivalencia del documento en soporte papel y electrónico de los artículos 286 y 288 CCyC y 3 y 6 de la Ley 25506, correspondiendo su aplicación a todo soporte, con la particularidad en el electrónico de que, una vez digitalizado, puede almacenarse, transferirse o cederse a una base de datos digital, sin haberse utilizado alguna técnica de disociación con el titular del dato que produzca su "anonimación" (art. 28 LPDP).

El artículo 318 CCyC se refiere a un criterio de confidencialidad propio de la dimensión papel y su limitación a la facilidad de transmisión, circulación, almacenamiento y tratamiento de los datos (información) contenidos, ateniéndose fundamentalmente al derecho a la intimidad, imagen o voz, que afectan la esfera íntima que hace a la dignidad humana y su honor. La cultura digital cambia la concepción de este presupuesto. En los medios digitales, la información o datos se almacenan (graban), tratan y transfieren con gran facilidad y mediante todos los medios audiovisuales de captación y reproducción inmediata, con fenómenos como la viralización, de todo tipo de mensajes electrónicos, digitalizados y/o encriptados. Esta flexibilidad de la realidad virtual hace que ya no se afecte solo la intimidad sino también la libertad para decidir si lo documentado debe o no ser divulgado por estos medios privados –como son las redes sociales– y el potencial efecto discriminatorio para con los titulares de tales datos. En definitiva, entra en consideración de la actuación de quien interviene el debido respeto de la autonomía informativa.

Más allá del consentimiento informado para el almacenamiento o provisión de datos sensibles según el artículo 6 LPDP, ello se circunscribe solo a las bases de datos, que tienen el deber de confidencialidad respecto de los datos objeto de tratamiento (art. 10). Por tal motivo, su solo almacenamiento en ellas no importa en principio la violación del deber de confidencialidad de esta ley si el dato es procesado respetando los fines de su recolección. Esta normativa no se aplica al protocolo notarial, por no ser una base de datos en los términos de esta ley.

La cuestión se relaciona con el principio de calidad del dato personal y, en consecuencia, sensible, como su especie, en cuanto debe ser adecuado, pertinente y no excesivo, acorde al ámbito y a la finalidad para la que se hubiere obtenido. Es justamente la finalidad del acta notarial la que hace que la protección de los datos personales y sensibles, en cuanto a su confidencialidad, esté resguardada, en principio, en la actividad notarial por la limitación de la exhibición y el destino para el que se recolectan los datos (mostrarlos al juez en el marco del proceso judicial, máxime si es de familia, con su general reserva procesal). En este caso se podrá labrar el acta en tanto en cuanto: a) no viole el deber de confidencialidad, b) sea adecuada según el fin requerido. En definitiva, son las mismas prevenciones que se cumplen en la confidencialidad de todo el contenido del documento objeto de la constatación.

2.3.1. Datos sensibles y la Ley de Derechos del Paciente. Incidencia en la acreditación del discernimiento de la persona

Al entrar en vigencia el CCyC, en el año 2015, se generó en ese primer momento debate acerca de si para realizar el juicio de discernimiento se debía exigir la partida de nacimiento del compareciente como único medio de acreditación –en atención a que el artículo 39 CCyC exige la registración de la sentencia de incapacidad o capacidad restringida al margen de la misma y a que el artículo 44 CCyC establece que son nulos los actos celebrados por esta persona después de la inscripción precedentemente impuesta– o si se podía acreditar por otros medios con independencia de esta registración, de hecho de imposible cumplimiento. La solución al debate fue que la misma no es operativa, por imposibilidades jurídicas y de hecho, concluyéndose que no es un elemento documental a solicitar para este juicio.

Como ya hemos sostenido, cuando el resultado de un juicio se refiere a conductas humanas, no basta el exclusivo tratamiento de datos personales que definan su perfil, sino que se debe priorizar la apreciación del ojo humano (art. 20 LPDP), que en ese caso puede apreciar el discernimiento para el acto, como ocurre en los intervalos lúcidos en el testamento, que permite evitar la injusta rigidez de resultado algorítmico que lleven a la inequitativa solución de privar a la persona de sus derechos. Entre los argumentos desarrollados en ese momento, se señaló con acierto que no solo se está ante datos personales de identidad, sino que también se afectan datos sensibles, es decir, su subespecie, en la que la enfermedad puede constituir un supuesto de discriminación, lesionando la expresa finalidad de la norma del artículo 43 de la Constitución Nacional. En este sentido, la Ley 26529 de Derechos del Paciente, en su artículo 2, incisos c y d, dice:

> c) *Intimidad*. Toda actividad médico-asistencial tendiente a obtener, clasificar, utilizar, administrar, custodiar y transmitir información y documentación clínica del paciente debe observar el estricto respeto por la dignidad humana y la autonomía de la voluntad, así como el debido resguardo de la intimidad del mismo y la confidencialidad de sus datos sensibles, sin perjuicio de las previsiones contenidas en la Ley Nº 25326; d) *Confidencialidad*. El paciente tiene derecho a que toda persona que participe en la elaboración o manipulación de la documentación clínica, o bien tenga acceso al contenido de la misma, guarde la debida

> reserva, salvo expresa disposición en contrario emanada de autoridad judicial competente o autorización del propio paciente.

Y su artículo 4 limita toda información a terceros a menos que se tenga autorización del paciente, o en caso de incapacidad o capacidad restringida, de su representante.

La Ley 26529 recepta las norma de los tratados de derechos humanos, reconociendo que se está ante datos sensibles, respecto de los cuales el artículo 7 LPDP establece que ninguna persona puede ser obligada a proporcionarlos, y su inciso 3 claramente impone que, pese a que puedan ser tratados excepcionalmente en interés general, "queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revelen datos sensibles"; mientras que los registros civiles establecen que sus asientos son por transcripción del título recibido, es decir, de la sentencia, con lo cual se hace pública la enfermedad, que constituye un dato sensible, afectando las normas precitadas.

Peyrano sostiene al respecto:

> La anotación marginal de las sentencias que declaren la incapacidad o restrinjan la capacidad de ejercicio, exigida por el art. 39 del CCCN, se contrapone con las disposiciones de la Convención sobre Derechos de las Personas con Discapacidad y previsiones de las leyes 25326, 26529 y 26657, resultando además inconstitucional. Es incompatible con esas normativas que puedan ser dadas a conocer –mediante la registración en archivos de acceso público de esas sentencias– las informaciones que constituyen el fundamento a las restricciones a la capacidad de ejercicio impuestas. La norma además cumple un objetivo de alcances limitados y consagra una instrumentación anacrónica. Se impone una revisión legislativa y prescindirse entre tanto de su aplicación.[12]

La armonización de las Leyes 26529 (Derechos del Paciente) y 25326 (Habeas Data), el artículo 43 de la Constitución Nacional y la Convención sobre los Derechos de las Personas con Discapacidad con los artículos 39 y 44 CCyC es uno de los argumentos que inciden en la justificación del modo en que se llega al juicio de discernimiento en el ejercicio de la función notarial.

2.4. Transferencia y cesión de datos personales: almacenamientos en servicios *cloud computing*

La transferencia o cesión de datos personales solo es admisible de conformidad con la finalidad con que han sido recolectados, en todos los casos, y con el debido consentimiento informado de su titular en los supuestos requeridos por la LPDP. El usuario o administrador de una base de datos nunca podrá afectar la calidad del dato, en particular en cuanto a no violentar la finalidad –legal o convencional– de su recolección (de modo análogo, cuando el notario envía al registro de la propiedad inmueble datos

12. Peyrano, Guillermo F., "Inscripción de las sentencias que declaran la incapacidad de ejercicio o que restringen dicha capacidad. Un recaudo anacrónico y violatorio de derechos constitucionalmente amparados" [online], [s.e.], 2015 [ponencia presentada en las XXV Jornadas Nacionales de Derecho Civil {Bahía Blanca, octubre 2015}], p. 1; en https://jndcbahiablanca2015.com/wp-content/uploads/2015/09/Peyrano_INSCRIPCI%C3%93N.pdf; última consulta: 31/7/2020.

del titular del derecho real para su toma de razón, lo hace conforme a esa finalidad). La transmisión del dato personal también podrá ser hecha en ciertos casos como anonimanizado o disociado de su titular, como en el caso de los datos sensibles. En estos casos, la transferencia del dato es para permitir la prestación de un servicio por parte del receptor, el cual no podría prestar si no es con dicha transferencia, y la misma tiene por fin la mejor satisfacción e interés del titular del dato. En cambio, en otros casos, la cesión del dato se hace en interés del cedente y no puede vulnerar la finalidad de la recolección, debiendo asegurar los derechos del titular del dato y contar con el consentimiento de este.

En este trabajo nos valdremos de la distinción de la terminología de "transferencia" para los primeros casos y de "cesión" para los segundos. Seguimos así la postura de González Allonca y Ruiz Martínez cuando dicen:

> Habrá cesión cuando los datos se transfieran a un tercero para que disponga de ellos a su arbitrio […] Por su parte, la prestación de servicios se refiere al caso en el cual el titular de un banco de datos transfiere toda o parte de la información en su poder a un tercero, para que le preste un servicio de tratamiento determinado contractualmente, conforme a una finalidad específica e instrucciones del responsable, con las medidas de seguridad y confidencialidad requeridas por ley y sin poder ceder los datos a terceros ni aun para su conservación, debiendo destruir o reintegrar la información una vez finalizado el contrato.[13]

El notario **transferirá** datos en la medida en que lo haga para cumplir con la finalidad de su recolección, cuando el destinatario preste un servicio con su tratamiento impuesto por la ley o que surja de la convención o de su finalidad, entendida en el doble sentido de la causa fin como dentro del elemento categórico del contrato o los motivos subjetivos que las partes tuvieron en común al contratar (notario-requirente). En tales casos, no se requiere consentimiento alguno del titular para su transferencia.

También podrá el notario **ceder** los datos, para tener una prestación de un servidor informático que permita asegurar la finalidad tenida en cuenta, haciendo más eficiente su almacenamiento o tratamiento, recurriendo a la contratación de la prestación de un servicio denominado *cloud computing* para la guarda de documentación digitalizada relativa al acto notarial, certificados o informes registrales o administrativos digitales, respuesta de consultas a registros o bases de datos públicas o privadas, entre otras, en vez de conservarlas en sus dispositivos locales, para evitar pérdidas, hackeos, respaldos por desperfectos de *software* o virus, mejor tratamiento de los datos o de la capacidad de almacenamiento.

El servicio de *cloud computing* es un modelo que permite acceder a requerimiento por demanda a un conjunto compartido de recursos computacionales configurables, como ser almacenamiento, aplicaciones, servicios, etc., que se usan solo cuando se los necesita, en forma ágil y rápida, y que son provistos y liberados con un esfuerzo mínimo de administración o interacción con el proveedor de estos servicios. Importa una

13. González Allonca, Juan C. y Ruiz Martínez, Esteban, "*Cloud computing*: la regulación de la transferencia internacional de datos personales y la prestación de servicios por parte de terceros" [online], en AA.VV., *Dossier: habeas data. Selección de jurisprudencia y doctrina*, Buenos Aires, Sistema Argentino de Información Jurídica - Ministerio de Justicia y Derechos Humanos, 2020, p. 178; en http://www.saij.gob.ar/docs-f/dossier-f/habeas_data.pdf; última consulta: 31/7/2020. (El artículo citado fue originalmente publicado en www.saij.gob.ar, el 1/10/2015).

economía de licencias, espacio y *hardware* propia del concepto de economía compartida o colaborativa, donde la infraestructura ya no es local sino en otro sitio (*cloud* o nube), administrado por el prestador del servicio pero con la exclusividad en su uso. Podemos apreciar las siguientes categorías de *cloud computing*:

a) ***Infrastructure as a Service (IaaS)***: El proveedor del servicio da al usuario una infraestructura de recursos IT, como procesamiento, energía, almacenamiento, redes y otros recursos básicos, para que el consumidor pueda implementar y ejecutar cualquier tipo de aplicación. El usuario tiene control sobre los sistemas operativos, almacenamiento, aplicaciones desplegadas; accede a ellos según su necesidad y de modo automatizado. En este esquema, la transferencia de datos sigue bajo el control del usuario y no se crea necesariamente una base de datos por el servidor, por lo cual, cumplidas estas condiciones establecidas en los términos de uso, no hay en principio lesión a la finalidad de la recolección del dato si el prestador no tiene acceso al tratamiento de los datos personales de las operaciones del usuario.

b) ***Platform as a Service (PaaS)***: El prestador del servicio permite que el usuario despliegue lo necesario para la construcción y puesta en marcha de aplicaciones y servicios web accesibles en internet. No controla la capa de infraestructura de la nube, pero gestiona las aplicaciones allí alojadas junto con la posibilidad de controlar su entorno y configuración. En principio, no garantiza la seguridad del dato; para su uso, será necesario el consentimiento del titular del dato que recolectó el usuario de servicio *cloud computing*.

c) ***Software as a Service (SaaS)***: El proveedor presta un servicio de *software* por el que el usuario puede utilizar las aplicaciones del prestador que se ejecutan en una infraestructura de nube, a las que puede accederse desde distintos dispositivos e interfaces del cliente. El notario que lo contrate no gestiona ni controla la infraestructura de nube subyacente, que incluye la red y servidores, ni tampoco sistemas operativos, o de almacenamiento, sin perjuicio de que pueda tener prevista la configuración o personalización de su uso exclusivo. En principio, se deberá tener el consentimiento informado del titular de los datos personales en estos servicios.

La utilización de servicios *clouding* para el almacenamiento de datos personales recolectados por el notario en su actuación, en tanto sean con la finalidad de su almacenamiento solo para conservación, no violenta la finalidad de recolección del dato, y el notario debe mantener el control de su uso e imposibilidad de cesión por el prestador del servicio en los términos y condiciones de contratación. En estos casos, no se requerirá consentimiento del titular del dato personal, que es típico del primer servicio *clouding*, IaaS. En los restantes servicios de *cloud computing*, en principio, sí lo deberá obtener, salvo que de los términos y condiciones de uso contratados surja su control de tales datos y la prohibición del servidor de ceder los mismos o tratarlos con intereses diversos a su mera conservación.

Las bases de datos de estos servidores usualmente no están en el país, y ni siquiera en países que nuestra legislación reconoce como seguros para el tratamiento de los datos

personales. El artículo 11 LPDP exige el consentimiento para su cesión y el artículo 12 lo prohíbe a bases de datos en el extranjero (con las excepciones que detalla), lo que se debe considerar al momento de evaluar la previsión contractual de exigir el consentimiento del requirente, a la vez, titular de esos datos personales.

3. Conclusión

Las finalidades de la Ley de Protección de Datos Personales, digitalizados o no, guardan relación con los deberes de la función notarial en sus leyes de organización local. Por tal motivo, en el actual estado de nuestra legislación, no son requeridas prevenciones especiales o consentimiento de los titulares sobre el uso, tratamiento y transferencia de los datos personales o sensibles insertos en documentos notariales por su autor en el marco de sus obligaciones legales y la finalidad de su función.

El mismo principio debe concluirse en cuanto a la contratación de servicios de almacenamiento o guarda de respaldos documentales en servidores *clouding*, en la medida en que la transferencia se limite a este destino, el notario mantenga su control y esté limitada la facultad de tratamiento o cesión a terceros por el servidor de servicio.

4. Bibliografía

González Allonca, Juan C. y Ruiz Martínez, Esteban, "*Cloud computing*: la regulación de la transferencia internacional de datos personales y la prestación de servicios por parte de terceros" [online], en AA.VV., *Dossier: habeas data. Selección de jurisprudencia y doctrina*, Buenos Aires, Sistema Argentino de Información Jurídica - Ministerio de Justicia y Derechos Humanos, 2020; en http://www.saij.gob.ar/docs-f/dossier-f/habeas_data.pdf; última consulta: 31/7/2020.

Masciotra, Mario, "Protección de datos personales y su integración en el marco de los derechos humanos" [online], en AA.VV., *Dossier: habeas data. Selección de jurisprudencia y doctrina*, Buenos Aires, Sistema Argentino de Información Jurídica - Ministerio de Justicia y Derechos Humanos, 2020; en http://www.saij.gob.ar/docs-f/dossier-f/habeas_data.pdf; última consulta: 31/7/2020.

Molina Quiroga, Eduardo, "Protección de datos personales como derecho autónomo. Principios rectores. Informes de solvencia crediticia. Uso arbitrario. Daño moral y material" [online], en AA.VV., *Dossier: habeas data. Selección de jurisprudencia y doctrina*, Buenos Aires, Sistema Argentino de Información Jurídica - Ministerio de Justicia y Derechos Humanos, 2020; en http://www.saij.gob.ar/docs-f/dossier-f/habeas_data.pdf; última consulta: 31/7/2020.

Peyrano, Guillermo F., "Datos sensibles: perfiles y regulaciones. El impacto del desarrollo tecnológico" [online], en AA.VV., *Dossier: habeas data. Selección de jurisprudencia y doctrina*, Buenos Aires, Sistema Argentino de Información Jurídica - Ministerio de Justicia y Derechos Humanos, 2020; en http://www.saij.gob.ar/docs-f/dossier-f/habeas_data.pdf; última consulta: 31/7/2020.

— "Inscripción de las sentencias que declaran la incapacidad de ejercicio o que restringen dicha capacidad. Un recaudo anacrónico y violatorio de derechos constitucionalmente amparados" [online], [s.e.], 2015 [ponencia presentada en las XXV Jornadas Nacionales de Derecho Civil {Bahía Blanca, octubre 2015}]; en https://jndcbahiablanca2015.com/wp-content/uploads/2015/09/Peyrano_INSCRIPCI%C3%93N.pdf; última consulta: 31/7/2020.

Jurisprudencia citada:

CS de los Estados Unidos de Norteamérica, 18/12/1944, "Kaorematsu v. United States".

CSJN, 6/3/2001, "Lascano Quintana, Guillermo Víctor c/ Veraz SA s/ habeas data" L.215.XXXV (*Fallos*, 324:567); en AA.VV., *Dossier: habeas data. Selección de jurisprudencia y doctrina*, Buenos Aires, Sistema

Argentino de Información Jurídica - Ministerio de Justicia y Derechos Humanos, 2020; en http://www.saij.gob.ar/docs-f/dossier-f/habeas_data.pdf; última consulta: 31/7/2020.

CSJN, 8/11/2011, "Catania, Américo Marcial c/ BCRA-(base de datos) y otro s/ habeas data" C.1380.XLII (*Fallos*, 334:1276); en AA.VV., *Dossier: habeas data. Selección de jurisprudencia y doctrina*, Buenos Aires, Sistema Argentino de Información Jurídica - Ministerio de Justicia y Derechos Humanos, 2020; en http://www.saij.gob.ar/docs-f/dossier-f/habeas_data.pdf; última consulta: 31/7/2020.

CSJN, 8/11/2011, "Napoli, Carlos Alberto c/ Citibank N.A. y otro s/ habeas data" N.112.XLII (*Fallos*, 334:1327); en AA.VV., *Dossier: habeas data. Selección de jurisprudencia y doctrina*, Buenos Aires, Sistema Argentino de Información Jurídica - Ministerio de Justicia y Derechos Humanos, 2020; en http://www.saij.gob.ar/docs-f/dossier-f/habeas_data.pdf; última consulta: 31/7/2020.

Normativa citada:

Código Civil y Comercial
Constitución Nacional
Convención sobre los Derechos de las Personas con Discapacidad (Nueva York, 2006)
Decreto 3887/1998 de la Provincia de Buenos Aires
Decreto nacional 1558/2001
Decreto-ley 9020/1978 de la Provincia de Buenos Aires
Disposición técnico registral 4/2020 del Registro de la Propiedad de la Provincia de Buenos Aires
Disposición técnico registral 6/2019 del Registro de la Propiedad de la Provincia de Buenos Aires
Ley 404 de la Ciudad Autónoma de Buenos Aires
Ley nacional 17801
Ley nacional 25326
Ley nacional 25509
Ley nacional 26413
Ley nacional 26529
Ley nacional 26743
Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018
Resolución general 17/2020 de la Inspección General de Justicia
Resolución general 6/2017 de la Inspección General de Justicia
Resolución general 8/2017 de la Inspección General de Justicia