

myf

132



Hábeas Data en la Provincia de Santa Fe: una deuda pendiente

Paula Pla Sasmut

Abogada (UNR). Diplomada en Derecho Constitucional (UCA). Especialista en Derecho de Daños (UCA). Especialista en magistratura (UNR).

“Por lo general, la gente teme el cambio porque teme lo desconocido. Pero la única y mayor constante de la historia es que todo cambia”.

- Yuval Noah Harari

Introducción

Vivimos en una época caracterizada por la digitalización masiva y el acceso constante a la información. Desde nuestras actividades en línea hasta los registros en instituciones públicas y privadas, nuestros datos personales son recopilados, almacenados y procesados a una escala sin precedentes. Este contexto plantea nuevos desafíos para el derecho, especialmente en lo que respecta a la protección de la intimidad y el control que las personas tienen sobre su propia información.

La protección de datos perso-

nales se ha convertido en un derecho fundamental en las democracias modernas que priorizan la privacidad y intereses individuales de sus ciudadanos y la discusión se ha instalado y mantenido en la agenda tanto a nivel nacional como internacional.

En Argentina, la Constitución Nacional, a través de su artículo 43, contempla la garantía del hábeas data, la que junto con la Ley Nacional N° 25.326 constituyen el marco normativo de regulación de la protección de datos personales, estableciendo los principios y procedimientos para asegurar el adecuado tratamiento de la información.

No obstante el marco legal imperante a nivel nacional, la provincia de Santa Fe no cuenta en la actualidad con una normativa específica que regule la protección de datos personales en su jurisdicción, con lo cual, la falta de desarrollo específico a nivel provincial subraya

la necesidad de una adecuación normativa que contemple las particularidades y demandas locales. Esta carencia es particularmente relevante considerando el desarrollo institucional de la provincia, que históricamente ha liderado iniciativas en diversas áreas del derecho, pero que en este caso presenta un vacío notable.

En un mundo donde la información fluye con rapidez y donde los riesgos de vulneración a la privacidad son cada vez mayores, la falta de una ley provincial específica constituye una deuda pendiente y una necesidad para garantizar un marco adecuado de derechos en Santa Fe. En este contexto, el presente artículo explora la importancia de contar con una legislación provincial sobre protección de datos personales y hábeas data.

Importancia de la regulación

El tráfico de información en la

red, el avance de las nuevas tecnologías y la velocidad con la que avanza la ciencia en general requiere mecanismos de protección jurídica para los derechos individuales.

En la actualidad descargamos en nuestros dispositivos móviles miles de aplicaciones, aceptamos términos y condiciones que rara vez hemos leído y compartimos gran parte de nuestra vida privada en redes sociales. Expresamos lo que sentimos y pensamos, bajo la idea de que las experiencias carecen de valor si no las compartimos con nuestros “seguidores”.

Sin embargo, cada acto que realizamos en la red es monitoreado por algoritmos que nos observan constantemente y que recopilan todo lo que hacemos, decimos e incluso pensamos. Todo ello nos lleva a perder nuestra privacidad, individualidad y autonomía; surgiendo distintas preguntas: ¿dónde se almacenan

todos esos datos? ¿Quiénes tienen acceso a ellos?

El filósofo e historiador Yuval Noah Harari¹ señala que la “religión de los datos” sostiene que todas nuestras palabras y acciones forman parte del gran flujo de información y que los algoritmos están siempre observándonos y prestando atención a todo lo que hacemos y sentimos. Para los verdaderos creyentes, estar desconectado de este flujo de datos implica arriesgarse a perder el sentido mismo de la vida. Harari se pregunta: “¿Qué sentido tiene hacer o experimentar algo si nadie lo sabe y si no contribuyo al intercambio global de información?”.

El autor continúa reflexionando sobre cómo el auge de internet ofrece una muestra de lo que está por venir. El ciberespacio es hoy crucial en nuestra vida cotidiana, economía y seguridad. Sin embargo, la selección crítica

de diseños alternativos para la web no se llevó a cabo mediante un proceso político democrático, a pesar de que involucraba cuestiones políticas tradicionales como soberanía, fronteras, privacidad y seguridad. ¿Alguna vez votó el lector sobre la configuración del ciberespacio? Decisiones tomadas por diseñadores de sitios web, alejados del escrutinio público, han dado forma a una internet que hoy es una zona libre y sin ley, que erosiona la soberanía estatal, ignora las fronteras, anula la privacidad y plantea un formidable riesgo global para la seguridad.

Sin duda, las herramientas digitales han incrementado la capacidad de empresas y gobiernos para desarrollar actividades de vigilancia, persuasión e interceptación, generando riesgos que pueden comprometer la privacidad. Esto resalta la necesidad innegable de brindar protección jurídica a la intimidad.

Los constantes desafíos informáticos requieren abordar el concepto de intimidad en un sentido dinámico, brindándole mayor protagonismo al sujeto interesado a los fines de que pueda ejercer un control adecuado de sus datos personales.

En el ámbito constitucional, es posible distinguir una cuestión “de fondo” vinculada a la protección de los datos personales, que da lugar a un nuevo concepto derivado de la intimidad conocido como “derecho fundamental a la autodeterminación informativa”². Este derecho puede considerarse el pilar de la protección de los datos personales y se presenta como un derecho autónomo con una doble faceta.

Por un lado, tiene una dimensión sustancial, ya que se configura como un derecho independiente. Por otro lado, posee una dimensión instrumental, actuando como un mecanis-

mo para salvaguardar otros derechos, como la intimidad, el honor y la dignidad. Su objetivo es proteger la información personal, tanto íntima como no íntima, frente a un uso inadecuado o descontrolado.

Asimismo, existe una garantía constitucional destinada a tutelar estos derechos de fondo. En este sentido, si admitimos que el derecho a la autodeterminación informativa otorga al individuo la facultad de conocer quiénes serán destinatarios de su información y qué uso le darán, se le debe permitir controlar la calidad de esos datos mediante los derechos de acceso, supresión, confidencialidad, rectificación y cancelación. Estas acciones se encuentran dentro del ámbito del hábeas data, en el cual, en rigor, siempre será posterior a la fase de acceso a la información.

Sagües³ señala que el origen del hábeas data responde al desarrollo del llamado “poder

informático” y que el actual derecho constitucional pretende dar una respuesta transaccional a los derechos constitucionales de “registrantes” y “registrados” en los bancos de datos. Este enfoque aborda tanto ‘cuestiones de fondo’ -los derechos de cada uno de aquéllos- y ‘de forma’ -el tipo de procedimiento de tales derechos-.

Aunque nos enfrentamos a una realidad dinámica y en constante evolución, donde “la tortuga gubernamental no puede seguir el ritmo de la liebre tecnológica⁴” debido a la abrumadora cantidad de datos, es esencial que el legislador encuentre remedios jurídicos adecuados en tiempo oportuno.

Finalidad del hábeas data

El derecho a la intimidad ha sido definido como la facultad que tiene cada persona

de disponer de una esfera de privacidad que no puede ser invadido por terceros mediante intromisiones. Si bien la privacidad cuenta con protección constitucional -Art. 19 CN⁵- , la pérdida de la intimidad es lo que conduce a la necesidad de contar con garantías adecuadas que resguarden a los individuos frente a la difusión de determinada información.

Afirma Marcela Basterra que “la protección de la información personal es la respuesta del derecho a las nuevas tecnologías, permitiendo transporlar la garantía del habeas corpus al habeas data: del tengo mi cuerpo al tengo mis datos, para controlarlos y determinarlos⁶”.

Así es que, el habeas data es un proceso constitucional que tiene por objeto “proteger determinados derechos constitucionales ante los excesos del poder informático” , operando como una

garantía cuya finalidad no es otra más que proteger a los individuos frente a la información en archivos, registros o bancos de datos, siempre que la misma refiera a determinados aspectos de su personalidad que se encuentren vinculados con su intimidad.

Lo que se procura tutelar es la intimidad y la autodeterminación informativa, es decir, la facultad de decidir y controlar a quién y cómo cedo mis datos. Lo que caracteriza al dato personal es precisamente la posibilidad de identificar con alguna precisión a la persona a la que esa información pertenece. En general se trata de información relativa a su actividad laboral, salud, afiliación política, información crediticia o financiera, datos biométricos, religión, en fin, un variopinto universo de datos.

Si bien hay datos que por sí mismos resultan inocuos o irrelevantes, si se los interrelaciona con otros, nos permiten ob-

tener un perfil de esa persona.

Esto es lo que autores como Bazán denominan “teoría del mosaico”, es decir, reconocer que existen datos -a priori irrelevantes- pero que, ligados con otros, pueden desnudar absolutamente la personalidad de un individuo: “al igual que ocurre con las pequeñas piedras que forman los mosaicos, que en sí no dicen nada, pero que unidas pueden formar conjuntos plenos de significado⁸”.

Esta información es la que posibilita la protección, ya que a través de esos datos se puede llegar a establecer conductas y prácticas que pueden trascender la esfera de su intimidad.

La garantía tutelada tiene dos finalidades, por un lado, tomar conocimiento de los datos a ella referidos y de su finalidad y, por otro, ejercer los derechos de supresión, rectificación, confidenciali-

dad o actualización de los datos, en caso de que su titular advierta que los mismos son inexactos o discriminatorios.

No resulta necesario que el dato lesione algún derecho, basta con que sea un dato falso o sensible para que pueda solicitarse la supresión. O bien que sea un dato obsoleto, pudiendo reclamarse así su actualización.

De este modo, queda claro que el habeas data cumple un rol esencial en la protección de la intimidad y la autodeterminación informativa. Ante la posibilidad de que datos aparentemente irrelevantes se combinen para crear un perfil detallado de una persona, es indispensable contar con herramientas que permitan conocer, rectificar o eliminar esa información cuando sea necesario para evitar el abuso y la manipulación de la información personal. En un mundo donde la tecnología avanza rápidamente y la información

circula de manera constante y en grandes volúmenes, garantizar el derecho a la autodeterminación informativa es fundamental para preservar la dignidad y la autonomía de cada persona.

La Protección de Datos en el Marco Constitucional

Señala Bazán que “si bien en la Ley Fundamental no se ha literalizado expresamente la denominación “hábeas data”, existe unanimidad en la doctrina y la jurisprudencia en cuanto a la plasmación del instituto en el artículo constitucional 43, párr. 3º”⁹ que reza que “...toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la

supresión, rectificación, confidencialidad o actualización de aquellos...”.

El autor nos enseña que la omisión de la nomenclatura se debió a que la ley que declaró la necesidad de la reforma¹⁰ habilitaba a la Convención a debatir sobre la incorporación del amparo y el hábeas corpus, sin mencionar al hábeas data. Y en caso de que los convencionales se extralimitaran, las modificaciones introducidas en violación a dicha normativa podían estar sujetas a la pena de nulidad de lo reformado.

De este modo, el artículo 43 consagró la acción de amparo, el hábeas corpus y, solapadamente, el hábeas data. Sin embargo, creemos que el hábeas data es una especie de amparo, es un “amparo especial que no se confunde con el género desde que tiene especificidad propia, por lo que no constituye acción subsidiaria de otras”¹¹.

La protección a la autodeterminación informativa se puede derivar de la normativa que encuentra sustento en tratados internacionales de derechos humanos que nuestro país ha suscripto y a los cuales se les ha otorgado jerarquía constitucional -Art. 75 inc. 22-, entre ellos la Convención Americana sobre Derechos Humanos -Art. 11 inc. 2º, 13 y 25-, la Declaración Americana sobre los Derechos y Deberes del Hombre -Arts. V y X- y el Pacto Internacional sobre Derechos Civiles y Políticos -Art. 17-.

A nivel nacional, también se ha sancionado la Ley 25.326 conocida como “Ley de protección de Datos Personales o Hábeas Data”, la cual ha sido blanco de muchas críticas por legislar únicamente la protección del derecho a la intimidad y al honor cuando, en rigor, la norma constitucional protege un amplio abanico de derechos que abarca no sólo el derecho a la intimi-

dad y al honor sino también el derecho a la privacidad, a la autodeterminación informativa, a la voz, a la imagen, a la identidad personal, a la verdad y al patrimonio¹².

Es a partir de dicha ley que la acción de hábeas data se ha esgrimido como una acción constitucional autónoma, sin necesidad de acreditar arbitrariedad o ilegalidad manifiesta, requisitos propios de la acción de amparo. También contamos a nivel nacional con la adhesión al Convenio 108 elaborado por el Consejo Europeo, que fuera aprobado a través de la Ley N° 27.483 y la Guía de Evaluación de Impacto en la Protección de Datos.

Todo este andamiaje jurídico ha contribuido a robustecer el derecho a la intimidad, sin perjuicio de que resulte pertinente actualizar la ley de protección de datos citada, por ser la misma del año 2000 y en virtud de no pre-

ver cuestiones que se han ido generando con la evolución de herramientas digitales y a partir del uso y aplicación de las nuevas tecnologías.

Necesidad de contar con legislación local en Santa Fe

Como hemos expuesto anteriormente, el uso de internet y de herramientas digitales ha aumentado significativamente en los últimos años. Esto no solo expone a los usuarios a la posibilidad de que su privacidad sea vulnerada mediante la recopilación masiva de datos en el “big data”, sino también a que empresas y gobiernos puedan controlar, recopilar e interceptar dicha información.

En consecuencia, consideramos necesario implementar mecanismos de protección que resguarden el derecho de los individuos a la autodeterminación informática cuando este se vea amenazado o vulnerado.

Actualmente, nuestra Provincia no ha satisfecho una antigua asignatura pendiente habida cuenta que si bien el hábeas data se encuentra reconocido en nuestra Carta Magna y regulado a nivel nacional por la Ley 25.326, carece de sustento en la normativa provincial.

Consideramos que esta figura debe regularse como una acción autónoma y diferenciada del amparo. Aunque ambas acciones comparten ciertos puntos en común, el hábeas data presenta características propias, por cuanto permite la posibilidad de acceder a información personal y conocer la finalidad de su uso sin necesidad de acreditar arbitrariedad o ilegalidad manifiesta, a diferencia de lo que ocurre en el amparo.

El proceso de hábeas data es el medio idóneo para que los ciudadanos accedan y controlen sus datos personales almacenados en registros públicos y privados. Por ello,

es una vía directa y principal para proteger el derecho a la autodeterminación informativa, tal como lo sostuvo la Corte Suprema de Justicia de la Nación en el fallo “Martínez, Matilde S. c. Organización Veraz S.A.”.

Asimismo, es fundamental que se determine la competencia de los juzgados provinciales dado que, en la práctica, surgen frecuentes conflictos de jurisdicción en casos vinculados con redes sociales, motores de búsqueda, correos electrónicos y otros medios digitales.

Una normativa provincial no solo ayudaría a resolver cuestiones como el proceso a seguir —dado que, ante la ausencia de un procedimiento específico, los juzgados suelen optar por el trámite más breve (sumarísimo), la ley de amparo provincial o la Ley Nacional 25.326, sino que también complementaría y fortalecería la legislación

nacional. Esto permitiría procedimientos más accesibles, rápidos y eficientes para los ciudadanos de la jurisdicción local, además de garantizar una mejor coordinación y control en la protección de datos, adaptándose a las particularidades y desafíos propios de la región.

Competencia

Este es un tema que ha generado y continúa generando numerosos inconvenientes a la hora de interponer este tipo de acciones.

En lo que respecta al fuero federal, cabe recordar que siempre es excepcional y restrictivo. Este regirá cuando, por razón de las personas, de la materia y del lugar, así debe ser. Asimismo, el legislador reputó que motiva la competencia federal en los casos en que se persiga eliminar datos o contenidos que obran en registros, archivos, bases o bancos de datos interconectados en redes de

alcance interjurisdiccional, nacional o internacional, en virtud de lo normado en los artículos 36 inciso b y 44 in fine de la ley 25.326¹³.

En el dictamen del Procurador Fiscal en la causa Svatzky¹⁴, al que adhirió la Corte Suprema, se estimó aplicable lo dispuesto en el art. 36, inc. b de la LPDP, en cuanto dispone que será competente la justicia federal cuando los archivos de datos se encuentren interconectados en redes interjurisdiccionales, nacionales o internacionales. Dado que los datos que se pretendía eliminar constaban en una base de datos de Internet, accesible desde cualquier lugar del país y del mundo, el Tribunal resolvió adjudicar competencia al Juzgado Nacional de Primera Instancia en lo Civil y Comercial Federal N° 10.

En igual sentido han resuelto las Salas I (Gutiérrez”, Auto N° 403 del 10.12.2018), II (“Arce”,

Auto N° 41 del 31.03.2011) y IV (“Olmos”, Auto N° 219 del 22.08.2017) de la Cámara Civil y Comercial de Rosario.

En este contexto, y respecto a la jurisdicción local, según lo resuelto por nuestro Címero Tribunal, la justicia local es competente siempre que no se vislumbre una afectación al normal funcionamiento de los servicios de tecnología de la información y las comunicaciones¹⁵.

Por ello, creemos que si la materia del sub examine se relaciona con situaciones reguladas por el derecho privado (civil o comercial) y el registro o base de datos pertenece a un particular, correspondería a la jurisdicción civil y comercial. En cambio, si la situación jurídica a tutelar está vinculada al ejercicio de la función administrativa y los registros o bases de datos pertenecen a la autoridad pública o quien ejerza la misma, el fuero competente debería ser el

contencioso administrativo.

La variada y, a veces, compleja realidad requiere que nos aferremos a las jurisdicciones especializadas, dado su conocimiento específico en la materia, su experiencia sobre la temática abordada y la coherencia que pueden tener sus pronunciamientos.

Legitimación

En cuanto a la legitimación activa, parece razonable que toda persona física o jurídica que considere que el dato concreto lo afecta, tenga legitimación activa para interponer acción de hábeas data.

Podría incluirse además a los herederos forzosos de la persona de la cual consten los datos, cuando la indagación tenga el propósito de defender el “honor familiar”.

Podría también ampliarse la legitimación a los herederos

de la persona registrada, ya que pueden estar interesados en conocer datos médicos de aquélla relativos a enfermedades hereditarias o bien, por el uso incorrecto de sus datos personales, en la medida que perjudican la memoria o afectan la dignidad, el honor y la imagen del difunto. Sería sumamente positivo incluir como legitimados al Defensor del Pueblo, al Ministerio Público Fiscal y a los grupos colectivos que acrediten legitimación suficiente en la representación de afectaciones colectivas.

Respecto a la legitimación pasiva, estimo criterioso extender la misma a los “administradores, responsables y usuarios de sistemas informáticos o bancos de datos”, tanto públicos como privados.

El concepto de archivo, registro, base o banco de datos refiere a “conjunto organizado de datos personales que sean objeto de tratamiento

o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso”.

Trámite

Es indudable que este remedio judicial es de carácter excepcional, sumario y rápido, con lo cual es menester regularlo mediante un proceso que cumpla con esa finalidad.

Sería aconsejable, en virtud del principio de buena fe, que previo a la interposición de la acción de hábeas data se solicite a la Administración o al privado titular del registro el suministro de la información necesaria y, de corresponder, su rectificación y/o demás aspectos abarcativos de este instituto.

El presupuesto fáctico y jurídico del hábeas data debe ser de sencilla acreditación, objetivo, ya que la hipotética complejidad de las cuestiones a interpretar podrían atentar contra

la ratio iuris del instituto.

Sin dudas que sería conveniente se incluya, como mínimo, el hábeas data exhibitorio o informativo -para averiguar lo que conste en un banco de datos-, cancelador o exclutorio -para suprimir datos sensibles-, rectificador o corrector -para casos de falsedad-, actualizador, impugnativo, bloqueador, disociador, asegurador, reparador o resarcitorio.

El derecho al olvido

Un punto ineludible frente a la legislación de normativa de este tenor es la recepción de este instituto. El derecho al olvido es un tema relativamente novedoso que se consolida a partir del fallo del Tribunal Superior Europeo “Costeja González¹⁶” y que no cuenta actualmente con regulación legal en nuestro país, por lo que su consolidación se está dando a través de la jurisprudencia.

Lo podríamos definir como el principio a tenor del cual cierta información debe ser eliminada de los archivos una vez transcurrido determinado lapso de tiempo, para evitar que el individuo quede prisionero de su pasado¹⁷.

Podemos afirmar que cuando existe información personal o una noticia en Internet que pierde actualidad, pero aún permanece disponible, en la medida que no tenga interés público su difusión o con potencialidad para afectar derechos de las personas, se aplicará el derecho al olvido, debiendo ser eliminada por el responsable del sitio o blog a fin de permitir al titular del dato no quedar estigmatizado por su pasado¹⁸.

Resulta trascendental diferenciar el derecho al olvido del derecho que le asiste a una persona a solicitar que se eliminen enlaces con imágenes o textos que puedan producirle un daño, cuando los in-

termediarios hayan sido debidamente requeridos y tomado conocimiento de la ilicitud.

En el caso de este derecho, la información o el dato personal ha perdido actualidad o dejado de ser relevante por el paso del tiempo, pero no es falsa, ni su vinculación con su titular es ilícita. Este derecho se aplica sobre información verdadera. Si la información es falsa cabe suprimirla por lesionar el honor y ser incorrecta.

Masciotra¹⁹ expresa que este derecho sólo encuentra consagración normativa a nivel nacional en el Artículo 26 inc. 4 de la Ley 25.326 al legislar el derecho al olvido en materia crediticia estableciendo que sólo podrán archivarse datos personales para evaluar la solvencia económica-financiera de una persona durante cinco años.

Por fuera de ese articulado, ha sido la jurisprudencia quien ha receptado este ins-

tituto. Así es que, la Cámara Nacional de Apelaciones en lo Civil de la Capital Federal en el caso “Denegri²⁰” hizo lugar a la demanda interpuesta y, en consecuencia, ordenó al motor de búsqueda Google la eliminación de ciertos videos, noticias y fotos que afectaban el derecho al honor e intimidad de la actora, al vincularla a la causa “Coppola²¹”.

Ante la apelación de la demandada, el Máximo Tribunal revocó la sentencia y determinó que no correspondía restringir el contenido solicitado ya que la medida interrumpe el proceso comunicacional y, en consecuencia, afectaría una de las libertades más priorizadas en nuestro ordenamiento constitucional que es la libertad de expresión.

Para así decidir tuvo en cuenta los antecedentes “Rodríguez”, “Gimbutas” y “Páquez²²” en los que había expuesto que toda restricción, sanción o limitación a la libertad de ex-

presión es de interpretación restrictiva, y que toda censura previa que sobre ella se ejerza padece una fuerte presunción de inconstitucionalidad²³.

En casos como el de la Causa “Denegri²⁴”, donde se debatió la colisión entre el derecho al honor y la libertad de expresión, surge el desafío de encontrar un equilibrio entre la memoria social y la protección de los derechos individuales. El reconocimiento del derecho al olvido en el ámbito provincial podría ayudar a avanzar hacia soluciones más claras y específicas en casos donde la información personal ha perdido actualidad, pero sigue afectando la vida privada de los individuos.

En definitiva, constituye un desafío la regulación de este instituto debiendo aportar criterios específicos y claros que reconozcan la limitación de información en supuestos absolutamente excepcionales para proteger los derechos a

la autodeterminación informativa de forma tal que se respete al mismo tiempo el acceso a la información pública y la libertad de expresión.

Conclusiones

En un contexto donde la información es poder, la protección de los datos personales debe ser considerada un derecho fundamental. La intimidad es un aspecto esencial de la personalidad, caracterizado por estar exento del conocimiento de los demás. Este derecho se materializa en la facultad que tiene cada individuo de impedir que otras personas accedan a información privada que no desea compartir.

El hábeas data se erige como una garantía constitucional fundamental destinada a proteger la privacidad de las personas, evitando la recopilación y divulgación de información en bases de datos o registros sin el consentimiento

explícito de su titular. Esta figura, como otras garantías jurídicas, busca reducir la distancia entre la norma y su efectiva aplicación, lo que resulta esencial para asegurar la plena protección de los derechos fundamentales.

La ausencia de una regulación adecuada en Santa Fe no solo deja a los ciudadanos en situaciones de vulnerabilidad, sino que también impide avanzar hacia un sistema jurídico más justo y acorde con los desafíos contemporáneos.

Frente a esta realidad, la deuda legislativa en materia de protección de datos debe ser abordada con prioridad. Es crucial que Santa Fe avance hacia la creación de un marco normativo moderno que asegure la privacidad y garantice los derechos de sus ciudadanos en el entorno digital. Tanto una reforma constitucional como la sanción de un código de procedimientos constitucionales podrían ser solucio-

nes adecuadas. Lo crucial es implementar medidas concretas que respondan a los retos de la era de la información.

En definitiva, esta deuda legislativa debe atenderse de manera prioritaria para garantizar que el sistema de derechos en la provincia esté en sintonía con las necesidades y exigencias del presente. La implementación de un marco normativo que contemple el habeas data no solo protegerá la intimidad de los ciudadanos, sino que también asegurará que sus derechos fundamentales sean respetados en un entorno digital en constante evolución. ■

Citas y referencias

1- HARARI, Yuval Noa, "Homo Deus", Ed. Debate, 14° Ed., CABA, 2020, Pág. 407.

2- "La autodeterminación informativa, también llamada libertad informática, derecho personalísimo de todo titular de gobernar los datos a él referidos, implica tres aristas a tener en cuenta: la autonomía de la voluntad del titular de los datos, el deber/derecho de información hacia el titular sobre los datos y acciones y condiciones de procesamiento que se efectúen sobre ellos y la información como sinónimo -inadecuadamente utiliza-

do- del objeto jurídico protegido, los datos. En relación con esto último, se protege todo dato que procesado pueda transformarse en información"⁹. FALIERO; Johanna C, "La protección de datos personales", Bs. As., Ed. Ad Hoc, 2021, 2° Ed., Pág. 86.

3- SAGÜES, Néstor P.; "Compendio de Derecho Procesal Constitucional, Ed. Astrea, 1° Ed., Bs. As., Año 2009, Pág. 622.

4- HARARI, Ob. Cit., Pág. 407.

5- Art. 19 CN: "Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe".

6- BASTERRA, Marcela; "El sistema de protección de datos personales en la Ciudad Autónoma de Buenos Aires", aDA, 2018, se puede consultar en [https://marcelabasterra.com.ar/wp-content/uploads/2018/07/El-sistema-de-proteccio%CC%8In-de-datos-personales-en-la-Ciudad-Auto%CC%](https://marcelabasterra.com.ar/wp-content/uploads/2018/07/El-sistema-de-proteccio%CC%8In-de-datos-personales-en-la-Ciudad-Auto%CC%8Inoma-de-Buenos-Aires-MIB.pdf)

[8Inoma-de-Buenos-Aires-MIB.pdf](https://marcelabasterra.com.ar/wp-content/uploads/2018/07/El-sistema-de-proteccio%CC%8Inoma-de-Buenos-Aires-MIB.pdf)

7- SAGÜES, Néstor P., "Derecho Constitucional", Tomo II, Ed. Astrea, Bs. As., Pág. 125.

8- BAZAN, Víctor; "El hábeas data como proceso constitucional autónomo. Protección del derecho a la autodeterminación informativa"; Cita: TR LALEY AR/DOC/5187/2012.

9- BAZÁN, Víctor; "Ob. Cit."; Cita: TR LALEY AR/DOC/5187/2012.

10- Ley 24.309.

11- GELLI, María Angélica; "Constitución de la Nación Argentina. Comentada y Concordada, 3° Ed., La Ley, Año 2005, Pág. 508.

12- MASCIOTRA, Mario; "El ámbito de aplicación del habeas data en la legislación argentina, Sistema Argentino de Información Jurídica, 2004, <http://saij.gob.ar/home>

13- CSJN; Fallos: 340:815.

14- https://www.mpf.gob.ar/dictamenes/2004/Obarrio/Dic/Svatzky_Betina_

Laura_comp_1355_L_XL.pdf

15- Secretaría de Jurisprudencia de la CSJN; “Redes sociales y competencia”, Diciembre 2023, Pág. 5.

16- El caso de inició en 2010 cuando el Sr. Costeja González presentó ante la Agencia Española de Protección de Datos un reclamo contra el Diario La Vanguardia, Google Inc y Google Spain. La solicitud se fundamentaba en que cuando una persona introducía su nombre en el motor de búsqueda de Google obtenía como resultado vínculos de dos publicaciones del periódico mencionados en las que figuraba un anuncio de una subasta de inmuebles del año 1998 relacionada con un embargo al actor por deudas que ya se encontraban saldadas y que habían perdido relevancia. El Tribunal Europeo consagró el derecho al olvido al resolver que el Sr. Costeja González podía legítimamente oponerse a la indexación de sus datos con base en el derecho fundamental a la protección de datos personales y en el derecho a su intimidad o vida privada, que engloba el derecho al olvido.

17- GOZAÍNI, Osvaldo A., El derecho de

amparo. Los nuevos derechos y garantías del artículo 43 de la Constitución Nacional, Depalma, Buenos Aires, 1995.

18- BASTERRA, Marcela I., Datos personales para fines publicitarios. Dirección Nacional de Protección de Datos Personales, en L.L., 2009-B 1037, AR/DOC/1357/2009.

19- MASCOTRA, Mario; “El derecho al olvido. Reparación del daño ante su violación”; Cita online: AR/DOC/4389/2012.

20- Este caso tenía una singularidad, aquí lo que se pretendía era la supresión de sitios web en los que se exponía información sobre hechos concernientes a la actora.

21- CNApel. en lo Civil de la Capital Federal, Sala H, “Denegri, Natalia Ruth c. Google Inc. s/ derechos personalísimos” (expediente CIV 50016/2016), sentencia del 10/08/2020.

22- En todos ellos la CSJN sentó la siguiente doctrina: “si el contenido es manifiestamente antijurídico, el buscador debe sustraer dicho contenido cuando es notificado extrajudicialmente por la

persona afectada, y, si no lo hace, es responsable por los daños. Por el contrario, en los casos en que el contenido dañoso que importe eventuales lesiones al honor o de otra naturaleza, pero que exijan un esclarecimiento que deba debatirse o precisarse en sede judicial o administrativa para su efectiva determinación, cabe entender que no puede exigirse al “buscador” que supla la función de la autoridad competente ni menos aún la de los jueces. Por tales razones, en estos casos corresponde exigir la notificación judicial o administrativa competente, no bastando la simple comunicación del particular que se considere perjudicado y menos la de cualquier persona interesada” (CSJN; Fallos: 337:1174, considerando 18).

23- Para un abordaje más profundo ver: PLÁ SASMUT, Paula; “Libertad de expresión y responsabilidad civil de los motores de búsqueda” – Revista Temas de Derecho Civil, Persona y Patrimonio – Ed. Erreius, Febrero 2021, Bs. As., Págs. 21/34.

24- CSJN; “Denegri, Natalia Ruth c/ Google Inc.s/ derechos personalísimos: Acciones relacionadas” del 28.06.2022.

myf

147