Hacia una reforma del proceso de protección de datos personales.

Por Marcela I. Basterra.

1. Introducción. 2. La legislación sobre protección de datos personales en Argentina. 3. La necesidad de una reforma al sistema jurídico actual. 4. El derecho al olvido. 4.1. El surgimiento del instituto. 4. 2. La regulación en el derecho comparado. 4. 3. El derecho al olvido en Argentina. 5. Conclusiones.

1. Introducción.

En la actualidad, las nuevas tecnologías de la información y comunicación, conocidas como NTICs, obligan a los individuos a brindar a diario determinada información acerca de sí mismas; tal como domicilio, número de documento, profesión, datos crediticios o patrimoniales. El avance de los dispositivos móviles y la expansión digital genera que el flujo de datos personales que circula en la red resulte abrumador, a punto tal que se habla hoy en día de una "*identidad digital de los individuos*"[1].

Toda esta información es susceptible de ser utilizada en forma indebida o -lo que es peor- de manera abusiva[2]. A partir del escándalo conocido como *"Cambridge Analytica"*, y de las declaraciones de Mark Zuckerberg ante el Senado de los Estados Unidos, tomamos conciencia del valor que los datos en la red tienen, incluso la potencialidad de manipular procesos eleccionarios[3].

En este contexto, la protección de datos personales, como disciplina que tutela el derecho a la autodeterminación informativa y a la intimidad, se ubica como temática prioritaria en las agendas legislativas y mantendrá vigencia mientras continúe desarrollándose este proceso global[4].

Es en este sentido, que diversos organismos internacionales señalan la importancia de garantizar debidamente la privacidad informativa. La Asamblea General de la ONU, destacó la obligación de los Estados de respetar y proteger el derecho a la privacidad en el contexto de las comunicaciones digitales, de conformidad con el derecho internacional de los derechos humanos. Enfatizó, por un lado, que las autoridades deben abstenerse de realizar intromisiones arbitrarias en el ámbito correspondiente a cada individuo, su información personal y sus comunicaciones y, por el otro, que deben garantizar que terceras personas no lleven a cabo conductas abusivas[5].

Por su parte, el Consejo de Derechos Humanos de Naciones Unidas reconoció que: "*el ejercicio de los derechos humanos, en particular del derecho a la libertad de expresión en Internet, es una cuestión que reviste cada vez más interés e importancia debido a que el rápido ritmo del desarrollo tecnológico permite a las personas de todo el mundo utilizar las nuevas tecnologías de la información y las comunicaciones*"[6].

En sentido similar, la Relatoría para la Libertad de Expresión de la Comisión Interamericana afirmó que el desarrollo de Internet ocasiona serios riesgos a la vida privada de las personas, motivando

---

[1] Roosendaal, Arnold, *Digital personae and profiles in law*. Wolf Legal Publishers, 2013, pág. 41.

[2] Ampliar de Basterra, Marcela I. *Protección de Datos Personales. Ley 25.326 y Dto. 1558/01 Comentados Derecho Constitucional Provincial Iberoamérica y México*. México, EDIAR, 2008, pág, 27.

[3] Véase "*Cambridge Analytica: la multa récord que deberá pagar Facebook por la forma en que manejó los datos de 87 millones de usuarios*" disponible en https://www.bbc.com/mundo/noticias-49093124

[4] Basterra, Marcela I., *Datos personales para fines publicitarios. A propósito de la Disposición 4/2009 de la Dirección Nacional de Protección de Datos Personales*, La Ley, 2009, pág. 1037. Cita Online: AR/DOC/1357/2009.

[5] Asamblea General de la Organización de las Naciones Unidas, Resolución *"El derecho a la privacidad en la era digital"*, aprobada el 18/12/2013, disponible en https://ap.ohchr.org/documents/

[6] Asamblea General de la Organización de las Naciones Unidas, Resolución "*Promoción, protección y disfrute de los derechos humanos en Internet"* aprobada el 27/6/2016, pàg. 2, disponible en https://ap.ohchr.org/documents/

numerosos desafíos en torno a la protección del derecho a la privacidad, tanto para el Estado en su rol de garante, como para los particulares, en su rol de usuarios[7].

En conclusión, el flujo de información en la sociedad digital actual adquirió una magnitud impensada generando que la protección de datos personales enfrente nuevos desafíos, riesgos y daños posibles a la intimidad. Por ello, el presente trabajo propone analizar el régimen vigente en Argentina a la luz del nuevo contexto internacional en la materia, a fin de reflexionar sobre la necesidad de una reforma a la ley nacional, de manera tal que se garantice la autodeterminación informativa, para reconocer a los usuarios el poder de controlar el uso y destino de sus datos. Asimismo, que contemple herramientas que se han incorporado a las leyes de protección de datos personales en las últimas décadas, entre otros temas, el derecho al olvido, el alcance de la responsabilidad de los buscadores de internet, la geolocalización, los nuevos estándares de protección de los datos de la salud en el contexto de pandemia mundial, etc.

2. La legislación sobre protección de datos personales en Argentina.

La Convención Constituyente de 1994 incorporó lineamientos trascendentales en materia de protección, en forma similar a los países del Sistema Interamericano en donde no se sancionaron normas generales o sectoriales como ocurrió en Europa o Estados Unidos, sino que, su inserción se realizó directamente en las Constituciones reformadas[8].

En efecto, la reforma constitucional argentina reguló la acción de habeas data reconociendo a los usuarios la posibilidad de acceder, rectificar, cancelar u oponerse al procesamiento de datos, lo que se denomina derechos ARCO[9]. De esta forma, el artículo 43, tercer párrafo constitucional establece 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 aquéllos. No podrá afectarse el secreto de las fuentes de información periodística".*

Asimismo, al otorgar jerarquía constitucional a distintos instrumentos internacionales, como lo prevé el artículo 75 inciso 22, se robusteció el derecho a la intimidad como prerrogativa fundamental. Recordemos que la Convención Americana sobre Derechos Humanos consagra la protección de la intimidad en el artículo 11 inciso 2º, en sentido concordante con el Pacto Internacional sobre Derechos Civiles y Políticos (artículo 17) y la Declaración Americana de los Derechos y Deberes del Hombre (artículo V y X).

Posteriormente, el Congreso de la Nación sancionó la Ley 25.326[10] conocida como Ley de Protección de Datos Personales o Habeas Data, reglamentada por el Poder Ejecutivo a través del decreto 1.558/2001[11]. En sentido similar, países varios países en América Latina como Brasil[12],

---

[7] Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, *Estándares para una Internet Libre, Abierta e Incluyente*, aprobado el 15/3/2017, pág. 78 disponible en http://www.oas.org/es/cidh/expresion/

[8] Basterra, Marcela I. La Garantía Constitucional de Habeas Data. Lineamientos Generales de la Ley de Protección de Datos Personales, 2013, disponible en http://marcelabasterra.com.ar/

[9] Faliero, Johanna C. *"El futuro de la regulación en protección de datos personales en la Argentina* en Abdelnabe Vila, Carolina y otros, #LegalTech: El Derecho ante la Tecnología, Ciudad Autónoma de Buenos Aires, Thomson Reuters La Ley, 2018, pág. 62.

[10] Ley 25.326 publicada en el B.O. el 02/11/2000.

[11] Decreto 1558/2001, publicado en el B.O. el 29/11/2001.

[12] Ley 9.507 de Brasil, publicada en el B.O. el 12/11/1997.

Chile[13], Paraguay[14], Perú[15] y Colombia[16] -entre otros-, dictaron sucesivas legislaciones, complementarias de las normas constitucionales.

La ley argentina tiene por objeto, de conformidad con el artículo 1º, "*la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional".*

El legislador se aparta de la norma constitucional, en tanto aquélla no menciona expresamente los derechos tutelados por la garantía, tomando únicamente el derecho a la intimidad y al honor, aún cuando la Constitución implícitamente, protege el derecho a la intimidad informática que implica la posibilidad de ejercer la autodeterminación informativa y, a través de ella, la protección del derecho a la imagen o el propio perfil. Esta es una de las críticas que formula Masciotra[17] al enfatizar que el artículo 43 protege una diversidad de derechos; a la intimidad, a la privacidad, a la autodeterminación informativa, al honor, a la voz, a la imagen, a la identidad personal, a la verdad y al patrimonio, por lo que no comparte el objetivo legal que señala el artículo 1º, al limitarlo a garantizar el honor y la intimidad de las personas.

En el año 2003 la Comisión de las Comunidades Europeas consideró que la legislación argentina comprendía los principios fundamentales necesarios para que las personas físicas reciban una protección adecuada, por lo que se encontraban satisfechos los estándares necesarios para permitir la transferencia de datos personales con países que formen parte de la Unión Europea[18].

Con posterioridad a la sanción de la ley 25.326 se registraron considerables avances en la materia. En primer lugar, se destaca la adhesión de Argentina al Convenio 108[19] elaborado por el Consejo Europeo, con el objeto de lograr unidad entre las legislaciones de los países adheridos, para fortalecer la privacidad de los individuos contra posibles abusos en el tratamiento de sus datos. Este instrumento, que fue aprobado por el Congreso a través de la ley 27.483[20], es el único tratado multilateral de carácter vinculante en la materia.

También podemos señalar la firma de la Guía de Evaluación de Impacto en la Protección de Datos[21] diseñada junto con la Unidad Reguladora de Control de Datos uruguaya, con el fin de implementar un mecanismo de carácter preventivo a los efectos de minimizar los potenciales daños a la privacidad.

A pesar de la evolución y el crecimiento logrado, la legislación vigente data del año 2000, por lo que es claro, como veremos a continuación, que resulta desactualizada al no contemplar los posibles riesgos y amenazas que se generan con el uso de las nuevas herramientas tecnológicas.

En este sentido, la Relatoría Especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión de Naciones Unidas alertó a los Estados que las leyes de protección de datos

---

[13] Ley 19.628 de Chile, publicada en el B.O. el 28/8/1999.

[14] Ley 1.682 de Paraguay, publicada en el B.O. del 16/1/2001.

[15] Ley 27.489 de Perú, publicada en el B.O. del 28/6/2001.

[16] Ley 221/2007 de Colombia, publicada en el B.O. del 04/6/2007.

[17] Masciotra, Mario, *El ámbito de aplicación del habeas data en la legislación argentina*, Sistema Argentino de Información Jurídica, 2004, disponible en http://www.saij.gob.ar/home

[18] Decisión 2003/490 EC fecha 30/6/2003.

[19] Convenio N° 108 del Consejo de Europa para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y protocolo adicional al convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos trasfronterizos de datos, elaborado el 28/1/1981 por el Consejo de Europa disponible en https://www.coe.int/web/portal/home

[20] Ley 27.483 publicada en el B.O. 02/1/2019.

[21] Elaborada el 28/1/2020 por la Agencia de Acceso a la Información Pública de Argentina y la Unidad Reguladora de Control de Datos Personales de Uruguay, disponible en https://www.argentina.gob.ar/sites/default/files/guia_final.pdf

resultan insuficientes o inadecuadas, por lo que es vuelve indispensable su modificación para adoptar normas claras, tanto respecto del Estado como del sector privado[22].

3. La necesidad de una reforma legislativa al sistema jurídico actual.

El contexto en el que se sancionó la ley de Habeas Data difiere mucho del escenario actual, toda vez que se reguló en un período en el que el desarrollo de Internet y el flujo de la información no poseían la envergadura que han adquirido en la actualidad. Más aún, el aislamiento social a raíz de la pandemia del COVID 19 produjo un aumento inusitado del uso de redes sociales y aplicaciones tecnológicas.

Las herramientas digitales, incrementan la capacidad de los gobiernos y las empresas de desarrollar actividades de vigilancia, interceptación y recopilación de datos, lo que podría constituir un riesgo que no se encuentra protegido por la regulación actual. Es evidente que los mecanismos de procesamiento de datos masivos, conocidos como "*big data*", generan nuevas formas de afectación a la privacidad que no se encuentran amparadas por la normativa.

Por ello, la protección jurídica de los derechos individuales constituye una de las mayores problemáticas que se presenta en la actualidad. El uso abusivo de la informática vulnera prerrogativas esenciales de la población, demandando innovaciones legislativas que garanticen un mayor resguardo jurídico a los titulares de la información.

A través de diversas consultas, la Dirección Nacional de Protección de Datos Personales expresó que el sistema actual estructurado por la Ley 25.326 requiere indispensablemente de serias reformas, ya que la nueva era digital aumenta las violaciones del derecho a la privacidad en detrimento de la dignidad y la reputación de las personas[23].

Las modificaciones legislativas en nuestro país deberán tomar como referencia, entre otras, los parámetros de las normas internacionales como la *APEC Privacy Framework*[24], cuyo objetivo es promover el comercio electrónico en toda la región de Asia Pacífico, en concordancia con las Directrices de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre la protección de la privacidad y los flujos transfronterizos de datos personales.

Un punto clave en la reforma es tener en cuenta los lineamientos del Reglamento (UE) 2016/679[25] relativo a la protección de datos personales que entró en vigencia en 2018, estableciendo nuevos estándares internacionales en la materia al derogar la Directiva 95/46/CE[26].

El nuevo instrumento legislativo posee un alcance que excede las fronteras de Europa al generar consecuencias jurídicas, para todo el mundo, por diversos motivos[27]. En primer lugar, Europa prohíbe la transferencia internacional de información si el país de destino no garantiza un nivel de protección *"adecuado"* en los términos de la normativa europea. Por lo tanto, los países que no sean miembros de la comunidad deberán compatibilizar su sistema con el europeo, para posibilitar los flujos de datos transfronterizos.

En segundo lugar, se amplia sustancialmente el ámbito de aplicación territorial, dado que el reglamento es aplicado cuando; a) la empresa responsable del tratamiento tiene su sede en la Unión

---

[22] Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, Op. cit, pág. 83.

[23] Dirección Nacional de Protección de Datos Personales. *Ley de Protección de los Datos Personales en Argentina. Sugerencias y aportes recibidos en el proceso de reflexión sobre la necesidad de su reforma,* Agosto-diciembre 2016, disponible en https://www.argentina.gob.ar/sites/default/files/documento_aportes_reforma_ley25326_0.pdf

[24] Publicada en agosto de 2017 disponible en https://www.apec.org/.

[25] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, sancionado el 27/04/2016.

[26] Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, sancionado el 24/10/1995.

[27] Abdelnabe Vila, María y Cisilino, Arnaldo, *Perspectivas de la Protección de Datos Personales: status quo y proyecciones,* pág. 2, Cita Online: AR/DOC/3772/2020.

Europea, b) se trate de datos personales relativos a ofertas de bienes y servicios a ciudadanos en suelo europeo y, c) en el caso de que se supervise el comportamiento de ciudadanos en la Unión Europea. De esta forma, al no limitarse al procesamiento de datos ocurrido en territorio europeo como disponía la Directiva 95/46/CE, la sanción del Reglamento UE genera un impacto significativo en cualquier empresa que procese datos de residentes europeos.

Por otro lado, un punto importante que debe tener en cuenta una eventual reforma es la ampliación de sanciones ante el incumplimiento. Con excelente criterio, el Reglamento agrava las sanciones impuestas contra los responsables del tratamiento que no cumplan con la nueva normativa, facultando a las autoridades nacionales a imponer multas de hasta veinte (20) millones de euros o el cuatro (4) % como máximo del volumen de negocio total anual global del ejercicio financiero anterior[28]. La normativa argentina establece montos prácticamente simbólicos al prever en el artículo 31, que se podrán aplicar multas de de mil pesos ($ 1.000) a cien mil pesos ($ 100.000), además de lo cuestionable que es como técnica legislativa poner el monto de las multas en moneda de curso legal, en un país con altos niveles históricos de inflación, en lugar de establecerlo en unidades de valor.

Asimismo, la reforma europea introduce otras novedades troncales tal como la designación del Delegado de Protección de Datos, cuando el tratamiento lo realice una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial. El funcionario será designado teniendo en cuenta sus cualidades profesionales y, en particular, sus conocimientos especializados del Derecho y la experiencia a en la materia[29].

Siguiendo la tendencia europea, el Proyecto de ley presentado en Argentina por el Poder Ejecutivo Nacional en 2018[30] con la colaboración técnica de la Dirección Nacional de Protección de Datos Personales, crea la figura del Delegado de Protección de Datos. El artículo 43 dispone que será obligatorio su designación cuando: a) se procesen datos por parte de autoridades u organismos públicos, b) se traten datos sensibles como parte de la actividad principal del responsable o encargado del tratamiento, y c) se realice tratamiento de datos a gran escala.

Además, el Reglamento refuerza el control de los usuarios sobre sus datos personales al regular el derecho a la portabilidad de datos (artículo 20), cuando el tratamiento se efectúe por medios automatizados. Así, reconoce que el interesado tendrá la prerrogativa de recibir los datos personales que le incumban y que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable de tratamiento sin que lo impida el responsable anterior al que se los hubiera facilitado. En sentido similar, el Proyecto argentino prevé, en el artículo 33, el derecho del titular a solicitar que sus datos personales se transfieran directamente de responsable a responsable cuando sea técnicamente posible.

En relación al consentimiento del interesado, el Reglamento requiere que se otorgue mediante un acto afirmativo claro que refleje "*una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal*". Además, admite que el consentimiento se otorgue ya sea marcando una casilla en un sitio o por cualquier otra declaración o conducta que indique en este contexto que el internauta acepta el tratamiento de sus datos personales[31]. Al responsable del tratamiento de los datos personales le asiste la carga de probar que la persona brindó su consentimiento, tal como lo prevé el artículo 7º. Concordantemente, la reforma prevista en nuestro país propone una regulación sobre el consentimiento acorde con la era digital y las nuevas tecnologías. En concreto, dispone que podrá ser obtenido por escrito, verbalmente, por medios electrónicos, así como por cualquier forma similar que la tecnología permita brindar.

---

[28] Reglamento (UE) 2016/679, Op. cit., artículo 83.

[29] Ibídem, artículo 37.

[30] Expediente Nº 283/18 "*Proyecto de Ley sobre Protección de Datos Personales*" presentado en la Cámara de Senadores de la Nación el 19/09/2018.

[31] Ibídem, consid. 32.

En otro orden de ideas, la normativa europea prevé distintos supuestos en los que, a pesar de no contar con el consentimiento, el tratamiento será lícito. Por ejemplo, si es necesario para el cumplimiento de una obligación legal del responsable del tratamiento, o para proteger intereses vitales del interesado o de otra persona física. A diferencia de la ley argentina, el Reglamento prevé, además, que el interés legitimo torna lícito el procesamiento, otorgando mejores posibilidades, por ejemplo, para el procesamiento de datos ante la emergencia sanitaria[32].

En definitiva, es innegable que la Ley 25.326 no proporciona una protección acorde a los estándares de la legislación europea, ni tampoco un resguardo efectivo ante los posibles riesgos y daños que la evolución tecnológica ocasiona. Por lo que se torna fundamental modificar sus disposiciones a fin de garantizar debidamente la autodeterminación informativa.

Por último, un punto ineludible ante una eventual reforma es la incorporación de la figura del derecho al olvido, instituto que prevé expresamente el nuevo marco regulatorio europeo, tal como veremos a continuación. El proyecto elaborado por la DNPDP argentina reconoce en el artículo 31, el derecho del titular de suprimir sus datos personales siempre que el tratamiento no persiga un fin público o no sea necesario para ejercer el derecho a la libertad de expresión e información.

4. El derecho al olvido.

Desde hace algunos años, se está dando un arduo debate, tanto a nivel nacional como internacional, sobre el derecho al olvido. Se trata de un tema que en nuestro país no tiene regulación normativa específica, por lo que su alcance y contenido está en proceso de consolidación a través de la vía jurisprudencial. Esta temática comenzó a analizarse a partir del fallo *"Costeja González"*[33] , en el que el Tribunal de Justicia de la Unión Europea discutió sobre la legitimidad de las medidas de remoción y desindexación de contenidos en línea.

El origen del derecho al olvido se ubica en el concepto legal francés del *"droit à l'oubli"* y el italiano *"diritto all'oblio"*, que en términos generales se entienden como *"el derecho a silenciar eventos pasados de la vida que ya no están sucediendo*"[34]. En los últimos tiempos adquirió un mayor peso porque empezó a ser considerado como una expresión particular del derecho a la intimidad[35].

La figura, también conocida en inglés como "*right to oblivion*", es definida como el principio a tenor del cual cierta información debe ser eliminada de los archivos una vez trascurrido determinado lapso de tiempo, para evitar que el individuo quede "*prisionero de su pasado*"[36].

Por su parte, Vaninetti[37] aclara que es la facultad que tiene un sujeto de que no se traigan al presente hechos verídicos realizados en el pasado, deshonrosos o no, que no son conocidos socialmente en la actualidad, pero que al ser divulgados ocasionan un descrédito público.

Autores como Cecile de Terwangne[38] lo conceptualizan como la prerrogativa de las personas físicas a solicitar que se borre información sobre ellas después de que transcurra un período de tiempo determinado. Otros, entienden que es aquel derecho que asiste al individuo para ser olvidado, es decir,

---

[32] Basterra, Marcela I, La protección de los datos personales y la geolocalización en el contexto de la pandemia, en Pizarro, Daniel y Ackerman, Mario E. (Coords.), *Efectos jurídicos de la pandemia Covid 19*,Tomo III, Ciudad Autónoma de Buenos Aires, Editorial Rubinzal Culzoni. 2020, pág. 2.

[33] TJUE, "Google Spain SL y Google Inc. vs. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González", sentencia del 13/5/2014.

[34] Pino, Giorgio, "The Right to Personal Identity en Italian Private Law: Constitutional Interpretation and Judge-Made Rights", en Van Hoecke Mark y Ost, Francois (Eds.), *The Harmonisation of European Private Law*, Bruselas, Hart Publishing, 2000, pág. 237.

[35] Rodotà, Stefano, *Riservatezza*, VII Appendice , Italia, Enciclopedia Italiana, 2007, pág.79.

[36] Gozaíni, Osvaldo A., *El derecho de amparo. Los nuevos derechos y garantías del artículo 43 de la Constitución Nacional*, Buenos Aires, Editorial Depalma 1995, pág. 40.

[37] Vaninetti, Hugo, *El derecho al olvido en Internet*, Tomo 242, El Derecho, pág.566.

[38] De Terwangne, Cécile. Privacidad en Internet y el derecho a ser olvidado/derecho al olvido en *Revista de los Estudios de Derecho y Ciencia Política*, N° 13, España Universitat Oberta de Catalunya, 2012, pág. 3.

para que la información que se refiera a éste sea borrada, en razón del paso del tiempo y por su contenido[39]. No obstante, ciertos especialistas, como Eduardo Bertoni[40], consideran que es un error hablar de derecho al olvido, sino más bien hacer referencia al "*derecho a no ser indexado por el buscador*", dado que la información que el usuario pretende "olvidar" no se borra, permaneciendo en el sitio donde está alojada.

Numerosos juristas[41] coinciden en que se relaciona con la protección de datos personales, que se puede definir como la prerrogativa que tiene el titular de un dato personal a borrar, bloquear o suprimir información que se considera obsoleta por el transcurso del tiempo, o que de alguna manera afecta el libre desarrollo de alguno de sus derechos fundamentales, salvo que en el caso concreto prevalezca un interés público. Así, podemos afirmar que cuando existe información personal o una noticia en la red que pierde actualidad, pero aún permanece disponible con potencialidad para afectar derechos de las personas, en la medida en que no tenga interés público en su difusión se aplicará el derecho al olvido, debiendo ser eliminada por el responsable a fin de permitir al titular del dato no quedar estigmatizado por su pasado.

La Corte Suprema de Chile, en el precedente "*G. L.-F., A. c. Empresa El Mercurio SAP"* [42], entendió que el contenido esencial de este instituto no es otro que evitar la difusión de información personal pasada, que ha dejado de cumplir su finalidad, tornándose capaz de producir un daño al titular del dato.

Es de suma trascendencia delimitar el concepto del derecho al olvido, para distinguirlo del que asiste a una persona a solicitar que se eliminen enlaces con imágenes o textos que puedan producirle un daño, cuando los intermediarios hayan sido debidamente requeridos y hayan tomado conocimiento de la ilicitud.

En el caso del derecho al olvido, la información o el dato personal perdió actualidad o dejado de ser relevante por el paso del tiempo, pero no es falsa, ni la vinculación con su titular es ilícita. Sobre este punto, Palazzi[43] aclara que se aplica sobre información verdadera, si la información es falsa cabe suprimirla por lesionar el honor y ser incorrecta.

Masciotra[44], en su obra el *"El derecho al olvido"*, expresa que en materia crediticia la información económica y financiera de una persona debe ser eliminada del archivo, base o banco de datos, transcurrido un determinado tiempo desde que se produjo el hecho motivante de la información. Así, considera que la ley 25.326 consagra el derecho al olvido, en el artículo 26 inciso 4º, al prescribir que sólo podrán archivarse datos personales para evaluar la solvencia económica-financiera de una persona durante cinco (5) años.

Agrega que "*configura una limitación temporal para el tratamiento de la información crediticia con la finalidad de permitir la recuperación de aquellas personas que superaron una situación adversa y procuran reincorporarse en la actividad económica, circunstancia que resultaría materialmente imposible, si se permitiese que dicha información se mantenga sine die"*[45].

---

[39] Fleischer, Peter, *The right to be forgotten, or how to edit your history*, en Peter Fleischer: ¿Privacy? 29/1/2012, disponible en *http://peterfleischer.blogspot.com/*

[40] Bertoni, Eduardo, "*El derecho al olvido: un insulto a la historia latinoamericana*", 24/9/2014, disponible en http://ebertoni.blogspot.com.ar/

[41] Ver conclusiones de la Comisión N° 10: "Derecho comparado. Daños derivados de la actividad de Internet", en las XXV Jornadas Nacionales de Derecho Civil, Universidad Nacional del Sur, 01, 02 y 03/10/2015.

[42] CS Chile, "G. L.-F., A. c. Empresa El Mercurio SAP" sentencia del 21/1/2016.

[43] Palazzi, Pablo A., *Derecho al olvido en Internet e información sobre condenas penales (a propósito de un reciente fallo holandés)*. Buenos Aires, La Ley, 2014.

[44] Masciotra, Mario. "El derecho al olvido. Reparación del daño ante su violación" en *Revista de Responsabilidad Civil y Seguros* 2012-IX, 83; Cita Online: AR/ DOC/4389/2012.

[45] Masciotra, Mario "El derecho al olvido a tenor del criterio de la CSJN Comentario al fallo Yas, Darco c/Citibank NA s/Sumarísimo" en *Revista de Derecho Constitucional* Numero 2, Cita online:IJ-LXVIII-186, 20/5/2013, disponible en https://ar.ijeditores.com/.

En definitiva, el instituto en análisis como manifestación de los derechos de cancelación y oposición, otorga a los individuos la posibilidad de requerir que la información sobre ellos publicada en Internet sea removida, bajo ciertas condiciones, protegiendo así el derecho a la intimidad, al honor y a la dignidad, en un equilibrio justo con el derecho a la información y a la libertad de expresión que asiste a la ciudadanía[46].

4. 1. El surgimiento del instituto.

La aparición del derecho al olvido, se centra específicamente en el proceso de consolidación jurisprudencial a partir de la sentencia del Tribunal Superior Europeo en el fallo "*Costeja Gonzalez*".

El caso se inició en 2010 cuando el actor, Mario Costeja González, presentó ante la Agencia Española de Protección de Datos (AEPD) un reclamo contra el Diario La Vanguardia, *Google Spain* y *Google Inc.* Esta solicitud se fundamenta en que, cuando un persona introducía su nombre en el motor de búsqueda de *Google*, obtenía como resultado vínculos de dos publicaciones del periódico mencionado, en las que figuraba un anuncio de una subasta de inmuebles del año 1998 relacionada con un embargo al actor por deudas a la Seguridad Social.

Por un lado, el Sr. Costeja solicitaba al periódico que elimine o modifique la publicación para que no aparecieran sus datos personales, o utilice las herramientas facilitadas por los motores de búsqueda para proteger esta información. Por otro lado, requería que se exigiese a *Google Spain* o a *Google Inc*. que eliminaran u ocultaran sus datos personales para que dejaran de incluirse en sus resultados de búsqueda y dejaran de estar ligados a los enlaces de La Vanguardia, bajo el argumento que el embargo estaba totalmente solucionado y carecía de relevancia en la actualidad.

La AEPD desestimó la pretensión respecto del diario, al considerar que la publicación estaba legalmente justificada, pero consideró procedente el reclamo efectuado a *Google Spain y Google Inc.* entendiendo que quienes gestionan motores de búsqueda están sometidos a la normativa vigente en materia de protección de datos, dado que llevan a cabo un tratamiento del que son responsables y actúan como intermediarios[47]. Además, se consideró facultada para ordenar el retiro de los datos del solicitante, y para determinar la imposibilidad a futuro del acceso a determinados datos cuando se pueda lesionar el derecho fundamental a la protección de datos y a la dignidad de la persona.

Consecuentemente, *Google Spain* y *Google Inc* interpusieron recursos extraordinario ante la Audiencia Nacional, que decidió suspender el procedimiento y plantear al Tribunal de Justicia las cuestiones prejudiciales siguientes.

Una de las ellas fue determinar el ámbito de aplicación de la Directiva [95/46] y la normativa española en materia de protección, ya que *Google* argumentaba que la legislación de la Unión Europea no resulta aplicable, porque en España se encontraba el gestor de publicidad, *Google Spain*, y no el gestor de búsqueda *Google Inc*.

Los magistrados intervinientes consideraron que, dado que la empresa comercializaba espacios publicitarios en España, el tratamiento de datos personales se realizaba en ese territorio y, por ende, esta legislación resultaba aplicable.

Por otro lado, se cuestionó si *Google Spain* puede ser calificada como responsable del tratamiento de datos, y consecuentemente, está legitimada para retirar la información del motor de búsqueda. El Tribunal sostuvo que el derecho de supresión puede ejercerse ante el responsable del tratamiento, y llegado el caso, ante el motor de búsqueda, el que es equiparado a todos los efectos a un responsable del tratamiento.

Una de las cuestiones más relevantes que se debatió en el precedente es la relativa al derecho al olvido. En efecto, la AEPD planteó: "*¿Debe interpretarse que los derechos de supresión y bloqueo de los datos, y el de oposición, regulados todos en la Directiva 95/46, comprenden que el interesado*

[46] Silberleib, Laura, El derecho al olvido y la persistencia de la memoria, en *Información, cultura y sociedad* Nº 35, Buenos Aires, Instituto de Investigaciones Bibliotecológicas de la Universidad de Buenos Aires, 2016.

[47] TJUE, Op. cit., consid. 7.

pueda dirigirse frente a los buscadores para impedir la indexación de la información referida a su persona, publicada en páginas web de terceros, amparándose en su voluntad de que la misma no sea conocida por los internautas cuando considere que puede perjudicarle o desea que sea olvidada, aunque se trate de una información publicada lícitamente por terceros?"[48].

En respuesta, el Tribunal refirió que los derechos de supresión y bloqueo pueden ser ejercidos cuando; a) los datos sean inadecuados, no pertinentes y excesivos en relación con los fines del tratamiento, y b) no estén actualizados o se conserven durante un período superior al necesario, salvo que se imponga su preservación por fines históricos, estadísticos o científicos. Por consiguiente, consideró que, verificado alguno de estos supuestos, la información y los vínculos de la lista de resultados obtenidos por una búsqueda a partir del nombre del interesado, deben ser eliminados.

Haciendo hincapié en que la información contenida en los anuncios resultaba lesiva para la vida privada del requirente, además de remontarse dieciséis años atrás, entendió que el actor tiene derecho a que aquélla ya no se vincule a su nombre. Ello, en tanto entre los derechos que le reconocen los artículos 7º y 8º de la Carta Europea de Derechos Humanos[49], se encuentra el de solicitar que la información no se ponga a disposición del público en general, y en el entendimiento de que estos derechos prevalecen, en principio, no sólo sobre el interés económico del gestor de búsqueda sino también sobre el acceso a esta información. En consecuencia, resolvió que el Sr. Costeja González puede 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.

Es indudable que la sentencia del Tribunal Europeo aclaró diversos puntos, como el ámbito aplicable de la legislación europea, la responsabilidad de los motores de búsqueda y el ejercicio del derecho al olvido. Sin embargo, a partir de la sentencia, surgieron dudas sobre el ámbito territorial de la aplicación del derecho a la supresión lo que motivó una nueva sentencia del TJUE.

En 2019 la Corte Europea tuvo que resolver un conflicto entre la Comisión Nacional de Informática y Libertades de Francia (CNIL), y *Google LLC*, en relación con una sanción impuesta por la agencia francesa. El caso se inició en 2015 cuando la Comisión de Francia requirió a *Google* que suprimiera de la lista de resultados, obtenida tras una búsqueda digital, todos los enlaces que direccionaban a diferentes páginas web. La empresa se negó a cumplir lo solicitado y se limitó a eliminar los enlaces correspondientes a los países europeos. En virtud de ello, la CNIL decidió imponer a *Google* una sanción de 100.000 euros.

Consecuentemente, la empresa interpuso demanda ante el Consejo de Estado de Francia para solicitar la anulación de la resolución mencionada. El Consejo de Francia, actuando como Tribunal Supremo en lo Contencioso-Administrativo, decidió suspender el juicio y someter a consideración del TJUE una serie de cuestiones prejudiciales.

En primer lugar, plantea si el "*derecho a la retirada de enlaces*", consagrado en "*Costeja Gonzalez*", obliga a *Google* a retirar todos los resultados de una búsqueda, incluso los que se encuentren fuera del ámbito de aplicación territorial de la normativa europea. En caso de respuesta negativa a este interrogante, el Consejo cuestiona si el derecho al olvido obliga a retirar solo los enlaces correspondientes al Estado en el que se presenta la solicitud, Francia en este caso particular, o de manera más general, los de todos los países miembros de la Comunidad Europea.

El Tribunal de Justicia Europeo reconoce que tanto la Directiva derogada como el Reglamento

---

[48] Ibídem, consid. 20.

[49] Artículo 7º "*Respeto de la vida privada y familiar Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones".* Artículo 8º "*Protección de datos de carácter personal 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente".*

UE 2016/679 permiten a los interesados la retirada de enlaces frente al gestor de un motor de búsqueda, con uno o varios establecimientos en el territorio de la Unión, independientemente de que el tratamiento de datos tenga lugar en territorio europeo.

Agrega que, en virtud de la globalización, el acceso de personas que están fuera de la Unión Europea a enlaces con información sobre individuos cuyo centro de interés está en Europa, puede generar efectos inmediatos y sustanciales para la Comunidad. Esta circunstancia podría justificar que el legislador europeo fuera competente para posibilitar la retirada de estos enlaces en todo el mundo.

Sin embargo, subraya que muchos países no prevén el derecho al olvido o lo abordan desde una perspectiva diferente. El derecho a la protección de datos personales no es un derecho absoluto, por lo que debe mantenerse el equilibrio con otras prerrogativas fundamentales con arreglo al principio de proporcionalidad. Este equilibrio entre el respeto a la vida privada y a la protección de datos personales, por un lado, y la libertad informática, por otro lado, puede cambiar significativamente en cada país.

El TJUE considera que el legislador europeo, lógicamente, no ha establecido tal equilibrio fuera de la Unión. En consecuencia, el Reglamento UE no le atribuye al derecho al olvido alcance fuera del territorio de la Unión, por lo que *Google* no está obligado a retirar los enlaces que no correspondan a países europeos.

En relación al segundo interrogante; si el derecho al olvido permite retirar los enlaces correspondientes a todos los países europeos, o únicamente del país donde se presentó la solicitud, el Tribunal expresa que en principio, dado que el Reglamento 2016/679 pretende garantizar un nivel uniforme de protección en toda la Unión, la aplicación del derecho al olvido debería verificarse en todos los países miembros. Sin embargo, el interés público en acceder a una información puede variar en cada Estado europeo, por lo que el resultado de la ponderación entre los derechos en juego no será necesariamente el mismo en todos los territorios.

En conclusión, la Corte de Luxemburgo entiende que cuando el gestor de un motor de búsqueda estime una solicitud de retirada de enlaces en virtud de las disposiciones de la normativa europea, estará obligado a retirar los enlaces no en todas las versiones de su motor, sino en las que correspondan al conjunto de los países europeos. De esta forma, la sentencia del TJUE limita la aplicación territorial del derecho al olvido a los enlaces que correspondan a los Estados miembros de la Unión Europea, sin tener efectividad en los países que no integren esta comunidad.

4. 2. La regulación en el derecho comparado.

La Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos, configuró el espíritu de lo que hoy se conoce como derecho al olvido. En este sentido, los artículos 6.1.c, 12 y 14, posibilitaron que los usuarios solicitaran la rectificación, supresión o bloqueo de los datos cuando sean inadecuados y excesivos con relación a los fines para los que se recabaron.

Si bien estas disposiciones constituyen el fundamento normativo de la sentencia del Tribunal de la Unión Europea en el caso *"Costeja Gonzalez"* no podemos considerar a la Directiva como una regulación específica del derecho al olvido. Es el Reglamento de la Unión Europea que incorporó expresamente este instituto, receptando los avances jurisprudenciales referidos.

En este sentido, el artículo 17 establece que el interesado puede solicitar la supresión de los datos personales que le conciernan al responsable del tratamiento, quien estará obligado sin dilación indebida. Específicamente, el derecho al olvido, procederá cuando a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; b) el interesado retire el consentimiento y no exista otro fundamento jurídico para su tratamiento; c) el interesado se oponga al mismo y no prevalezcan otros motivos legítimos; d) los datos personales hayan sido tratados ilícitamente; e) los datos deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento; o f) se hayan obtenido en relación con la oferta directa a niños de servicios de la sociedad

de la información.

En busca de una solución justa ante la eventual confrontación con otros derechos, la normativa prevé una serie de excepciones a la supresión. Así, no se podrá ejercer el derecho al olvido cuando el tratamiento sea necesario; a) para ejercer el derecho a la libertad de expresión e información, b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, c) por razones de interés público en el ámbito de la salud pública, d) con fines de archivo en interés público, de investigación científica, histórica o fines estadísticos, o e) para la formulación, el ejercicio o la defensa de reclamaciones.

Bernal[50] afirma que la presunción debería estar a favor del individuo, mientras que sobre aquellos que deseen preservarlos rige la carga de probar lo contrario. Asimismo, sostiene que el derecho de supresión debe incluir los perfiles automáticos de los usuarios, como el historial en los navegadores o motores de búsqueda. A mi entender, resulta razonable defender la inversión de la carga probatoria, ya que el titular de los datos resulta ser el sujeto vulnerable en esta relación.

El derecho al olvido en España se ha convertido una pieza clave en materia de protección de datos personales. En este sentido, el Tribunal Constitucional, analizando el artículo 18 de la Constitución Española[51], sostiene que "*el constituyente era consciente de los riesgos que podría entrañar el uso de la informática y encomendó al legislador la garantía tanto de ciertos derechos fundamentales como del pleno ejercicio de los derechos de la persona. Esto es, incorporando un instituto de garantía como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, pero que es también, en sí mismo, un derecho o libertad fundamental*"[52].

La doctrina española ha utilizado el término para referirse en la jurisdicción civil a la aplicación de la Ley Orgánica 1/1982[53] sobre protección civil del derecho al honor, intimidad personal y familiar, la propia imagen, y de los preceptos que regulan la responsabilidad contractual y extracontractual.

Asimismo, la Ley Orgánica 3/2018 de Protección de Datos Personales[54] permite retirar o bloquear los datos en Internet, o el cese de un determinado tratamiento, por ejemplo, la cancelación de antecedentes penales y policiales, así como la oposición a prácticas comerciales o publicitarias[55]. Específicamente, en el capítulo relativo a los derechos de las personas, regula el derecho de supresión el que será ejercido de acuerdo con lo establecido en el artículo 17 del Reglamento (UE) 2016/679.

Sin embargo, debemos reconocer que la incorporación del derecho al olvido no fue aceptada unánimemente por la doctrina. En este sentido, Bertoni explica que la propuesta de la Comisión Europea fue recibida con resistencia entre algunos académicos, activistas y representantes de la industria de Internet, quienes consideran que su aplicación podría afectar otros derechos igualmente importantes y contribuir al derrumbe de la red[56].

---

[50] Bernal, Paul, A Right to Delete?, en *European Journal of Law and Technology*, Vol. 2, Nº 2, 2011 disponible en https://ejlt.org/index.php/ejlt

[51] La disposición establece que la ley "(…) *limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".*

[52] Tribunal Constitucional de España, Sala primera, Sentencia 254/1993, del 20/7/1993.

[53] Ley Orgánica 1/1982 publicada en el B.O.E el 14/5/1982.

[54] Ley Orgánica 3/2018 publicada en el B.O.E el 06/12/2018.

[55] Gervas de la Pisa, Luis, *Código del derecho al olvido*, Catálogo de Publicaciones de la Administración General del Estado, España, 2021, pág 23.

[56] Cortés Castillo, Carlos, "Derecho al olvido: entre la protección de datos, la memoria y la vida personal en la era digital" en Bertoni, Eduardo, (Comp.) *Internet y derechos humanos. Aportes para la discusión en América Latina*, Centro de Estudios en Libertad de Expresión y Acceso a la Información, Ciudad Autónoma de Buenos Aires, Centro de Estudios en Libertad de Expresión y Acceso a la Información, 2014, pág. 140.

Peter Fleischer[57], afirma que el derecho al olvido permitirá suprimir información de interés público, mientras que otros doctrinarios norteamericanos como Paul Schawartz[58], alegan que el derecho a la supresión, en los términos previstos por el artículo 17 del Reglamento UE, podría colisionar con la primera enmienda de la Constitución de Estados Unidos que reconoce el derecho a la libertad de expresión y de prensa.

4. 3. El derecho al olvido en Argentina.

En nuestro país la figura del derecho al olvido no está regulada expresamente en ninguna normativa. Sin embargo, siguiendo la tendencia internacional, la jurisprudencia argentina con buen criterio, receptó la aplicación de este instituto.

En efecto, la Cámara Nacional de Apelaciones en lo Civil de la Capital Federal en el caso *"Denegri*"[59] hizo lugar a la demanda interpuesta con objeto de solicitar que *Google* proceda a eliminar ciertos videos, noticias y fotos que afectaban el derecho al honor e intimidad de la actora, al vincularla a la causa *"Cóppola"*.

La sentencia de primera instancia hizo lugar parcialmente a la demanda, considerando que los videos o imágenes que aparecen como resultado de la búsqueda *"Natalia Denegri"* reproducen escenas de discusiones de la actora que no representan interés periodístico alguno, sino que su publicación sólo se funda en razones de morbosidad. Es por ello que el magistrado acogió parcialmente la pretensión respecto de los enlaces referenciados.

El fallo de segunda instancia, entiende que a pesar de no existir una norma específica que regule el derecho al olvido, la temática puede ser abordada como derivación del derecho al honor o a la intimidad. En su voto, el juez Kipper recordó que el ejercicio del derecho al olvido no suprime la información cuestionada, sino que limita su difusión y circulación para restringir y obstaculizar su acceso por parte de los medios tradicionales de búsqueda. Es por ello, que reconoce que colisiona con el derecho del público a ser informado, así como también con el derecho a la libertad de expresión, afirmando que "*Si cada persona decidiera qué información sobre ella puede, o no, darse a conocer, el derecho a la información, con todo lo que implica y acarrea, se vería seriamente lesionado"*[60].

Agregando, que hay cierto tipo de información que involucra hechos de interés público, específicamente lo relacionado con la investigación penal que condujo a la condena de un juez federal por hechos de corrupción, por lo que suprimir esta información implicaría vulnerar el derecho de la sociedad a estar informada.

Para así decidir, toma en consideración los argumentos de la CSJN en el caso "*Rodríguez*"[61], en el que estableció que el bloqueo del acceso a contenidos digitales debe estar precedido de un examen relacionado con su licitud. Esta doctrina establecida por la Corte Suprema se encuentra en consonancia con el criterio expuesto por la Comisión Interamericana de Derechos Humanos en el "Informe sobre Libertad de Expresión e Internet", en donde afirmó que *"las medidas de filtrado o bloqueo deben diseñarse y aplicarse de modo tal que impacten, exclusivamente, el contenido reputado ilegítimo, sin afectar otros contenidos*"[62].

En la misma línea argumental, la "*Declaración conjunta sobre libertad de expresión e Internet*" de 2011, reconoció que el bloqueo obligatorio de enlaces constituye una medida extrema, más aún

---

[57] Fleischer, Peter, Op. cit.

[58] Schwartz, Paul, The E.U.-US Privacy Collision: A Turn to Institutions and Procedures, Harvard Law Review, 2012, pág. 29, disponible en: http://www.harvardlawreview.org/

[59] Cámara Nacional de Apelaciones en lo Civil de la Capital Federal, Sala H, *"Denegri, Natalia Ruth C/ Google Inc S/ Derechos Personalísimos"*, sentencia del 10/8/2020.

[60] Ibídem, pág. 10.

[61] CSJN, "Rodríguez, María Belén c/ Google Inc. s/ daños y perjuicios", sentencia del 28/10/2014.

[62] Relatoría Especial para la libertad de expresión de la Comisión Interamericana de Derechos Humanos, *Informe sobre Libertad de Expresión e Internet*, 31/12/2013, párr. 84, disponible en http://www.oas.org/es/cidh/expresion/index.asp

cuando se trata de hechos que pueden merecer especial protección por estar vinculados con el ejercicio de funciones públicas[63].

En conclusión, la Cámara entendió improcedente el derecho al retiro de los enlaces relacionados con la investigación penal que involucra hechos de interés público.

Por otro lado, el Tribunal reconoce que en el caso en análisis también se cuestiona la remoción de enlaces que reproducen escenas mediáticas de la actora sin contenido periodístico o informativo para la sociedad que, de ninguna forma, se relacionan con la causa penal sobre corrupción. En consecuencia, considera que suprimir esta información no implica un supuesto de censura, ni tampoco afecta el derecho de acceso a la información pública.

Por las consideraciones expuestas el Tribunal de Alzada confirmó la sentencia de primera instancia, admitiendo el derecho al olvido solo respecto de aquellos enlaces que reproducen discusiones protagonizadas por la actora, bajo el entendimiento de que esta decisión no vulnera el derecho de acceso a la información, ni tampoco la libertad de prensa.

Teniendo en consideración que las leyes de protección de datos en nuestro país, y en el sistema interamericano, no reconocen el derecho al olvido el fallo analizado constituye un precedente realmente significativo. Para arribar a esta solución, dada la ausencia de norma expresa que regule esta prerrogativa en Argentina, los jueces decidieron abordar la cuestión como una derivación del derecho a la intimidad.

Como hemos visto a lo largo del presente trabajo, en la era digital el derecho al olvido constituye un aspecto fundamental de la autodeterminación informativa. Por ello, es trascendental reformar la normativa vigente para incorporar criterios específicos y concretos que aclaren la aplicación del derecho al olvido, de manera excepcional y con carácter restrictivo, de forma tal que su ejercicio no suponga la vulneración indebida de derechos fundamentales, como son la libertad de expresión y el acceso a la información pública.

Cabe destacar que el Proyecto de la DNPDP contempla la regulación del derecho al olvido, en el artículo 31, al prever que podrán suprimirse los datos personales cuando: a) ya no sean necesarios en relación con los fines para los que fueron recolectados; b) el titular de los datos revoque el consentimiento en que se basa el tratamiento de datos y éste no se ampare en otro fundamento jurídico; c) el titular de los datos haya ejercido su derecho de oposición, y no prevalezcan otros motivos legítimos para el tratamiento de sus datos; d) los datos personales hayan sido tratados ilícitamente; y e) los datos personales deban suprimirse para el cumplimiento de una obligación legal.

Cabe agregar que algunas organizaciones de la sociedad civil reconocieron que hay casos de funcionarios públicos de diversos países, que estarían utilizando el derecho al olvido para cancelar información de interés público, reemplazando acciones de calumnias e injurias ante los tribunales por acciones de oposición ante la autoridad de protección de datos personales[64]. Esta situación es de suma gravedad, dado que implica, sin duda, la utilización distorsiva de una herramienta instrumental en materia de protección de datos.

Por ello, si no se regula su ejercicio con parámetros precisos se puede generar una supresión inadecuada, por ejemplo, porque se corre el riesgo de eliminar información que no sea obsoleta o en ningún modo afecte derechos fundamentales del individuo. Por dicho motivo, es trascendental promover medidas para que sea implementado únicamente como forma de protección de datos

[63] Declaración Conjunta sobre Libertad de Expresión e Internet, adoptada por el Relator Especial de la ONU para la Libertad de Opinión y de Expresión, la Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Relatora Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión y la Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP), 2011, punto 3.a, disponible en http://www.oas.org/es/cidh/expresion/index.asp

[64] Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, Op. cit. pág 54.

personales, evitando que ocasione una eliminación masiva de datos y que se traduzca en última instancia en un método de censura indirecta.

La Comisión IDH advirtió sobre las consecuencias negativas que puede generar la orden de retirar un enlace existente en un diario digital. Así, en el caso "*Mauricio Herrera Ulloa vs. Costa Rica"*[65], expresó que la orden de retirar enlaces sobre información relacionada con un funcionario público de la página web del periódico La Nación (de Costa Rica), vulneraba el artículo 13 de la Convención Americana dado que tiene como efecto directo la censura previa.

En sentido similar, la Relatoría Especial estima que la aplicación de un sistema de remoción y desindexación privada de contenidos en línea con criterios vagos y ambiguos, resulta particularmente problemático a la luz de la protección de la libertad de expresión reconocida por el Pacto San José de Costa Rica.

A partir del fallo "*Costeja Gonzalez"*, se inició un arduo debate sobre la legitimidad de las medidas de indexación dispuestas, y sobre las restricciones, generando que cierta parte de la doctrina considere a la figura del derecho al olvido como un concepto ambiguo, con un contenido y alcance sumamente indefinido, lo que representa un grave riesgo para los derechos fundamentales de la ciudadanía. En efecto, argumentan su inconstitucionalidad o inconvencionalidad, por ser incompatible con la prohibición de censura que reconoce la Convención Americana[66].

Más allá de las consideraciones precedentes considero que diseñar una legislación con criterios específicos para la aplicación de derecho al olvido genera mayor seguridad jurídica para los operadores del sistema judicial, y permite que la remoción responda a robustos y sólidos estándares. Las disposiciones del marco europeo tuvieron un resultado sumamente positivo, en tanto generaron directrices claras y eficientes para las demás legislaciones al consagrar requisitos de procedencia estrictos bajo los cuales sea posible la remoción de contenidos en línea.

En definitiva, es fundamental incorporar a nuestra normativa criterios específicos y claros que reconozcan la desindexación, de manera absolutamente excepcional para proteger los derechos a la privacidad y la dignidad de las personas, de forma tal que se respete al mismo tiempo la libertad de expresión y el acceso a la información pública.

5. Conclusiones.

Resulta innegable que con la evolución de Internet surgieron importantes desafíos para la protección del derecho a la privacidad, tanto para el Estado en su rol de garante como para los particulares en su carácter de usuarios.

La obligación estatal de garantizar el derecho a la privacidad ante las nuevas tecnologías se traduce en el compromiso de adaptar su normativa con la finalidad de proteger adecuadamente a todos los usuarios en la red. En este contexto, observamos que en Argentina los mecanismos jurídicos que proporciona la legislación actual para la tutela del derecho a la protección de los datos personales, resultan deficientes y muy por debajo de los estándares internacionales.

Sin duda, es fundamental reformar la ley nacional Nº 25.326, a fin de lograr un marco jurídico con directrices sólidas y específicas que permitan acompañar y dar una respuesta adecuada a las lagunas jurídicas que se plantean ante la evolución tecnológica de las últimas décadas.

La eventual modificación debe procurar la implementación de una estrategia integral de privacidad, teniendo en cuenta los reclamos de los organismos internacionales y también las expectativas de los titulares de los datos. En este contexto, se torna primordial la incorporación del derecho al olvido para dotar de mayor seguridad jurídica al sistema y generar una protección tuitiva más robusta. De allí que una legislación razonable asegurará el acceso a la información pública, al

[65] Corte IDH, "Mauricio Herrera Ulloa vs. Costa Rica" sentencia del 02/6/2004.

[66] Pérez de Acha, Gisela. Una panorámica sobre el derecho al olvido en la región, en Derechos Digitales, 2015, disponible en https://www.derechosdigitales.org/.

mismo tiempo que generará un sistema de protección eficiente para la libertad de información, garantizando plenamente la autodeterminación informativa.