



**INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN
EN TECNOLOGÍAS DE LA INFORMACIÓN Y
COMUNICACIÓN**

**DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS**

**“EL DERECHO AL OLVIDO ANÁLISIS Y
PROPUESTA DE FORMULARIO”**

**PROPUESTA DE INTERVENCIÓN
Que para obtener el grado de MAESTRA EN DERECHO DE LAS TECNOLOGÍAS
DE LA INFORMACIÓN Y LA COMUNICACIÓN**

Presenta:

Stephany Dafne Méndez Pérez

Asesora:

Dra. Ana Josefina Bello Jiménez

Ciudad de México, 8 de abril de 2021



Autorización de impresión



AUTORIZACIÓN DE IMPRESIÓN Y NO ADEUDO EN BIBLIOTECA MAESTRÍA EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Ciudad de México, 8 de abril de 2021
INFOTEC-DAIC-GCH-SE-0126/2021.

La Gerencia de Capital Humano / Gerencia de Investigación hacen constar que el trabajo de titulación intitulado

EL DERECHO AL OLVIDO ANÁLISIS Y PROPUESTA DE FORMULARIO

Desarrollado por la alumna **Stephany Dafne Méndez Pérez** y bajo la asesoría de la **Dra. Ana Josefina Bello Jiménez**; cumple con el formato de biblioteca. Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

Asimismo se hace constar que no debe material de la biblioteca de INFOTEC.

Vo. Bo.



Lic. Susana Argelia Salomón Jalili
Coordinadora de Biblioteca

Anexar a la presente autorización al inicio de la versión impresa del trabajo referido que ampara la misma.

C.p.p Servicios Escolares

Agradecimientos

Agradezco a la Doctora Ana Josefina Bello Jiménez por haber aceptado la dirección de mi trabajo. Le estoy agradecida por haberme dado el beneficio de su gran competencia, rigor intelectual, profesionalismo y eficacia, a lo largo de este trabajo, que nunca olvidaré. Puede estar segura de mi compromiso y mi profunda gratitud.

Agradezco especialmente a Rita Segovia por sus consejos y su invaluable amistad y a Circe Lara por su apoyo, su amor y su paciencia.

Tabla de contenido

INTRODUCCIÓN	1
CAPÍTULO 1: ESBOZO DE LA EVOLUCIÓN JURÍDICA DEL DERECHO AL OLVIDO	6
1.1 Antecedentes	6
1.2 La Naturaleza del Derecho al Olvido	12
1.3 Crítica al concepto del Derecho al Olvido	14
1.4 El Derecho al Olvido en México	15
1.4.1. Generalidades de la Protección de Datos Personales en México	15
1.4.2 Principios relacionados con el Derecho al Olvido	17
1.4.2.1. Calidad	17
1.4.2.2. Finalidad.....	21
1.4.3 Derecho al Olvido frente a los derechos de cancelación y oposición	25
1.4.3.1. Derecho de Cancelación	26
1.4.3.2. Derecho de Oposición.....	36
1.4.4 Antecedentes del Derecho al Olvido en México	43
1.4.5 Iniciativas de Reforma en materia del Derecho al Olvido.....	45
1.4.6 Casos relacionados con el Derecho Olvido en México	52
CAPÍTULO 2.....	7
DIVERGENCIAS Y EFECTOS DEL DERECHO AL OLVIDO SEGÚN EXPERIENCIA DEL TRIBUNAL DE JUSTICIA EUROPEO.....	7
2.1 El Caso Costeja	68
2.1.1 Preámbulo.....	68
2.1.2 Temas sustanciales dirimidos por el Tribunal	69
2.1.3 Comentarios al Caso Costeja.....	72
2.2 Directrices para la implementación de la Sentencia del Tribunal De Justicia de la Unión Europea en el juicio "Google España y INC Vs. Agencia Española de Protección de Datos y Mario González Costeja" C-131/12	77
2.3 Detalles técnicos y estadísticos de la Implementación de Google del Caso Costeja.....	80
2.4 ¿Cómo funciona el proceso de Google para solicitar la retirada de información personal?	82
2.5 El Reconocimiento el Derecho al Olvido Digital en España y en la Unión Europea.....	93
2.6 Efectos tras la sentencia del Tribunal de Justicia de la Unión Europea. ...	95
2.7 El papel de las Autoridades Europeas de Protección de Datos.	95
2.8 La incorporación del Derecho al Olvido en el Proceso de reforma de la Directiva 95/46/CE	97
CAPÍTULO 3. REGULACIÓN DEL DERECHO AL OLVIDO DESDE EL RGPD	112
3.1 Principios del RGPD.....	113
3.2 Derechos de los Individuos bajo el RGPD	118
3.3 Estudio del Derecho al Olvido a partir del RGPD	120
3.3.1 ¿Cuándo es aplicable el derecho de supresión (Derecho al Olvido)? .	129
3.3.2 ¿Cuándo no es aplicable el derecho de supresión?.....	130

3.3.3 ¿Es necesario informar a otras organizaciones sobre la eliminación de datos personales?	131
3.3.4 ¿Es necesario borrar los datos personales de los sistemas de copia de seguridad?	132
3.3.5 ¿Cómo se aplica el Derecho al Olvido a los datos recopilados de niños?	132
3.3.6 ¿Es posible negarse a cumplir con una solicitud por otras razones?..	133
3.3.7 ¿Qué se debe hacer si se niega una solicitud de supresión?	134
3.3.8 ¿Cómo reconocer una solicitud de supresión?	135
3.3.9 ¿El derecho de supresión es gratuito?	135
3.3.10 ¿En cuánto tiempo se debe cumplir con una solicitud de supresión?	136
3.3.11 ¿Es posible ampliar el tiempo de respuesta a una solicitud de supresión?.....	136
3.3.12 ¿Se puede pedir una identificación a un titular?	136
3.4 Desafíos técnicos y jurídicos del Derecho al Olvido.....	137
3.5 Caso de aplicación de multa conforme al RGPD	140
3.6 Herramientas para la aplicación del Derecho al Olvido.....	141
3.6.1 Puntos clave sobre el Derecho al Olvido.....	141
3.6.2 Listado de Verificación	141
3.6.3 Formulario para ejercer el derecho de supresión (Derecho al Olvido)	142
CONCLUSIONES	146
BIBLIOGRAFÍA	152
ANEXOS	162
ANEXO I	163
ANEXO II	171
ANEXO III	176

Índice de figuras

Figura 1. Diagrama sobre el Plazo de conservación.	32
Figura 2. Procedimiento de cancelación, bloqueo y supresión.....	35
Figura 3. Grafica de URL suprimidas por Google.....	82
Figura 4. Solicitantes del Derecho al Olvido.....	89
Figura 5. Tipos de sitios que se someten a solicitudes de supresión.....	91
Figura 6. Afectación de los resultados de búsquedas de Google.....	140

Índice de cuadros

Cuadro 1. Derecho de Cancelación en México.	29
Cuadro 2. Cancelación en documentos internacionales.	36
Cuadro 3. Oposición en documentos internacionales.	40
Cuadro 4. Caso Ulrich Richter Vs Google	53
Cuadro 5. Cronología del caso Carlos Sánchez de la Peña Vs Google México ...	61
Cuadro 6. Ejemplos de solicitudes que fueron procedentes, Google	85
Cuadro 7. Ejemplos de solicitudes negadas por Google.....	87
Cuadro 8. Aproximaciones de la definición de Derecho al Olvido.....	108
Cuadro 9. Principios del RGPD.....	115
Cuadro 10. Comparativa de principios entre el RGPD y la LFPDPPP.	118
Cuadro 11. Comparativa de derechos de los individuos entre el RGPD y la LFPDPPP.....	120
Cuadro 12. Check list Solicitudes de supresión	142

Siglas y abreviaturas

AEPD	Agencia Española de Protección de Datos
APD	Autoridad(es) de Protección de Datos
CJEU	Corte de Justicia de la Unión Europea (Court of Justice of the European Union)
Directrices	Directrices de la Organización para la Cooperación y el Desarrollo Económicos (OCDE)
RIPD	Red Iberoamericana de Protección de Datos Personales
RGPD	Regulación General de Protección de Datos (General Data Protection Regulation)
GT29	Grupo de Trabajo del Artículo 29, en este trabajo se puede llegar a usar indistintamente WP29
UE	Unión Europea
Directiva (95/46/EC)	Directiva (95/46/EC), de la Unión Europea, 1995, también llamada Directiva de Protección de Datos.
LFPDPPP	Ley Federal de protección de datos personales en posesión de los particulares
RLFPDPPP	El Reglamento de la Ley Federal de protección de datos personales en posesión de los particulares
Resolución	Resolución de Madrid 2009

Introducción

La presente investigación se dedica a estudiar el Derecho al Olvido, en donde se realiza un somero análisis del marco jurídico en México y de los alcances de los derechos de cancelación y oposición del Caso Costeja, tanto sus implicaciones materiales y en el impacto regulatorio que motivó la incorporación de un nuevo derecho en la reciente regulación europea, el Reglamento General de Protección de Datos.

La característica principal del Caso Costeja, resuelto por el Tribunal de Justicia Europeo en el año 2014, es que trajo consigo un nuevo paradigma en cuanto a los alcances de la protección de los datos personales en el entorno digital, particularmente, respecto al entendimiento de lo que implica un tratamiento de datos personales realizado por un motor de búsqueda y de la aplicación territorial de la Directiva 95/46/CE¹ a Google, Inc., en donde se analizaron factores como los servicios de publicidad dirigidos a ciudadanos europeos que emplea Google para fijar competencia en territorio Europeo.

Tal fue el impacto del Caso Costeja que el Parlamento Europeo incorporó el Derecho al Olvido (regulado bajo el nombre de Derecho de supresión)², como un nuevo derecho para los titulares de datos personales, dentro del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, 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 y por el que se deroga la Directiva

¹ En este trabajo se utiliza indistintamente “Directiva” o “Directiva 95/46” para referirse a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, 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, La Directiva fue adoptada en 1995, entró en vigencia en 1998 y fue la primera legislación de la UE que protegió la privacidad y los datos personales de las personas. Fue reemplazada por el Reglamento General de Protección de Datos (RGPD) el 24 de mayo de 2018. Disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=ES> Consultada el 20 de abril de 2020.

² El artículo 17 del Reglamento General de Protección de Datos regula el Derecho de supresión al cual también lo identifica bajo el Derecho al Olvido.

95/46/CE (Reglamento General de Protección de Datos, “RGPD” por sus siglas en español)³, mismo que entró en vigor el pasado 25 de mayo de 2018.

Para analizar esta problemática es necesario mencionar sus causas. Una de ellas es que en la legislación mexicana no existe como tal un Derecho al Olvido, pensado como un derecho de supresión en el entorno digital, así como tampoco existe un derecho expresamente diseñado para desindexar resultados que contengan datos personales en un motor de búsqueda en Internet, sin embargo, la legislación mexicana sí contempla derechos como el de cancelación que materialmente logra la supresión del dato, o bien, el de oposición que impide la continuación del tratamiento.

La investigación de esta problemática se realizó por el interés de analizar si es necesario implementar un nuevo derecho para los titulares de datos personales o si la legislación mexicana actual alcanza para que los sujetos de derechos ejerzan el llamado Derecho al Olvido en el entorno digital.

Particularmente, este análisis se hace a la luz del derecho comparado en donde se estudian los alcances de los derechos de Cancelación y Oposición contemplados por la Ley Federal de Protección de Datos Personales frente a las particularidades del llamado Derecho al Olvido, a partir de la sentencia del Tribunal de Justicia Europeo.

El punto de partida en la presente investigación es la relación que existe entre Derecho al Olvido y los derechos de oposición y cancelación que actualmente se protege en la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP).

Asimismo, exploramos diversos precedentes de derecho internacional con el que se han construido los precedentes internacionales sobre el Derecho al Olvido, ejemplo de ello es el Caso Costeja, un procedimiento que versó sobre la aplicación

³ El nombre oficial es Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 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 y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos)

de la Directiva sobre protección de datos a un motor de búsqueda en Internet que Google gestiona como proveedor de servicios. En específico este procedimiento significó un parteaguas en la fundamentación y el derecho aplicable sobre el Derecho al Olvido en 1998, para un medio impreso frente a uno digital.

La hipótesis de la presente investigación será analizar si el Derecho al Olvido es un derecho nuevo o es un derecho programático, que en el ámbito del internet puede resultar ineficaz por la naturaleza técnico computacional de la red.

El objetivo de la propuesta que se plantea pretende valorar si los derechos que contempla la legislación mexicana vigente son suficientes para hacer frente a una solicitud de supresión de datos personales en el entorno digital y, en todo caso, analizar a qué nos enfrentamos en el derecho mexicano ante una posible aplicación del llamado Derecho al Olvido.

Asimismo, la aportación de esta intervención es proponer un formulario para que un titular de datos personales pueda ejercer el llamado Derecho al Olvido, entendido como una forma de supresión de datos personales en el entorno digital, desde el diseño del RGPD. El formulario busca ser una herramienta que facilite el ejercicio de derechos de titulares de datos personales, a partir de un diseño amigable e intuitivo que permita que más individuos puedan ejercer sus derechos de protección de datos sin tener que ser expertos en la materia.

Esta investigación se divide en cuatro capítulos en los cuales se trata de desarrollar las variables que sustentan nuestra investigación, a saber:

En el capítulo primero, se refiere al contexto del Derecho Mexicano, en donde se estudian los alcances del derecho de cancelación y oposición y se exponen algunos de los más recientes criterios emitidos por los tribunales mexicanos.

En el capítulo segundo exponemos las divergencias y efectos del Derecho al Olvido según experiencia del tribunal de justicia europeo, en la cual se estudia el Caso Costeja, se explora la expansión de este derecho hacia una consolidación de la aplicación, su jurisdicción y nuevas facultades que exponen una conversión de

roles entre autoridades y actores principales en la red y se revisa la aplicación que ha dado Google a partir del fallo de 2014.

El capítulo tercero, se analiza desde la perspectiva internacional inherente al Internet porque el Derecho al Olvido ha crecido a partir de una serie adaptaciones a las fórmulas del conocimiento libre e informado que ha propiciado emerger criterios interpretativos ante supuestos.

El capítulo cuarto es el estudio del Derecho al Olvido y su incorporación a la Regulación General de Protección de Datos (RGPD), se exploran los alcances y limitantes de este derecho, los desafíos tecnológicos, un caso de una multa recientemente impuesta en el marco del RGPD y, por último, se proponen algunas herramientas para la incorporación de este derecho.



Capítulo 1

Esbozo de la Evolución Jurídica del Derecho al Olvido



Capítulo 1: Esbozo de la Evolución Jurídica del Derecho al Olvido

Lo que de los hombres se dice, verdadero o falso, ocupa tanto lugar en su destino, y sobre todo en su vida, como lo que hacen.

Víctor Hugo, Los Miserables, 1862.

1.1 Antecedentes

El Derecho a la privacidad, además de ser un derecho de la personalidad es un Derecho Humano de Tercera Generación⁴ en virtud del cual se tiene la facultad de excluir o negar a las demás personas del conocimiento de ciertos aspectos de la vida.

No debe dejar de señalarse que el derecho a la privacidad se trata de una figura de origen anglosajón basada en las doctrinas del llamado *Right to be Let Alone* (derecho a ser dejado en paz)⁵ impulsada por Thomas Cooley desde 1888 y

⁴ “El reconocimiento de la tercera generación de derechos, reivindicó el derecho a la intimidad, ya que surgen como una respuesta a la denominada *liberties pollution* o contaminación de libertades es así como surgen, el derecho a la paz, el derecho a la calidad de vida, el derecho a la libertad informática el cual se encuentra íntimamente ligado con el derecho a la intimidad entre otros.” Texto tomado de Álvarez Rodríguez, Lilibeth, “Derecho al Olvido como garantía para la autodeterminación informativa en las redes sociales”, IV Foro Internacional Derechos humanos y tecnologías de la Información y Comunicación (TIC). Disponible en <https://www.repositoriodigital.ipn.mx/bitstream/123456789/3987/1/Memoria%204to%20Foro%20DH%20TIC%2015.pdf>. Consultado el 16 de abril de 2020. La propia Isabel Davara, en la obra “El Derecho al Olvido en relación con el derecho a la protección de datos personales”, del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, sostiene que “el derecho a la protección de datos personales y a la autodeterminación informativa es un derecho independiente y autónomo, de tercera generación” (p.21) citando a Aristeo García González, “La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado”, Boletín Mexicano de Derecho Comparado, núm. 120, septiembre-diciembre de 2007, México, Instituto de Investigaciones Jurídicas de la UNAM.

⁵ *Olmstead vs. U.S.* 1928: Este caso estudia las conversaciones telefónicas intervenidas obtenidas ilegalmente, por conspiración para violar la Ley de prohibición nacional mediante la importación, posesión y venta de licores ilegales. Roy Olmstead era un presunto contrabandista de alcohol. Sin aprobación judicial, los agentes federales instalaron escuchas telefónicas en el sótano del edificio de Olmstead (donde mantenía una oficina) y en las calles cercanas a su casa. Olmstead fue condenado

del *Right to Privacy* a través del famoso artículo de Warren y Brandeis, publicado en 1890 en la *Harvard Law Review*,⁶ el cual es un artículo que fue un parteaguas en el entendimiento de este derecho, y tal es su vigencia que sigue siendo un artículo citado en decisiones de la Suprema Corte de Justicia de Estados Unidos como lo es en el caso *Kyllo v. United States*, 535 U.S. 27 (2001).^{7,8}

En efecto, tal y como lo define una tesis de nuestros tribunales federales, el derecho a la privacidad dispone que las personas tienen derecho a gozar de un ámbito de proyección de su existencia que quede reservado de la invasión y la mirada de los demás, que les concierna sólo a ellos y les provea de condiciones adecuadas para el despliegue de su individualidad, para el desarrollo de su autonomía y su libertad.⁹

con pruebas obtenidas de las escuchas telefónicas. El Tribunal sostuvo que no se violaron los derechos de la Cuarta ni la Quinta Enmienda de las partes, porque la mera intervención telefónica no constituye una autoincriminación, pesquisa (investigación) o cateo. Este caso fue revocado por el caso *Katz vs U.S.* (1967). Sin embargo, se cita uno de los razonamientos más célebres de esta sentencia en donde se cita el "Derecho a ser dejado en paz": "La protección garantizada por las Enmiendas tiene un alcance mucho más amplio. Los creadores de nuestra Constitución se comprometieron a asegurar las condiciones favorables para la búsqueda de la felicidad. Reconocieron el significado de la naturaleza espiritual del hombre, de sus sentimientos y de su intelecto. Sabían que sólo una parte del dolor, el placer y las satisfacciones de la vida se encuentran en las cosas materiales. Buscaron proteger a los americanos en sus creencias, sus pensamientos, sus emociones y sus sensaciones. Conferían, en contra del Gobierno, *el derecho a ser dejado en paz - el más completo de los derechos, y el más valorado por los hombres civilizados. Para proteger ese derecho, toda intrusión injustificable del Gobierno en la privacidad del individuo, cualquiera que sea el medio empleado, debe ser considerada una violación de la Cuarta Enmienda.* Y el uso, como evidencia en un proceso criminal, de hechos comprobados por tal intrusión debe ser considerado una violación de la Quinta." <https://www.law.cornell.edu/supremecourt/text/277/438>

⁶ Warren, Samuel D.; Brandeis, Louis D., *The Right to Privacy*, Harvard Law Review, Vol. 4, No. 5. (diciembre 15, 1890), pp. 193-220, disponible en https://www.jstor.org/stable/1321160?seq=2#metadata_info_tab_contents (URL permanente) Consultada el 15 de abril de 2020.

⁷ *Kyllo v. United States*, 533 U.S. 27 (2001): Tras sospechas de que el actor [Kyllo] cultivaba marihuana en su casa, agentes de la policía utilizaron un dispositivo infrarrojo (sin orden judicial) para escanear la casa para determinar si la cantidad de calor que emanaba coincidía con el de las lámparas de alta intensidad típicamente utilizadas para el cultivo de marihuana en interiores. Finalmente, se decidió por mayoría de 5 sobre 4 votos que el uso de un dispositivo infrarrojo, desde un punto de vista público para vigilar la radiación de calor de la casa de una persona consistía en una "pesquisa" (investigación) en el sentido de la Cuarta Enmienda de la Constitución de los Estados Unidos [misma que protege dos derechos fundamentales: el derecho a la privacidad y el derecho a no sufrir una invasión arbitraria], y por lo tanto requería una orden judicial. Caso disponible en <https://www.law.cornell.edu/supct/html/99-8508.ZO.html> Consultada el 15 de abril de 2020.

⁸ SOLOVE, Daniel J.; SCHWARTZ, Paul M., *Information Privacy Law*, 4th Ed., Wolters Kluwer Law & Business, *Information Privacy Law: Origins and types*, P.10-27.

⁹ Tesis: 1a. CCXIV/2009, Registro:165823, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXX, diciembre de 2009, p. 277.

Por su parte, la doctrina mexicana suele acompañar el estudio del derecho de la privacidad con el principio de autodeterminación informativa,¹⁰ por ejemplo, los expertos José Luis Piñar Mañas y Lina Ornelas Núñez señalan:

A él [Alan F. WESTIN] se debe precisamente la definición de privacidad en términos de autodeterminación, de “self determination”, concepto éste que más tarde fue expresamente asumido por el Tribunal Constitucional Federal Alemán en su conocida sentencia de 15 de diciembre de 1983 sobre el Censo, y que también ha sido utilizado por el Tribunal Constitucional español [...].¹¹

De la citada sentencia alemana se desprende que el principio a la autodeterminación informativa refiere que “el titular de los datos es el único que tiene derecho a decidir cómo, cuándo, dónde y por quién se tratan sus datos.”¹² La importancia de este principio se encuadra perfectamente en la reflexión que hizo el expresidente del Tribunal Constitucional Federal Alemán, Dr. Benda, “el peligro para la privacidad del individuo no radica en que se acumule información sobre él sino, más bien, en que pierda la capacidad de disposición sobre ella y respecto a quién y con qué objeto se transmite”.¹³

¹⁰ “La preocupación por los datos personales se da a partir de la Declaración de Teherán de 1968 al establecer en una de sus cláusulas que los avances científicos y tecnológicos son importantes para el desarrollo económico, social y cultural de los países, sin embargo estos avances pueden atentar contra derechos fundamentales; es decir *la autodeterminación informativa surge cuando se fue consciente de que utilizando las nuevas tecnologías era posible almacenar una gran cantidad de información y además de ello se sometía a tratamiento informatizado, dicho tratamiento suponía un riesgo a la intimidad* es por eso que se configura como garantía y medio de defensa para tener control de la información personal que se encuentra en registros públicos y privados almacenados en medios informáticos.” Texto tomado de Álvarez Rodríguez, Lilibeth, “Derecho al Olvido como garantía para la autodeterminación informativa en las redes sociales”, IV Foro Internacional Derechos humanos y tecnologías de la Información y Comunicación (TIC). Disponible en <https://www.repositoriodigital.ipn.mx/bitstream/123456789/3987/1/Memoria%204to%20Foro%20DH TIC%2015.pdf> Consultado el 16 de abril de 2020.

¹¹ Piñar Mañas, José Luis y Ornelas Núñez, Lina (Coord.) “Protección de Datos Personales en México”, Tirant Lo Blanch, México, 2013, Capítulo II, *De los Orígenes a la consideración de la protección de Datos como derecho fundamental*, p. 42-43.

¹² Davara F. De Marcos, Isabel, “El Derecho al Olvido en relación con el derecho a la protección de datos personales”, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, México, 2014, p. 20, disponible en <http://www.infodf.org.mx/capacitacion/publicacionesDCCT/ensayo23/23ensayo2014.pdf> Consultado el 17 de abril de 2020.

¹³ *Idem.*

Por otro lado, Lina Ornelas y José Piñar explican que la propia evolución de la protección de los datos personales siempre ha estado influenciada por las tecnologías de la información y su impacto en el “Derecho a no sufrir injerencias en la vida privada”, siendo éste un derecho que se reguló desde la Declaración Universal de Derechos Humanos o el Pacto Internacional de Derechos Civiles y Políticos de 1966.”¹⁴

En los últimos años, la protección de datos personales ha ido evolucionado de manera importante debido a retos tecnológicos¹⁵ que exponen a la protección de la dignidad humana,¹⁶ al respecto, el informe “Estándares para una Internet Libre, Abierta e Incluyente”, emitido por la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, expone de manera ilustrativa, cinco de los principales desafíos generados o magnificados a partir de internet: a) la protección de datos personales; b) la vigilancia, monitoreo e interceptación; c) la encriptación y el anonimato; d) *big data* y e) Internet de las cosas.¹⁷

Por su parte, el derecho positivo mexicano reconoce el derecho humano a la protección de datos personales, con el propósito de garantizar la privacidad y la prerrogativa a la autodeterminación informativa de las personas en los artículos 6o., apartado A, fracción II y 16, segundo párrafo, constitucionales:

¹⁴ Piñar Mañas, José Luis y Ornelas Núñez, Lina (Coord.), *Op. cit.*

¹⁵ Cfr. cuarto (4) párrafo, de los considerandos del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, *Op. cit.* Disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Consultado el 16 de abril de 2020.

¹⁶ “La dignidad humana la encontramos en muchos instrumentos internacionales empezando por la Declaración Universal de los Derechos Humanos de 1948 en donde se le vincula con la libertad e igualdad, también encontramos referencia en la Declaración y programa de acción de Viena, aprobada el 25 de junio de 1993, la cual afirma que todos los derechos humanos tienen su origen en la dignidad y el valor de la persona humana.” Texto tomado de Álvarez Rodríguez, Lilibeth, “Derecho al Olvido como garantía para la autodeterminación informativa en las redes sociales”, IV Foro Internacional Derechos humanos y tecnologías de la Información y Comunicación (TIC). Disponible en

<https://www.repositoriodigital.ipn.mx/bitstream/123456789/3987/1/Memoria%20to%20Foro%20DH%20TIC%202015.pdf> Consultado el 16 de abril de 2020.

¹⁷ Lanza, Edison, “Estándares para una Internet Libre, Abierta e Incluyente”, Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, Organización de los Estados Americanos, OEA/Ser.L/V/II, CIDH/RELE/INF.17/17, 15 de marzo 2017, p. 80-92, Disponible en http://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf Consultado el 16 de abril de 2020.

Artículo 6o. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.

Párrafo reformado DOF 13-11-2007, 11-06-2013

[...]

A. Para el ejercicio del derecho de acceso a la información, la Federación y las entidades federativas, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

Párrafo reformado (para quedar como apartado A) DOF 11-06-2013.

Reformado DOF 29-01-2016

[...]

II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

...

Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. En los juicios y procedimientos seguidos en forma de juicio en los que se establezca como regla la oralidad, bastará con que quede constancia de ellos en cualquier medio que dé certeza de su contenido y del cumplimiento de lo previsto en este párrafo.

Párrafo reformado DOF 15-09-2017

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de estos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones

de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Por otro lado, en tratándose de derechos humanos, se debe considerar que ningún derecho es absoluto,¹⁸ por ejemplo, el derecho a la privacidad se vincula necesariamente con otros derechos como la libertad de expresión y el derecho a la información. Lo anterior, debido a que la vida privada constituye un límite al ejercicio de estas libertades.

Y es justamente en esta búsqueda de armonización de derechos que nace el Derecho al Olvido, en medio de una tensión de derechos, provocada por el avance y el uso indiscriminado de tecnologías de la comunicación, en donde, por un lado, está el derecho a la información bajo el llamado “derecho a saber” y, por otro lado, está el derecho a la privacidad bajo la protección de datos personales, en donde lo que se busca es que no persista un tratamiento indebido de datos personales.

Aquí, vale la pena citar a Isabel Davara quien hace un análisis de las implicaciones contemporáneas del derecho a la privacidad frente a las tecnologías de la información y establece que:

La privacidad, como dijimos, no puede ser ya hoy entendida como el derecho a ser dejado solo [citando el famoso artículo de WARREN y BRANDEIS], sino que conlleva el poder controlar la información personal, y en concreto el flujo de la misma. La protección de datos personales cambia el paradigma, basándose ahora en la posibilidad del individuo a acceder a su información personal en posesión de cualesquiera terceros, ejerciendo éste un poder de

¹⁸ En la obra “Derechos fundamentales, ponderación y racionalidad” *Revista Iberoamericana de Derecho Procesal Constitucional*, núm. 11, enero-junio 2009, pp. 8-9, el filósofo y jurista Robert Alexy señala que “los derechos fundamentales son mandatos de optimización, como tales son normas de principio que ordenan la realización de algo en la más alta medida, relativamente a las posibilidades materiales y jurídicas. [...] cuando no pueden evitarse los costos o el sacrificio, se hace necesaria una ponderación. [...] “Ley de ponderación”, la cual dice: Como alto sea el grado de incumplimiento o perjuicio de un principio, tanto tiene que ser la importancia de la realización del otro.” Disponible en <https://www.corteidh.or.cr/tablas/r25294.pdf>. Consultado el 17 de abril de 2020.

control sobre los sujetos, públicos o privados, que disponen de sus datos personales.¹⁹

Por otro lado, y siguiendo con la postura de Isabel Davara, se destaca que el derecho a la protección de datos personales, se trata de un derecho independiente y autónomo, lo anterior, a partir de la Sentencia del Tribunal Constitucional Español 292/00 del 30 de noviembre de 2000, misma que asentó jurisprudencia en España, diferenciando este derecho frente al de la intimidad,²⁰ y concluye que “el derecho a la protección de datos personales y a la autodeterminación informativa es un derecho independiente y autónomo, de tercera generación.”²¹

1.2 La Naturaleza del Derecho al Olvido

Luego del apartado anterior, al estudiar la naturaleza jurídica del Derecho al Olvido tenemos que es un derecho de protección de datos personales y a la vez, se trata de un mecanismo que busca garantizar la autodeterminación informativa²² en el

¹⁹ Davara F. De Marcos, Isabel; El Derecho al Olvido en relación con el derecho a la protección de datos personales, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, México, 2014, p. 22, disponible en <http://www.infodf.org.mx/capacitacion/publicacionesDCCT/ensayo23/23ensayo2014.pdf>. Consultado el 17 de abril de 2020.

²⁰ *Ibidem*, p. 25

²¹ *Ibidem*, p. 21.

²² Para mayor referencia se cita una tesis aislada en materia civil del Tercer Tribunal Colegiado en materia Civil del Primer Circuito, que relaciona el derecho a la intimidad con la autodeterminación informativa: “Derecho a la intimidad. Su objeto y relación con el derecho de la autodeterminación de la información. Los textos constitucionales y los tratados internacionales de derechos humanos recogen el derecho a la intimidad como una manifestación concreta de la separación entre el ámbito privado y el público. Así, el derecho a la intimidad se asocia con la existencia de un ámbito privado que se encuentra reservado frente a la acción y conocimiento de los demás y tiene por objeto garantizar al individuo un ámbito reservado de su vida frente a la acción y conocimiento de terceros, ya sea simples particulares o bien los Poderes del Estado; tal derecho atribuye a su titular el poder de resguardar ese ámbito reservado por el individuo para sí y su familia; asimismo garantiza el derecho a poseer la intimidad a efecto de disponer del control sobre la publicidad de la información tanto de la persona como de su familia; lo que se traduce en el derecho de la autodeterminación de la información que supone la posibilidad de elegir qué información de la esfera privada de la persona puede ser conocida o cuál debe permanecer en secreto, así como designar quién y bajo qué condiciones puede utilizar esa información. En este contexto, el derecho a la intimidad impone a los poderes públicos, como a los particulares, diversas obligaciones, a saber: no difundir información de carácter personal entre los que se encuentran los datos personales, confidenciales, el secreto bancario e industrial y en general en no entrometerse en la vida privada de las personas; asimismo, el Estado a través de sus órganos debe adoptar todas las medidas tendentes a hacer efectiva la

entorno digital y, es un derecho que, particularmente, surge de una tensión de derechos entre el derecho a la privacidad y la protección de datos personales frente a la libertad de expresión y el derecho a la información, tal y como se expone enseguida.

El llamado Derecho al Olvido cobró relevancia a partir de mayo de 2014, debido al fallo emitido por el Tribunal de Justicia Europeo en contra del motor de búsqueda Google. Los temas derivados de esta resolución son de gran trascendencia por tratarse del “primer asunto en el que se solicita al Tribunal de Justicia que interprete la Directiva en relación con los motores de búsqueda en Internet, una cuestión aparentemente tónica para las autoridades nacionales de protección de datos y los tribunales de los Estados miembros de la Comunidad Europea.”²³

Las grandes cuestiones que se plantearon fueron el alcance territorial de la aplicación de la Directiva 95/46/CE y el alcance de la definición de tratamiento de datos personales, en donde se buscaba definir si los motores de búsqueda incurrían o no en un tratamiento de datos personales.

Luego de este fallo, el llamado Derecho al Olvido se ha adoptado dentro del derecho positivo europeo y actualmente forma parte del Reglamento General de Protección de Datos (RGPD), el cual determina que los interesados (titulares de datos personales) deben poder tener un Derecho al Olvido si la retención de tales datos es contraria a derecho.

protección de este derecho.” TERCER TRIBUNAL COLEGIADO EN MATERIA CIVIL DEL PRIMER CIRCUITO. Amparo en revisión 73/2008. 6 de mayo de 2008. Mayoría de votos. Disidente: Neófito López Ramos. Ponente: Víctor Francisco Mota Cienfuegos. Secretario: Erick Fernando Cano Figueroa. Tesis: I.3o.C.695 C, Registro: 168944, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXVIII, septiembre de 2008, p. 1253.

²³ Cfr. Asunto C-131/12, Google Spain, S.L., Google Inc. Contra Agencia Española de Protección de Datos (AEPD), Mario Costeja González, sentencia del 13 de Mayo de 2014, Tribunal de Justicia de la Unión Europea Disponible en: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=E S&mode=lst&dir=&occ=first&part=1&cid=384212>. Consultado el 20 de abril de 2020.

En particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse bajo las siguientes circunstancias:²⁴

- Si ya no son necesarios para los fines para los que fueron recogidos,
- Si ahora son tratados de otro modo,
- Si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o
- Si el tratamiento de sus datos personales incumple de otro modo la regulación aplicable.

Como se ha dicho, el Derecho al Olvido busca resolver la tensión de derechos creada entre el ejercicio de la privacidad frente a los derechos de libertad de expresión e información y, en ese sentido, los considerandos del RGPD señalan que la retención ulterior de los datos personales debe ser lícita cuando sea necesaria en cualquiera de los supuestos que se citan enseguida:²⁵

- (a) Para el ejercicio de la libertad de expresión e información,
- (b) Para el cumplimiento de una obligación legal,
- (c) Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento,
- (d) Por razones de interés público en el ámbito de la salud pública,
- (e) Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o
- (f) Para la formulación, el ejercicio o la defensa de reclamaciones.

1.3 Crítica al concepto del Derecho al Olvido

La gran paradoja a la que se enfrenta el concepto del Derecho al Olvido es que se diseñó como una medida jurídica frente a un medio que nada olvida. Como es bien sabido, la propia arquitectura de Internet es descentralizada, ubicua, híper accesible

²⁴ Ver Artículo 17 del Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo. Disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=EN> Consultado el 16 de abril de 2020.

²⁵ Cfr. Párrafo sesenta y cinco (65), de los considerandos del Reglamento (UE) 2016/679 Del Parlamento Europeo y Del Consejo, *Op. cit.* Disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Consultado el 16 de abril de 2020.

y su diseño favorece la perennidad de la información, es decir, el concepto impone una paradoja, dado que existe una imposibilidad material de borrar permanentemente cualquier información o contenido.

Sin duda alguna, el nombre surgió en el marco de una tensión entre el derecho a la privacidad y el derecho a la información, por lo que puede considerarse que el concepto del Derecho al Olvido busca poner énfasis en el elemento temporal que hace referencia a hechos del pasado, es decir, el concepto tenía que adaptarse a una semántica que fuera compatible con una sociedad democrática en donde la definición no hiciera ruido con la legitimación de un derecho al borrado de información en un entorno digital que vela por un derecho a saber.

Sirve mencionar que la nueva regulación en materia de Protección de Datos en Europa, el Reglamento general de protección de datos (RGPD), que entró en vigor el pasado 25 de mayo de 2018, al regular esta figura la denominó Derecho de supresión (el Derecho al Olvido), en su artículo 17.

Se considera que el Derecho al Olvido no es otra cosa más que el ejercicio de los derechos de cancelación y oposición aludiendo al elemento de temporalidad y aplicado a un entorno digital, en donde el ejercicio de estos derechos debe ser congruente con los principios de finalidad y calidad.

1.4 El Derecho al Olvido en México

1.4.1. Generalidades de la Protección de Datos Personales en México

En el año 2009, hubo una reforma constitucional que fue histórica en materia de Datos Personales, ya que fue la primera vez que se reconoció como derecho humano la protección a los datos personales, incorporando tal derecho en el artículo 16º de la Constitución política de los Estados Unidos Mexicanos:

Artículo 16: [...] Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a

manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Párrafo adicionado DOF 01-06-2009

Posteriormente, el 5 de julio de 2010, se publicó en el Diario Oficial de la Federación, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y el 21 de diciembre de 2011, se publicó el Reglamento respectivo.

Y bien, la regulación mexicana en materia de protección de datos personales (en lo que toca a las entidades privadas), se basa en los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.²⁶ Estos principios se traducen en obligaciones para el responsable y deben ser observados en todas las fases del tratamiento.

Ahora bien, los principios en materia de Protección de Datos Personales posibilitan el ejercicio de los derechos de los titulares del dato, es decir, los derechos de Acceso, Rectificación, Cancelación y Oposición (en adelante, “Derechos ARCO”), mismos que se encuentran consagrados en el artículo 16 Constitucional.

Por otro lado, vale la pena señalar que para la vigilancia del cumplimiento de los *Derechos ARCO*, la LFPDPPP establece un *procedimiento de protección de derechos* (artículos 45 al 58 de la LFPDPPP), el cual inicia con una solicitud presentada ante el responsable del tratamiento de los datos y a falta de respuesta o si el titular del dato no se está conforme con ella, el titular de los datos puede acudir vía procedimiento de protección de derechos ante el citado Instituto.²⁷

²⁶ Cfr. Artículo 6 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

²⁷ Cfr. Artículos 45 a 58 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Contra las resoluciones que emita el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), los particulares pueden promover un juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa (TFJA),²⁸ sin embargo, recientemente se publicó una tesis aislada en donde se señala que el TFJA carece de competencia para conocer de las demandas promovidas contra las resoluciones emitidas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, al ser éste un organismo constitucional autónomo, por lo que habrá que seguir con atención el progreso que pueda tener este criterio.²⁹

1.4.2 Principios relacionados con el Derecho al Olvido

Particularmente, este estudio está estrechamente relacionado con los principios de calidad y finalidad, de ahí que vale la pena profundizar en los alcances de estos principios:

1.4.2.1. Calidad

Este principio se encuentra previsto en los artículos 11 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y 36 del Reglamento:

Ley Federal de Protección de Datos Personales en Posesión de los Particulares

²⁸ Cfr. Artículo 56 de la LFPDPPP. Cabe señalar que el Tribunal es administrativo y no pertenece al Poder Judicial de la Federación.

²⁹ Tesis: I.5o.A.13 A (10a.), Registro: 2020767, Semanario Judicial de la Federación y su Gaceta, Décima Época, t. I.5o.A.13 A (10a.), Libro 71, Octubre de 2019, Tomo IV, p. 3640. Tribunal Federal De Justicia Administrativa. Carece de competencia para conocer de las demandas promovidas contra las resoluciones emitidas por el instituto nacional de transparencia, acceso a la información y protección de datos personales, al ser éste un organismo constitucional autónomo. Amparo directo 669/2018. Google México, S. de R.L. de C.V. 5 de junio de 2019. Unanimidad de votos. Ponente: Pablo Domínguez Peregrina. Secretario: David Caballero Franco. *Nota: Esta tesis es objeto de la denuncia relativa a la contradicción de tesis 525/2019, pendiente de resolverse por la Segunda Sala.*

Artículo 11.- El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.

Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados.

El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.

[Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares]

Artículo 36. Se cumple con el principio de calidad cuando los datos personales tratados sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.

Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por el titular, y hasta que éste no manifieste y acredite lo contrario, o bien, el responsable cuente con evidencia objetiva que los contradiga.

Cuando los datos personales no fueron obtenidos directamente del titular, el responsable deberá adoptar medidas razonables para que éstos respondan al principio de calidad, de acuerdo con el tipo de datos personales y las condiciones del tratamiento.

El responsable deberá adoptar los mecanismos que considere necesarios para procurar que los datos personales que trate sean exactos, completos, pertinentes, correctos y actualizados, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que el titular se vea afectado por dicha situación.

Considerando que los principios son una obligación con la que debe cumplir el responsable del tratamiento³⁰, del principio de calidad se advierten las siguientes obligaciones:

(a) El responsable debe tratar datos personales que sean exactos, completos, pertinentes, correctos y actualizados de conformidad con las finalidades.³¹

(b) Cuando los datos son obtenidos indirectamente³² del titular, el responsable deberá adoptar los mecanismos necesarios a fin de que no se altere la veracidad de los datos, sin embargo, cuando los datos son obtenidos de manera directa,³³ opera una presunción legal a favor del responsable y se entenderá que cumple con el principio de calidad.

³⁰ El responsable es la persona física o moral de carácter privado que decide sobre el tratamiento de datos personales en términos del artículo 3 de la LFPDPPP.

³¹ Las siguientes definiciones fueron tomadas de la Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, INAI, p. 56. Disponible en: http://inicio.ifai.org.mx/DocumentosdelInteres/Guia_obligaciones_lfpdppp_junio2016.pdf. Consultada el 19 de abril de 2020.

- Los datos personales son *exactos* cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles. Por ejemplo, un dato no sería exacto si se registra en la base de datos que una persona cuenta con Doctorado en derecho, si el título que en realidad tiene es una Maestría en derecho.
- Los datos personales están *completos* cuando no falta ninguno de los que se requiera para las finalidades para las cuales se obtuvieron y son tratados, de forma tal que no se cause un daño o perjuicio al titular. Por ejemplo, los datos de salud del titular están completos cuando el expediente médico contiene todos los documentos clínicos e información que debe estar integrada al mismo.
- Los datos personales son *pertinentes* cuando corresponden efectivamente al titular. Por ejemplo, los datos del adeudo son pertinentes cuando corresponden al deudor y no a una homonimia.
- Los datos están *actualizados* cuando están al día y corresponden a la situación real del titular. Por ejemplo, el número telefónico que se tiene registrado en la base de datos está actualizado cuando, efectivamente, corresponde al titular con el que está vinculado.
- Los datos personales son *correctos* cuando cumplen con todas las características anteriores, es decir, son exactos, completos, pertinentes y actualizados.

³² De acuerdo con el artículo tercero, fracción IV, de los Lineamientos del Aviso de Privacidad “Obtener los datos personales de forma indirecta” se refiere al acto en el cual el responsable obtiene los datos personales sin que el titular se los haya proporcionado de forma personal o directa, como por ejemplo a través de una fuente de acceso público o una transferencia.

³³ De acuerdo con el artículo tercero, fracción III, de los Lineamientos del Aviso de Privacidad “Obtener los datos personales de forma directa de su titular” se refiere al acto en el cual el propio titular proporciona los datos personales por algún medio que permite su entrega directa al responsable, entre ellos, medios electrónicos, ópticos, sonoros, visuales o cualquier otra tecnología, como correo postal, internet o vía telefónica, entre otros.

(c) El responsable tiene la obligación de cancelar los datos personales cuando dejen de ser necesarios para las finalidades previstas o bien por disposición legal.

(d) El responsable tiene la obligación eliminar la información después de setenta y dos meses contados a partir de la fecha calendario en que se presente el mencionado incumplimiento.

El Diccionario del INAI por su parte, sostiene que los alcances del principio de calidad se reducen a lo siguiente:³⁴

a) el responsable del tratamiento debe adoptar las medidas necesarias a su alcance para mantener los datos personales en su posesión exactos, completos, correctos y actualizados a fin de que no se altere su veracidad, y

b) el responsable debe proceder a la cancelación de los datos personales cuando han dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables.

De este análisis se desprende que el principio de calidad está estrechamente vinculado a los principios de finalidad y proporcionalidad, además, este principio también responde a uno de los Derechos ARCO³⁵, especialmente, al derecho de cancelación, mismo será detallado en las siguientes más adelante.

Por último, conviene señalar que el principio de calidad que recoge la legislación mexicana tiene alcances muy similares a los previstos en los Estándares de Protección de Datos para los Estados Iberoamericanos ("Estándares")³⁶ emitidos

³⁴ Davara F. De Marcos, Isabel, Coord., "Diccionario de Protección de Datos Personales, Conceptos fundamentales", Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), noviembre 2019, México, p. 649, disponible en http://inicio.ifai.org.mx/PublicacionesComiteEditorial/DICCIONARIO_PDP_digital.pdf. Consultado el 20 de abril de 2020.

³⁵ Derechos de Acceso, Rectificación, Cancelación y Oposición.

³⁶ El 20 de junio de 2017, la Red Iberoamericana de Protección de Datos (RIPD) aprobó los Estándares de Protección de Datos para los Estados Iberoamericanos, esto implica que, por primera vez, los Estados Iberoamericanos cuentan con una base normativa para crear un marco jurídico común y regional de protección de datos personal, los estándares están disponibles en https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logos_RIPD.pdf. Consultada el 18 de abril de 2020.

por la Red Iberoamericana de Protección de Datos en el año 2017, tal y como se muestra enseguida:

Artículo 19. Principio de Calidad

19.1. El responsable adoptará las medidas necesarias para mantener exactos, completos y actualizados los datos personales en su posesión, de tal manera que no se altere la veracidad de éstos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento.

19.2. Cuando los datos personales hubieren dejado de ser necesarios para el cumplimiento de las finalidades que motivaron su tratamiento, el responsable los suprimirá o eliminará de sus archivos, registros, bases de datos, expedientes o sistemas de información, o en su caso, los someterá a un procedimiento de anonimización.

19.3. En la supresión de los datos personales, el responsable implementará métodos y técnicas orientadas a la eliminación definitiva y segura de éstos.

1.4.2.2. Finalidad

Este principio se encuentra previsto en los artículos 12 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y 40 a 43 del Reglamento:

Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Artículo 12.- El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos en aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular.

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Artículo 40. Los datos personales solo podrán ser tratados para el cumplimiento de la finalidad o finalidades establecidas en el aviso de privacidad, en términos del artículo 12 de la Ley.

Para efectos del párrafo anterior, la finalidad o las finalidades establecidas en el aviso de privacidad deberán ser determinadas, lo cual se logra cuando con claridad, sin lugar a confusión y de manera objetiva se especifica para qué objeto serán tratados los datos personales.

Diferenciación de finalidades

Artículo 41. El responsable identificará y distinguirá en el aviso de privacidad entre las finalidades que dieron origen y son necesarias para la relación jurídica entre el responsable y el titular, de aquéllas que no lo son.

Oposición del tratamiento para finalidades distintas

Artículo 42. El titular podrá negar o revocar su consentimiento, así como oponerse para el tratamiento de sus datos personales para las finalidades que sean distintas a aquéllas que son necesarias y den origen a la relación jurídica entre el responsable y el titular, sin que ello tenga como consecuencia la conclusión del tratamiento para estas últimas finalidades.

Tratamiento para finalidades distintas

Artículo 43. El responsable no podrá llevar a cabo tratamientos para finalidades distintas que no resulten compatibles o análogas con aquéllas para las que hubiese recabado de origen los datos personales y que hayan sido previstas en el aviso de privacidad, a menos que:

I. Lo permita de forma explícita una ley o reglamento, o

II. El responsable haya obtenido el consentimiento para el nuevo tratamiento.

Tal como se mencionó anteriormente, los principios implican obligaciones para el responsable del tratamiento, así conviene citar las obligaciones que propone la Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares del INAI, entorno al principio de finalidad:³⁷

1. Tratar los datos personales únicamente para la finalidad o finalidades que hayan sido informadas al titular en el aviso de privacidad y, en su caso, consentidas por éste;
2. Informar en el aviso de privacidad todas las finalidades para las cuales se tratarán los datos personales, y redactarlas de forma tal que sean determinadas;³⁸,
3. Identificar y distinguir en el aviso de privacidad entre las finalidades primarias y secundarias;³⁹
4. Ofrecer al titular de los datos personales un mecanismo para que pueda manifestar su negativa al tratamiento de sus datos personales para todas o algunas de las finalidades secundarias;⁴⁰
5. Cuando el aviso de privacidad se dé a conocer a través de un medio indirecto, como el correo postal, informar al titular que tiene cinco días hábiles para manifestar su negativa para el tratamiento de su información para finalidades secundarias;

³⁷ INAI. (2016, junio). Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, p. 23.

³⁸ Cfr. LINEAMIENTOS del Aviso de privacidad, Artículo Vigésimo cuarto, fracción I, “el listado de finalidades descritas deberá ser completo y no utilizar frases inexactas, ambiguas o vagas, como “entre otras finalidades”, “otros fines análogos” o “por ejemplo””; y fracción III “En el listado de finalidades se deberán incluir las relativas al tratamiento con fines de mercadotecnia, publicidad o prospección comercial, en caso de que el responsable trate los datos personales para dichos fines;”

³⁹ *Ibidem*, fracción IV, “Se deberá identificar y distinguir entre las finalidades que dieron origen y son necesarias para la existencia, mantenimiento y cumplimiento de la relación jurídica entre el responsable y titular, de aquéllas que no lo son,”

⁴⁰ *Ibidem*, fracción V, “Se deberá informar sobre el mecanismo que el responsable tiene implementado para que el titular pueda manifestar su negativa para el tratamiento de sus datos personales con relación a las finalidades que no son necesarias para la relación jurídica entre el responsable y titular.”

6. No condicionar el tratamiento para finalidades primarias, a que se puedan llevar a cabo las finalidades secundarias;

7. Tratar los datos personales para finalidades distintas que no resulten compatibles o análogas con aquéllas para las que se hubiese recabado de origen los datos personales y que hayan sido previstas en el aviso de privacidad, al menos que lo permita una ley o reglamento, o se obtenga el consentimiento del titular de los datos.

A su vez en el Diccionario del INAI antes citado, se refieren al principio de finalidad como un principio toral, al considerar que del efectivo cumplimiento de este principio depende la verificación de los principios de calidad, consentimiento y proporcionalidad y, en consecuencia, se alcanza la consecución de los otros principios: licitud, lealtad y la responsabilidad:

Este principio es toral porque va a definir la eficiencia y eficacia del resto de los principios, pues su especificación determinará la viabilidad del tratamiento en su conjunto. Es decir, si la finalidad no está legítimamente determinada, el consentimiento se verá viciado, pues se presta respecto de ésta. La calidad también estará cuestionada, puesto que solo que se podrá definir si los datos cumplen con la calidad respecto de la finalidad del tratamiento, ya que no hay datos correctos, actualizados o pertinentes en abstracto, sino respecto de una finalidad, lo mismo podemos decir del principio de proporcionalidad o de minimización.⁴¹ Por lo tanto, la finalidad define el tratamiento y con ello su licitud, lealtad y la responsabilidad de quien lo lleva a cabo.⁴²

De igual modo, el principio de finalidad, que recoge la legislación mexicana tiene alcances muy similares a los previstos en los Estándares de Protección de

⁴¹ A juicio de la autora de este estudio, conforme a la legislación Mexicana, la minimización no es un principio, sino un criterio en el tratamiento de datos personales que definitivamente está estrechamente relacionado con el principio de proporcionalidad. Cfr. Artículo 46 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares: (Criterio de minimización) El responsable deberá realizar esfuerzos razonables para que los datos personales tratados sean los mínimos necesarios de acuerdo con la finalidad del tratamiento que tenga lugar. A diferencia del RGPD en donde sí está regulado como un principio.

⁴² Davara F. De Marcos, Isabel, Coord., "Diccionario...", *Op. cit.* p. 656, disponible en http://inicio.ifai.org.mx/PublicacionesComiteEditorial/DICCIONARIO_PDP_digital.pdf. Consultado el 20 de abril de 2020.

Datos para los Estados Iberoamericanos ("Estándares")⁴³ emitidos por la Red Iberoamericana de Protección de Datos en el año 2017, el cambio sustancial es que se agrega el elemento de finalidades "legítimas" tal y como se muestra enseguida:

Principio de finalidad

17.1. Todo tratamiento de datos personales se limitará al cumplimiento de finalidades determinadas, explícitas y legítimas.

17.2. El responsable no podrá tratar los datos personales en su posesión para finalidades distintas a aquéllas que motivaron el tratamiento original de éstos, a menos que concurra alguna de las causales que habiliten un nuevo tratamiento de datos conforme al principio de legitimación.

17.3. El tratamiento ulterior de datos personales con fines archivísticos, de investigación científica e histórica o con fines estadísticos, todos ellos, en favor del interés público, no se considerará incompatible con las finalidades iniciales.

1.4.3 Derecho al Olvido frente a los derechos de cancelación y oposición

Se ha buscado encasillar el Derecho al Olvido entre alguna figura jurídica existente en materia de protección de datos personales y así se ha asociado con los Derechos de Cancelación y de Oposición puesto que son los derechos más relacionados con el principio de calidad del dato.

Oscar Guerra Ford (comisionado del INAI), ha señalado que el Derecho al Olvido es una figura que legalmente no está reglamentada, pero que es posible

⁴³ Estándares de Protección de Datos para los Estados Iberoamericanos, RIPD, 2017, disponibles en https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf. Consultada el 18 de abril de 2020.

materializarlo mediante el ejercicio del derecho a la cancelación u oposición de datos personales, que forman parte de los denominados Derechos ARCO.⁴⁴

Por su parte, Isabel Davara señala que “la normatividad de protección de datos personales que nos ocupa busca garantizar el respeto a la privacidad y a la autodeterminación informativa, esto es, la capacidad de los individuos de decidir qué es lo que se hace con su información y, en relación con el Derecho al Olvido, se concreta especialmente en relación con el límite temporal de tratamiento de dicha información.”⁴⁵ Refiere que el Derecho al Olvido puede estar amparado, por su semejanza, con el derecho a la cancelación o, en su caso, con el derecho de oposición, derechos dentro de los denominados ARCO [...].⁴⁶ De ahí que, en este apartado se estudian los derechos de cancelación y oposición puntualmente para después compararlos frente al Derecho al Olvido.

1.4.3.1. Derecho de Cancelación

El derecho de cancelación es el derecho que mayor relación guarda con el Derecho al Olvido debido a que el resultado material de la aplicación de este derecho provoca la supresión del dato. En la legislación mexicana se encuentra regulado principalmente en los artículos 25 y 26 de la Ley Federal de Protección de Datos Personales en posesión de Particulares, de donde se desprenden conceptos como el “periodo de bloqueo” y “plazos de conservación, lo que se explica más adelante, sin embargo, para efectos prácticos se propone una explicación de los alcances del derecho de cancelación a través del siguiente cuadro:

⁴⁴ “Ponderación y equilibrio entre los derechos al olvido y de información, plantean expertos”, Comunicado del INAI, no. INAI/226/16, 23 de agosto de 2016, disponible <http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-226-16.pdf>. Consultado el 25 de abril de 2020.

⁴⁵ Davara F. De Marcos, Isabel; “El Derecho al Olvido...” *Op. cit.* p. 33, disponible en <http://www.infodf.org.mx/capacitacion/publicacionesDCCT/ensayo23/23ensayo2014.pdf>. Consultado el 17 de abril de 2020.

⁴⁶ *Ibidem.* p.34

CANCELACIÓN DE DATOS	
¿Cuándo procede? ⁴⁷	<ul style="list-style-type: none"> • Cuando el titular del derecho opta por cancelar los datos • Cuando el titular considere que los mismos no están siendo tratados conforme a la ley • Cuando finalice el tratamiento de datos personales • Por mandamiento judicial <p>La cancelación procede respecto de la totalidad de los datos o solo parte de ellos, según se haya solicitado.</p>
Qué debe hacerse ⁴⁸	<p>Si procede la solicitud de Cancelación o si ya concluyó el tratamiento de datos personales:</p> <ul style="list-style-type: none"> • Se debe avisar al tercero al que se haya transmitido el dato para que proceda a cancelarlo • Se debe iniciar de manera inmediata con el periodo de bloqueo⁴⁹ • El periodo del bloqueo dura lo que el plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento • Después del periodo de bloqueo se procederá a la supresión del dato. • Una vez cancelado el dato se dará aviso al titular
No es obligado cancelar datos cuando ⁵⁰	<ul style="list-style-type: none"> • Se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento;

⁴⁷ Cfr. artículo 25 LFPDPPP: El titular tendrá en todo momento el derecho a cancelar sus datos personales.

La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. El responsable podrá conservarlos exclusivamente para efectos de las responsabilidades nacidas del tratamiento. El periodo de bloqueo será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en los términos de la Ley aplicable en la materia.

Una vez cancelado el dato se dará aviso a su titular.

Cuando los datos personales hubiesen sido transmitidos con anterioridad a la fecha de rectificación o cancelación y sigan siendo tratados por terceros, el responsable deberá hacer de su conocimiento dicha solicitud de rectificación o cancelación, para que proceda a efectuarla también.

[Ejercicio del derecho de cancelación] RLFPDPPP: Artículo 106. El titular podrá solicitar en todo momento al responsable la cancelación de los datos personales cuando considere que los mismos no están siendo tratados conforme a los principios y deberes que establece la Ley y el presente Reglamento.

La cancelación procederá respecto de la totalidad de los datos personales del titular contenidos en una base de datos, o solo parte de ellos, según lo haya solicitado.

⁴⁸ *Idem.*

⁴⁹ Sobre el Bloqueo, confrontar los artículos 107 y 108 del RLFPDPPP

⁵⁰ Cfr. Artículo 26 LFPDPPP: El responsable no estará obligado a cancelar los datos personales cuando:

	<ul style="list-style-type: none"> • Deban ser tratados por disposición legal; • Obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas; • Sean necesarios para proteger los intereses jurídicamente tutelados del titular; • Sean necesarios para realizar una acción en función del interés público; • Sean necesarios para cumplir con una obligación legalmente adquirida por el titular, y • Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto.
<p>Medidas de Seguridad (administrativas, técnicas y físicas)^{51,52}</p>	<ul style="list-style-type: none"> • Definir alcances, objetivos y políticas, en el tratamiento de datos personales, incluidos los procesos que requieran borrado seguro.⁵³ • Tener un inventario de los datos personales en los sistemas de tratamiento. • Gestionar los medios de almacenamiento involucrados en el tratamiento de • datos personales. • Establecer plazos de conservación de los datos personales y de los medios de almacenamiento. • Tener una visión de las responsabilidades legales y contractuales que se tienen sobre el resguardo y eliminación de los medios de almacenamiento.

I. Se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento;

II. Deban ser tratados por disposición legal;

III. Obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas;

IV. Sean necesarios para proteger los intereses jurídicamente tutelados del titular;

V. Sean necesarios para realizar una acción en función del interés público;

VI. Sean necesarios para cumplir con una obligación legalmente adquirida por el titular, y

VII. Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto.

⁵¹ El deber de seguridad establece la obligación del responsable del tratamiento de implementar y mantener medidas de seguridad administrativas, técnicas y físicas, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

⁵² Guía para el Borrado Seguro de Datos Personales publicada por el INAI Disponible en http://inicio.ifai.org.mx/DocumentosdelInteres/Guia_Borrado_Seguro_DP.pdf. Consultada el 24 de abril de 2020.

⁵³ El borrado seguro es la medida de seguridad mediante la cual se establecen métodos y técnicas para la eliminación definitiva de los datos personales, de modo que la probabilidad de recuperarlos sea mínima. *Cfr.* Guía para el Borrado Seguro de Datos Personales publicada por el INAI, *Op. cit.*

- Contar con revisiones y auditorías para validar los procesos de borrado seguro.
- Documentar los procesos que requieran borrado seguro de los datos personales.

Cuadro 1. Derecho de Cancelación en México.

Fuente: Elaboración propia.

Del derecho de cancelación se derivan las siguientes obligaciones para el responsable del tratamiento y en su caso, el encargado, lo que se desarrolla enseguida:

- Atender la solicitud de cancelación en los términos de la ley
- Cumplir con el plazo de conservación de los datos personales
- Implementar operativamente el bloqueo de datos personales
- Verificados los plazos de conservación y de bloqueo, deberá suprimir los datos de forma segura

Estudio del plazo de conservación de los datos personales

De acuerdo con la Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares del INAI, el plazo de conservación de los datos personales no debe exceder el tiempo estrictamente necesario para llevar a cabo las finalidades que justificaron el tratamiento, ni aquél que se requiera para cumplir con (i) las disposiciones legales aplicables en la materia de que se trate;⁵⁴ (ii) los aspectos administrativos,

⁵⁴ En relación con el plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en los términos de la Ley aplicable en la materia se señala que esto debe ser revisado caso por caso, de acuerdo con la ley aplicable, pero a manera ejemplificativa, se señala que el Código Civil Federal establece los siguientes plazos de prescripción negativa:

Artículo 1159.- Fuera de los casos de excepción, se necesita el lapso de diez años, contado desde que una obligación pudo exigirse, para que se extinga el derecho de pedir su cumplimiento.

Artículo 1161.- Prescriben en dos años:

I. Los honorarios, sueldos, salarios, jornales u otras retribuciones por la prestación de cualquier servicio. La prescripción comienza a correr desde la fecha en que dejaron de prestarse los servicios;
II. La acción de cualquier comerciante para cobrar el precio de objetos vendidos a personas que no fueren revendedoras.

La prescripción corre desde el día en que fueron entregados los objetos, si la venta no se hizo a plazo;

III. La acción de los dueños de hoteles y casas de huéspedes para cobrar el importe del hospedaje; y la de éstos y la de los fondistas para cobrar el precio de los alimentos que ministren.

La prescripción corre desde el día en que debió ser pagado el hospedaje, o desde aquel en que se ministraron los alimentos;

contables, fiscales, jurídicos e históricos de la información, y (iii) el periodo de bloqueo.⁵⁵

Lo anterior se desprende de la interpretación armónica los artículos, 25 de la Ley Federal de Protección de Datos Personales en posesión de Particulares, así como de los artículos 37, 38 y 39 del Reglamento:

Ley Federal de Protección de Datos Personales en posesión de Particulares

Artículo 25: El titular tendrá en todo momento el derecho a cancelar sus datos personales.

La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. El responsable podrá conservarlos exclusivamente para efectos de las responsabilidades nacidas del tratamiento. El periodo de bloqueo será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en los términos de la Ley aplicable en la materia.

Una vez cancelado el dato se avisará a su titular.

Cuando los datos personales hubiesen sido transmitidos con anterioridad a la fecha de rectificación o cancelación y sigan siendo tratados por terceros, el responsable deberá hacer de su conocimiento dicha solicitud de rectificación o cancelación, para que proceda a efectuarla también.

Reglamento de la Ley Federal de Protección de Datos Personales en posesión de Particulares

IV. La responsabilidad civil por injurias ya sean hechas de palabra o por escrito, y la que nace del daño causado por personas o animales, y que la ley impone al representante de aquéllas o al dueño de éstos.

La prescripción comienza a correr desde el día en que se recibió o fue conocida la injuria o desde aquel en que se causó el daño;

V. La responsabilidad civil proveniente de actos ilícitos que no constituyan delitos. La prescripción corre desde el día en que se verificaron los actos.

⁵⁵ Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, INAI, p. 57. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf. Consultada el 19 de abril de 2020.

Plazos de conservación de los datos personales

Artículo 37. Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron el tratamiento, y deberán atender las disposiciones aplicables a la materia de que se trate, y tomar en cuenta los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información. Una vez cumplida la o las finalidades del tratamiento, y cuando no exista disposición legal o reglamentaria que establezca lo contrario, el responsable deberá proceder a la cancelación de los datos en su posesión previo bloqueo de los mismos, para su posterior supresión.

Procedimientos para conservación, bloqueo y supresión de los datos personales

Artículo 38. El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales, que incluyan los periodos de conservación de los mismos, de conformidad con el artículo anterior.

Prueba del cumplimiento de los plazos de conservación

Artículo 39. Al responsable le corresponde demostrar que los datos personales se conservan o, en su caso, bloquean, suprimen o cancelan cumpliendo los plazos previstos en el artículo 37 del presente Reglamento, o bien, en atención a una solicitud de derecho de cancelación.

Por otro lado, se destaca que el Código Civil Federal dispone que, fuera de los casos de excepción, las acciones civiles para ejercer el derecho a pedir el cumplimiento de una obligación prescriben en el lapso de 10 años, contados desde que una obligación pudo exigirse (artículo 1159) o 2 años cuando se tratan de acciones por responsabilidad civil proveniente de actos ilícitos que no constituyan delitos, contado desde el día en que se verificaron los actos (artículo 1161).

Por su parte el Código de Comercio, en sus artículos 38 y 49, impone a los comerciantes un plazo de conservación de diez años de los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones.⁵⁶

Por otro lado, debe considerarse que la conservación de la información se debe hacer de conformidad con la Norma Oficial Mexicana NOM-151-SCFI-2016,⁵⁷ que establece los “Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos” en vigor desde el 28 de septiembre de 2017. Lo anterior se explica gráficamente con el siguiente esquema:



Figura 1. Diagrama sobre el Plazo de conservación.
Fuente: Elaboración propia.

⁵⁶ Código de Comercio:

Artículo 38.- El comerciante deberá conservar, debidamente archivados, los comprobantes originales de sus operaciones, en formato impreso, o en medios electrónicos, ópticos o de cualquier otra tecnología, siempre y cuando, en estos últimos medios, se observe lo establecido en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emita la Secretaría, de tal manera que puedan relacionarse con dichas operaciones y con el registro que de ellas se haga, y deberá conservarlos por un plazo mínimo de diez años.

Artículo 49.- Los comerciantes están obligados a conservar por un plazo mínimo de diez años los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones. Para efectos de la conservación o presentación de originales, en el caso de mensajes de datos, se requerirá que la información se haya mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta. La Secretaría de Economía emitirá la Norma Oficial Mexicana que establezca los requisitos que deberán observarse para la conservación de mensajes de datos.

⁵⁷ NOM-151-SCFI-2016 Este documento define los requisitos que deben ser analizados para la digitalización de documentos y conservación de mensajes de datos, conforme a lo establecido en los artículos 33, 34, 38, 46 bis, 49 y 89 del Código de Comercio y cancela la NOM-151-SCFI-2002. Disponible en http://dof.gob.mx/nota_detalle.php?codigo=5478024&fecha=30/03/2017. Consultada el 23 de abril de 2020.

Por último, conviene citar un ejemplo que propone el INAI en la Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares:

Por ejemplo: En la Norma Oficial Mexicana NOM-004-SSA3-2012, Del expediente clínico, se señala en su apartado 5.4 que “[...] por tratarse de documentos elaborados en interés y beneficio del paciente, deberán ser conservados por un periodo mínimo de 5 años, contados a partir de la fecha del último acto médico”. En ese sentido, supongamos que una persona es paciente del Dr. Pérez por 10 años, entonces el Doctor tendría que conservar los datos personales contenidos en el expediente médico, por esos 10 años, más los cinco que establece la Norma, más el periodo de bloqueo (se explicará más adelante qué es el bloqueo), suponiendo que no hay plazos administrativos, contables, fiscales, jurídicos o históricos adicionales.

Ahora bien, es importante señalar que, en particular, el artículo 11 de la LFPDPPP establece la obligación del responsable de eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contados a partir de la fecha en que se presente el mencionado incumplimiento.⁵⁸

El Periodo de bloqueo

Ley Federal de Protección de Datos Personales en posesión de Particulares:

Artículo 3.- Para los efectos de esta Ley, se entenderá por: [...]

III. Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo,

⁵⁸ Guía para cumplir con los principios y deberes... *Op. cit.* p. 57-58. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf. Consultada el 19 de abril de 2020.

los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponde.

Reglamento de la Ley Federal de Protección de Datos Personales en posesión de Particulares:

Bloqueo

Artículo 107. De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá:

I. Establecer un periodo de bloqueo con el único propósito de determinar posibles responsabilidades en relación con su tratamiento hasta el plazo de prescripción legal o contractual de éstas, y notificarlo al titular o a su representante en la respuesta a la solicitud de cancelación, que se emita dentro del plazo de veinte días que establece el artículo 32 de la Ley;

II. Atender las medidas de seguridad adecuadas para el bloqueo;

III. Llevar a cabo el bloqueo en el plazo de quince días que establece el artículo 32 de la Ley, y

IV. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas por el responsable.

Propósitos del bloqueo

Artículo 108. En términos del artículo 3, fracción III de la Ley, el bloqueo tiene como propósito impedir el tratamiento, a excepción del almacenamiento, o posible acceso por persona alguna, salvo que alguna disposición legal prevea lo contrario.

El periodo de bloqueo será hasta el plazo de prescripción legal o contractual correspondiente.

Supresión:

Obligaciones del encargado

Artículo 50. El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: [...]

V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, [...]

Lo anterior se puede explicar gráficamente con el siguiente esquema:

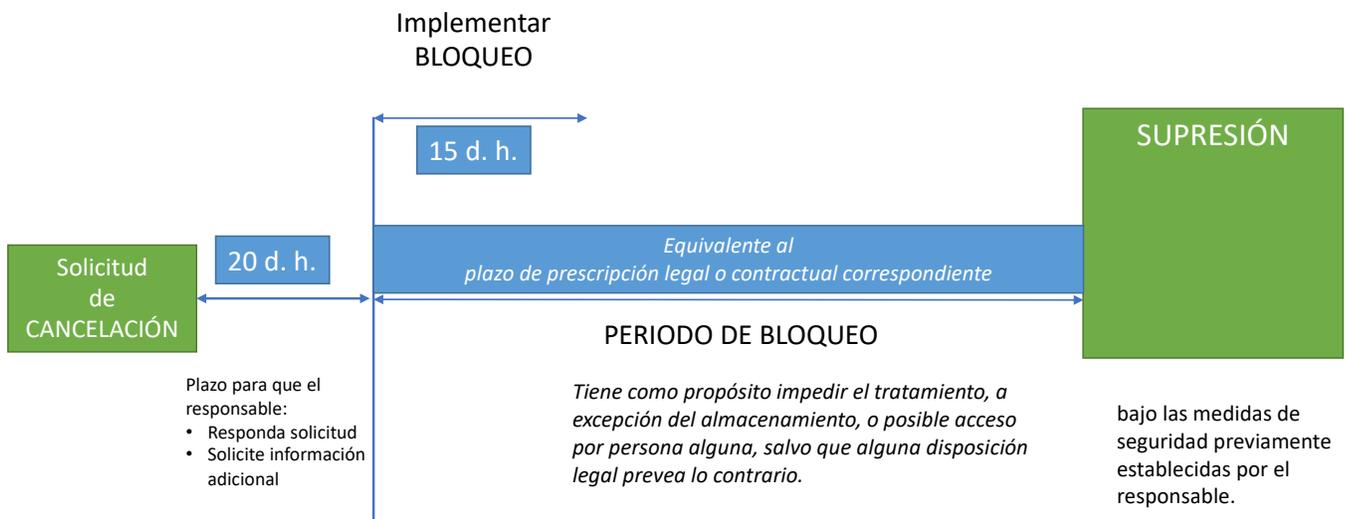


Figura 2. Procedimiento de cancelación, bloqueo y supresión.
Fuente: Elaboración propia.

Por último, se destaca que en el marco internacional se tienen las siguientes disposiciones que regulan el derecho de cancelación:

Derecho de Cancelación en documentos internacionales	
Resolución de Madrid 2009.	Art. 17: frente a datos que “pudieran resultar incompletos, inexactos, innecesarios o excesivos” ⁵⁹
Estándares de Protección de Datos de	27.1. El titular tendrá derecho a solicitar la cancelación o supresión de sus datos personales de los archivos,

⁵⁹ *Idem*

los Estados Iberoamericanos, 2017 ⁶⁰	registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.
Convenio 108	<p>Artículo 9 - Derechos del interesado</p> <p>1. Todo individuo tendrá un derecho: ...</p> <p>e. Obtener, previa solicitud, gratuitamente y sin demora excesiva, la rectificación o la supresión, según sea el caso, de esos datos si se están procesando o han sido procesados en contra de las disposiciones de la presente Convención;</p>

Cuadro 2. Cancelación en documentos internacionales.
Fuente: Elaboración propia.

No debe confundirse el derecho de rectificación con el derecho de cancelación, el primero supone la corrección del dato y la continuación del tratamiento, en tanto que el segundo implica eliminar definitivamente el dato y la finalización del tratamiento.⁶¹

1.4.3.2. Derecho de Oposición

El derecho de oposición permite al titular del dato, evitar el tratamiento de sus datos o solicitar el cese de este y está regulado por el artículo 27 de la Ley Federal de Protección de Datos Personales en posesión de Particulares, así como los artículos 109 a 111 del Reglamento:

Ley Federal de Protección de Datos Personales en posesión de Particulares

⁶⁰ Véase art. 27 de los Estándares de Protección de Datos para los Estados Iberoamericanos, RIPD, 2017, disponibles en https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf. Consultada el 18 de abril de 2020.

⁶¹ Cfr. Artículos 25 LFPDPPP y 105 RLFPDPPP.

Artículo 27.- El titular tendrá derecho en todo momento y por causa legítima a oponerse al tratamiento de sus datos. De resultar procedente, el responsable no podrá tratar los datos relativos al titular.

Reglamento de la Ley Federal de Protección de Datos Personales en posesión de Particulares

Derecho de Oposición

Artículo 109. En términos del artículo 27 de la Ley, el titular podrá, en todo momento, oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo cuando:

I. Exista causa legítima y su situación específica así lo requiera, lo cual debe justificar que aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un perjuicio al titular, o

II. Requiera manifestar su oposición para el tratamiento de sus datos personales a fin de que no se lleve a cabo el tratamiento para fines específicos.

No procederá el ejercicio del derecho de oposición en aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación legal impuesta al responsable.

Listados de exclusión

Artículo 110. Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas.

Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales.

En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.

Registro Público de Consumidores y Registro Público de Usuarios

Artículo 111. El Registro Público de Consumidores previsto en la Ley Federal de Protección al Consumidor y el Registro Público de Usuarios previsto en la Ley de Protección y Defensa al Usuario de Servicios Financieros, continuarán vigentes y se regirán de conformidad con lo que establezcan las leyes en cita y las disposiciones aplicables que de ellas deriven.

De la lectura de los artículos antes citados, se advierte que el derecho a la oposición procede en los siguientes escenarios:

- (a) Cuando el tratamiento es ilícito
- (b) Cuando el titular desea limitar el tratamiento de sus datos personales para ciertas finalidades que no sean las que dieron origen al tratamiento, o bien, que sean necesarias para la existencia, mantenimiento y cumplimiento de la relación jurídica entre el responsable y titular.

Particularmente, el Reglamento de la ley mexicana prevé la figura del listado de exclusión, como un mecanismo para evitar el tratamiento de los datos personales.

El derecho a la oposición no procederá cuando los datos personales sean necesarios para las finalidades primarias o bien que permitan la relación jurídica, por ejemplo, un empleado no puede negarse a dar sus datos personales de identificación, contacto, de salud o experiencia laboral en el marco de su relación laboral con el empleador, puesto que el tratamiento es necesario para el cumplimiento de una obligación contractual o una disposición legal.

Casos en los que procede el derecho de oposición según documentos internacionales:⁶²

Derecho de Oposición en documentos internacionales:	
Resolución Madrid 2009	Art. 18: “cuando concorra una razón legítima derivada de su concreta situación personal”
Estándares de Protección de Datos de los Estados Iberoamericanos, 2017 ⁶³	<p>28.1. El titular podrá oponerse al tratamiento de sus datos personales cuando:</p> <p>a. Tenga una razón legítima derivada de su situación particular.</p> <p>b. El tratamiento de sus datos personales tenga por objeto la mercadotecnia directa, incluida la elaboración de perfiles, en la medida que esté relacionada con dicha actividad.</p> <p>28.2 Tratándose del inciso anterior, cuando el titular se oponga al tratamiento con fines de mercadotecnia directa, sus datos personales dejarán de ser tratados para dichos fines.</p>

⁶² Aquí no se considera el Reglamento General de Protección de Datos dado que no es un documento internacional sino un documento regional vinculante para la Unión Europea

⁶³ Véase art. 27 de los Estándares de Protección de Datos para los Estados Iberoamericanos, RIPD, 2017, disponibles en https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf. Consultada el 18 de abril de 2020.

Convenio 108+ ⁶⁴	<p>Artículo 9 - Derechos del interesado</p> <p>1. Todo individuo tendrá un derecho: [...]</p> <p>d. A oponerse en cualquier momento, por motivos relacionados con su situación, al tratamiento de los datos personales que le conciernen, a menos que el responsable del tratamiento demuestre motivos legítimos para el tratamiento que prevalezcan sobre sus intereses o derechos y libertades fundamentales;</p>
-----------------------------	---

Cuadro 3. Oposición en documentos internacionales.
Fuente: Elaboración propia.

El derecho de oposición procede cuando:

Marco Internacional

- Casos de publicidad
- Casos de prospección comercial
- Razón legítima

Legislación Mexicana

- Alegue causa legítima⁶⁵ (tratamiento ilegítimo)
- Cuando cause perjuicio al titular o ponga en riesgo sus derechos (tratamiento legítimo)

Por regla general en el contexto internacional y nacional, el derecho de oposición no procede cuando: “El tratamiento sea necesario para el cumplimiento

⁶⁴ Convenio no. 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, emitido por el Consejo de Europa fue el primer instrumento internacional jurídicamente vinculante en el ámbito de la protección de datos. En virtud de este Convenio, las Partes deben adoptar las medidas necesarias en su Derecho nacional para aplicar sus principios, a fin de garantizar, en su territorio, el respeto de los derechos humanos fundamentales en el ámbito de la aplicación de la protección de datos. En junio de 2018 se hizo una modernización a este Convenio, llamándolo “Convenio 108+”, El texto vigente del Convenio se encuentra disponible en: <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>. Consultado el 26 de abril de 2020.

⁶⁵ *Cfr.* artículo 42 del RLFPDPPP, que señala que es ilegítimo el tratamiento cuando las finalidades sean distintas a las que dieron origen a la relación entre el responsable y el titular o sean necesarias para el tratamiento.

de una obligación impuesta sobre la persona responsable por la legislación nacional aplicable.”

Del estudio de los derechos de cancelación y oposición se puede concluir que el diseño de la ley mexicana impone muchas cargas operativas y procesales a los responsables del tratamiento de datos personales.

En efecto, la implementación de las medidas técnicas y organizacionales que tiene que adoptar el responsable para la implementación de procesos que permitan la efectividad del derecho de cancelación implican un gasto económico importante para el responsable, especialmente, si se considera que durante el periodo de bloqueo (que puede durar hasta 10 años, considerándolo como el plazo máximo de ley para que opere la prescripción de acciones) es necesario que el responsable erogue gastos de almacenamiento y de seguridad para conservar los datos personales durante el plazo de conservación. Es decir, el responsable tendrá que seguir invirtiendo en la protección de datos personales aun cuando ya haya finalizado el aprovechamiento del dato (ya sea porque las finalidades hayan sido cumplidas o bien porque operó el derecho de cancelación).

Lo anterior da cabida a la siguiente reflexión respecto del diseño de la ley: el tener un plazo de conservación que puede llegar a ser muy amplio, puede llegar a inhibir el debido cumplimiento de la protección de datos personales ya sea por costos o por falta de una debida implementación, tan solo pensar en empresas que, por un lado, tienen clientes (personas físicas) y a su vez empleados, implica tener una doble gestión de tratamiento de datos personales con diferentes esquemas para la implementación del Derecho al Olvido.

Claro que hay otras consideraciones como que, al final del día, las empresas ya obtuvieron un aprovechamiento económico a partir del uso (explotación) de datos personales,⁶⁶ y que, por otro lado, el diseño de la ley mexicana, permite al titular del

⁶⁶ *El ingreso promedio por usuario estimado en la publicidad digital, principalmente controlada por Google y Facebook, alcanzó los 59 dólares por persona en 2017. Multiplicando este número por un promedio de 3.800 millones de usuarios activos en Internet, podemos estimar aproximadamente el*

dato que goce no solo de su derecho humano a la protección de datos personales, sino que también se pueda beneficiar de otro derecho humano que es el de acceso a la justicia y tutela efectiva,⁶⁷ gracias a que uno de los propósitos del periodo de bloqueo es dar el mismo plazo equivalente al de las prescripciones de ley aplicables, para que el titular pueda determinar posibles responsabilidades en relación con su tratamiento hasta el plazo de prescripción legal o contractual de éstas.

Como se mencionó al principio de este apartado, los derechos de cancelación y oposición encuentran ciertas similitudes frente al Derecho al Olvido (también llamado derecho de supresión) que se encuentra regulado por el artículo 17 del RGPD, estas similitudes radican esencialmente en el resultado material que se obtiene con el ejercicio de uno o de otro, puesto que se logra la supresión del dato.

Sin duda, la diferencia sustancial es que el Derecho al Olvido está especialmente diseñado para solucionar una tensión de derechos entre el derecho a la protección de datos personales frente a los derechos de libertad de expresión y de información, cuando en nuestra legislación, los derechos de cancelación y oposición tienen como fin fundamental, el cumplimiento de los principios de calidad y finalidad. Sirve agregar que la regulación del Derecho al Olvido en el marco jurídico mexicano sí es una tarea pendiente del legislador que incluso ha sido una observación realizada por el Comité Consultivo del Convenio 108 al estado mexicano.⁶⁸

tamaño de este negocio. Ver “The Value of Personal Online Data”, European Union Agency for Cybersecurity, April 23, 2018, disponible en <https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data>. Consultado el 24 de abril de 2020. Traducción de la autora de este trabajo.

⁶⁷ *Cfr.* Tesis 1a./J. 42/2007, Tomo XXV, Abril de 2007, página: 124. Semanario Judicial de la Federación y su Gaceta. Garantía a la tutela jurisdiccional prevista en el artículo 17 de la Constitución Política De Los Estados Unidos Mexicanos. Sus alcances.

⁶⁸ Davara F. De Marcos, Isabel, Coord., “Diccionario...” *Op. cit.* p. 289, disponible en http://inicio.ifai.org.mx/PublicacionesComiteEditorial/DICCIONARIO_PDP_digital.pdf. Consultado el 20 de abril de 2020.

1.4.4 Antecedentes del Derecho al Olvido en México

En un estudio dedicado al Derecho al Olvido en México, Isabel Davara ha señalado que “El concepto del Derecho al Olvido está fundado sobre instituciones jurídicas previas, como son la prescripción de delitos, la eliminación de antecedentes penales o las amnistías en temas financieros y fiscales.”⁶⁹

De acuerdo con Guadalupe Tafoya y Consuelo Guadalupe Cruz, existe un antecedente a nivel legislativo en donde se tuvo la intención de agregar el concepto de Derecho al Olvido, se trata del “Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Ley para Regular las Sociedades de Información Crediticia”⁷⁰ (Publicado en el Diario Oficial de la Federación el 1o de febrero de 2008)⁷¹ cuyo artículos 23, 23 bis y 24⁷² regulan los historiales crediticios

⁶⁹ Davara F. De Marcos, Isabel, “El Derecho al Olvido...” *Op. cit.* p. 34, disponible en <http://www.infodf.org.mx/capacitacion/publicacionesDCCT/ensayo23/23ensayo2014.pdf>. Consultado el 23 de abril de 2020.

⁷⁰ De conformidad con el artículo 2 de la LFPDPPP, los sujetos regulados son todas aquellas personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusiva- mente personal y sin fines de divulgación o utilización comercial.

⁷¹ La Iniciativa pretende resolver los problemas detectados en los dos años de operación de estas sociedades. Se modifica e *introduce el concepto de Derecho al Olvido*, lo que significa que, pasando 7 años de un pago parcial o una mensualidad, este será borrado obligatoriamente del historial crediticio de esa persona; así, se eliminarán de la base de datos los registros con la información de personas físicas y morales sobre créditos vencidos anteriores al 1° de enero de 2000, cuyo importe a dicha fecha sea inferior a 3,000 pesos para personas físicas y a 10,000 pesos en el caso de personas morales.

A partir del 1o de enero de 2004, los registros de los pagos correspondientes a las personas físicas hasta antes del 1o de enero de 1997, serán borrados sin excepción de sus historiales crediticios. Los saldos de menos de mil UDIS para personas físicas de antes del 1° de enero de 2000, quedarán cancelados; beneficiará a un millón 600 mil personas. Lo anterior permitirá eliminar por completo el registro de aproximadamente 2.5 millones de créditos en beneficio de cerca de 2 millones de personas.

⁷² Artículo 23.- Las Sociedades están obligadas a conservar los historiales crediticios que les sean proporcionados por los Usuarios, correspondientes a cualquier persona física o moral, al menos durante un plazo de setenta y dos meses.

Las Sociedades podrán eliminar del historial crediticio del Cliente aquella información que refleje el cumplimiento de cualquier obligación, después de setenta y dos meses de haberse incorporado tal cumplimiento en dicho historial.

En caso de información que refleje el incumplimiento ininterrumpido de cualquier obligación exigible así como las claves de prevención que les correspondan, las Sociedades deberán eliminarlas del historial crediticio del Cliente correspondiente, después de setenta y dos meses de haberse incorporado el incumplimiento por primera vez en dicho historial.

En el caso de créditos en los que existan tanto incumplimientos como pagos, las Sociedades deberán eliminar la información de cada periodo de incumplimiento, en el plazo señalado en el párrafo anterior, contado a partir de la fecha en que se incorpore en el historial crediticio el primer incumplimiento de cada periodo.

En el caso de créditos en los cuales se registren incumplimientos y posteriormente un pago parcial del saldo insoluto, las Sociedades deberán eliminar la información relativa al crédito así como las claves de prevención correspondientes, en el plazo señalado en el tercer párrafo de este artículo, contado a partir de la fecha en que se incorpore en el historial crediticio el primer incumplimiento.

En el caso de que el Cliente celebre un convenio de finiquito y pague lo establecido en éste, el Usuario deberá enviar a la Sociedad la información respectiva, a fin de que ésta refleje que el pago se ha realizado, con la correspondiente clave de observación. Las Sociedades deberán eliminar la información relativa a estos créditos, así como las claves de observación correspondientes, en el plazo señalado en el tercer párrafo de este artículo, contado a partir de la fecha en que se incorpore en el historial crediticio el primer incumplimiento.

Para efectos de este artículo se entenderá por periodo de incumplimiento el lapso que transcurra entre la fecha en que se deje de cumplir con una o más obligaciones consecutivas exigibles y la fecha en que se realice el pago respectivo.

Las Sociedades deberán eliminar la información relativa a créditos menores al equivalente a mil UDIS en los términos que establezca el Banco de México mediante disposiciones de carácter general; asimismo, en dichas disposiciones se podrá determinar un monto y plazo de referencia para eliminar el registro de saldos residuales de cuantías mínimas, el cual no podrá ser superior a cuarenta y ocho meses.

Se exceptúa a las Sociedades de la obligación de eliminar la información relativa al incumplimiento correspondiente del historial crediticio, en el plazo señalado en el segundo párrafo de este artículo, cuando en la fecha en que corresponda eliminarla, el incumplimiento en el pago exigible esté siendo objeto de juicio en tribunales. Lo anterior, con base en la información que al efecto y bajo protesta de decir verdad le proporcione el Usuario que corresponda, a la Sociedad de que se trate.

En el supuesto al que se refiere el párrafo anterior, la Sociedad deberá eliminar del historial crediticio la información sobre el incumplimiento de que se trate, una vez transcurridos seis meses contados a partir de que se haya cumplido el plazo señalado al efecto en el aludido segundo párrafo de este artículo, salvo que el Usuario acredite nuevamente que el juicio sigue pendiente de resolución, en cuyo caso el mencionado plazo de seis meses se prorrogará por un periodo igual y así sucesivamente hasta que proceda la eliminación correspondiente.

Las Sociedades incluirán en sus manuales operativos procedimientos que les permitan a éstas revisar el razonable cumplimiento de lo establecido en el artículo 20 primer párrafo así como el procedimiento de eliminación de la información que les envíen los Usuarios en los términos de este artículo. La Comisión autorizará estos manuales.

Las Sociedades deberán establecer criterios aplicables a todas ellas para la implementación operativa del presente artículo, respecto de la información que reciban de Usuarios. La Comisión estará facultada para resolver consultas respecto de la implementación operativa del presente artículo.

Artículo reformado DOF 23-01-2004, 01-02-2008

Artículo 23 Bis. - Las Sociedades, sin perjuicio de lo dispuesto en el artículo 23 de esta Ley podrán, bajo su más estricta responsabilidad, conservar información una vez vencidos los plazos a que se refiere dicho artículo, a fin de asegurarse de que la información que reciban de sus Usuarios con posterioridad a tales plazos, no esté relacionada con aquella que debió haber sido eliminada. En caso de recibirla, deberán dar aviso a la Comisión, si el Usuario que la entregue es supervisado por dicho órgano desconcentrado.

Asimismo, las Sociedades deberán notificar a la Comisión, los controles con que cuentan para el resguardo de dicha información.

Artículo adicionado DOF 10-01-2014

Artículo 24.- La eliminación del historial crediticio prevista en el artículo anterior no será aplicable en los supuestos siguientes:

I. Tratándose de uno o más créditos cuyo monto adeudado al momento de la falta de pago de alguna cantidad adeudada a un acreedor sea igual o mayor que el equivalente a cuatrocientas mil UDIS, de

y los plazos para eliminar la información crediticia sobre deudores, sin embargo la redacción final (y vigente) no incorporó el concepto del Derecho al Olvido y en cambio se reguló como “eliminación de información crediticia”.⁷³

Es de agregar que en términos del artículo 24 de la Ley para Regular las Sociedades de Información Crediticia, la eliminación de información crediticia no procederá cuando el adeudo sea igual o mayor que el equivalente a cuatrocientas mil UDIS o cuando haya una sentencia firme por un delito patrimonial intencional relacionado con algún crédito y que en el año 2008, se adicionó el artículo 23 bis que señala las condiciones bajo las cuales se puede conservar la información crediticia una vez vencidos los plazos que establece el artículo 23 y se impone como obligación notificar a la Comisión sobre los controles con que cuentan para el resguardo de dicha información.

1.4.5 Iniciativas de Reforma en materia del Derecho al Olvido

Durante la investigación de este trabajo se han identificado tres iniciativas de reforma que buscan regular el Derecho al Olvido.

Por ejemplo, el 17 de julio de 2013, la Senadora María Verónica Martínez Espinoza, del Grupo Parlamentario del Partido Revolucionario Institucional (PRI), propuso un proyecto para adicionar diversas disposiciones a la Ley Federal de Protección de Datos Personales en Posesión de Particulares, mismo que no prosperó pero que vale la pena citar como antecedente, y en especial, algo que llama la atención de esta propuesta es que adiciona conceptos como el de “información personal en las redes” considerando que este concepto debe abarcar

conformidad con el valor de dicha unidad aplicable en la o las fechas en que se presenten las faltas de pago respectivas, independientemente de la moneda en que estén denominados.

II. En los casos en que exista una sentencia firme en la que se condene a un Cliente persona física por la comisión de un delito patrimonial intencional relacionado con algún crédito y que tal circunstancia se haya hecho del conocimiento de la Sociedad por alguno de sus Usuarios.

Artículo reformado DOF 01-02-2008

⁷³ Tafoya Hernández, J. Guadalupe; Cruz Ramos, Consuelo Guadalupe, “Reflexiones en torno al Derecho al Olvido”, Revista del Instituto Federal de Defensoría Pública del Consejo de la Judicatura Federal, No. 18, diciembre de 2014, p. 92 y 93 Disponible en <https://www.ifdp.cjf.gob.mx/resources/revistas/Revista18.pdf>. Consultado el 1 de junio de 2020.

“todo el contenido que se publica en una red social, entendido como texto, comentarios, mensajes, interacciones con otros usuarios, interacciones en aplicaciones, ubicaciones, fechas y horas, invitaciones, enlaces web, fotografías, videos”.⁷⁴ Este alcance es positivo cuando se piensa en el ejercicio de Derechos ARCO o en el derecho de portabilidad que regula el RGPD ya que el titular podría disponer de manera efectiva sobre los datos que se generan a partir del análisis de sus datos, porque en muchas ocasiones el tratamiento de los datos personales no gira entorno al nombre de una persona sino en el perfilamiento del usuario para generar publicidad comportamental, y por regla general estos datos que resultan del tratamiento los conserva el responsable justamente para hacer análisis predictivos.

Para mayor proveer se citan los artículos relevantes de este proyecto de reforma:⁷⁵

Artículo 3: Para efectos de esta Ley, se entenderá por:

I. a X. (...)

XI. Información personal en las redes: Todos los hechos y datos (nombre, dirección de correo electrónico, fecha de nacimiento y sexo) vertidos en el sitio web que sirven para relacionar la identidad de las personas, es también todo el contenido que se publica en una red social, entendido como texto, comentarios, mensajes, interacciones con otros usuarios, interacciones en aplicaciones, ubicaciones, fechas y horas, invitaciones, enlaces web, fotografías, videos.

...

Artículo 25 Bis. Todos los usuarios de servicios digitales y redes sociales tienen derecho, como parte de su derecho de cancelación referido en el artículo 25 de esta Ley, a solicitar la eliminación definitiva de los datos y

⁷⁴ Iniciativa de la Sen. María Verónica Martínez Espinoza, del Grupo Parlamentario del Partido Revolucionario Institucional, la que contiene proyecto de decreto por el que se adicionan diversas disposiciones a la Ley Federal de Protección de Datos Personales en Posesión de Particulares. Disponible en: https://www.senado.gob.mx/64/gaceta_comision_permanente/documento/42432 Consultada el 26 de abril de 2020.

⁷⁵ *Idem.*

contenidos que así lo manifiesten y que se encuentren en los servidores de los prestadores de servicios cibernéticos.

Los responsables digitales tienen la obligación de eliminar de manera inmediata y definitiva datos e información de un usuario cuando éste así lo solicite de forma explícita y no exista ninguna razón legítima para retenerlos. La eliminación de una cuenta de cualquier red social implica la revocación de todos los permisos conferidos al responsable digital para el tratamiento de los datos personales del usuario.

La segunda propuesta fue presentada el 3 de diciembre de 2019 por el senador Ricardo Monreal del grupo parlamentario de Movimiento de Regeneración Nacional (MORENA), la cual prevé que el derecho a la cancelación, o Derecho al Olvido, es la garantía de usuarios del mundo digital para solicitar a los motores de búsqueda, plataformas digitales y demás herramientas virtuales, la supresión de sus datos personales.⁷⁶

De la exposición de motivos se desprende que en lo que toca al derecho de cancelación (pretendiendo incorporar el Derecho al Olvido) la iniciativa propone:

- a) Se incorpora la noción de datos personales digitalizados, especificando que son todos aquellos que se encuentran disponibles en medios electrónicos y van desde simples textos hasta contenido multimedia e incluso, antecedentes penales.
- b) Se reconoce, de manera expresa, la ampliación del derecho a la cancelación; a partir de la reforma planteada, éste procederá para toda la información que se encuentre disponible en medios digitales, plataformas

⁷⁶ Cfr. Iniciativa con proyecto de decreto que reforma, adiciona y modifica diversas disposiciones de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en materia de Derecho de Olvido, Grupo Parlamentario MORENA, México, 3 de diciembre de 2019, disponible en: https://infosen.senado.gob.mx/sgsp/gaceta/64/2/2019-12-03-1/assets/documentos/Inic_Morena_Sen_Monreal_Posesion_Particulares.pdf. Consultada el 23 de abril de 2020.

virtuales y demás sitios informáticos, habilitándose al titular de los datos para solicitar la supresión de los mismos.

Además, conforme al principio de reinserción social que rige en materia penal la cancelación de los datos disponibles en internet se amplía a los antecedentes penales del titular, siempre que se configuren las circunstancias que para tal efecto ordene la regulación penal.

c) Se establecen las causales que deben configurarse para ejercer el derecho a la cancelación en materia digital, así como los límites del mismo. El establecimiento de causales específicas permitirá que se haga uso responsable de este derecho, evitando así el traspaso del límite entre la protección de los datos personales y la limitación exacerbada de la libertad de expresión o censura.

La propuesta de reforma es extensa y en realidad no está considerando que el derecho de protección de datos personales se pondere frente a la libertad de expresión y derecho a la información, solo pretende regular “datos digitales” lo que lejos de otorgar una protección más amplia, puede llegar a restringir las vías de protección obedeciendo a los medios en donde se origina el tratamiento.

Artículo 25.- El titular tendrá en todo momento el derecho a cancelar sus datos personales.

...

Tratándose de datos personales digitalizados, el derecho de cancelación abarcará la eliminación y supresión de todos los contenidos que se encuentren en medios electrónicos plataformas digitales, buscadores de internet y demás medios digitales, incluyendo textos, comentarios, interacciones, ubicaciones, contenido multimedia, antecedentes penales y demás información.

El responsable digital tendrá la obligación de realizar las operaciones necesarias para cancelar de manera inmediata y definitiva los datos personales digitalizados que hayan sido objeto de la solicitud del titular, así como las copias de seguridad y demás respaldos electrónicos existentes.

...

Artículo 26 Bis. Para que proceda la cancelación de los datos personales digitalizados deberá configurarse, al menos, una de las circunstancias siguientes:

- a) que la información sea innecesaria en relación con los fines para los cuales fue recogida o proporcionada;
- b) que los datos personales digitalizados hayan sido tratados ilícitamente; c) que la información sea inexacta, y
- d) que la información sea obsoleta o irrelevante.

En todo caso, la ampliación del derecho a la cancelación de los datos personales digitalizados no podrá ejercerse cuando su ejercicio vulnere la seguridad nacional y el orden público.

Esta iniciativa busca garantizar el derecho de los ciudadanos a que se eliminen contenidos personales que se encuentren en medios electrónicos, plataformas web, buscadores de Internet y demás medios digitales, incluyendo textos, comentarios, interacciones, ubicaciones, contenido multimedia, y antecedentes penales.⁷⁷

La tercera iniciativa es muy reciente, de fecha 3 de marzo de 2020, del Grupo Parlamentario del Partido del Trabajo (PT) por parte De la Senadora, Alejandra Del

⁷⁷ Becerril, Andrea, "Morena impulsa una ley para el Derecho al Olvido en plataformas digitales", La Jornada, 25 de enero de 2020, p. 7, disponible en <https://www.jornada.com.mx/2020/01/25/politica/007n2pol>. Consultada el 23 de abril de 2020.

Carmen León Gastélum cuya exposición de motivos también está basada en la inclusión del Derecho al Olvido, pero la sugerencia de reforma recae en dos cuestiones (a) ampliar el espectro de los sujetos regulados, para incluir a personas físicas o morales extranjeras y (b) incluir las operaciones que realizan los servicios de motores de búsqueda dentro del tratamiento. Por considerarlo relevante, se cita parte de la exposición de motivos de esta propuesta de reforma:

Especialmente en el caso de México, ejercer el derecho de olvido ha sido un asunto complicado no sólo por los vacíos legales en la materia sino porque las empresas transnacionales dedicadas al tratamiento de datos personales han sostenido que dicho tratamiento no lo realizan dentro del territorio nacional sino en sus respectivos países de origen. Argumento que es lógicamente débil por el hecho de que realizan actividades dentro de la jurisdicción del Estado Mexicano de manera directa o indirecta a través de sus filiales, pero que en la mayoría de las ocasiones les resultó efectivo para desechar las solicitudes de los usuarios que buscaron ejercer este derecho.

Por lo que resulta indispensable reformar Ley Federal de Protección de Datos Personales en Posesión de los Particulares para definir de una manera más efectiva el tratamiento de datos personales y para acotar de una manera más precisa las obligaciones del tipo de empresas en comento.

Por otro lado, como respuesta a los pronunciamientos manifestados con preocupación, debe de aclararse que el derecho de olvido no limita el derecho a la información o a la libertad de expresión pues estos son derechos protegidos por nuestra constitución y por los tratados internacionales en materia de derechos humanos suscritos por el Estado Mexicano.⁷⁸

⁷⁸ Iniciativa de la Sen. Alejandra del Carmen León Gastélum y de las senadoras y senadores del Grupo Parlamentario del Partido del Trabajo, con proyecto de decreto por el que se reforma la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Gaceta del Senado, 3 de marzo de 2020, México, Disponible en https://www.senado.gob.mx/64/gaceta_del_senado/documento/104767. Consultada el 26 de abril de 2020.

De este proyecto se desprende la siguiente propuesta de reforma:

Ley Federal de Protección de Datos Personales en Posesión de los Particulares

...

Artículo 2. Son sujetos regulados por esta Ley, los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de:

...

Los particulares extranjeros o nacionales que realicen el tratamiento total o parcial de datos personales desde el territorio de otro Estado y/o lo realicen dentro del territorio nacional de manera directa o indirecta a través de o en coordinación con sus filiales o terceros sujetaran las operaciones que lleven a cabo en los límites de la jurisdicción del Estado Mexicano a lo establecido en el presente ordenamiento y a las demás disposiciones legales aplicables.

Artículo 3.-Para los efectos de esta Ley, se entenderá por:

...

XVIII. Tratamiento: Cualquier operación o conjunto de operaciones efectuadas sobre datos personales mediante procedimientos manuales o automatizados que tengan como propósito o consecuencia la obtención, uso, divulgación, almacenamiento, registro, modificación, organización, estructuración, consulta, comunicación o indexación de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

Al respecto, la Organización Civil Red en Defensa de los Derechos Digitales (R3D) ha sido una de las voces más críticas a esta reforma y a sus alcances, argumentando principalmente tres factores (a) que implica una herramienta que favorece la violación a la libertad de expresión y acceso a la información (b) que es inconstitucional permitir que los particulares tengan la facultad de suprimir definitivamente información en línea y (c) que dicha medida es incompatible con el marco normativo y con la realidad cultural del país: “la

iniciativa pasa por alto las diferencias entre el sistema europeo y el interamericano en materia de libertad de expresión, especialmente en un contexto donde la corrupción y el abuso de poder buscan silenciar las voces críticas”.⁷⁹ La R3D apuesta por la preservación de la memoria histórica como un elemento indispensable en una sociedad democrática.

Así también, miembros del organismo Artículo 19 llaman la atención sobre los riesgos a la libertad de expresión que puede implicar la aprobación de la iniciativa de reforma, especialmente porque a juicio de esta organización, la propuesta de reforma carece de candados suficientes para evitar el abuso de este mecanismo y que dé lugar a que se eliminen hechos de corrupción o de violaciones a derechos humanos, puesto que ya se ha visto que con la legislación vigente, son los narcotraficantes o exfuncionarios corruptos quienes apelan al derecho de cancelación para borrar sus antecedentes.⁸⁰

1.4.6 Casos relacionados con el Derecho Olvido en México

Ulrich Richter Vs Google⁸¹

En el año 2015, tuvo origen el primer caso que ha sido asociado con el Derecho al Olvido en México, este es el caso de Ulrich Richter Morales contra Google, en donde la litis planteada versó sobre la eliminación del blog titulado “Ulrich Richter Morales y sus chingaderas a la patria”⁸² publicado en la plataforma de Blogger (operado por

⁷⁹ Iniciativa del senador Ricardo Monreal sobre supuesto Derecho al Olvido amenaza la libertad de expresión en línea, Red en Defensa de los Derechos Digitales, México, enero 24, 2020, Disponible en: <https://r3d.mx/2020/01/24/iniciativa-del-senador-ricardo-monreal-sobre-supuesto-derecho-olvido-amenaza-la-libertad-de-expresion-en-linea/> Consultada el 17 de abril de 2020.

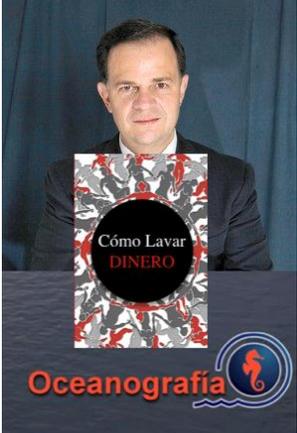
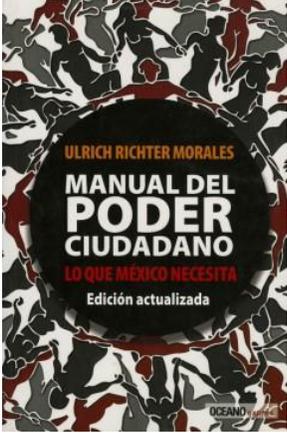
⁸⁰ Tudón Maldonado, Martha A., “El Derecho al Olvido y lo que se pretende borrar”, Animal Político, México, 7 de febrero, 2020, disponible en: <https://www.animalpolitico.com/altoparlante/el-derecho-al-olvido-y-lo-que-se-pretende-borrar/> Consultada el 17 de abril de 2020.

⁸¹ <http://ulrichrichtermoraless.blogspot.com> Consultado el 20 de abril de 2020.

⁸² “Ulrich Richter Morales y sus chingaderas a la patria” anónimo, disponible en <http://ulrichrichtermoraless.blogspot.com>. Consultado el 25 de abril de 2020

Google, LLC),⁸³ en donde, desde el anonimato se le acusaba de lavado de dinero y corrupción.

El blog fue publicado por primera vez el 4 de marzo de 2014, sin un autor o fuente identificable, a través de la plataforma de Blogger y, hoy en día, su contenido no ha sido bajado y sigue disponible al público.⁸⁴ Para mayor proveer, se inserta una fotografía obtenida del Blog antes mencionado, a efecto de ilustrar la controversia planteada:

Imagen que aparece en el blog no autorizado ⁸⁵	Portada original del libro tomada de la Editorial Océano ⁸⁶
	

Cuadro 4. Caso Ulrich Richter Vs Google
Fuente: Elaboración propia.

A pesar de que este caso se ha referenciado en la prensa mexicana como el primer caso del Derecho al Olvido, lo cierto es que este juicio no derivó de un ejercicio de Derechos ARCO, ni del intento de cancelar u oponerse al tratamiento de datos personales, en cambio, el fondo de este procedimiento se refiere a una

⁸³ De acuerdo con los Términos y Condiciones del sitio Blogger, el prestador de servicio es Google LLC, ver "Privacidad y Condiciones" disponible en <https://policies.google.com/terms?hl=es> Consultado el 25 de abril de 2020.

⁸⁴ *Op. Cit.* <http://ulrichrichtermoraless.blogspot.com> Consultado el 25 de abril de 2020

⁸⁵ *Idem*

⁸⁶ Disponible en <http://www.oceano.mx/obras/manual-del-poder-ciudadano-ulrich-richter-morales-12001.aspx> Consultado el 25 de abril de 2020.

indemnización por daño moral (de conformidad con el artículo 1916 del Código Civil de la Ciudad de México⁸⁷, iniciado por la vía ordinaria civil ante el Juzgado 8º Civil de la Ciudad de México bajo el expediente 907/2015, en donde Ulrich Richter Morales y otros⁸⁸, alegaron violaciones al honor, a la reputación e incluso suplantación de identidad,⁸⁹ (aquí vale la pena aclarar que la usurpación de identidad es un delito que debe perseguirse por la vía penal y no civil),⁹⁰ por otro

⁸⁷ Código Civil de la Ciudad de México, Artículo 1916. Por daño moral se entiende la afectación que una persona sufre en sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspectos físicos, o bien en la consideración que de sí misma tienen los demás. Se presumirá que hubo daño moral cuando se vulnere o menoscabe ilegítimamente la libertad o la integridad física o psíquica de las personas.

Cuando un hecho u omisión ilícitos produzcan un daño moral, el responsable del mismo tendrá la obligación de repararlo mediante una indemnización en dinero, con independencia de que se haya causado daño material, tanto en responsabilidad contractual como extracontractual. Igual obligación de reparar el daño moral tendrá quien incurra en responsabilidad objetiva conforme al artículo 1913, así como el Estado y sus servidores públicos, conforme a los artículos 1927 y 1928, todos ellos del presente Código.

La acción de reparación no es transmisible a terceros por acto entre vivos y solo pasa a los herederos de la víctima cuando ésta haya intentado la acción en vida.

El monto de la indemnización lo determinará el juez tomando en cuenta los derechos lesionados, el grado de responsabilidad, la situación económica del responsable, y la de la víctima, así como las demás circunstancias del caso.

⁸⁸ Claudia Ramírez Tavera y Richter Ramírez y Asociados, sociedad civil.

⁸⁹ “[...] Extracto tomado del Amparo 422/2016 resuelto por el Juzgado 11o de Distrito en Materia Civil en la Ciudad de México: A) La indemnización por daño moral en términos de lo dispuesto por el artículo 1916 del Código Civil, como consecuencia de las acciones u omisiones llevadas a cabo en forma dolosa y culposa por las demandadas, que constituyen hechos ilícitos de los cuales deriva su responsabilidad al haber causado un daño a los suscritos, lesionándonos en nuestros valores, afectando nuestros sentimientos, decoro, honor, reputación, así como la en la (sic) consideración que de nosotros tienen las personas con quienes tratamos tanto social como profesionalmente, mismos que deberán ser determinados por su señoría tomando en cuenta los derechos lesionados, el grado de responsabilidad y la situación económica de las demandadas y la de los suscritos, así como de las demás circunstancias del caso que surjan durante el presente juicio, al haber permitido y tolerado de manera consciente y con pleno conocimiento de causa, pese a haber sido advertidas, de la publicación y puesta a disposición en su buscador un blog copiado y dolosamente alterado del original, con intenciones de hacerlo pasar como el verdadero del suscrito actor ***, es decir, suplantando y usurpando nuestra identidad, lo que en materia de comunicación electrónica se le conoce también como rodo (sic) de identidad, al inducir a confusión a las personas que pretendieran acceder al mismo, para causarnos deshonra y perjuicio a nuestra integridad como personas, pretendiendo exponernos al desprecio público, amén de que en dicho blog ilegal, llamado “ ”, también de manera falsa, tendenciosa y dolosa, nos imputan hechos determinados y calificados como delito por la Ley, lo que evidentemente nos ha causado afectación a nuestro patrimonio moral. B) La publicación o divulgación de la sentencia condenatoria que recaiga en el presente juicio, a costa de los demandados en todo medio y formato donde fueron difundidos los hechos, opiniones y/o comentarios que han vertido a través de la página de internet ***y constituyen la afectación que hoy se reclama respecto del derecho moral.

⁹⁰ Código Penal para la Ciudad de México: USURPACIÓN DE IDENTIDAD: Artículo 211 Bis. - Al que por cualquier medio usurpe, con fines ilícitos, la identidad de otra persona, u otorgue su consentimiento para llevar a cabo la usurpación en su identidad, se le impondrá una pena de uno a cinco años de prisión y de cuatrocientos a seiscientos días multa.

lado, exigen las reparaciones del daño material (en términos del artículo 216bis de la Ley Federal del Derecho de Autor) por el uso no autorizado de su retrato (que es un derecho vinculado con el derecho a la imagen regulado en la Ley Federal del Derecho de Autor),⁹¹ así como la reparación material (nuevamente, en términos del artículo 216bis de la Ley Federal del Derecho de Autor) por las modificaciones a su obra, aduciendo violaciones a sus derechos morales. Y exigen las siguientes pretensiones: (i) La eliminación del blog ilegal, (ii) el pago de los daños y perjuicios causados a los co-actores (iii) el pago de los gastos y costas.

En el juicio de origen, Google, Inc., en calidad de demandada, opuso como excepción la incompetencia por declinatoria, bajo el argumento de que tiene su domicilio social en el extranjero (Santa Clara, California) y que proporciona los servicios de motor de búsqueda y del sitio “blogger” desde Estados Unidos, sin contar con “sucursales” en la República Mexicana.⁹² Esta excepción fue admitida por el Juzgado Octavo Civil de la Ciudad de México y remitió al tribunal de alzada la declinatoria, misma que le tocó conocer a la Sala Octava del Tribunal Superior de Justicia de la Ciudad de México.

Se aumentarán en una mitad las penas previstas en el párrafo anterior, a quien se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito establecido en el presente artículo.

⁹¹ En opinión de la autora de esta tesis, los defensores de Ulrich Richter Morales confunden dos figuras del derecho, el derecho a la imagen (que es un derecho de la personalidad, inalienable, imprescriptible e inembargable) frente al *derecho del retrato*, previsto por el artículo 87 de la Ley Federal del Derecho de Autor (LFDA), mismo que en realidad es un límite al derecho de autor frente al derecho de imagen de una persona, es decir, un fotógrafo (titular del derecho de autor) no puede “retratar” a una persona (titular del derecho de imagen) sin su consentimiento expreso, de acuerdo con Eduardo de la Parra, lo que se regula en el artículo 87 de la LFDA es “el derecho a prohibir el uso de la representación visual de una persona, lo que no es otra cosa que el derecho a la imagen” Cfr. De La Parra, Eduardo, “El Derecho a la Propia Imagen”, IPIDEC, Tirant lo Blanch, 2014, México, p. 209.

⁹² “Conviene precisar que Google Inc. tiene presencia en México a través de Google México, S. de R.L. de C.V. y de Google Operaciones de México, S. de R.L. de C.V. Esta última compañía revende los programas y servicios de publicidad de Google Inc. También vale la pena recordar que luego de una resolución en su contra impuesta por la oficina de protección de datos personales en México, conocida en enero de 2015, Google México modificó su objeto social para retirar la mención de “prestación de todo tipo de servicios a través de medios electrónicos, incluyendo sin limitar, servicios de motor de búsqueda”. Ver GALINDO SOTO, Javier José, “Richter vs. Google va a la Suprema Corte”, El Economista, 13 de agosto de 2017, México, disponible en <https://www.economista.com.mx/opinion/Richter-vs.-Google-va-a-la-Suprema-Corte-20170813-0001.html> Consultado el 25 de abril de 2020

La Sala admitió la declinatoria bajo el Toca 1515/2015, pero resolvió que la excepción era infundada, debido a que la parte actora, en ejercicio de una acción personal, exige la indemnización por daño moral, lo cual implica que es autoridad jurisdiccional competente la del domicilio del demandado, en términos del artículo 156, fracción II (sic. Lo correcto es fracción IV), del Código de Procedimientos Civiles de la Ciudad de México⁹³ y que Google, Inc., al dar contestación, se sometió de manera tácita a la competencia del juez natural y por otro lado no es suficiente aducir que su domicilio se ubica en el extranjero pues los hechos de los cuales se duele la parte actora tienen efectos en la Ciudad de México.

Inconforme con lo anterior, Google interpuso el Amparo Directo 422/2016 que le tocó conocer al Juzgado 11^o de Distrito en materia Civil en la Ciudad de México, en donde los actos reclamados consisten en (a) la resolución de once de abril de dos mil dieciséis, emitida por la Octava Sala Civil del Tribunal Superior de Justicia de la Ciudad de México, mediante la cual se declaró infundada la excepción de incompetencia por declinatoria opuesta por el primer enjuiciado aludido; y (b) el acatamiento a esa determinación, por parte del juez de origen.

Seguidas las secuelas procesales, el Juez 11^o de Distrito en materia Civil en la Ciudad de México, el 21 de septiembre de 2017, negó el Amparo a Google, Inc., al no existir transgresión a las prerrogativas de legalidad, seguridad jurídica y acceso a la justicia en perjuicio de Google, Inc.

En contra de la sentencia de Amparo Directo 422/2016, Google, Inc. Interpuso un recurso de revisión no. 587/2017 ante la Suprema Corte de Justicia, del cual conoció la Primera Sala, para determinar si los tribunales mexicanos tienen competencia para conocer de la demanda de daño moral en contra de una empresa

⁹³ N.B. La sentencia de amparo directo 422/2016 hace referencia al artículo 156, fracción II, de Código de Procedimientos Civiles de la Ciudad de México, siendo que lo correcto es la fracción IV, Cfr.: *Artículo 156.- Es Juez competente:*

II. El del lugar señalado en el contrato para el cumplimiento de la obligación. Tanto en este caso como en el anterior, surte el fuero no solo para la ejecución o cumplimiento del contrato, sino para la rescisión o nulidad; ...

IV. El del domicilio del demandado, si se trata del ejercicio de una acción sobre bienes muebles, o de acciones personales o del estado civil.

con domicilio en el extranjero, sin embargo, en el curso de este procedimiento, Google, Inc. se desistió del recurso, lo que provocó que la resolución de la Sala Octava del Tribunal Superior de Justicia de la Ciudad de México que declaró infundada la excepción de competencia por declinatoria, quedara confirmada y firme.

Por tanto, el asunto regresó al Juez Octavo de lo Civil del Tribunal Superior de Justicia del Distrito Federal (hoy Ciudad de México) considerado como juzgado competente en términos del artículo 156, fracción IV, del Código de Procedimientos Civiles de la Ciudad de México para entrar al estudio del fondo del asunto.

Carlos Sánchez de la Peña Vs INAI

Otro caso emblemático y que sí derivó del ejercicio de derechos de cancelación y oposición es el caso de Carlos Sánchez de la Peña quien, en principio, solicitó a Google México la remoción de diversos enlaces, entre los que se destaca la nota periodística “Fraude en Estrella Blanca alcanza a Vamos México”,⁹⁴ y dado que Google no atendió su petición, el interesado inició un Procedimiento de Protección de Datos Personales ante el entonces IFAI (hoy INAI), en donde se resolvió medularmente lo siguiente:

“... 1. Por lo que respecta al derecho de oposición, con fundamento en el artículo 27 de la Ley de la materia, se abstenga de tratar los datos personales del Titular, consistentes en su nombre y apellidos, de tal manera que, al ser tecleados en el motor de búsqueda del responsable, no aparezcan los links o URL'S -indexación- que dicho Titular refirió en su solicitud de ejercicio de Derechos ARCO de fecha veintidós de julio de dos mil catorce.

2. En cuanto al derecho de cancelación, con fundamento en los artículos 25, primer párrafo, de la Ley Federal de Protección de Datos Personales en

⁹⁴ “Fraude en Estrella Blanca alcanza a Vamos México”, Revista Fortuna, México, Agosto 24, 2016, disponible https://revistafortuna.com.mx/opciones/archivo/2007/febrero/htm/fraude_estrella_blanca_vamos_mexico.htm# Consultada el 26 de abril de 2020

Posesión de Particulares, y 106, 107 y 108 de su Reglamento, cancele los datos personales del Titular antes mencionados, de modo que no obren en las bases de datos del responsable.”⁹⁵

Inconformes con lo anterior, la Revista Fortuna y la organización R3D,⁹⁶ interpusieron un amparo indirecto [574/2015] que fue turnado al Juzgado Decimoquinto de Distrito en Materia Administrativa en la Ciudad de México, por considerar que se había violado el derecho de audiencia de la revista y que la resolución constituía un caso de censura, dicho amparo fue sobreseído por falta de interés jurídico, particularmente, en el amparo los quejosos no acreditaron la titularidad del nombre de dominio “https://revistafortuna.com.mx/opciones/archivo/2007/febrero/htm/fraude_estrella_blanca_vamos_mexico.htm#” y por tanto el juzgado estimó que no existía una afectación en su esfera jurídica.

Luego del sobreseimiento, la Revista Fortuna y la organización R3D interpusieron un recurso de revisión y el Séptimo Tribunal Colegiado de Circuito del Centro Auxiliar de la Primera Región concedió el amparo para dejar sin efectos a resolución del INAI y ordenar la reposición del procedimiento de protección de derechos deberá reponerse el procedimiento para otorgar el derecho de audiencia a la Revista Fortuna.

Para efectos prácticos se cita la cronología de eventos preparada por la organización R3D y se incluyen algunas notas para precisar ciertos datos:⁹⁷

⁹⁵ Amparo indirecto 574/2015, resuelto por el Juzgado Decimoquinto de Distrito en Materia Administrativa en la Ciudad de México, ver p. 41.

⁹⁶ *La Red en Defensa de los Derechos Digitales (R3D) es una organización mexicana dedicada a la defensa de los derechos humanos en el entorno digital. Utilizamos diversas herramientas legales y de comunicación para hacer investigación de políticas, litigio estratégico, incidencia pública y campañas con el objetivo de promover los derechos digitales en México. En particular, la libertad de expresión, la privacidad, el acceso al conocimiento y la cultura libre. Cfr. <https://r3d.mx>. Consultada el 26 de abril de 2020*

⁹⁷ ¡GANAMOS! Tribunal anula resolución del INAI sobre el Falso «Derecho al Olvido» R3D, México, disponible en: <https://r3d.mx/2016/08/24/amparo-inai-derecho-olvido/> Consultada el 26 de abril de 2020.

Cronología del caso Carlos Sánchez de la Peña Vs Google México
No. de expediente PPD.0094/14 - INAI

Febrero de 2007

La revista Fortuna publica la nota periodística “Fraude en Estrella Blanca alcanza a Vamos México”.⁹⁸

Julio de 2014

Carlos Sánchez de la Peña solicita a Google México la remoción de varios enlaces⁹⁹; entre ellos, el de la nota de la Revista Fortuna. Google no atiende la solicitud.

Septiembre de 2014

Carlos Sánchez de la Peña interpone un procedimiento de protección de derechos en contra de Google México ante el IFAI (ahora INAI) (No. de expediente PPD.0094/14).

Enero de 2015

El INAI resuelve en favor de Carlos Sánchez de la Peña y ordena a Google México:

- Abstenerse de tratar su nombre y apellidos, de tal manera que, al ser tecleados en el motor de búsqueda del sitio de internet respectivo, no apareciera el link

⁹⁸ “Fraude en Estrella Blanca alcanza a Vamos México”, Revista Fortuna, México, Agosto 24, 2016, disponible

https://revistafortuna.com.mx/opciones/archivo/2007/febrero/htm/fraude_estrella_blanca_vamos_mexico.htm#. Consultada el 26 de abril de 2020

⁹⁹ Las páginas Web a las que Sánchez de la Peña buscaba impedir el acceso, bajo argumento de afectar “[no solo] mi esfera más íntima sino también mis relaciones comerciales y financieras actuales”, eran tres sitios cuyo contenido describe los actos ilegales que se le atribuyen y sus relaciones con figuras públicas presuntamente involucradas : un foro de discusión de Yahoo! Answers>, una nota en un sitio de autotransporte y un reportaje de investigación de la Revista Fortuna sobre un supuesto fraude. La decisión del INAI se encuentra en litigio y actualmente en suspensión. Ver “El erróneamente llamado Derecho al Olvido no es un derecho, es una forma de censura”, R3D, Julio 12, 2016, México, disponible en: <https://r3d.mx/2016/07/12/el-erroneamente-llamado-derecho-al-olvido-no-es-un-derecho-es-una-forma-de-censura/>. Consultada el 26 de abril de 2020.

https://revistafortuna.com.mx/opciones/archivo/2007/febrero/htm/fraude_estrella_blanca_vamos_mexico.htm# y otros

- Y que cancelara los datos personales de sus bases de datos,

Esto no implicaba que desde su servicio de motor de búsqueda no resultara posible acceder directamente al enlace de la nota periodística o la revista digital.¹⁰⁰

Febrero de 2015

R3D interpone demanda de amparo en representación de la revista Fortuna en contra del INAI por violar su derecho a la libertad de expresión y su derecho de audiencia. El Juzgado Decimoquinto de Distrito en Materia Administrativa en la Ciudad de México admite la demanda (Amparo indirecto 574/2015).¹⁰¹

Febrero de 2016

El Juzgado Decimoquinto de Distrito en Materia Administrativa de la Ciudad de México sobresee el amparo por falta de interés jurídico (no se acreditó la titularidad sobre el nombre de dominio https://revistafortuna.com.mx/opciones/archivo/2007/febrero/htm/fraude_estrella_blanca_vamos_mexico.htm#

Marzo de 2016

R3D interpone un recurso de revisión en contra de la sentencia del juzgado. El Segundo Tribunal Colegiado en Materia Administrativa del Primer Circuito admite el recurso (Amparo en revisión 95/2016)¹⁰² y lo envía al Séptimo Tribunal Colegiado de Circuito del Centro Auxiliar de la Primera Región (Expediente Auxiliar 355/2016)

Agosto de 2016

¹⁰⁰ Amparo indirecto 574/2015, resuelto por el Juzgado Decimoquinto de Distrito en Materia Administrativa en la Ciudad de México, ver p. 41. Disponible en http://sise.cjf.gob.mx/SVP/word1.aspx?arch=734/07340000167577970037031.doc_1&sec=Carlos_Ivan_Velasco_Dominguez&svp=1

¹⁰¹ *Idem*

¹⁰² Amparo en revisión 95/2016, Séptimo Tribunal Colegiado de Circuito del Centro Auxiliar de la Primera Región, disponible en http://sise.cjf.gob.mx/SVP/word1.aspx?arch=15/00150000186773530009005002.docx_1&sec=Victor_Ivan_Segura_Velazquez_&svp=1

El Séptimo Tribunal Colegiado de Circuito del Centro Auxiliar de la Primera Región modifica la decisión del juzgado, sobresee por falta de interés jurídico de ciertos quejosos, no entra al estudio del ejercicio de la libertad de expresión por no ser materia de la litis del amparo y concede el amparo para el efecto de que el INAI deje si efectos la resolución del INAI (PPD.0094/14) y reponga el procedimiento para efecto de otorgar el derecho de audiencia a la Revista Fortuna.¹⁰³

Cuadro 5. Cronología del caso Carlos Sánchez de la Peña Vs Google México
Fuente: Basada en la Cronología del artículo “¡GANAMOS!...” *Op. Cit.* R3D, México, disponible en: <https://r3d.mx/2016/08/24/amparo-inai-derecho-olvido/> Consultada el 26 de abril de 2020.

Caso Pablo Agustín M. Vs Google¹⁰⁴

El contexto de este caso es el siguiente: Pablo Agustín M. es un empresario mexicano que fue señalado por el Departamento de Tesoro de Estados Unidos por vínculos con el narcotráfico,¹⁰⁵ y después de litigarlo en Estados Unidos, logró que fuera borrado de la lista de extranjeros implicados en operaciones sospechosas; sin embargo, al hacer búsquedas en motores de búsqueda, su nombre aún es asociado a notas periodísticas relacionadas con las acusaciones del Departamento del Tesoro.¹⁰⁶

Bajo este contexto, Pablo Agustín M. solicitó a Google México que los resultados del motor de búsqueda dejaran de asociar su nombre a contenidos de terceros en donde lo relacionaran con actos de corrupción o narcotráfico.

¹⁰³ *Idem*

¹⁰⁴ Amparo directo 535/2018. Décimo Tribunal Colegiado en Materia Administrativa del Primer Circuito. Disponible en http://sise.cjf.gob.mx/SVP/word1.aspx?arch=79/00790000235100940012009004.doc_1&sec=Angel_Garcia_Cotonieto&svp=1 Consultada el 26 de abril de 2020

¹⁰⁵ “Treasury Targets Drug Trafficking Networks in Colombia and Mexico”, Treasury US, Julio 15, 2020, disponible en <https://www.treasury.gov/press-center/press-releases/Pages/tg775.aspx>. Consultado el 26 de abril de 2020

¹⁰⁶ Murillo Eduardo “Por primera vez, discutirá la Corte "Derecho al Olvido"”, La Jornada, México, 4 de noviembre 2019, disponible en: <https://www.jornada.com.mx/ultimas/politica/2019/11/04/por-primera-vez-discutira-la-corte-derecho-al-olvido-1265.html>. Consultado el 16 de abril de 2020

Google México respondió la solicitud por correo electrónico señalando que dicha empresa no presta servicios de *motor de búsqueda* y, por tanto, no lleva a cabo un tratamiento de datos personales del señor Caso Pablo Agustín M.

Luego de promover un procedimiento de protección de datos personales ante el INAI el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales confirmó que Google México no realiza un tratamiento de datos personales al no ser el responsable de la operación del motor de búsqueda.

El titular del dato, Pablo Agustín M. impugnó la resolución del INAI ante el Tribunal Federal de Justicia Administrativa (TFJA), seguidas las secuelas procesales, el caso fue atraído por la Sala Superior de dicho tribunal bajo el número de expediente J.N. 5622/17-17-14-6/453/18-PL-04-04, en donde al final se confirmó la resolución del INAI contenida en el oficio de 24 de enero de 2017.¹⁰⁷

Inconforme con lo anterior, Pablo Agustín M. promovió un amparo directo del que le tocó conocer al Décimo Tribunal Colegiado en Materia Administrativa del Primer Circuito resolvió Amparo bajo el expediente 535/2018,¹⁰⁸ en donde el tribunal concedió el amparo para efectos de revocar la sentencia de la sala superior del TFJA y se considere que Google México sí realiza un tratamiento de datos personales al ser la licenciataria de la marca “Google” (cuyo titular es Google Inc.) misma que ampara servicios de motor de búsqueda, luego, entonces si es licenciataria de una marca que presta servicios de motor de búsqueda, se desprende que la empresa Google México, sí realiza servicios de motor de búsqueda.

¹⁰⁷ Juicio de Nulidad J.N. 5622/17-17-14-6/453/18-PL-04-04, Sala Superior del Tribunal Federal de Justicia Administrativa, Disponible en <http://sentencias.tfja.gob.mx:8080/SICSEJLDOC/faces/content/public/consultasentencia.xhtml;jsessionid=TY-9Za8vSy3kliZrYuU5LYhncNMEIZU-EsrSg-VWC8q5aYmL6FFp!-1090808339>

¹⁰⁸ Amparo directo 535/2018. Décimo Tribunal Colegiado en Materia Administrativa del Primer Circuito. Disponible en http://sise.cjf.gob.mx/SVP/word1.aspx?arch=79/00790000235100940012009004.doc_1&sec=Angel_Garcia_Cotonieto&svp=1. Consultada el 26 de abril de 2020.

De este amparo se desprenden las tesis que se citan enseguida:

DATOS PERSONALES. LA LICENCIA DE USO DE UN SIGNO MARCARIO RELATIVO A LA PRESTACIÓN DEL SERVICIO DE MOTOR DE BÚSQUEDA EN INTERNET CONCEDIDA POR UNA EMPRESA EXTRANJERA EN FAVOR DE UNA SOCIEDAD MERCANTIL MEXICANA, ES APTA PARA CONSIDERAR LA RESPONSABILIDAD DE ÉSTA POR EL TRATAMIENTO DE AQUÉLLOS CONFORME A LA NORMATIVA CONSTITUCIONAL Y LEGAL RESPECTIVA. De acuerdo con los artículos 87, 88, 125, 126, 136, 139, 140 y 141 de la Ley de la Propiedad Industrial, el titular de una marca puede conceder una licencia de uso a favor de un tercero, quien quedará obligado a vender los productos o prestar los servicios de que se trate, con la misma calidad que los comercializados por el titular, ejercer las acciones legales de protección de los derechos y usar la marca como si fuera el propietario del registro. Así, la licencia de uso de un signo marcario relativo a la prestación del servicio de motor de búsqueda en Internet concedida por una empresa extranjera en favor de una sociedad mercantil constituida en términos de los artículos 3o., 4o., 6 bis y 15 del Código de Comercio y 1o., fracción III, 4o., 5o., 58, 59 y 73 de la Ley General de Sociedades Mercantiles, es apta para considerar la responsabilidad de ésta por el tratamiento de datos personales de un gobernado, en tanto que su constitución en territorio nacional, en adición a la licencia concedida en su favor, la legitiman y obligan a prestar ese servicio en México y, por tanto, a responder por su actuación conforme a la Constitución Federal y a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.¹⁰⁹

PROTECCIÓN DE DATOS PERSONALES. EL DEBER DEL ESTADO DE SALVAGUARDAR EL DERECHO HUMANO RELATIVO DEBE POTENCIALIZARSE ANTE LAS NUEVAS HERRAMIENTAS

¹⁰⁹ Tesis: I.10o.A.120 A (10a.), Registro 2020549, Semanario Judicial de la Federación, Décima Época, 06 de septiembre de 2019.

TECNOLÓGICAS, DEBIDO A LOS RIESGOS QUE ÉSTAS REPRESENTAN POR SUS CARACTERÍSTICAS. Conforme al proceso legislativo de la adición del segundo párrafo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, publicada el 1 de junio de 2009 en el Diario Oficial de la Federación, en relación con la interpretación del artículo 11, numeral 2, de la Convención Americana sobre Derechos Humanos, efectuada en diversos criterios emitidos por la Corte Interamericana de Derechos Humanos, el deber del Estado frente al derecho de los gobernados a decidir qué aspectos de su vida deben o no ser conocidos o reservados por el resto de los individuos que integran la sociedad, y que conlleva la obligación de dejarlos exentos e inmunes a invasiones agresivas o arbitrarias por parte de terceros o de la autoridad pública, debe potencializarse ante las nuevas herramientas tecnológicas. Lo anterior, por el efecto multiplicador de los medios de comunicación digitales de Internet y las redes sociales, a través de los cuales se facilita la difusión y durabilidad de su contenido, al permanecer de manera indefinida en los medios electrónicos en los que se publican, sin restricción territorial alguna; constituyéndose así en una constante invasión positiva o negativa, según el caso, a los derechos inherentes al ser humano, vinculados con el mencionado, como son la intimidad, el honor, la reputación, la vida privada y, consecuentemente, la dignidad humana.¹¹⁰

PROTECCIÓN DE DATOS PERSONALES. CONSTITUYE UN DERECHO VINCULADO CON LA SALVAGUARDA DE OTROS DERECHOS FUNDAMENTALES INHERENTES AL SER HUMANO. El párrafo segundo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos reconoce los denominados Derechos ARCO, relativos al acceso, rectificación, cancelación y oposición de datos personales, como un medio para garantizar el derecho de los individuos a decidir qué aspectos de su vida

¹¹⁰ Tesis: I.10o.A.6 CS (10a.), Registro: 2020564, Semanario Judicial de la Federación, viernes 06 de septiembre de 2019.

deben o no ser conocidos o reservados por el resto de la sociedad, y la posibilidad de exigir su cumplimiento a las autoridades y particulares que conocen, usan o difunden dicha información. Así, dichas prerrogativas constituyen el derecho a la protección de los datos personales, como un medio de salvaguarda de otros derechos fundamentales previstos en la propia Constitución y en los tratados internacionales de los que México es Parte, conforme a los cuales, el Estado tiene la obligación de garantizar y proteger el derecho de todo individuo a no ser interferido o molestado por terceros o por una autoridad, en ningún aspecto de su persona –vida privada–, entre los que se encuentra el relativo a la forma en que se ve a sí mismo y como se proyecta a los demás –honor–, así como de aquellos que corresponden a los extremos más personales de la vida y del entorno familiar –intimidad–, o que permiten el desarrollo integral de su personalidad como ser humano –dignidad humana.¹¹¹

En opinión de la autora de este trabajo, este amparo tiene dos principales lecturas:

(a) Por un lado, es un criterio que acaba con los obstáculos procesales que Google acostumbra a usar como, por ejemplo, que Google México no presta servicios de motor de búsqueda sino que esos servicios se prestan desde California por Google Inc. y que en México no tienen sucursales, o bien, las prácticas relacionadas con la modificación del objeto social de Google México para eliminar el servicio de “motor de búsqueda” y, finalmente, determina que Google México si realiza servicios de motor de búsqueda al ser licenciataria de Google Inc. para usar la marca “Google” en la clase de servicios de “motor de búsqueda” y por tanto, realiza un tratamiento de datos personales.

(b) Por otro lado, el hecho de que el Tribunal haya determinado que la licencia de una marca para servicios de motor de búsqueda es un criterio que hay que tomar

¹¹¹ Tesis: I.10o.A.5 CS (10a.), Registro: 2020563, Semanario Judicial de la Federación, Décima Época, viernes 06 de septiembre de 2019.

con cierta reserva, ya que al final si lo que se busca es fijar competencia del INAI o tribunales mexicanos, o bien, demostrar que existe un tratamiento de datos personales, no parece que la vía de propiedad intelectual sea la más adecuada, especialmente porque la rama de marcas tiene reglas especiales, en donde, por ejemplo, una licencia de marcas es idónea para acreditar el uso de una marca pero no para acreditar el tratamiento de datos personales.

Sin embargo, es una buena noticia que los tribunales mexicanos sean propositivos con criterios novedosos como este, porque al final, solo gracias a los precedentes que se generen es que la práctica se enriquece, los criterios de interpretación se robustecen y entonces se logra una mejor práctica en la protección de datos personales.

No omito señalar que, de acuerdo con notas periodísticas, actualmente, la Segunda Sala de la Suprema Corte de Justicia de la Nación se encuentra estudiando un amparo derivado de un juicio civil iniciado por Pablo Agustín “M” en contra de Google.¹¹²

Lo que podemos concluir de estos tres casos es que, los tribunales solo han resuelto temas adjetivos como: competencia, interés jurídico, derechos de audiencia, pero aun no se ha hecho un verdadero análisis en torno al ejercicio de protección de datos frente a motores de búsqueda, en donde se tenga que ponderar el derecho a la privacidad frente a la libertad de expresión o el derecho a la información (bajo el llamado derecho a saber).

¹¹² Murillo Eduardo “Por primera vez...” *Op. cit.* disponible en: <https://www.jornada.com.mx/ultimas/politica/2019/11/04/por-primera-vez-discutira-la-corte-derecho-al-olvido-1265.html>. Consultado el 16 de abril de 2020



Capítulo 2

Divergencias y Efectos del Derecho al Olvido según experiencia del Tribunal de Justicia Europeo



Capítulo 2: Divergencias y Efectos del Derecho al Olvido según experiencia del Tribunal de Justicia Europeo

En el capítulo precedente expusimos como en diversos instrumentos internacionales se ha reconocido el Derecho al Olvido y en otros se ha identificado como el derecho de cancelación y/o oposición sin embargo es importante advertir las divergencias y efectos de este derecho a fin de conocer una dimensión viable de aplicación de este derecho. En ese sentido como explicaremos en los siguientes párrafos en la medida de ejemplo el caso Costeja¹¹³ precedente emblemático del Derecho al Olvido que demostró la capacidad de los tribunales para ponderar este derecho frente al derecho a la información, a la expresión o a la determinación informativa.

2.1 El Caso Costeja

2.1.1 Preámbulo

El procedimiento versa sobre la aplicación de la Directiva¹¹⁴ sobre protección de datos a un motor de búsqueda en Internet que Google gestiona como proveedor de servicios. En el procedimiento nacional es pacífico que, en 1998, un periódico español publicó en dos ejemplares de su edición impresa, que posteriormente se publicaron en formato digital disponible en Internet, ciertos datos personales relativos al interesado. El interesado considera que esta información ya no debería mostrarse en los resultados de búsqueda ofrecidos por el motor de búsqueda en

¹¹³ Asunto C-131/12, Google Spain, S.L., Google Inc. Contra Agencia Española de Protección de Datos (AEPD), Mario Costeja González, sentencia del 13 de Mayo de 2014, Tribunal de Justicia de la Unión Europea Disponible en: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=384212>. Consultado el 20 de abril de 2020

¹¹⁴ Cfr. Directiva 95/46, *Op. cit.* Disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=ES>. Consultada el 20 de abril de 2020.

Internet gestionado por Google cuando se realiza en él una búsqueda de su nombre y apellidos.

La denuncia fue presentada por el Sr. Costeja González, de nacionalidad española y con domicilio en España, contra el editor de un diario español, La Vanguardia, y en contra de Google Spain y Google Inc. Básicamente, la denuncia se refería al hecho de que cuando se llevó a cabo una búsqueda en Google motor de búsqueda ("Search Google") contra el nombre de la reclamante los resultados proporcionados enlaces a artículos en La Vanguardia desde 1998 mencionar el Sr. González en relación con los procedimientos de quiebra. Sr. González quiso poner esas cuestiones detrás de él y aunque él había fallado en su demanda contra el periódico (que podría beneficiarse de la exención periodístico en la Directiva), sostuvo que la publicación continuada por Google Búsqueda de esos resultados de búsqueda violó sus derechos en virtud la Directiva. Él solicitó que se condenara a Google a eliminar o bloquear los resultados de búsqueda.

2.1.2 Temas sustanciales dirimidos por el Tribunal

1. Si la actividad de un motor de búsqueda para encontrar información en Internet, indexar información, almacenarla temporalmente y poner la información disponible al público en forma de resultados de búsqueda con enlaces a otros sitios web equivale a "tratamiento de datos personales".
2. Si el operador de un motor de búsqueda que realiza las actividades antes mencionadas puede ser considerado como un "responsable del tratamiento de datos".
3. Si el alcance territorial de la Directiva 95/46¹¹⁵ puede extenderse a Google Inc., con sede en Estados Unidos, por tener una filial en la Unión Europea.
4. Si la responsabilidad del operador de un motor de búsqueda alcanza para eliminar los enlaces a páginas web que aparecen en sus propios resultados de búsqueda, pero que son publicados por terceros, incluso en

¹¹⁵ *Idem.*

circunstancias en donde la información sigue estando disponible en el sitio web de la fuente original.

5. Cuáles serán los criterios que aplicará el operador del motor de búsqueda para decidir si atiende o no una solicitud para eliminar ciertos enlaces de sus resultados de búsqueda.
6. Si hay un "Derecho al Olvido" en virtud de la Directiva, que da derecho a al titular para exigir que la información -que considere como desactualizada- sea eliminada de los resultados de búsqueda de un motor de búsqueda.

Dada la amplitud de las definiciones de "tratamiento", "datos personales" y "responsable del tratamiento de datos" bajo la Directiva, el tribunal sostuvo que las actividades de los motores de búsqueda sí implican un tratamiento de datos personales y que los operadores de motores de búsqueda son los responsables del tratamiento de datos personales.

En relación con el alcance territorial de la Directiva, el tribunal determinó que, toda vez que Google Spain (como filial de Google Inc.) comercializa espacios publicitarios ofrecidos por Google Search y como Google Search y su publicidad estaban inextricablemente ligada, el tratamiento de datos personales por parte de Google Search se llevó a cabo dentro del contexto de las actividades de Google España, siendo éste un establecimiento del responsable del tratamiento en el territorio de un Estado miembro de la Comunidad Europea.

El tribunal sostuvo que los motores de búsqueda son responsables de asegurar que los resultados de búsqueda que se publicarán son compatibles con los derechos de las personas bajo la Directiva de Protección de Datos. En este contexto, el tribunal hizo hincapié en la forma en que los resultados de la búsqueda equivalen a una visión estructurada de la información relativa a una persona que se puede encontrar en el Internet,¹¹⁶ tal información afecta potencialmente un gran

¹¹⁶ Ver párrafo 80 disponible en "Asunto C-131/12..." *Op. cit.* Disponible en: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=E S&mode=lst&dir=&occ=first&part=1&cid=384212>. Consultado el 27 de abril de 2020.

número de aspectos de su vida privada y puede llegar a establecer un perfil detallado de él, en este sentido, el tribunal enfatizó el importante papel de internet en la sociedad moderna.¹¹⁷

En cuanto a la ponderación de los derechos de los titulares del dato frente al derecho del público a recibirlo, el tribunal declaró que los titulares de los datos tienen prioridad sobre los intereses de los usuarios de Internet en tener acceso a la información, “no obstante este equilibrio puede depender, en supuestos específicos, de la naturaleza de la información de que se trate y del carácter sensible para la vida privada de la persona afectada y del interés del público en disponer de esta información, que puede variar, en particular, en función del papel que esta persona desempeñe en la vida pública”¹¹⁸

De manera que, el tribunal sostuvo que la Directiva de protección de datos incluye un "Derecho al Olvido", que se deriva de los principios generales establecidos en el artículo 6 de la Directiva:¹¹⁹

[94] Por consiguiente, en el supuesto en el que se aprecie, tras una solicitud del interesado en virtud del artículo 12, letra b), de la Directiva 95/46, que la inclusión en la lista de resultados obtenida como consecuencia de una búsqueda efectuada a partir de su nombre, de vínculos a páginas web, publicadas legalmente por terceros y que contienen datos e información verídicos relativos a su persona, es, en la situación actual, incompatible con dicho artículo 6, apartado 1, letras c) a e), debido a que esta información, habida cuenta del conjunto de las circunstancias que caracterizan el caso de

¹¹⁷ Ver párrafo 135 de las conclusiones del abogado general Sr. Niilo Jääskinen presentadas el 25 de junio de 2013, Asunto C-131/12, Google Spain, S.L., Google Inc. Contra Agencia Española de Protección de Datos (AEPD), Mario Costeja González: *Como ha observado el Grupo del artículo 29, es posible que la responsabilidad secundaria de los proveedores de servicio de motor de búsqueda con arreglo al Derecho nacional implique la existencia de deberes que exijan bloquear el acceso a páginas web de terceros con contenidos ilegales, como las páginas web que vulneran derechos de propiedad intelectual, o que muestran información injuriosa o delictiva.*

¹¹⁸ Ver párrafo 81 en Asunto C-131/12, Google Spain, S.L., Google Inc. Contra Agencia Española de Protección de Datos (AEPD), Mario Costeja González <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=384212>. Consultado el 29 de mayo de 2020.

¹¹⁹ *Ibidem*, párrafos 94 y 95.

autos, es inadecuada, no es pertinente, o ya no lo es, o es excesiva en relación con los fines del tratamiento en cuestión realizado por el motor de búsqueda, la información y los vínculos de dicha lista de que se trate deben eliminarse.

[95] En lo que atañe a las solicitudes en el sentido de este artículo 12, letra b), basadas en el supuesto incumplimiento de los requisitos establecidos en el artículo 7, letra f), de la Directiva 95/46 y con arreglo al artículo 14, párrafo primero, letra a), de dicha Directiva, ha de señalarse que cada tratamiento de datos personales debe ser legítimo, en virtud del artículo 7, durante todo el período en el que se efectúa.

Derivado de lo antes citado, el tribunal sostuvo que el efecto de este nuevo derecho es que los individuos tienen derecho a exigir los motores de búsqueda de Internet que eliminen la información que el individuo no desea que se encuentre publicada, sin perjuicio de que la información siga estando disponible en el sitio web de la editorial (fuente) original -como fue el caso- y sin tener que demostrar el perjuicio. En consecuencia, en los hechos de este caso, Google Inc. violó de los derechos del Sr. Costeja González y el Sr. Costeja tenía derecho a que se ordenara a Google Inc. que eliminara los enlaces a los artículos de sus resultados de búsqueda.

2.1.3 Comentarios al Caso Costeja

En apoyo del nuevo "Derecho al Olvido", el tribunal hace referencia frecuente a los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la UE (el derecho al respeto de la vida privada y la protección de los datos personales, respectivamente).

Lo que, sorprendentemente, quedó ausente del juicio es cualquier referencia al artículo 11 de la Carta, que protege la libertad de expresión, o la relevancia de ese derecho al equilibrio necesario entre los derechos de los titulares de los datos, los derechos de los responsables del tratamiento y de público en general que reciben la información que se publica.

Para examinar la relación con los derechos concurrentes de libertad de expresión y de información, conviene citar parte de las conclusiones del abogado general Sr. Niilo Jääskinen, en el caso:¹²⁰

120. El presente asunto afecta, desde múltiples puntos de vista, a la libertad de expresión e información consagrada en el artículo 11 de la Carta, concordante con el artículo 10 CEDH. El artículo 11, apartado 1, de la Carta establece que «toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras.»

121. El derecho de los usuarios de Internet a buscar o recibir información disponible en Internet está protegido por el artículo 11 de la Carta. Afecta tanto a la información contenida en las páginas web fuente cuanto a la información proporcionada por los motores de búsqueda. Como ya he mencionado, Internet ha revolucionado el acceso a todo tipo de información y su difusión, y ha puesto en marcha nuevos medios de comunicación y de interacción social entre particulares. A mi juicio, el derecho fundamental a la información merece protección particular en Derecho de la Unión Europea, particularmente a la luz de la tendencia cada vez mayor de los regímenes autoritarios en todo el mundo a limitar el acceso a Internet o a censurar el contenido disponible en él.

122. Los editores de páginas web disfrutan igualmente de protección con arreglo al artículo 11 de la Carta. Poner contenidos a disposición del público en Internet equivale, como tal, a la libertad de expresión, máxime cuando el editor ha enlazado su página a otras y no ha limitado su indexación o archivo por parte de los motores de búsqueda, indicando de este modo su deseo de

¹²⁰ Conclusiones del abogado general Sr. Niilo Jääskinen, *Op. cit.* Disponible en: <http://curia.europa.eu/juris/document/document.jsf?docid=138782&text=&doclang=ES&pageIndex=0&cid=5298824#Footnote1>. Consultado el 24 de abril de 2020.

que su contenido se difunda ampliamente. La publicación en la web es un medio para que los particulares participen en debates o difundan sus propios contenidos, o contenidos cargados por otros, en Internet.

123. En particular, la presente petición de decisión prejudicial versa sobre datos personales publicados en la hemeroteca de un periódico. En la sentencia *Times Newspapers Ltd. v. Reino Unido* (nº 1 y 2), el Tribunal Europeo de Derechos Humanos observó que los archivos en Internet realizan una contribución sustancial a la preservación y a la puesta a disposición de noticias e información: «tales archivos constituyen una fuente importante para la educación y la investigación histórica, en especial cuando están disponibles al público y son gratuitos con carácter general [...] Sin embargo, el margen de apreciación concedido a los Estados para ponderar los derechos en liza es más probable que sea mayor cuando se trata de archivos de noticias relativas a eventos pasados, más que a noticias que cubren asuntos de actualidad. Más concretamente, el deber de la prensa de actuar de acuerdo con los principios de periodismo responsable al garantizar la exactitud de la información histórica, antes de la actual, puede ser más estricto a falta de toda urgencia a la hora de publicar el material».

124. Los proveedores de servicios de motor de búsqueda en Internet comerciales ofrecen sus servicios de localización de información en el marco de actividad empresarial que tiene por objeto obtener beneficios de la publicidad a partir de palabras clave. Ello los convierte en empresas, cuya libertad reconoce el artículo 16 de la Carta con arreglo al Derecho de la Unión Europea y al Derecho nacional.

125. Además, debe recordarse que ninguno de los derechos controvertidos en el presente asunto es absoluto. Pueden limitarse, siempre que exista una justificación aceptable a la luz de los requisitos establecidos en el artículo 52, apartado 1, de la Carta.

Con este fallo se rompió con la tradición de la Corte Europea de Derechos Humanos, consagrada en el artículo 10, relativo a la protección de la libertad de expresión, entendido éste como uno de los fundamentos esenciales de una “sociedad democrática”, en este caso, el estudio relativo ha sido simplemente ignorado.

Lina Ornelas Núñez, jefa de Políticas Públicas y Relaciones con Gobierno para México, Centroamérica y el Caribe de Google, en el “Foro Derecho al Olvido, tutela integral de la privacidad. Visión Iberoamericana” dijo: “este buscador lo que hace es organizar la información que se sube a nivel mundial en la Web, por lo que no es responsable de eliminar datos con base en el Derecho al Olvido. Contrario a lo que sucede en la Unión Europea, añadió, en América Latina las cortes han resuelto que el ejercicio del derecho a la libertad de prensa, de expresión y buscar información, no puede estar sujeta a previa censura sino a restricciones determinadas por las leyes.”¹²¹

La Directiva de Protección de Datos fue promulgada en 1995¹²² para regular la recolección y tratamiento de datos personales, tanto de organismos privados como públicos; pero nunca tuvo la intención de regular las publicaciones en Internet.

Por tanto, la transposición del régimen de protección de datos de publicaciones en el mundo en general en Internet es muy problemático. Diferentes consideraciones surgen en relación con el contenido de publicaciones en internet, a las que se aplican a la gestión interna de la información de los organismos públicos y privados e incluso el intercambio de datos entre dichos organismos.

¹²¹ Cfr. “Ponderación y equilibrio entre los derechos al olvido y de información, plantean expertos”, Comunicado del INAI, no. INAI/226/16, 23 de agosto de 2016, disponible <http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-226-16.pdf>. Consultado el 25 de abril de 2020.

¹²² En este trabajo se utiliza indistintamente “Directiva” o “Directiva 95/46” para referirse a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, 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, disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=ES>. Consultada el 20 de abril de 2020.

En el contexto de la gestión de los datos personales por parte de organismos públicos y privados, una amplia definición de datos personales (cualquier información relativa a una persona física identificada o identificable) tiene sentido. Cuando se aplica sin mayor reflexión y análisis de las publicaciones para el público en general en Internet, esta amplia definición y la resultante falta de distinción significativa entre lo que es realmente privado y lo que es o debería ser público se vuelve muy problemático.

Actualmente, en Europa, Google ha atendido varias solicitudes de usuarios que quieren que sus nombres desaparezcan del buscador. Desde el lanzamiento de su formulario web para ejercer el Derecho al Olvido, en mayo de 2014, 174,266 solicitudes han sido presentadas para retirar 602,479 enlaces. Google ha eliminado 352,450 enlaces o el 58,5% de los resultados de búsqueda solicitados de toda Europa.¹²³

Francia ocupa el primer lugar con 34,632 solicitudes de 105,593 enlaces, Alemania en segundo lugar con 29,528 solicitudes de 103,089 enlaces y la tercera del Reino Unido con 22,467 solicitudes de 81,413 enlaces.¹²⁴

No obstante, atender las peticiones no es tarea fácil, ya que no solo implican un esfuerzo técnico y económico para Google, sino que implica asumir el rol de “juzgador”, al decidir si una solicitud es procedente o no.

Por esta razón, el grupo de reguladores y expertos en temas de privacidad de diferentes países de la Unión Europea conocido como el “Grupo de Trabajo del Artículo 29”,¹²⁵ creó una guía con 13 criterios para que Google y otros buscadores sepan cómo atender estas solicitudes.

¹²³ Texto traducido por la autora del presente ensayo, extraído de Samuel Gibbs, “EU to Google: expand ‘right to be forgotten’ to Google.com”, The Guardian, Thursday 27 Noviembre 2014 <http://www.theguardian.com/technology/2014/nov/27/eu-to-google-expand-right-to-be-forgotten-to-googlecom>

¹²⁴ *Idem*.

¹²⁵ El Grupo de Trabajo del Artículo 29 (GT29) (*The Article 29 Working Party*, en inglés) fue una organización de la Unión Europea que funcionaba como órgano asesor independiente sobre protección de datos y privacidad y estaba integrado por las autoridades de protección de datos recopilados de los Estados miembros. Fue sustituido por el Comité Europeo de Protección de Datos

2.2 Directrices para la implementación de la Sentencia del Tribunal De Justicia de la Unión Europea en el juicio "Google España y INC Vs. Agencia Española de Protección de Datos y Mario González Costeja" C-131/12¹²⁶

El 26 de noviembre de 2014, las autoridades europeas de protección de los datos reunidos en el Grupo de Trabajo del Artículo 29 (GT29)¹²⁷ adoptaron las directrices sobre la aplicación de la sentencia del TJUE. Estas directrices contienen la interpretación común de la sentencia, así como los criterios comunes para ser utilizados por las autoridades de protección de datos al tratar las quejas relacionadas con el Derecho al Olvido.¹²⁸

Las directrices del GT29 hacen diversas aclaraciones respecto al fallo del Tribunal de Justicia de la Unión Europea, entre ellas:¹²⁹

(CEPD) (*European Data Protection Board, EDPB*), constituida de forma similar, el 25 de mayo de 2018, cuando entró en vigor el Reglamento General de Protección de Datos (RGPD).

¹²⁶ Durante su primera reunión plenaria, el Comité Europeo de Protección de Datos (CEPD) aprobó las directrices del Grupo de Trabajo 29 relacionadas con el RGPD, disponibles en <https://edpb.europa.eu/node/89> Consultada el 18 de abril de 2020

¹²⁷ Es el sucesor del Grupo de Trabajo del Artículo 29 es el Comité Europeo de Protección de Datos (CEPD) (*European Data Protection Board, EDPB*) es un organismo europeo independiente que contribuye a la aplicación coherente de las normas de protección de datos en toda la Unión Europea y promueve la cooperación entre las autoridades de protección de datos de la UE. El CEPD está compuesto por representantes de las autoridades nacionales de protección de datos y del Supervisor Europeo de Protección de Datos (SEPD). También son miembros las autoridades de control de los Estados AELC de la AEMA en lo que respecta a los asuntos relacionados con el RGPD, sin derecho a voto ni a ser elegidos Presidente o Vicepresidentes. El CEPD se creó mediante el Reglamento General de Protección de Datos (RGPD) y tiene su sede en Bruselas. La Comisión Europea y (en lo que respecta a los asuntos relacionados con el RGPD) el Órgano de Vigilancia de la AELC tienen derecho a participar en las actividades y las sesiones del Consejo, sin derecho a voto. Información tomada de la página oficial del CEPD disponible en https://edpb.europa.eu/about-edpb/about-edpb_es. Consultada el 18 de abril de 2020

¹²⁸ Directrices para la implementación de la sentencia del tribunal de justicia de la unión europea en el juicio "Google España y Inc. v. Agencia Española de Protección de Datos (AEPD) Y Mario González Costeja" C-131/12, adoptadas el 26 de noviembre de 2014, disponibles en inglés en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf. Consultadas el 18 de abril de 2020.

¹²⁹ *Press Release Issued by the Article 29 Data Protection Working Party*, traducido por la autora del presente trabajo. Disponible en inglés, en http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20141126_wp29_press_release_ecj_de-listing.pdf. Consultado el 29 de mayo de 2020.

a) Confirmó la aplicabilidad de la Directiva 95/46¹³⁰ a un motor de búsqueda en cuanto exista un tratamiento de datos personales que se realice en el territorio de un Estado miembro, y establezca hasta la promoción y venta de espacios publicitarios en su motor de búsqueda del este Estado miembro con el objetivo de hacer que el servicio rentable.

b) Confirmó que la sentencia declara expresamente que el derecho sólo afecta a los resultados obtenidos de las búsquedas realizadas sobre la base del nombre de una persona y no requiere la supresión del enlace de los índices del motor de búsqueda en conjunto. Es decir, la información original siempre será accesible utilizando otros términos de búsqueda, o mediante acceso directo a la fuente.

c) De acuerdo con la legislación comunitaria, todo el mundo tiene derecho a la protección de datos. En la práctica, las Autoridades de Protección de Datos se centrarán en las reclamaciones donde hay un vínculo claro entre el interesado y la UE, por ejemplo, cuando el interesado es ciudadano o residente de un Estado miembro de la UE.

e) Los motores de búsqueda no deben informar a los web masters de las páginas afectadas por el traslado del hecho de que algunas páginas web no se pueden acceder desde el motor de búsqueda en respuesta a una consulta basada en el nombre específico. No hay ninguna base legal para tal comunicación de rutina bajo la ley de protección de datos de la UE.¹³¹

Las directrices también contienen la lista de criterios comunes que se aplicarán las autoridades de protección de datos para manejar las quejas

¹³⁰ Cfr. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, 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, disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=ES>. Consultada el 20 de abril de 2020.

¹³¹ Esta directriz se encuentra reflejada en el artículo 17.2 del RGPD y el razonamiento sigue siendo vigente, de acuerdo con las Directrices 5/2019 sobre los criterios del Derecho al Olvido en los casos de motores de búsqueda en el marco del RGPD (*Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR*) adoptadas el 2 de diciembre de 2019, por la Junta Europea de Protección de Datos (*European Data Protection Board, EDPB*), disponible en https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201905_rtbsearchengines_fo_rpublicconsultation.pdf. Consultado el 17 de abril de 2020.

presentadas ante sus oficinas nacionales tras la negativa de exclusión de la lista de motores de búsqueda. La lista contiene 13 criterios principales que deben servir a las Autoridades de Protección de Datos durante los procesos de toma de decisiones.¹³²

Los criterios serán aplicados en una base de caso por caso y de acuerdo con las legislaciones nacionales pertinentes. Ningún criterio tratado aisladamente ni es, en sí mismo, determinante. Cada uno de ellos tiene que ser leído a la luz de los principios establecidos por el Tribunal de Justicia y, en particular, a la luz del "interés del público en general en tener acceso a la información".¹³³

Luego de este breve estudio sobre el Derecho al Olvido, podemos decir que la resolución del Caso Costeja no trajo consigo la creación de un nuevo derecho, sino que se trata de la manifestación del Derecho de Cancelación o de Oposición, dependiendo del caso concreto.

Hemos analizado las causales de procedencia y de improcedencia del llamado Derecho al Olvido, y se destaca que esta prerrogativa busca defender el honor, el buen nombre de las personas, así como su integridad personal, siempre que existan razones legítimas para ejercerlo.

Por otro lado, gracias al estudio de las Directrices emitidas por el Artículo 29 para la interpretación del fallo del Tribunal de Justicia Europeo en el Caso Costeja,¹³⁴ pudimos acotar el alcance del fallo y se esclarecieron las dudas en

¹³² Cfr. Directrices para la implementación de la sentencia del tribunal de justicia de la unión europea en el juicio "Google España y Inc. v. Agencia Española de Protección de Datos (AEPD) Y Mario González Costeja" C-131/12, adoptadas el 26 de noviembre de 2014, disponibles en inglés en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf. Consultadas el 18 de abril de 2020.

¹³³ Los criterios fueron redactados por el Grupo de Trabajo del Artículo 29 y se encuentran disponible en <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommenda>. Consultadas el 18 de abril de 2020.

¹³⁴ Cfr. "Directrices para la implementación de la sentencia..." *Op. cit.* disponibles en inglés en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf. Consultadas el 18 de abril de 2020.

relación con el posible conflicto entre la libertad de expresión y el derecho a la información frente a la protección de la vida privada.

Especialmente porque las directrices dejan en claro que los buscadores no están facultados para cancelar información arbitrariamente sino mediante causa legítima.

Así también, las directrices señalan criterios y comentarios comunes que se aplicarán a las Autoridades de Protección de Datos para manejar las quejas presentadas ante sus oficinas nacionales tras la negativa de exclusión de la lista de motores de búsqueda.

Como hemos explicado en este capítulo las directrices de la organización artículo 29 constituyen una guía para que los tribunales puedan ponderar en sus resoluciones el derecho a la privacidad en torno a los contextos en que la información fue proveída –personal, laboral, informativo, de interés público- en los que se configura una esfera de situaciones que delimitan la aplicación del derecho.

2.3 Detalles técnicos y estadísticos de la Implementación de Google del Caso Costeja

En este apartado se destacan datos técnicos y estadísticos del Informe de Transparencia de Google¹³⁵ vigente al día 4 de octubre de 2019, con información de solicitudes de eliminación a partir del 29 de mayo de 2014.

Las Preguntas frecuentes sobre las solicitudes europeas de privacidad relacionadas con la eliminación de resultados de la búsqueda, se acompañan a esta investigación como ANEXO I.

Este informe brinda datos acerca de las URL eliminadas, el volumen de las solicitudes, las personas que las enviaron, y el contenido de los sitios web y las URL

¹³⁵ El reporte completo de transparencia de Google es interactivo y se encuentra disponible en: <https://transparencyreport.google.com/eu-privacy/overview>. Consultadas el 18 de abril de 2020

identificados en dichas solicitudes. Del informe más reciente de Google se desprenden las siguientes cifras:¹³⁶

a) El motor de búsqueda recibió 849,568 solicitudes de eliminación, lo que incluía 3,4 millones de páginas web en sus evaluaciones del Derecho al Olvido,

b) Se ha suprimido el 45 % de los enlaces problemáticos, la mayoría de los cuales eran de Facebook.

c) Las categorías de los sitios web que son mayormente eliminados son Directorios, medios sociales y noticias

d) Los sitios más afectados al momento de eliminar URL en búsquedas de Google son: Facebook, annuaire.118712.fr, Twitter y YouTube

e) Los países con el mayor número de solicitudes son Francia, Alemania y Reino Unido

f) Causales dominantes: eliminar información personal encontrado en redes sociales y sitios de directorio; y eliminar de la lista el historial legal y la información profesional reportada por medios de noticias y páginas gubernamentales.¹³⁷

¹³⁶ *Idem.*

¹³⁷ Bertram, Theo "Three Years of the Right to be Forgotten" (2018) <https://drive.google.com/file/d/1H4MKNwf5MgezTG7OnJRnl3ym3gIT3HUK/view>. Consultado el 1 de junio de 2020.

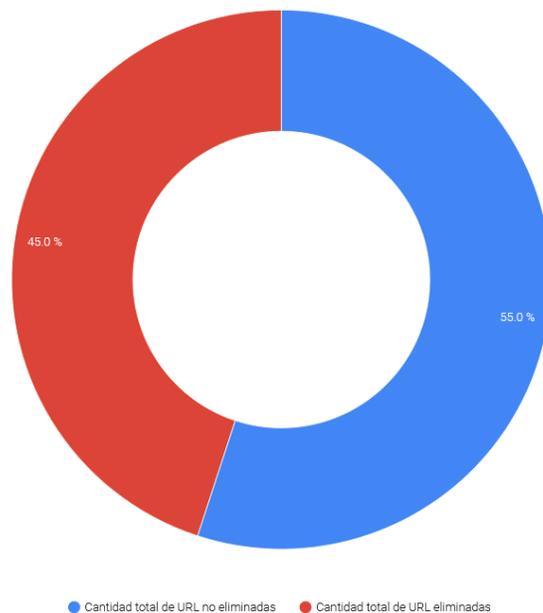


Figura 3. Grafica de URL suprimidas por Google

Fuente: Tomada del reporte de transparencia de Google, disponible en: <https://transparencyreport.google.com/eu-privacy/overview> Consultada el 18 de febrero de 2020.

2.4 ¿Cómo funciona el proceso de Google para solicitar la retirada de información personal?¹³⁸

Para efectos ejemplificativos, enseguida se expone la forma en la que Google aplica las solicitudes de supresión, de conformidad con el fallo del Tribunal de Justicia de la Unión Europea de mayo de 2014¹³⁹, mediante el cual, se decidió que los ciudadanos Europeos tienen el derecho de solicitar a los motores de búsqueda como Google que eliminen algunos resultados que se relacionen con ellas. Las instrucciones medulares son las siguientes:

¹³⁸ Información disponible en el apartado de Preguntas frecuentes sobre las solicitudes europeas de privacidad relacionadas con la eliminación de resultados de la búsqueda, disponible en: <https://support.google.com/transparencyreport/answer/7347822>

¹³⁹ “Asunto C-131/12...” *Op. cit.* Disponible en: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=E S&mode=lst&dir=&occ=first&part=1&cid=384212>. Consultado el 20 de abril de 2020

- a) Las personas interesadas o sus representantes deben completar un formulario web¹⁴⁰ (disponible en el ANEXO II).
- b) La persona recibirá una respuesta automática en la que se le confirmará la recepción de la solicitud.
- c) Las solicitudes se evalúan una por una. En algunos casos, es posible que Google solicite que la persona proporcione más información. Una vez que se tiene una decisión, la persona recibirá un correo electrónico en el que se le informará sobre la decisión y, en caso de que no se elimine el vínculo (URL o eliminar la página de los resultados de búsqueda en Google), se proporcionará una breve explicación. Aquí es importante destacar que no se elimina el contenido de la página, solo se eliminan URLs o páginas de los resultados de búsqueda.

Durante la evaluación de solicitudes de supresión, Google considera los siguientes criterios para determinar si la solicitud de supresión es procedente o no, enseguida se enlistan los criterios más relevantes:

- a) ¿La solicitud contiene toda la información necesaria para que podamos tomar una decisión?
- b) ¿La persona que presenta la solicitud tiene una conexión con un país europeo, como residencia o ciudadanía?
- c) ¿Las páginas aparecen en los resultados de la búsqueda del nombre del solicitante y el nombre del solicitante figura en las páginas que se piden eliminar?
- d) ¿La página que se solicita eliminar contiene información que es inadecuada, irrelevante, excesiva o que ya no se considera relevante, sobre la base de la información que proporciona el solicitante? ¿Existe un interés público de que

¹⁴⁰ Formulario para solicitar la retirada de información personal de Google, disponible en https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=637058084475494486-3571962074&rd=1 Consultado el 20 de febrero de 2020.

esa información se mantenga disponible en los resultados de la búsqueda que se generan al buscar el nombre del solicitante?

Considerando los criterios antes citados y después de hacer la evaluación correspondiente, Google procede a emitir el resultado de la solicitud de supresión. A este respecto, se investigaron los resultados emitidos por Google respecto de solicitudes, en donde se seleccionaron solicitudes al azar y los criterios de búsqueda fueron país y año; para efectos prácticos se diseñó un cuadro de resultados que ofrece el detalle de los resultados de las solicitudes de supresión que fueron seleccionadas por la autora de este trabajo, mismo que se inserta a continuación:

PAÍS	AÑO	SOLICITUD	RESULTADO
Alemania	2014	La víctima de una violación nos solicitó que elimináramos un vínculo a un artículo periodístico acerca del delito.	Eliminamos la página de los resultados de búsquedas que incluyen el nombre de la persona.
Reino Unido	2015	Después de que quitamos una noticia acerca de un delito menor, el periódico publicó una noticia sobre la eliminación La Oficina del Comisionado de Información nos ordenó eliminar la segunda noticia de los resultados de búsqueda del nombre de la persona.	Eliminamos la página de los resultados de búsquedas correspondientes al nombre de la persona.
Finlandia	2016	Recibimos una solicitud de la esposa de una persona fallecida en Finlandia para que	Eliminamos la URL en virtud de la ley de

		elimináramos una página de un foro de Búsqueda de Google que alegaba que la persona fallecida había cometido varios crímenes sexuales. La solicitud era para que elimináramos el contenido por respeto a la persona fallecida	protección de datos de Finlandia.
Chequia	2017	Recibimos una solicitud de un empresario para que elimináramos 3 URL de Búsqueda de Google, incluido 1 artículo periodístico, en el que se informaba sobre acusaciones de fraude contra la persona.	Como el empresario presentó prueba de absolución, eliminamos las 2 URL. No eliminamos la URL restante porque no estaba indexada en Búsqueda de Google.

Cuadro 6. Ejemplos de solicitudes que fueron procedentes, Google

Fuente: Elaboración propia (2019) con información del Explorador de solicitudes del Reporte de Transparencia de Google en: <https://transparencyreport.google.com/eu-privacy/overview>

Durante esta investigación llamó la atención los resultados que negaron la procedencia de las solicitudes supresión presentadas ante Google y se advirtió que las razones más recurrentes por las que Google decide no suprimir la página web de los resultados del motor de búsqueda son las que se enlistan enseguida:

- a) Existencia de soluciones alternativas, motivos técnicos o URL duplicadas.
- b) También es posible que determinemos que la página contiene información que es de gran interés público.
- c) Determinar si el contenido es de interés público es complejo y puede significar que se consideren diversos factores que incluyen, con carácter meramente taxativo, si el contenido se relaciona con la vida profesional del

solicitante, un delito que se cometió en el pasado, un cargo político, su posición en la vida pública o si el contenido es de autoría del solicitante, se trata de documentos del Gobierno o es de carácter periodístico.

Estos son algunos ejemplos solicitudes recibidas por Google, en donde el URL no fue eliminado:

PAÍS	AÑO	SOLICITUD	RESULTADO
Bélgica	2018	Recibimos una solicitud de un exconcejal del partido político Vlaams Blok para que elimináramos 8 URL de Búsqueda de Google. Estas páginas contenían información sobre el juicio y la condena del solicitante por un cargo de homicidio y dos de intento de homicidio.	No eliminamos ninguna de las URL debido a la anterior función política del solicitante y la gravedad de los crímenes.
España	2018	Recibimos una solicitud de un ministro de Infraestructura regional para que elimináramos 4 artículos periodísticos de Búsqueda de Google que mencionaban su condena por agredir a un miembro de su familia.	No eliminamos las 4 URL debido al interés público significativo que se generó debido al rol del demandante como funcionario del Gobierno.
Alemania	2016	Recibimos una solicitud para eliminar 4 artículos periodísticos sobre una investigación académica que contenía la fotografía de una persona,	No eliminamos los artículos, ya que todavía son relevantes para la

		porque el académico cambió de género y de nombre.	investigación y la vida profesional del académico.
Austria	2016	Recibimos un reclamo de la Autoridad de Protección de Datos de Austria en nombre de un empresario y expolítico austríaco para eliminar 22 URL, entre las que se incluían fuentes de noticias confiables y un informe del gobierno, de Búsqueda de Google.	No eliminamos las URL debido a su carácter anterior de figura pública, su prominencia en su profesión actual y la naturaleza de las URL en cuestión
Reino Unido	2014	Recibimos una solicitud de un ex clérigo para que elimináramos 2 vínculos a artículos que trataban sobre una investigación de acusaciones de abuso sexual durante su período de actividad profesional.	No eliminamos las páginas de los resultados de búsqueda.
Italia	2014	En reiteradas oportunidades, una persona nos solicitó que elimináramos veinte vínculos a artículos recientes acerca de su detención. El arresto se produjo por una serie de delitos financieros que la persona cometió como profesional.	No eliminamos las páginas de los resultados de búsqueda.

Cuadro 7. Ejemplos de solicitudes negadas por Google.

Fuente: Elaboración propia (2019) con información del Explorador de solicitudes del Reporte de Transparencia de Google en: <https://transparencyreport.google.com/eu-privacy/overview>

Categorías por solicitante:

Por otro lado, es importante destacar las categorías de los solicitantes de supresión, ya que con esto se puede determinar cuál es la población relevante que está haciendo ejercicio de este derecho:

- a) **Entidad corporativa:** El solicitante se comunica en nombre de una empresa o una corporación.
- b) **Persona fallecida:** El solicitante se comunica en nombre de una persona fallecida.
- c) **Funcionario público:** El solicitante es un político o funcionario del Gobierno actual o anterior.
- d) **Menor:** El solicitante es menor a la edad de consentimiento sexual.
- e) **Figura pública que no pertenece al Gobierno:** El solicitante es conocido a nivel internacional (p. ej., es una actriz o un actor famoso), o cumple un papel importante en la vida pública de una región o área específica (p. ej., es una académica reconocida en su campo).
- f) **Persona privada:** No se aplica ninguna de las otras categorías a esta persona.



Figura 4. Solicitantes del Derecho al Olvido.

Fuente: Michee Smith, "Updating our "right to be forgotten" Transparency Report", Febrero 26, 2018, disponible en <https://blog.google/around-the-globe/google-europe/updating-our-right-be-forgotten-transparency-report/> Consultada el 20 de febrero de 2020.

De la figura que antecede se puede concluir que en su gran mayoría (89%), los solicitantes de supresión son personas físicas y el restante son otros tipos de sujetos, en donde en primer orden hay solicitantes que son menores de edad, entidades corporativas y funcionarios públicos o políticos. Esto implica que este

derecho está beneficiando principalmente a ciudadanos con intereses de proteger su privacidad, o bien, hacer uso de sus derechos de protección de datos personales.

Categorías para el contenido de la página

- a) **Crimen:** El contenido de la página hace referencia al solicitante en relación con actos criminales. Por ejemplo, el contenido se relaciona con una condena del solicitante, su testimonio en un juicio o su condición de víctima.
- b) **No se encontró el nombre:** No se puede encontrar ninguna referencia al nombre del solicitante en la URL indicada. Sin embargo, es posible que el nombre de la persona aparezca en la URL.
- c) **Información insuficiente:** No se categorizó el contenido de la página porque Google requiere más información para procesar la solicitud. Por ejemplo, el solicitante proporcionó una URL incompleta o no indicó una razón para la eliminación de una URL.
- d) **Varios:** El contenido de la página no corresponde a ninguna de las otras categorías de contenido.
- e) **Información personal:** El contenido de la página incluye la dirección personal del solicitante, su residencia u otra información de contacto; imágenes o videos de la persona; o demás información personal no confidencial.
- f) **Política:** El contenido de la página incluye críticas sobre las actividades políticas o gubernamentales del solicitante, o información que es relevante al perfil, la plataforma o la trayectoria política pública de la persona.
- g) **Información profesional:** El contenido de la página incluye la dirección de trabajo del solicitante, su información de contacto o información general sobre sus actividades comerciales.
- h) **Ofensas profesionales:** El contenido de la página hace referencia a actividades criminales o penales (crímenes, absoluciones o exoneraciones) específicamente relacionadas con un rol profesional.
- i) **Autoría propia:** El solicitante es el autor, total o parcial, del contenido de la página.

- j) **Información personal confidencial:** El contenido de la página menciona el estado médico, la orientación sexual, el credo, el origen étnico o la afiliación política del solicitante.



Figura 5. Tipos de sitios que se someten a solicitudes de supresión.
Fuente: Michee Smith, "Updating our "right to be forgotten" Transparency Report", Febrero 26, 2018, disponible en <https://blog.google/around-the-globe/google-europe/updating-our-right-be-forgotten-transparency-report/> Consultada el 20 de febrero de 2020.

Como es de observar, las solicitudes recaen principalmente sobre directorios, redes sociales, artículos periodísticos y páginas de gobierno.

Alcances de la supresión del URL

Por último, es importante dejar claro que las páginas solo se eliminan de los resultados en respuesta a consultas relacionadas con el nombre de una persona, pero no se elimina la página per se. En este sentido, Google expone el siguiente ejemplo:

“Si se aceptara la solicitud para eliminar un artículo de John Smith sobre su viaje a París, no se mostraría el resultado para las consultas

relacionadas con [John Smith], pero sí se mostraría para una consulta como [viaje a París]. Eliminamos URL de todos los dominios europeos de Búsqueda de Google (google.fr, google.de, google.es, etc.) y usamos señales de ubicación geográfica para restringir el acceso a la URL desde el país de la persona que solicita la eliminación.

Por ejemplo, si elimináramos una URL como resultado de una solicitud de John Smith en el Reino Unido, los usuarios en esa ubicación no verían la URL en los resultados de la búsqueda para las consultas que incluyeran [John Smith] al buscar en cualquier dominio de Búsqueda de Google, incluido google.com. Por el contrario, los usuarios fuera del Reino Unido podrían ver la URL en los resultados al buscar [John Smith] en cualquier dominio no europeo de Búsqueda de Google.”¹⁴¹

Actualmente, Google establece mecanismos para retirar contenido que se encuentra en alguna plataforma Google, dependiendo del tipo de producto o aplicativo que sea operado por Google, el procedimiento es muy intuitivo y gratuito. Estos mecanismos están desarrollados para hacer frente a conflictos diversos a las regulaciones de privacidad, también buscan conciliar temas de propiedad intelectual.¹⁴²

¹⁴¹ Respuesta a Preguntas frecuentes sobre las solicitudes europeas de privacidad relacionadas con la eliminación de resultados de la búsqueda, ¿Las páginas se eliminan completamente de los resultados de la búsqueda? Disponible en <https://support.google.com/transparencyreport/answer/7347822>. Consultado el 06 de abril de 2020.

¹⁴² Cómo retirar contenido de Google <https://support.google.com/legal/troubleshooter/1114905#ts=1115657>. Consultado el 06 de abril de 2020.

2.5 El Reconocimiento el Derecho al Olvido Digital en España y en la Unión Europea

El debate sobre la existencia, extensión y límites del Derecho al Olvido es una de las cuestiones que se debaten en el derecho producto de las transformaciones originadas por el mundo digital. En este capítulo nos dispondremos a analizar la consolidación del Derecho al Olvido digital en Europa, para correlacionarlo con la experiencia nacional en la protección de datos en México. Como se observará en este trabajo el fundamento a partir del cual se puede derivar un Derecho al Olvido que ponga límites a la perennidad de la información en línea. En este orden de ideas precisaremos que a partir del derecho a la protección de datos y del derecho a la intimidad o a la vida privada es posible articular un derecho de las personas a oponerse a verse perseguidas por las informaciones del pasado.

Una de las primeras resoluciones de la Agencia Española de Protección de Datos (AEPD), fue el caso TD/00266/2007 en el que se asentó el precedente en cuanto a obligar a los motores de búsqueda a cancelar o desindexar ciertos enlaces¹⁴³, con el paso del tiempo estos criterios han adquirido matices, por

¹⁴³ En la Resolución TD/00266/2007 se exponen argumentos a favor de dotar de derechos a los titulares de datos frente a la perennidad de la información en la red: “[...] cabe proclamar que ningún ciudadano que ni goce de la condición de personaje público ni sea objeto de hecho noticiable de relevancia pública tiene que resignarse a soportar que sus datos de carácter personal circulen por la red sin poder reaccionar ni corregir la inclusión ilegítima de los mismos en un sistema de comunicación universal como Internet. Si requerir el consentimiento individualizado de los ciudadanos para incluir sus datos personales en Internet o exigir mecanismos técnicos que impidieran o filtraran la incorporación consentida de datos personales podría suponer una insoportable barrera al libre ejercicio de las libertades de expresión e información a modo de censura previa (lo que resulta constitucionalmente proscrito), no es menos cierto que resulta palmariamente legítimo que el ciudadano que no esté obligado a someterse a la disciplina del ejercicio de las referidas libertades (por no resultar sus datos personales de interés público ni contribuir, en consecuencia, su conocimiento a forjar una opinión pública libre como pilar básico del Estado democrático) debe gozar de mecanismos reactivos amparados en Derecho (como el derecho de cancelación de datos de carácter personal) que impidan el mantenimiento secular y universal en la red de su información de carácter personal.”

ejemplo, en la Resolución TD/01178/2012 de la AEPD, se recomendó a los medios de comunicación el uso de protocolos de exclusión para evitar la indexación por parte de los motores de búsqueda, respecto a aquellas noticias que habían dejado de ser relevantes; este mismo criterio se ha extendido a boletines públicos por considerar que ya no se verifica la finalidad que originó el tratamiento.¹⁴⁴

Contrario a lo que pudiera pensarse, la doctrina del Derecho al Olvido digital es un resultado de una participación activa de la Agencia Española de Protección de Datos (AEPD), en efecto, desde el año 2013, la AEPD ha estudiado casi un centenar de casos relacionados con el Derecho al Olvido digital frente a motores de búsqueda, en donde solo estimó como fundados 26 casos, bajo el supuesto de que era procedente el ejercicio de los derechos de oposición y cancelación en los casos en los que la información era obsoleta o no se cumplía con un finalidad legítima, o cuando el buscador hace caso omiso a los protocolos de exclusión.¹⁴⁵

Sin lugar a duda, se debe a la Agencia Española de Protección de Datos el reconocimiento al Derecho al Olvido digital, puesto que “fue la primera autoridad de datos que estimó la tutela de los derechos de cancelación y oposición, bajo la terminología del Derecho al Olvido digital frente a los motores de búsqueda”.¹⁴⁶ Y esta doctrina se basa en los principios de finalidad y consentimiento en el tratamiento de datos personales.

Por otro lado, la posición de la AEPD ha sido cuestionada desde la perspectiva de la doctrina pues se considera que atribuir a los buscadores la responsabilidad de garantizar la cancelación de datos y no a los responsables de la publicación de la información es excesiva.

¹⁴⁴ Castellano, Pere Simón, El reconocimiento del Derecho al Olvido en España y en la Unión Europea, Primera Edición, España, 2015. p. 297

¹⁴⁵ *Idem.*

¹⁴⁶ *Idem.*

2.6 Efectos tras la sentencia del Tribunal de Justicia de la Unión Europea.

De la Sentencia del Tribunal de Justicia de la Unión Europea (C-131/12, §28, 60) se advierten tres efectos trascendentales, mismos que se enuncian enseguida:

- (1) Jurisdicción: La empresa gestora de un motor de búsqueda está sujeta a la normativa europea de protección de datos, sin importar que la matriz radique fuera de la Unión Europea, siempre que: mantenga un establecimiento en un Estado Miembro a través del cual desarrolle una actividad económica vinculada con el motor de búsqueda (como lo es la venta de publicidad dirigida a los residentes de ese Estado Miembro).
- (2) Alcance de la Directiva 95/46/CE: Se concluye que la actividad de indexación que realiza un motor de búsqueda implica un tratamiento de datos personales.
- (3) Alcance de la Directiva 95/46/CE: El motor de búsqueda es responsable del tratamiento de datos personales al “establecer los fines y los medios” del tratamiento.

Estos criterios emitidos en la sentencia de referencia han abierto la posibilidad de que los afectados por la indexación del motor de búsqueda, pueda iniciar acciones de reparación de daño.¹⁴⁷

2.7 El papel de las Autoridades Europeas de Protección de Datos.

En 1982, la Autoridad Francesa de Protección de Datos Personales (Commission Nationale de l'Informatique et les Libertés, CNIL) reconoció la existencia del

¹⁴⁷ Cfr. Sentencia del Tribunal de Gran Instancia de París 16 de septiembre de 2014 y Sentencia de la Audiencia Provisional de Barcelona, núm. 364/2014, 17 de julio de 2014.

Derecho al Olvido en el contexto del principio de finalidad. De hecho, el propio ex presidente de la CNIL, Alex Türk abordó en Derecho al Olvido como un “derecho a desaparecer del sistema” (droit à l’oubli numérique), que se traduce en la facultad de impedir que terceros accedan a información que carece de notoriedad pública.¹⁴⁸ Más adelante, en 2009, la CNIL reconoció el Derecho al Olvido como “el derecho a cambiar de opinión, religión, opinión política, la posibilidad de cometer errores en la juventud, o incluso el derecho a cambiar de vida”.¹⁴⁹

Por otro lado, en una línea muy parecida a la doctrina que ha elaborado la AEPD, desde 2004, la Autoridad de Protección de Datos de Italia (Garante per la Protezione dei Dati Personali) fundó sus decisiones en el principio de finalidad, bajo el argumento de que sólo pueden utilizarse para una finalidad legítima y concreta, y una vez que desaparecen estos supuestos, se debe proceder a la cancelación.¹⁵⁰

En el caso de la Agencia Española de Protección de Datos, la concepción del Derecho al Olvido va más allá puesto que lo que se interpreta desde el ejercicio del derecho de cancelación y oposición, en el marco de los principios de finalidad y calidad, en efecto, la AEPD considera responsable del tratamiento a “aquél que difunde originariamente información en la red, como a aquellos intermediarios que por su actividad en la propia arquitectura de Internet se encargan de seleccionar, clasificar y ofrecer resultados de búsqueda a cibernautas”.¹⁵¹

En conclusión, se observa que tanto las autoridades de Francia e Italia ya reconocían la existencia del Derecho al Olvido a través de los principios previstos

¹⁴⁸ Castellano, Pere Simón, El reconocimiento del Derecho al Olvido en España y en la Unión Europea, Primera Edición, España, 2015. p. 228 y 298 a 299.

¹⁴⁹ 30ème rapport d’activité de la CNIL, 2009, Paris, La Documentation Française, pág. 29, disponible en https://www.cnil.fr/sites/default/files/typo/document/CNIL-30erapport_2009.pdf. Consultado el 29 de mayo de 2020.

¹⁵⁰ *Ibidem*, p. 299

¹⁵¹ *Ibidem*, p. 299 y 300.

en el marco de la Directiva 95/46/CE, en especial el principio de finalidad, no obstante, el aporte de la Agencia Española de Protección de Datos reside en estimar que el Derecho al Olvido debía configurarse a través de los derechos de cancelación y oposición frente a tratamientos ilegítimos a cargo de motores de búsqueda.

2.8 La incorporación del Derecho al Olvido en el Proceso de reforma de la Directiva 95/46/CE

El Derecho al Olvido fue ganando mayor importancia en el debate público de Europa, luego de que diversas autoridades de datos optaran por imponer el Derecho al Olvido para hacer frente a la perennidad de la información en la red y considerando la preocupación de la sociedad frente a la sobreexposición y sobreutilización de los datos personales en el entorno digital.

Es bajo este contexto que, en junio de 2011, se emitió el “Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Un enfoque global de la protección de los datos personales en la Unión Europea”. En dicho dictamen se advierte que el Derecho al Olvido es derecho necesario para objetar el tratamiento ulterior de los datos personales, así como una obligación para el responsable del tratamiento de suprimir la información cuando ya no sea necesaria a los fines del tratamiento.¹⁵²

¹⁵² *Cfr.* “Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Un enfoque global de la protección de los datos personales en la Unión Europea”, disponible en https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_es.pdf Consultado el 1 de junio de 2020.

6.5. La portabilidad de los datos y el Derecho al Olvido

83. La portabilidad de los datos y el derecho a ser olvidado son dos nociones interrelacionadas y presentadas en la comunicación con el fin de reforzar los derechos de los interesados. Vienen a complementar los principios ya indicados en la Directiva, que establecen el derecho del interesado

Desde entonces, la Comisión Europea ha considerado necesario el establecimiento de un marco más sólido y coherente de protección de datos que armonice las diferencias existentes entre las distintas legislaciones nacionales, fue así como inició el proceso de reforma de la ya desactualizada Directiva 95/46/CE, para culminar en el Reglamento General de Protección de Datos (RGPD) de la Unión Europea cuya propuesta contempla expresamente en su artículo 17 una regulación del Derecho al Olvido. el cual incorpora dentro de su normativa al Derecho al Olvido, también llamado “Derecho de Supresión”.¹⁵³

En efecto, el RGPD en su capítulo de “Considerandos” se pronuncia entorno a la necesidad de regular el llamado Derecho al Olvido y por su relevancia, se cita íntegramente:

(65) Los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un «Derecho al Olvido» si la retención de tales datos infringe el presente Reglamento o el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento. En particular, los interesados deben

a expresar una objeción al tratamiento ulterior de sus datos personales así como una obligación para el responsable del tratamiento de suprimir la información cuando ya no sea necesaria a los fines del tratamiento.

84. Estos dos nuevos conceptos tienen, ante todo, un valor añadido en el contexto de la sociedad de la información, en la que cada vez es mayor el número de datos que se almacena de manera automática y se conservan durante periodos indeterminados. En la práctica se demuestra que, incluso cuando es el propio interesado quien aporta los datos, su grado de control efectivo sobre los mismos es muy limitado, lo cual resulta aún más incuestionable a la vista de la enorme memoria que representa hoy en día Internet. Además, desde un punto de vista económico, resulta más costoso para el responsable del tratamiento suprimir los datos que conservarlos almacenados. El ejercicio de los derechos de las personas es contrario, por tanto, a la tendencia económica natural.

85. Tanto la portabilidad de los datos como el Derecho al Olvido podrían contribuir a inclinar la balanza a favor del interesado. La portabilidad de los datos tendría por objeto proporcionar un mayor grado de control a las personas sobre su información, mientras que el Derecho al Olvido garantizaría que la información desaparece automáticamente al cabo de un determinado periodo, incluso si el interesado no realiza ninguna acción en este sentido o desconoce que los datos fueron almacenados.

¹⁵³ Cfr. Artículo 17 del Reglamento General de Protección de Datos (RGPD).

tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento. Este derecho es pertinente en particular si el interesado dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet. El interesado debe poder ejercer este derecho, aunque ya no sea un niño. Sin embargo, la retención ulterior de los datos personales debe ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones.

(66) A fin de reforzar el «Derecho al Olvido» en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la

tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales.¹⁵⁴

La Comisión Europea ante las experiencias que hemos narrado en párrafos precedentes decidió avanzar hacia la redacción de una propuesta de Reglamento que regula el Derecho al Olvido digital. Dicho reglamento en el artículo 17 dejó prescrito lo siguiente:

“Artículo 17. Derecho al Olvido y a la supresión.

1. El interesado tendrá derecho a que el responsable del tratamiento suprima los datos personales que le conciernen y se abstenga de darles más difusión, especialmente en lo que respecta a los datos personales proporcionados por el interesado siendo niño, cuando concurra alguna de las circunstancias siguientes:
 - a) Los datos ya no son necesarios en relación con los fines para los que fueron recogidos o tratados;
 - b) El interesado retira el consentimiento en que se basa el tratamiento de conformidad con lo dispuesto en el artículo 6, apartado 1, letra a), o ha expirado el plazo de la conversación autorizado y no existe otro fundamento jurídico para el tratamiento de los datos;
 - c) El interesado se opone al tratamiento de datos personales con arreglo a lo dispuesto en el artículo 19;
 - d) El tratamiento de datos no es conforme con el presente Reglamento por otros motivos”.

¹⁵⁴ “Reglamento (UE) 2016/679...” *Op. cit.* párrafos 65 y 66, pp. 12-13. Disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=EN> Consultado el 1 de junio de 2020.

El primer apartado del artículo 17 establece así el derecho del interesado al olvido, conectándolo fundamentalmente con la facultad de cancelación de supresión de los datos personales, si bien exigiendo que el responsable del tratamiento se abstenga de darles mayor difusión.

Cuatro son las circunstancias que permitirían el ejercicio del Derecho al Olvido digital:

1. Cuando se retira el consentimiento del titular de los datos o ha expirado el plazo de conservación autorizado;
2. Cuando el interesado se opone al tratamiento de datos personales;
3. Cuando el tratamiento de datos no es legítimo ya sea porque no existe consentimiento o porque no existe ninguna razón o fin legítimo que justifique su tratamiento;
4. Las excepciones a la facultad de suprimir los datos que se incorporan especialmente en el artículo 17.

El primer apartado del artículo 17 establecía así el derecho del interesado al olvido, conectándolo fundamentalmente con la facultad de cancelación de supresión de los datos personales, si bien también exigiendo que el responsable del tratamiento se abstenga de darles mayor difusión. Cuatro son las circunstancias o situaciones a las que se refería el apartado primero del artículo 17 que permitiría el ejercicio del Derecho al Olvido digital:

Cuando los datos ya no son necesarios para la finalidad por la que fueron recogidos o tratados:

1. Cuando se retira el consentimiento del titular de los datos o ha expirado el plazo de conservación autorizado
2. Cuando el interesado se opone al tratamiento de los datos personales salvo que el tratamiento acredite motivos imperiosos y legítimos para el tratamiento

prevalezcan sobre los intereses o derechos y libertades fundamentales de interesado;

3. Cuando el tratamiento de datos no es legítimo que justifique su tratamiento, ya sea porque no existe ninguna razón o fin legítimo que justifique su tratamiento;
4. Las excepciones a la facultad de suprimir datos personales se incorporan en el artículo 17 del reglamento, que, a nuestro juicio, recoge casos en que existe un interés legítimo para el tratamiento y difusión de los datos personales, los pueda eliminar.

La conservación de datos personales se permitirá en aquellos casos en que sean necesarios para el ejercicio del derecho de libertad de expresión, para el ejercicio de la investigación histórica, estadística y científica para el cumplimiento de una obligación legal impuesta por el derecho de la unión o por la legislación de un Estado miembro. Se concibe el Derecho al Olvido digital básicamente como un derecho a cancelar o eliminar los datos personales cuando se han agotado las finalidades legítimas para las que se recogieron o trataron, cuando se ha revocado el consentimiento o cuando se trata de un tratamiento de datos lícito.

Actualmente, el RGPD supone el máximo estándar legal en la protección de datos personales y su alcance extraterritorial ha puesto sobre la agenda internacional, la necesidad de adecuación de normas nacionales o domésticas para homologar estándares de protección,¹⁵⁵ en aras de dotar de mayores recursos a los

¹⁵⁵ “Desde la aplicación del Reglamento General de Protección de Datos (RGPD) el pasado mes de mayo de 2018, se ha vivido en todo el mundo, no solo en Europa, una revolución normativa con el objetivo de adaptar la legislación de todos los países a la nueva realidad imperante en materia de protección de datos.” Gonzalo Domenech Juan José, Sección “Cinco días”, periódico en línea “El País”, Madrid, 23 de septiembre de 2019, disponible en: https://cincodias.elpais.com/cincodias/2019/09/20/legal/1568964983_535059.html Consultado el 15 de abril de 2020.

titulares para un efectivo ejercicio del derecho humano de privacidad y de protección de datos personales.

2.9 Vacío legal y Derecho al Olvido, percepción en el contexto mexicano de la sentencia del Tribunal de Justicia de la Unión Europea.

El Derecho al Olvido como resultado del ejercicio de los derechos de cancelación y oposición previstos en la normativa de protección de datos, ha sido objeto de numerosas críticas.

Algunos doctrinarios consideran que los derechos de Acceso, Rectificación, Cancelación y Oposición, por sus siglas “ARCO” no alcanzan para ejercer el Derecho al Olvido, de ahí que en nuestro país no sea posible borrar nuestra huella digital.

Se tiene poco o casi nulo control sobre cualquier tipo de información que se publica en internet, pues en este país no es posible ejercer el Derecho al Olvido para eliminar los datos personales de la web. “Además, el Derecho al Olvido contempla solicitar que no se muestren datos personales e información pública de registros oficiales. Por ejemplo, que sea obsoleta o que ponga en riesgo algún otro derecho del titular de la información; mientras los Derechos ARCO sólo contemplan datos personales.”

El principal argumento en contra del reconocimiento del Derecho al Olvido en nuestro país y otros sistemas jurídicos es que supondría hacer posible borrar o reescribir la historia. Implicaría otorgar a las personas la facultad de alterar la objetividad de lo ocurrido, modificando su contenido o imposibilitando a los demás el acceso a esa información.

Sin embargo, tanto la Ley Federal de Protección de Datos Personales en Posesión de Particulares, como la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, señalan que los datos personales (cualquier información concerniente a una persona física identificada o identificable. Por ejemplo: el nombre, domicilio, imagen o número telefónico) es susceptible de protección de los Derechos ARCOS en el contexto digital.

Así, tenemos que, los usuarios de Internet tienen el derecho a solicitar que se supriman sus datos en posesión de particulares, tales como redes sociales y buscadores en Internet. Bajo esta perspectiva la primera aproximación del Derecho al Olvido se identifica con el derecho de oposición y cancelación en el derecho mexicano, a saber:

Aproximaciones de la Definición del Derecho al Olvido	
Derecho de Oposición	Derecho al Olvido
LFPDPPP Artículo 27.- El titular tendrá derecho en todo momento y por causa legítima a oponerse al tratamiento de sus datos. De resultar procedente, el responsable no podrá tratar los datos relativos al titular.	1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernen, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:
Derecho de Cancelación	

<p>LFPDPPP Artículo 25.- El titular tendrá en todo momento el derecho a cancelar sus datos personales.</p> <p>La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual <u>se procederá a la supresión del dato</u>. El responsable podrá conservarlos exclusivamente para efectos de las responsabilidades nacidas del tratamiento. El periodo de bloqueo será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en los términos de la Ley aplicable en la materia.</p> <p>Una vez cancelado el dato se dará aviso a su titular.</p> <p>Cuando los datos personales hubiesen sido transmitidos con anterioridad a la fecha de rectificación o cancelación y sigan siendo tratados por terceros, el responsable deberá hacer de su conocimiento dicha solicitud de</p>	<p>a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;</p> <p>b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;</p> <p>c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;</p> <p>d) los datos personales hayan sido tratados ilícitamente;</p> <p>d) los datos personales 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;</p>
---	---

<p>rectificación o cancelación, para que proceda a efectuarla también.</p> <p>LFPDPPP Artículo 26.- El responsable no estará obligado a cancelar los datos personales cuando:</p> <ul style="list-style-type: none"> I. Se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento; II. Deban ser tratados por disposición legal; III. Obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas; IV. Sean necesarios para proteger los intereses jurídicamente tutelados del titular; V. Sean necesarios para realizar una acción en función del interés público; 	<p>e) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.</p> <p>2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.</p> <p>3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:</p> <ul style="list-style-type: none"> a) para ejercer el derecho a la libertad de expresión e información;
---	--

<p>VI. Sean necesarios para cumplir con una obligación legalmente adquirida por el titular, y</p> <p>VII. Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto.</p> <p>Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponde.</p>	<p>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;</p> <p>c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;</p> <p>d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o</p> <p>e) para la formulación, el ejercicio o la defensa de reclamaciones.</p>
---	---

Cuadro 8. Aproximaciones de la definición de Derecho al Olvido.
Fuente: Elaboración Propia.

Estas leyes establecen que los titulares pueden ejercer en todo momento los derechos de acceso, rectificación, cancelación y oposición de sus datos personales. Es importante recalcar que muchos proveedores de servicios por Internet no se encuentran asentados en México, esto se traduce en jurisdicción y límites de territorialidad poco claras, en otras palabras, no es posible aplicar la normatividad y por tanto el Derecho al Olvido no puede ser plenamente garantizado.

La principal confrontación de derechos que produce la ausencia de la regulación del Derecho al Olvido en el contexto mexicano se ubica en la frontera del Derecho al Olvido y la actuación de los medios de comunicación. El conflicto entre el Derecho al Olvido y el ejercicio de la libertad de expresión e información por los medios de comunicación puede darse en dos hipótesis principales: la publicación actual de una información pasada y el mantenimiento de noticias publicadas en los archivos digitales del medio de comunicación accesibles en línea. El primer grupo de casos puede resolverse a partir de los criterios consolidados sobre los conflictos entre los derechos de la personalidad y las libertades comunicativas. El segundo, en cambio, presenta algunas peculiaridades que precisan una adaptación de los criterios generales de ponderación.

Como expusimos en este capítulo a nivel internacional España a través de sentencia del Tribunal de Justicia de la Unión Europea sentó un precedente en el que determinó que el motor de búsqueda de Google sí realiza tratamiento de datos personales y que sus filiales deben responder a las solicitudes de cancelación de estos.

Sin embargo, la autoridad garante de los Derechos ARCO en México, el INAI, a pesar de haber atendido diversos recursos donde el ciudadano solicita al instituto la protección de sus datos personales de plataformas como Google, Yahoo! y

YouTube, entre otros. El instituto ha desechado los recursos porque las filiales de las empresas señaladas indican que sus matrices de Estados Unidos son las que se encargan de administrar los servicios o porque simplemente, no tienen sede en el país. En ese mismo orden de ideas el único caso que procedió fue uno que se presentó contra Google en 2014 donde un ciudadano solicitaba retirar su información de los resultados de la búsqueda.

Ello refleja una postura conservadora de la autoridad nacional mexicana, en la que se ha omitido recuperar los elementos valiosos de la experiencia europea, a saber:

- a) No se considera que el Derecho al Olvido sólo procede en casos que no tengan relevancia pública ni interés histórico.
- b) No se considera que la ausencia de reconocimiento del derecho se convierte en un mecanismo paradójico de defensa de la corrupción y de restricción a la libertad de información.

De otro modo el INAI no ha realizado un trabajo de ponderación de derechos, en esencia no recupera las excepciones del Derecho al Olvido que prevé la resolución para que la sociedad pueda conocer datos y hechos que son de claro interés público. Es decir, el INAI otorga protección en contra del derecho a saber, contrariando su naturaleza como órgano garante de las tendencias internacionales al respecto.

El Derecho al Olvido debe ser discutido con sus matices, pero evidentemente en ningún caso debe ser instrumento para coadyuvar a la corrupción, alimentar la falta de rendición de cuentas y fomentar, en última instancia, la impunidad.”¹⁵⁶

¹⁵⁶ Villanueva, Ernesto. “Derecho al olvido.” Proceso Portal de Noticias. 1 octubre de 2016, México. Disponible en: <https://www.proceso.com.mx/457073/derecho-al-olvido>. Consultado el 01 de junio de 2020.

En estos casos cuando el sistema judicial no funciona adecuadamente, desde nuestro punto de vista corresponde a la autoridad nacional protectora de datos personales analizar la ilicitud en el tratamiento de datos del sitio de internet porque ellos tendrían que decirles a los titulares de los datos que también se van a publicar para la finalidad del buscador y no poner un robot de exclusión, motores de búsqueda quienes desarrollan una función esencial de organización de la información disponible en la red y de facilitar el acceso a ello.



Capítulo 3

Regulación del Derecho al Olvido desde el RGPD



Capítulo 3. Regulación del Derecho al Olvido desde el RGPD

El pasado 25 de mayo de 2018, entró en vigor la nueva regulación en materia de Protección de Datos en Europa¹⁵⁷ (el Reglamento general de protección de datos (en adelante, “RGPD”, por sus siglas en inglés), dicha regulación se funda en el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, el cual reconoce que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

De las consideraciones del RGPD, se desprende que el espíritu de esta norma reconoce que el derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad.¹⁵⁸

Por otro lado, señala que el tratamiento de datos personales debe estar concebido para servir a la humanidad y que este derecho debe ser armónico con otros derechos fundamentales y libertades como: la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística.¹⁵⁹

Bajo este contexto, esta Regulación establece parámetros que buscan reforzar el Derecho al Olvido¹⁶⁰ en el entorno digital, a través del “derecho de supresión” que se funda en el artículo 17 del RGPD:

¹⁵⁷ “Reglamento (UE) 2016/679...” *Op. cit.* Disponible en <https://eur-lex.europa.eu/eli/reg/2016/679/oj/spa> Consultado el 16 de abril de 2020.

¹⁵⁸ *Ibidem*, Cuarto párrafo de los considerandos, p. 2. Disponible en <https://eur-lex.europa.eu/eli/reg/2016/679/oj/spa> Consultado el 16 de abril de 2020.

¹⁵⁹ *Idem*.

¹⁶⁰ Se hace notar que el Reglamento General de Protección de Datos en el artículo 17 sí hace referencia al llamado Derecho al Olvido, de hecho, el título de ese artículo es Artículo 17 Derecho de supresión («el Derecho al Olvido»), Cfr. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo

“El derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales.”¹⁶¹

3.1 Principios del RGPD

El artículo 5 del RGPD enumera los principios que deben regir todo tratamiento de datos personales: licitud, lealtad y transparencia; Limitación de la finalidad; Minimización de datos; Exactitud; Limitación en el plazo de conservación; Integridad y confidencialidad; y responsabilidad proactiva, cada uno se describe en el siguiente cuadro:

PRINCIPIO	ALCANCES
LICITUD, LEALTAD Y TRANSPARENCIA (Lawfulness, fairness and transparency)	Los datos serán tratados de manera lícita, leal y transparente en relación con el interesado
LIMITACIÓN DE LA FINALIDAD	Los datos serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; el tratamiento

que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) Disponible en <https://eur-lex.europa.eu/eli/reg/2016/679/oj/spa> Consultado el 16 de abril de 2020.

¹⁶¹ *Ibidem*, párrafo 66.

(Purpose limitation)	ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales
MINIMIZACIÓN DE DATOS (Data minimisation)	Los datos serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados
EXACTITUD (Accuracy)	Los datos serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan [estrecha relación con el Derecho al Olvido]
LIMITACIÓN DEL PLAZO DE CONSERVACIÓN (Storage limitation)	Los datos serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas
INTEGRIDAD Y CONFIDENCIALIDAD (Integrity and confidentiality)	Los datos serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la <u>protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental</u> , mediante la aplicación de medidas técnicas u organizativas apropiadas

RESPONSABILIDAD PROACTIVA (accountability)	El responsable del tratamiento será responsable del cumplimiento de los principios y capaz de demostrarlo
--	---

Cuadro 9. Principios del RGPD.
Fuente: Elaboración Propia.

Como se puede apreciar del cuadro antes insertado, el RGPD comparte prácticamente los mismos principios con la LFPDPPP, es decir, licitud, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad; las grandes diferencias que encontramos son:

- a) Consentimiento: La legislación mexicana sí recoge el “Consentimiento” como un principio fundamental en el tratamiento de datos personales, mientras que el RGPD le apuesta a un tratamiento en el marco de una base legal o un interés legítimo, en donde cabe la recolección basada en la obtención del consentimiento. Los estándares del tratamiento basado en el consentimiento del RGPD son muy estrictos, puesto que debe obtenerse: mediante un acto afirmativo claro que establezca una indicación libremente dada, específica, informada y sin ambigüedades (todos, elementos acumulativos).
- b) Seguridad: El RGPD eleva como principio la “integridad y confidencialidad” en el tratamiento de datos personales, mientras que, en la regulación mexicana, recoge estos estándares de seguridad como obligaciones del responsable.
- c) Plazo de conservación: El RGPD también impone como principio la “limitación del plazo de conservación” en aras de obligar a los responsables a mantener la información solo por el tiempo que sea necesario conforme a las finalidades del tratamiento, para el caso de la legislación mexicana, los plazos de conservación también dependerán de las finalidades del tratamiento, pero no representan un principio sino una obligación para los responsables del tratamiento.

Lo anterior se expone de manera didáctica en el siguiente cuadro comparativo:

PRINCIPIO	LFPDPPP MX 2010	RGPD 2018
LICITUD	✓ LFPDPPP, art. 7 RLFPDPPP, art. 10	✓
LEALTAD	✓ LFPDPPP, art. 7 RLFPDPPP, art. 44 (expectativa razonable de privacidad)	✓
TRANSPARENCIA	✓ [Principio de información] LFPDPPP, art. 15 RLFPDPPP, art. 23	✓
LIMITACIÓN DE LA FINALIDAD	✓ [Principio de finalidad] LFPDPPP, art. 12 RLFPDPPP, art. 40	✓
MINIMIZACIÓN DE DATOS	[Principio de proporcionalidad] LFPDPPP, art. 13 RLFPDPPP, art. 45 La minimización es un criterio y no un principio RLFPDPPP Artículo 46.	✓
EXACTITUD	[Principio de Calidad] LFPDPPP, art. 11	✓

	<p>pertinentes, correctos y actualizados</p> <p>RLFPDPPP art.36 exactos, completos, pertinentes, correctos y actualizados</p>	
LIMITACIÓN DEL PLAZO DE CONSERVACIÓN	<p>X</p> <p>[Plazos de conservación de los datos personales]</p> <p>LEY Artículo 12 RLFPDPPP Artículo 37. (es un deber no es un principio)</p>	✓
INTEGRIDAD Y CONFIDENCIALIDAD	<p>X</p> <p>[Seguridad]</p> <p>LFPDPPP, art. 19, 21 (La confidencialidad es un deber no es un principio)</p>	✓
RESPONSABILIDAD PROACTIVA	<p>✓</p> <p>[Responsabilidad]</p> <p>LFPDPPP, art. 14 RLFPDPPP Art. 47 (el responsable tiene la carga de la prueba)</p>	✓
CONSENTIMIENTO	<p>✓</p> <p>LFPDPPP Art. 8 RLFPDPPP Art. 11</p>	<p>X</p> <p>[Bases legales]¹⁶²</p>

¹⁶² El Reglamento General de Protección de Datos requiere que los responsables (controladores) de datos demuestren una de estas seis bases legales para el procesamiento: consentimiento, necesidad, requisito de contrato, obligación legal, protección del interesado, interés público o interés legítimo del controlador. Se requiere que el controlador proporcione un aviso de privacidad, especifique en el aviso de privacidad la base legal para el procesamiento de datos personales en cada instancia de procesamiento, y cuando confíe en el motivo de interés legítimo debe describir los intereses legítimos perseguidos. Cfr. RGPD, Art. 6.

	(El consentimiento deberá ser previo al tratamiento)	
--	--	--

Cuadro 10. Comparativa de principios entre el RGPD y la LFPDPPP.
Fuente: Elaboración Propia.

A pesar de que los principios son muy similares, cada regulación propone estándares especiales, en donde destaca el cuidado en los detalles tecnológicos del RGPD y en las reglas que se deben seguir para que cada principio sea asequible y verificable en la mejor medida posible.

3.2 Derechos de los Individuos bajo el RGPD

Y bien, el RGPD incorpora derechos de la protección de datos que están diseñados para el entorno digital:

- a) **Derecho a la portabilidad:** El artículo 20 del RGPD establece que en ciertas circunstancias, generalmente cuando el procesamiento de datos se realiza sobre la base de un consentimiento o un contrato, los interesados tienen derecho a recibir sus datos personales, que han proporcionado a un controlador, en un formato estructurado, de uso común y legible por máquina y tiene derecho a transmitir esos datos a otro controlador sin obstáculos del controlador al que se le han proporcionado los datos personales.
- b) **Derechos relacionados con decisiones individuales automatizadas, incluida la elaboración de perfiles:** El artículo 22 del RGPD prevé disposiciones sobre:
 - toma de decisiones individual automatizada (tomar una decisión únicamente por medios automatizados sin ninguna participación humana); y
 - elaboración de perfiles (procesamiento automatizado de datos personales para evaluar ciertas cosas sobre un individuo). La creación de perfiles puede ser parte de un proceso automatizado de toma de decisiones.

c) Derecho al Olvido: El artículo 17 (1) del RGPD establece que los interesados tienen derecho a borrar sus datos personales si: los datos ya no son necesarios para su propósito original y no existe un nuevo propósito legal; la base legal para el procesamiento es el consentimiento del interesado, el interesado retira ese consentimiento y no existe ningún otro motivo legal; el interesado ejerce el derecho a oponerse, y el controlador no tiene motivos fundamentales para continuar el procesamiento; los datos han sido procesados ilegalmente; o el borrado es necesario para cumplir con la ley de la UE o la ley nacional del estado miembro correspondiente. Este derecho será estudiado a fondo en este capítulo

Nuevamente, bajo un marco comparativo, enseguida se exponen los derechos que otorga el RGPD y la LFPDPPP:

DERECHOS	LFPDPPP MX 2010	RGPD 2018
DERECHO A SER INFORMADO	X (Es un principio, no es un derecho)	✓
DERECHO DE ACCESO	✓	✓
DERECHO DE RECTIFICACION	✓	✓
DERECHO DE SUPRESION (DERECHO AL OLVIDO)	X Similitudes con el derecho de Cancelación	✓
DERECHO A RESTRINGIR EL PROCESAMIENTO	✓	✓
DERECHO A LA PORTABILIDAD DE DATOS	X	✓

DERECHO DE OPOSICION	✓	✓
DERECHOS RELACIONADOS CON LA TOMA DE DECISIONES AUTOMATIZADAS INCLUYENDO PERFILES	X No es un derecho, es una obligación de informar: Tratamiento para fines mercadotécnicos, publicitarios o de prospección comercial RLFPDPPP, art 30 Tratamiento de datos personales en decisiones sin intervención humana valorativa RLFPDPPP, art 112	✓

Cuadro 11. Comparativa de derechos de los individuos entre el RGPD y la LFPDPPP
Fuente: Elaboración Propia.

3.3 Estudio del Derecho al Olvido a partir del RGPD

Para efectos de este estudio, se insertan los artículos y disposiciones que se refieren al derecho de supresión o Derecho al Olvido:

Artículo 6 Licitud del tratamiento

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

- a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
- b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
- c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
- d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
- e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
- f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades en el ejercicio de sus funciones.

2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:

a) el Derecho de la Unión, o

b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

4. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;

b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;

c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;

d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;

e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.

Artículo 9 Tratamiento de categorías especiales de datos personales

1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida o las orientaciones sexuales de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del

interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de

los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

Artículo 12 Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado

1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

2. El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado.

3. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

4. Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de

presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

5. La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:

a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o

b) negarse a actuar respecto de la solicitud.

El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

6. Sin perjuicio de lo dispuesto en el artículo 11, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

7. La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente.

8. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 92 a fin de especificar la información que se ha de presentar a través de iconos y los procedimientos para proporcionar iconos normalizados.

Artículo 17 Derecho de supresión («el Derecho al Olvido»)

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concorra alguna de las circunstancias siguientes:

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 en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;

c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales 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;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

3. Los apartados 1 y 2 no se aplicarán 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 de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;
- d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o
- e) para la formulación, el ejercicio o la defensa de reclamaciones.

3.3.1 ¿Cuándo es aplicable el derecho de supresión (Derecho al Olvido)?

El llamado Derecho de supresión (Derecho al Olvido) establece que las personas tienen derecho a que se borren sus datos personales, “sin dilación indebida”, bajo determinadas circunstancias, mismas que se exponen enseguida:¹⁶³

Las personas tienen derecho a que se supriman sus datos personales si:

- i. Los datos personales ya no son necesarios para el propósito para el que fueron recopilados o tratados;
- ii. Cuando el consentimiento es la base legal para el tratamiento de los datos y la persona retira su consentimiento;

¹⁶³ Schultze-Melling, Jyn, “Data Subjects’ Rights”, en Ustaran, Eduardo, “European Data Protection, Law and Practice, International Association of Privacy Professionals” (IAPP), 2018, p. 162

- iii. Cuando un interés legítimo es la base para el tratamiento, los individuos se oponen al procesamiento de sus datos y no prevalecen otros motivos de un interés legítimo para continuar con el tratamiento;
- iv. Cuando exista un tratamiento de los datos personales para fines de marketing directo y la persona objeto esa clase de tratamiento;
- v. Cuando se han procesado los datos personales de manera ilegal (es decir, en violación al principio de licitud).
- vi. Cuando es necesario para cumplir con una obligación legal; o
- vii. Cuando se han procesado los datos personales para ofrecer servicios de la sociedad de la información a un niño.

3.3.2 ¿Cuándo no es aplicable el derecho de supresión?

El derecho de supresión no se aplica si el tratamiento es necesario por una de las siguientes razones:

- para ejercer el derecho a la libertad de expresión e información;
- para cumplir con una obligación legal;
- para el desempeño de una tarea de interés público o en el ejercicio de autoridad;
- con fines de archivo de interés público, investigación científica, histórica o con fines estadísticos en los que es probable que la supresión sea imposible o menoscabe gravemente el logro de ese procesamiento; o
- para el establecimiento, ejercicio o defensa de reclamaciones legales.

El RGPD también especifica dos circunstancias en las que el derecho de supresión no se aplicará a los datos de categorías especiales:

- si el tratamiento es necesario para fines de salud pública en interés público (por ejemplo, proteger contra amenazas transfronterizas graves para la salud, o garantizar altos estándares de calidad y seguridad de la atención de la salud y de los medicamentos o dispositivos médicos); o

- si el tratamiento es necesario para fines de medicina preventiva u ocupacional; o para la gestión de los sistemas o servicios de salud o de atención social). Esto sólo aplica cuando los datos están siendo tratados bajo responsabilidad de un profesional sujeto a una obligación legal de secreto profesional (por ejemplo, un profesional de la salud)

3.3.3 ¿Es necesario informar a otras organizaciones sobre la eliminación de datos personales?

El RGPD especifica dos escenarios en los que se debe informar a otras organizaciones sobre la eliminación de datos personales:

- Cuando los datos personales han sido divulgados a terceros; o
- Cuando los datos personales se han hecho públicos en un entorno digital (por ejemplo, en redes sociales, foros o sitios web).

En caso de que se divulguen los datos personales a terceros, es necesario que el controlador se ponga en contacto con cada destinatario para informarle sobre la supresión de datos personales, a menos que esto resulte imposible o implique un esfuerzo desproporcionado.

El RGPD define a un destinatario como una persona física o jurídica, autoridad, agencia u otro organismo al que se divulgan los datos personales. La definición incluye controladores, procesadores y personas que, bajo la autoridad directa del responsable o encargado del tratamiento, están autorizadas a tratar datos personales.

En caso de que los datos personales se hayan divulgado en un entorno digital, es necesario tomar medidas adecuadas para informar a otros controladores del tratamiento de datos personales para borrar enlaces, copias o replicación de esos datos.

3.3.4 ¿Es necesario borrar los datos personales de los sistemas de copia de seguridad?

Cuando se recibe una solicitud de supresión válida y no se aplica ninguna exención, es necesario tomar medidas para garantizar la supresión de los sistemas de copia de seguridad, así como de los sistemas activos. Estos pasos dependerán de circunstancias particulares como la programación de retención (particularmente en el contexto de copias de seguridad) y los mecanismos técnicos disponibles.

Es necesario informar de manera clara a los titulares lo que sucederá con sus datos cuando se cumpla con su solicitud de supresión, incluyendo a los sistemas de copia de seguridad.

Es posible que la solicitud de supresión pueda ser completada de manera inmediata en sistemas activos, sin embargo, los datos permanecerán algún tiempo dentro de la copia de seguridad durante cierto período de tiempo hasta que se sobrescriban.

El problema principal es situar los datos de copia de seguridad "inutilizables", incluso si no se pueden sobrescribir inmediatamente. Es preciso asegurarse de no utilizar los datos dentro de la copia de seguridad para ningún otro propósito, es decir, que la copia de seguridad simplemente se mantiene en el sistema hasta que es reemplazada de acuerdo con una programación establecida. Siempre que este sea el caso, es poco probable que la retención de datos personales dentro de la copia de seguridad suponga un riesgo significativo, aunque esto será específico del contexto.

3.3.5 ¿Cómo se aplica el Derecho al Olvido a los datos recopilados de niños?

Conforme al artículo 9, relacionado con los datos especiales, el derecho de suprimir o borrar datos personales cuando la solicitud se refiere a datos recopilados de niños. Esto refleja el aumento en la protección de la información de niños, especialmente en entornos digitales, dentro del marco del RGPD.

En caso de tratamiento de datos recopilados de niños, es necesario prestar especial atención a la solicitud de supresión si el tratamiento se basa en el consentimiento otorgado por un niño, especialmente el tratamiento de sus datos personales en Internet. Incluso sigue aplicando cuando el solicitante ya es adulto, ya que un niño pudo no haber sido plenamente consciente de los riesgos involucrados en el tratamiento al momento del consentimiento.

3.3.6 ¿Es posible negarse a cumplir con una solicitud por otras razones?

Si se aplica una exención, es posible que se niegue el cumplimiento de una solicitud de supresión (total o parcialmente). No todas las exenciones se aplican de la misma manera, y es necesario examinar cada exención cuidadosamente para ver cómo se aplica a cada solicitud en particular.

También es posible que se niegue el cumplimiento de una solicitud si es:

- a) Manifiestamente Infundada: Una solicitud puede ser manifiestamente infundada si:
- la persona claramente no tiene intención de ejercer su derecho de borrado, y su finalidad es conseguir otros beneficios;
 - la solicitud tiene intención maliciosa y se está utilizando para acosar a una organización con el único fin de causar perjuicio.

No se debe asumir que una solicitud es manifiestamente infundada porque el titular haya presentado previamente solicitudes manifiestamente infundadas o excesivas o si incluye un lenguaje agresivo o abusivo.

La inclusión de la palabra "manifiestamente" significa que debe haber una cualidad obvia o clara de que sea infundada.

b) Excesiva. Una solicitud puede ser excesiva si:

- se repite el contenido de solicitudes anteriores; o
- se superpone con otras solicitudes.

No será necesariamente una solicitud excesiva si el titular:

- hace una solicitud respecto al mismo tema. El titular puede tener razones legítimas para hacer solicitudes que repitan el contenido de solicitudes anteriores.
- realiza una solicitud superpuesta, mientras se refiera a información separada;
o
- solicitudes presentadas previamente que hayan sido manifiestamente infundadas o excesivas

Al final, para decidir si una solicitud es manifiestamente infundada o excesiva, debe considerarse cada solicitud de manera particular, sin tener una regla general. Sobre todo, se debe informar al titular sobre las razones por las cuales se considera que la solicitud es manifiestamente infundada o excesiva y, de ser necesario a la APD.

3.3.7 ¿Qué se debe hacer si se niega una solicitud de supresión?

El controlador debe informar al titular sin demora y en el plazo de un mes a partir de la recepción de la solicitud acerca de:

- los motivos por los que no se procederá con la solicitud;
- su derecho a presentar una queja ante alguna autoridad supervisora; y
- su capacidad para hacer valer este derecho a través de un recurso judicial.

Esta información también debe de ser proporcionada en caso del cobro de alguna tarifa razonable o en caso de que se requiera información adicional para identificar al titular.

3.3.8 ¿Cómo reconocer una solicitud de supresión?

El RGPD no es muy específico en cuanto a cómo realizar una solicitud válida y dada la amplitud, se puede asumir que el titular puede hacer una solicitud de supresión verbalmente o por escrito.

Sin embargo, los controladores tienen la responsabilidad legal de identificar cuando un titular ha hecho una solicitud y manejarla en consecuencia. Es importante que se tengan políticas, procedimientos y capacitación de empleados para identificar una solicitud de supresión.

Dentro del apartado 4.6.2 (Listado de Verificación) de esta investigación, propongo un listado de verificación y un formulario para las solicitudes de supresión que sirve como referencia en casos de solicitudes de supresión (Derecho al Olvido).

3.3.9 ¿El derecho de supresión es gratuito?

En la mayoría de los casos no se puede cobrar una tarifa con la finalidad de cumplir con una solicitud de supresión.

Sin embargo, si puede cobrarse una "tarifa razonable" por los costos administrativos de cumplir con la solicitud si es manifiestamente infundada o excesiva.

En caso de aplicar esta tarifa el controlador deberá informar de inmediato al titular de la solicitud y podrá proceder con el cumplimiento de esta hasta que la tarifa haya sido pagada.

Alternativamente, es posible que el controlador se niegue a cumplir con una solicitud manifiestamente infundada o excesiva.

3.3.10 ¿En cuánto tiempo se debe cumplir con una solicitud de supresión?

Se debe cumplir sin demora indebida y a más tardar dentro de un mes a partir de la recepción de la solicitud o en su caso dentro de un mes de la recepción de:

- a) cualquier información solicitada para confirmar la identidad del titular; o
- b) el pago de una tarifa (cuando aplique)

3.3.11 ¿Es posible ampliar el tiempo de respuesta a una solicitud de supresión?

Si la solicitud es compleja o si existe una serie de solicitudes del mismo titular es posible extender el tiempo de respuesta por otros dos meses, sin embargo, el controlador deberá informar al titular en el plazo de un mes a partir de la recepción de su solicitud y explicar los motivos por los que es necesaria la extensión.

3.3.12 ¿Se puede pedir una identificación a un titular?

Si existen dudas sobre la identidad de la persona que realiza la solicitud es posible que el controlador solicite más información, siempre y cuando esta sea exclusivamente con la finalidad de corroborar la identidad del titular para poder proceder con la solicitud.

Es necesario solicitar al titular sin demora indebida y dentro del plazo de un mes la información necesaria para confirmar su identidad, esto puede extender el tiempo de respuesta y cumplimiento de una solicitud.

3.4 Desafíos técnicos y jurídicos del Derecho al Olvido

Parte del debate que derivó del Caso Costeja, giró alrededor del desafío técnico y jurídico para hacer cumplir el Derecho al Olvido de manera efectiva.

La primera problemática está estrechamente relacionada con los alcances del borrado u olvido de un dato, es decir, ¿cuál será la forma aceptable para tener por cumplimentada la supresión del dato?

A este respecto, desde 2011 la Agencia Europea de Seguridad de Redes e Información (European Network and Information Security Agency, ENISA) hizo un estudio sobre las expectativas y la práctica del Derecho al Olvido, en donde abordan diferentes grados en los que se entendería que es aceptable el borrado de información:

“Una interpretación estricta requeriría que todas las copias de los datos se borren y se eliminen de cualquier representación derivada o agregada hasta el punto en que la recuperación de los datos sea imposible por cualquier medio técnico conocido. Una interpretación un poco más débil (y posiblemente más práctica) permitiría la supervivencia de las copias cifradas de los datos, siempre que no puedan ser descifradas por terceros no autorizados. Una interpretación aún más débil (y más práctica) permitiría que sobrevivieran copias de texto claro de los datos, siempre que los datos ya no aparezcan en índices públicos, resultados de consultas de bases de datos o en los resultados de motores de búsqueda.”¹⁶⁴

¹⁶⁴ Druschel Peter, et. Al. “The right to be forgotten –between expectations and practice”. ENISA, 2011 Texto original en inglés: What constitutes “forgetting” a data item? Our next question concerns the question of what is an acceptable way of “forgetting” information. A strict interpretation would require that all copies of the data be erased and removed from any derived or aggregated representations to the point where recovering the data is impossible by any known technical means. A slightly weaker (and possibly more practical) interpretation would allow encrypted copies of the data to survive, as long as they cannot be deciphered by unauthorized parties. An even weaker (and more practical) interpretation would allow clear text copies of the data to survive, as long as the data would no longer appear in public indices, database query results, or in the results of search engines.

Aquí es de reconocer que en un sistema completamente abierto como la world wide web, cualquiera puede hacer copias de un elemento de datos públicos y almacenarlos en ubicaciones arbitrarias.

Esto se vuelve más complicado si se considera que el sistema no está diseñado para rastrear el número, el propietario o la ubicación de dichas copias.

En un sistema tan abierto, generalmente no es posible para una persona localizar todos los elementos de datos personales (exactos o derivados) almacenados sobre ellos;

Por lo tanto, hacer cumplir el Derecho al Olvido es imposible en un sistema abierto y global, en general. La capacidad de hacer cumplir un "Derecho al Olvido" depende de manera crucial de las capacidades del sistema de información subyacente.

En pocas palabras, esta capacidad es técnicamente factible solo en sistemas "cerrados", que representan de manera confiable el procesamiento, el almacenamiento y la difusión de toda la información, y evitan la difusión de datos a lugares donde no se puede forzar un borrado.

Algunos de los desafíos técnicos y jurídicos que se pueden mencionar son:

- a) Dota de facultades a un ente privado: Permitir que una persona u organización identifique y localice los elementos de datos personales almacenados sobre ellos;
- b) La imposibilidad material de rastrear todas las copias de un elemento y todas las copias de la información derivada del elemento de datos;
- c) Jurisdicción: todas las entidades participantes deben residir en una jurisdicción que haga cumplir el Derecho al Olvido, cada solicitud de datos

https://iapp.org/media/pdf/knowledge_center/right_to_be_forgotten-between_expectations_and_practice.pdf Traducción de la autora de esta investigación, 2019.

debe ser autenticada y registrada, y los principales deben estar vinculados a personas u organizaciones del mundo real.

- d) hacer cumplir el Derecho al Olvido es imposible en un sistema abierto y global, en general
- e) La información no es eliminada permanentemente, por ejemplo, Google elimina URLs en todos los dominios europeos, pero no elimina el contenido en sí, ya que esto provocaría un riesgo al derecho a la información o a la libertad de expresión y recordemos que ningún derecho es absoluto, es decir, solo se desindexa el resultado de los buscadores de Google Europa, pero la información sigue estando disponible bajo otros criterios de búsqueda o desde ubicaciones fuera de la Unión Europea.
- f) Provoca afectaciones a la disponibilidad de la información: El propio Google es el primer detractor de la implementación del llamado Derecho al Olvido, y actualmente impulsa una campaña importante que busca dar su perspectiva sobre “cómo las leyes de privacidad europeas afectan los resultados de Búsqueda de Google”

“Desde julio de 2014, la ley de privacidad europea ha afectado la disponibilidad de la información para ciertas consultas en Búsqueda de Google. Las cifras que se muestran en este informe cuantifican y explican ese impacto.”

Obtén información sobre cómo las leyes de privacidad europeas afectan los resultados de Búsqueda de Google

Desde julio de 2014, la ley de privacidad europea ha afectado la disponibilidad de la información para ciertas consultas en Búsqueda de Google. Las cifras que se muestran en este informe cuantifican y explican ese impacto.

OBTÉN MÁS INFORMACIÓN SOBRE LA RELACIÓN ENTRE LA PRIVACIDAD Y EL ACCESO A LA INFORMACIÓN EN LÍNEA. 



Figura 6. Afectación de los resultados de búsquedas de Google

Fuente: Imagen tomada del Informe de Transparencia de Google, en el apartado de Solicitudes de eliminación de contenido en conformidad con la ley de privacidad europea, disponible en: https://transparencyreport.google.com/eu-privacy/overview?privacy_requests=country:GB;year:2017;decision:not%20delisted&lu=privacy_requests. Consultada el 20 de febrero de 2020.

3.5 Caso de aplicación de multa conforme al RGPD¹⁶⁵

El pasado 26 de agosto de 2019, la Autoridad de Protección de Datos de Letonia (Director de la Inspección Estatal de Datos, DSI) impuso una sanción de 7,000 euros contra un vendedor minorista en línea, por incumplir con el derecho de supresión (Derecho al Olvido) del RGPD y por no cooperar con la autoridad supervisora.

Durante la investigación del caso, la APD de Letonia, encontró que en 2018 el reclamante había solicitado, en repetidas ocasiones, al minorista que eliminara todos sus datos personales, incluido el número de teléfono móvil del reclamante.

El vendedor minorista incurrió en las siguientes infracciones: (a) no ejecutó la solicitud de supresión del interesado, (b) no proporcionó la información solicitada por la APD de Letonia y (c) no acató la orden de restricción de tratamiento de datos personales emitida por la APD de Letonia, violando los siguientes artículos del RGPD fueron: Artículos 17 y 58 (2) (c) y (g).

Al determinar el monto de la multa, la autoridad tomó en cuenta la naturaleza, la gravedad y la duración de la infracción, el grado de cooperación con la autoridad supervisora, el número de interesados afectados, la facturación anual total del año fiscal anterior del minorista (artículo 83 (5) (b) y (e) del RGPD).

La APD de Letonia ha señalado que, de conformidad con los artículos 288 y 289 del Código de infracciones administrativas de Letonia, el minorista tiene

¹⁶⁵ “Director de la Inspección Estatal de Datos de Letonia impuso una sanción de 7,000 euros contra un vendedor minorista en línea” (Data State Inspectorate of Latvia imposes a financial penalty of 7000 euros against online retailer), 3 de septiembre de 2019, publicado por el Comité Europeo de Protección de Datos, disponible en https://edpb.europa.eu/news/national-news/2019/data-state-inspectorate-latvia-imposes-financial-penalty-7000-euros-against_en. Consultada el 28 de abril de 2020.

derecho a apelar la decisión ante el Tribunal de distrito (ciudad) dentro de los diez días hábiles a partir de la fecha de recepción de la decisión.

3.6 Herramientas para la aplicación del Derecho al Olvido

3.6.1 Puntos clave sobre el Derecho al Olvido

- a) El RGPD introduce un derecho para que las personas borren sus datos personales en determinadas circunstancias, es comúnmente conocido como Derecho al Olvido.
- b) Las personas pueden hacer una solicitud de supresión verbalmente o por escrito.
- c) El responsable tiene un mes para responder a una solicitud.
- d) El derecho no es absoluto y solo se aplica en ciertas circunstancias.
- e) Este derecho no es la única forma en que el RGPD impone la obligación de considerar si se deben eliminar datos personales.

3.6.2 Listado de Verificación

Para efectos prácticos, se ofrece un listado de los puntos más relevantes a considerar por una organización, al momento de evaluar una situación de derecho a la supresión conforme al artículo 17 del RGPD:

Medidas para solicitudes de supresión	
	Nuestra organización sabe cómo reconocer una solicitud de supresión o Derecho al Olvido
	Nuestra organización entiende cuando es procedente aplicar el Derecho al Olvido
	Nuestra organización tiene política sobre cómo registrar las solicitudes que recibimos verbalmente

Nuestra organización entiende cuándo se puede rechazar una solicitud y conoce la información que necesitamos proporcionar a las personas cuando lo hacemos.
Medidas para el cumplimiento de solicitudes de supresión
Nuestra organización cuenta con procesos para garantizar que respondamos a una solicitud de supresión sin demora indebida y dentro del mes siguiente a la recepción.
Nuestra organización conoce las circunstancias en que podemos extender el límite de tiempo para responder a una solicitud.
Nuestra organización entiende que hay un énfasis particular en el derecho de supresión si la solicitud se refiere a datos recopilados de niños.
Nuestra organización tiene procedimientos establecidos para informar a los destinatarios si borramos cualquier información que hayamos compartido con ellos.
Nuestra organización tiene métodos apropiados para borrar la información

Cuadro 12. Check list Solicitudes de supresión
Fuente: Elaboración propia.

3.6.3 Formulario para ejercer el derecho de supresión (Derecho al Olvido)

El RGPD no establece un mecanismo preciso para ejercer el derecho de supresión (Derecho al Olvido), esto no se trata de un defecto de la regulación, sino que, al ser una regulación diseñada para un alcance multisectorial, no puede prever todos los escenarios para solicitar el derecho de supresión, puesto que, al final del día el análisis de la procedencia del derecho se hará caso por caso, dependiendo de si se configuran o no los supuestos que refiere el artículo 17 del RGPD y que ya han sido discutidos con anterioridad.

Por tanto, esta investigación propone un formulario que puede ser adoptado por organizaciones privadas, para que el ejercicio de este derecho sea más amigable tanto para los interesados como para los responsables.

Sirve hacer notar que el ejercicio del derecho de supresión no depende simplemente de la existencia del formulario, es de recordar que para que un individuo sea candidato al ejercicio de este derecho, debe caer en por lo menos uno de los siguientes supuestos:

- i. Los datos se utilizan para fines de prospección;
- ii. Los datos no son o han dejado de ser necesarios para los fines para los que se recogieron o procesaron originalmente;
- iii. El titular del dato retira su consentimiento para el uso de sus datos;
- iv. Sus datos se procesan de forma ilegal (por ejemplo, la publicación de datos piratas);
- v. Sus datos fueron recogidos cuando era menor de edad en el contexto de la sociedad de la información (blog, foro, red social, sitio web...);
- vi. Sus datos deben ser eliminados para cumplir con una obligación legal;
- vii. El titular del dato se ha opuesto al tratamiento de sus datos y el responsable de la base de datos no tiene ninguna razón legítima o convincente para no cumplir con esta solicitud.

Y bien, una vez que el titular del dato ha confirmado que encuadra en por lo menos uno de los supuestos antes citados, es recomendable que realice las siguientes acciones:

(a) Identificar la organización a la que hay que solicitar el derecho de supresión: Es importante que el titular del dato identifique a la organización y revise los términos que establece la organización para el ejercicio de sus derechos, esto puede ser en el sitio web de la organización, los más comunes suelen encontrarse a través de la "política de privacidad", "aviso de privacidad", "términos y condiciones", "aviso legal", entre otros.

Cuando existan dificultades para obtener los datos de contacto del responsable de protección de datos o de la persona encargada, se sugiere contactar a un experto en protección de datos personales o buscar el centro de atención

ciudadana de la Autoridad de Protección de Datos Personales del país de que se trate, en el caso de México es el INAI.

(b) Identificar los medios de ejercicio del derecho de supresión: El RGPD permite que el ejercicio del derecho de supresión ocurra por diversos medios, por ejemplo, a través de medios electrónicos existen diversas opciones, tales como: (a) formularios predeterminados, (b) dirección de correo electrónico, (c) botones inteligentes para el control de los datos de los usuarios, servicios automatizados de atención al cliente, como *bots* de charla o *bots* conversacionales (también conocidos como *chatbot*), o bien, medios tradicionales como correo postal, o de manera personal ante las oficinas de la organización responsable del tratamiento. La finalidad es dotar de medios que sean accesibles al titular del dato para el ejercicio de su derecho sin que tenga que incurrir en esfuerzos desproporcionales para lograr la supresión de su dato.

(c) Identificar qué datos desea suprimir (eliminar): Es importante considerar que el ejercicio del derecho de supresión no conduce a la simple y definitiva supresión de todos sus datos en poder de la organización. Por ejemplo, una solicitud de eliminación de su foto en un sitio no resultará necesariamente en la eliminación de su cuenta. Del mismo modo, una solicitud de supresión de su cuenta no dará lugar a la eliminación de las facturas y otros documentos contables relacionados con sus compras, para los cuales existe la obligación legal del responsable para retenerlos.

(d) Comprobar la identidad del titular: En caso de que la organización tenga dudas razonables sobre la identidad del titular del dato, puede pedir que adjunte cualquier documento que pruebe su identidad, esto sirve para evitar el robo de identidad. Por otra parte, no puede pedirle documentos de apoyo que no sean razonables, irrelevantes y desproporcionados a su solicitud.

(e) Documentar la solicitud del derecho de supresión: Es altamente recomendable que el titular del dato documente la solicitud del derecho de supresión, así como los pasos que tomó para contactar al responsable, esto

es esencial si se desea iniciar algún procedimiento frente a la Autoridad de Protección de Datos o acciones legales para la reparación del daño, en caso de que el responsable emita una respuesta insatisfactoria o simplemente no emita respuesta alguna. Se sugiere que para la documentación de esta solicitud el titular use medios electrónicos que permitan rastrear el origen, destinatario y fecha de la solicitud, por ejemplo, usando correo electrónico y solicitando acuse de recibo o implementar mecanismos de notificación de recepción o de solicitud de respuesta, o bien, puede optar por hacer capturas de pantalla de su solicitud o de la respuesta, guardar una copia del correo electrónico o de tu solicitud hecha electrónicamente.

Luego de estas recomendaciones aplicables al ejercicio del derecho de supresión en el marco del RGPD se propone un formulario predeterminado para que el ejercicio del derecho de supresión (Derecho al Olvido) sea amigable e intuitivo tanto para el titular del dato como para el responsable del tratamiento, este formulario se acompaña como ANEXO III a esta investigación.

Conclusiones

Conclusiones

- I. El Derecho al Olvido encuentra buen fundamento en dos derechos fundamentales. Por un lado, el derecho de protección de datos permite que los afectados puedan cancelar sus datos personales cuando estos ya no sean adecuados y necesarios, por razón de haber devenido obsoletos, o bien puedan oponerse al tratamiento de esos datos. Por otro lado, el derecho a la intimidad o a la vida privada permite dar cobertura a las expectativas de que, tras un lapso temporal, ciertos datos, aunque públicos en su día, puedan considerarse razonablemente privados o reservados.
- II. El Derecho al Olvido es la respuesta a la amenaza que supone para el libre desarrollo de la personalidad el almacenamiento permanente en Internet de información personal cuya difusión, pasado el tiempo, puede afectar negativamente a la persona, al producirse un desajuste entre el dato publicado y la realidad actual.
- III. Las personas tenemos un interés legítimo en controlar la información sobre nosotros mismos y que puede ser utilizada por otros para realizar juicios sobre nuestra valía, cualidades o personalidad.
- IV. El Derecho al Olvido, como cualquier otro derecho, no es absoluto y debe acomodarse a la coexistencia con otros derechos que lo limitan. El establecimiento de equilibrios razonables en los supuestos de conflicto es la vía adecuada para preservar los intereses contrapuestos de acceder libremente a toda la información en línea y de precaverse frente al conocimiento permanente de informaciones pasadas que nos perjudican.
- V. El Derecho al Olvido es la última manifestación de la necesidad de preservar la privacidad de las personas frente a las amenazas que entraña el progreso tecnológico. Los riesgos que pueden surgir de una sociedad tecnológicamente avanzada están en el origen, como reconoció tempranamente el Tribunal Constitucional, del reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que

por cualquier medio pueden realizarse sobre los espacios o ámbitos en los que las personas desarrollan su esfera personal.

- VI. Los contornos del derecho a la vida privada se han ido modelando al paso del surgimiento de nuevas amenazas derivadas del avance tecnológico. En esa evolución, la formulación del derecho a la protección de datos ha constituido la respuesta jurídica al radical cambio que suponía la informática y la digitalización de la información.
- VII. La noción de interés público, y la necesidad de que se tenga en cuenta la actualidad o vigencia de este para valorar si este resulta suficiente o no para justificar la permanencia de ciertas informaciones en Internet, es un ejemplo entre muchos otros de la necesidad de aplicar, contextualizar y adecuar los principios jurídicos de nuestro ordenamiento a un nuevo escenario, el digital, que incorpora nuevas realidades que deben ser observadas y estudiadas.
- VIII. En el caso de internet, las publicaciones e informaciones vertidas en la red se conservan por defecto y ocupan un lugar en los resultados de los motores de búsqueda que puede prolongarse por largo tiempo, es decir, una noticia puede ocupar la primera página de los resultados de búsqueda durante años, lo que significa que la difusión y divulgación constante, en la tribuna pública de esos contenidos.
- IX. En muchos casos a falta de regulación específica los criterios interpretativos y de ponderación pueden ayudar a encontrar una solución adecuada y son, por lo general plenamente vigentes y aplicables a los cambios que han introducido las nuevas tecnologías.
- X. En el ámbito europeo, el debate sobre el reconocimiento y alcance del Derecho al Olvido está decisivamente condicionado por dos hechos. Por un lado, la sentencia del Tribunal de Justicia dictada sobre la cuestión prejudicial planteada con motivo del recurso interpuesto por Google contra una resolución de la Agencia Española de Protección de Datos que le obligaba a eliminar de sus resultados de búsqueda el link a la publicación, en una página del diario. Mediante esta cuestión prejudicial se planteaba sustancialmente si de la Directiva 95/46/CE en materia de protección de datos puede derivarse

un Derecho al Olvido, y la respuesta del Tribunal tiene fuerza vinculante general sobre el alcance de la interpretación que deba darse a la norma europea sobre este punto.

- XI. A la hora de fundar el Derecho al Olvido, en lugar de optar por configurarlo como derecho autónomo, existen dos alternativas: bien construirlo como proyección de ciertos derechos de la personalidad, en particular, los derechos a la intimidad o a la vida privada, en la terminología del Convenio Europeo de Derechos Humanos, y al honor; bien como proyección del derecho a la protección de datos. La primera alternativa ha sido la transitada por la doctrina y la jurisprudencia tanto en España como en varios países de nuestro entorno en relación con los medios tradicionales de comunicación, pero que también puede extenderse a las formas de divulgación en línea de la información. La segunda es la adoptada por distintas autoridades nacionales de protección de datos a la hora de aplicar la normativa en esta materia y la desarrollada por la Comisión Europea a través de la propuesta del Reglamento general de protección de datos.
- XII. Mientras la tutela a partir de los derechos al honor y a la intimidad es un ámbito regido por las normas nacionales (en el caso de España, Ley de protección civil de protección al honor, a la intimidad personal y familiar y a la propia imagen, básicamente), la protección derivada del derecho a la protección de datos es un espacio sujeto a la armonización de la normativa europea. Otra diferencia relevante se produce en los instrumentos de tutela: mientras que los derechos al honor y a la intimidad gozan de la tutela dispensada por jueces y tribunales, el derecho a la protección de datos cuenta con un sistema administrativo de protección a través de una agencia independiente.
- XIII. Para considerar que del derecho a la intimidad o el derecho al honor puede derivarse una protección frente a informaciones obsoletas del pasado, estas deben lesionar los bienes jurídicos protegidos por estos derechos, lo cual exige una interpretación amplia de su ámbito de protección. En cambio, el derecho a la protección de datos tiene por objeto el tratamiento de todo dato

que identifique o permita identificar a una persona, lo cual determina un ámbito de cobertura mucho más amplio. Si tomamos como ejemplo el caso de la información sobre la anorexia sufrida por la gimnasta al que se hacía referencia más arriba, parece clara, prima facie, la afectación del derecho a la protección de datos personales, pero resulta menos evidente que resulte concernido el honor o la intimidad de la persona afectada.

XIV. El Reglamento de protección de datos propuesto establece el equilibrio adecuado entre el derecho a la protección de datos personales y libertad de expresión

XV. La Directiva 95/46/CE del Parlamento Europeo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y “la Carta de los Derechos Fundamentales de la Unión Europea coinciden en que:

- La actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de “tratamiento de datos personales”.
- Para respetar los derechos establecidos en la Directiva 95/46/CE, un gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona.
- El Derecho al Olvido prevalece sobre el interés económico del gestor del motor de búsqueda y sobre el interés del público en acceder a la mencionada información en una búsqueda relacionada al nombre de esa persona. Sin embargo, en el caso de una figura de la vida pública, la injerencia en sus derechos fundamentales está justificada por el interés preponderante del público en tener acceso a la información de que se trate.”

XVI. Dada la amplitud de las definiciones de "tratamiento", "datos personales" y "responsable del tratamiento de datos" bajo la Directiva, el tribunal sostuvo

que las actividades de los motores de búsqueda sí implican un tratamiento de datos personales y que los operadores de motores de búsqueda son los responsables del tratamiento de datos personales.

Bibliografía

¡GANAMOS! TRIBUNAL ANULA RESOLUCIÓN DEL INAI SOBRE EL FALSO “DERECHO AL OLVIDO” R3D, México, disponible en: <https://r3d.mx/2016/08/24/amparo-inai-derecho-olvido/>

30ème rapport d'activité de la CNIL, 2009, Paris, La Documentation Française, disponible en https://www.cnil.fr/sites/default/files/typo/document/CNIL-30erapport_2009.pdf

ALEXY, Robert, “Derechos fundamentales, ponderación y racionalidad” Revista Iberoamericana de Derecho Procesal Constitucional, núm. 11, enero-junio 2009. Disponible en <https://www.corteidh.or.cr/tablas/r25294.pdf>

ÁLVAREZ RODRÍGUEZ, Lilibeth, “Derecho al Olvido como garantía para la autodeterminación informativa en las redes sociales”, IV Foro Internacional Derechos humanos y tecnologías de la Información y Comunicación (TIC). Disponible en <https://www.repositoriodigital.ipn.mx/bitstream/123456789/3987/1/Memoria%20to%20Foro%20DHTIC%2015.pdf>.

Amparo directo 535/2018. Décimo Tribunal Colegiado en Materia Administrativa del Primer Circuito. Disponible en http://sise.cjf.gob.mx/SVP/word1.aspx?arch=79/00790000235100940012009004.doc_1&sec=Angel_Garcia_Cotonieto&svp=1

Amparo en revisión 587/2017, Primera Sala de la Suprema Corte de Justicia de la Nación. Disponible en: <http://www2.scjn.gob.mx/ConsultaTematica/PaginasPub/DetallePub.aspx?AsuntoID=218201>

Amparo en revisión 95/2016, Segundo Tribunal Colegiado en Materia Administrativa del Primer Circuito admite el recurso, expediente Auxiliar 355/2016 del índice

del Séptimo Tribunal Colegiado de Circuito del Centro Auxiliar de la Primera Región, disponible en:
http://sise.cjf.gob.mx/SVP/word1.aspx?arch=15/00150000186773530009005002.docx_1&sec=Victor_Ivan__Segura__Velazquez_&svp=1

Amparo Indirecto 422/2016, Juzgado Décimo Primero de Distrito en Materia Civil en la Ciudad de México. Disponible en:
http://sise.cjf.gob.mx/SVP/word1.aspx?arch=87/00870000189764940007018003.docx_1&sec=Gabriela_Alejandra_Rodr%C3%ADguez_Huitr%C3%B3n&svp=1

Amparo indirecto 574/2015, Juzgado Decimoquinto de Distrito en Materia Administrativa en la Ciudad de México. Disponible en
http://sise.cjf.gob.mx/SVP/word1.aspx?arch=734/07340000167577970037031.doc_1&sec=Carlos_Ivan_Velasco_Dominguez&svp=1

Aprobación de las directrices del GT29 del RGPD por la Junta Europea de Protección de Datos (European Data Protection Board, EDPB)
<https://edpb.europa.eu/node/>

Asunto C-131/12, Google Spain, S.L., Google Inc. Contra Agencia Española de Protección de Datos (AEPD), Mario Costeja González, sentencia del 13 de Mayo de 2014, Tribunal de Justicia de la Unión Europea Disponible en:
<http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=384212>

BECERRIL, Andrea, “Morena impulsa una ley para el Derecho al Olvido en plataformas digitales”, La Jornada, 25 de enero de 2020, disponible en
<https://www.jornada.com.mx/2020/01/25/politica/007n2pol>

CARRUZO, Barahona, Derecho Digital, Perspectiva Interdisciplinar, Primer Edición, España, 2017.

CASTELLANO, Pere Simón, El reconocimiento del Derecho al Olvido en España y en la Unión Europea, Primera Edición, España, 2015.

Código Civil para la Ciudad de México

Código Penal para la Ciudad de México

Conclusiones del abogado general Sr. Niilo Jääskinen, presentadas el 25 de junio de 2013, Asunto C-131/12, Google Spain, S.L., Google Inc. contra Agencia Española de Protección de Datos (AEPD), Mario Costeja González (Petición de decisión prejudicial planteada por la Audiencia Nacional) Disponible en: <http://curia.europa.eu/juris/document/document.jsf?docid=138782&text=&doclang=ES&pageIndex=0&cid=5298824#Footnote1>

Constitución Política de los Estados Unidos Mexicanos, Última Reforma DOF 09-08-2019

Convenio no. 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, emitido por el Consejo de Europa, disponible en: <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>

DAVARA F. DE MARCOS, Isabel, “El Derecho al Olvido en relación con el derecho a la protección de datos personales”, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, México, 2014, disponible en <http://www.infodf.org.mx/capacitacion/publicacionesDCCT/ensayo23/23ensayo2014.pdf>

DAVARA F. DE MARCOS, Isabel, Coord., “Diccionario de Protección de Datos Personales, Conceptos fundamentales”, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), noviembre

2019, México, disponible en http://inicio.ifai.org.mx/PublicacionesComiteEditorial/DICCIONARIO_PDP_digital.pdf (Consultado el 20 de abril de 2020).

DE LA PARRA, Eduardo, "El Derecho a la Propia Imagen", IPIDEC, Tirant lo Blanch, 2014, México.

Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Un enfoque global de la protección de los datos personales en la Unión Europea", disponible en https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_es.pdf

Directrices 5/2019 sobre los criterios del Derecho al Olvido en los casos de motores de búsqueda en el marco del RGPD (Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR) adoptadas el 2 de diciembre de 2019, por la Junta Europea de Protección de Datos (European Data Protection Board, EDPB), disponible en https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201905_rtbsearchengines_forpublicconsultation.pdf

Directrices para la implementación de la sentencia del tribunal de justicia de la unión europea en el juicio "Google España y Inc. v. Agencia Española de Protección de Datos (AEPD) Y Mario González Costeja" C-131/12, adoptadas el 26 de noviembre de 2014, disponibles en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf

El erróneamente llamado Derecho al Olvido no es un derecho, es una forma de censura, R3D, Julio 12, 2016, México, disponible en: <https://r3d.mx/2016/07/12/el-erroneamente-llamado-derecho-al-olvido-no-es-un-derecho-es-una-forma-de-censura/>

Fraude en Estrella Blanca alcanza a Vamos México, Revista Fortuna, México, Agosto 24, 2016, disponible https://revistafortuna.com.mx/opciones/archivo/2007/febrero/htm/fraude_estrella_blanca_vamos_mexico.htm#

GALINDO SOTO, Javier José, “Richter vs. Google va a la Suprema Corte”, El Economista, 13 de agosto de 2017, México, disponible en <https://www.eleconomista.com.mx/opinion/Richter-vs.-Google-va-a-la-Suprema-Corte-20170813-0001.html>

Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, INAI. Disponible en: http://inicio.ifai.org.mx/DocumentosdelInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

Guía para el Borrado Seguro de Datos Personales, INAI Disponible en http://inicio.ifai.org.mx/DocumentosdelInteres/Guia_Borrado_Seguro_DP.pdf

Iniciativa con proyecto de decreto que reforma, adiciona y modifica diversas disposiciones de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en materia de Derecho de Olvido, Grupo Parlamentario MORENA, México, 3 de diciembre de 2019, disponible en: https://infosen.senado.gob.mx/sgsp/gaceta/64/2/2019-12-03-1/assets/documentos/Inic_Morena_Sen_Monreal_Posesion_Particulares.pdf

Iniciativa de la Sen. Alejandra del Carmen León Gastélum y de las senadoras y senadores del Grupo Parlamentario del Partido del Trabajo, con proyecto de decreto por el que se reforma la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Gaceta del Senado, 3 de marzo de 2020, México, Disponible en https://www.senado.gob.mx/64/gaceta_del_senado/documento/104767

Iniciativa de la Sen. María Verónica Martínez Espinoza, del Grupo Parlamentario del Partido Revolucionario Institucional, la que contiene proyecto de decreto por el que se adicionan diversas disposiciones a la Ley Federal de Protección de Datos Personales en Posesión de Particulares. Disponible en: https://www.senado.gob.mx/64/gaceta_comision_permanente/documento/42432

Iniciativa del senador Ricardo Monreal sobre supuesto Derecho al Olvido amenaza la libertad de expresión en línea, Red en Defensa de los Derechos Digitales, México, enero 24, 2020, Disponible en: <https://r3d.mx/2020/01/24/iniciativa-del-senador-ricardo-monreal-sobre-supuesto-derecho-al-olvido-amenaza-la-libertad-de-expresion-en-linea/>

Juicio de Nulidad J.N. 5622/17-17-14-6/453/18-PL-04-04, Sala Superior del Tribunal Federal de Justicia Administrativa, Disponible en <http://sentencias.tfjfa.gob.mx:8080/SICSEJLDOC/faces/content/public/consultasentencia.xhtml;jsessionid=TY-9Za8vSy3kliZrYuU5LYhncNMEIZU-EsrSg-VWC8q5aYmL6FFp!-1090808339>

Kyllo v. United States, 533 U.S. 27 (2001). Caso disponible en <https://www.law.cornell.edu/supct/html/99-8508.ZO.html>

LANZA, Edison, “Estándares para una Internet Libre, Abierta e Incluyente”, Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, Organización de los Estados Americanos, OEA/Ser.L/V/II, CIDH/RELE/INF.17/17, 15 de marzo 2017, Disponible en http://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 2010

MURILLO Eduardo “Por primera vez, discutirá la Corte "Derecho al Olvido"”, La Jornada, México, 4 de noviembre 2019, disponible en: <https://www.jornada.com.mx/ultimas/politica/2019/11/04/por-primera-vez-discutira-la-corte-derecho-al-olvido-1265.html>

Olmstead vs. U.S. 1928. Caso disponible en <https://www.law.cornell.edu/supremecourt/text/277/438>

ORNELAS NÚÑEZ, Lina y PIÑAR MAÑAS, José Luis (Coord.), La protección de Datos Personales en México, México, Tirant Lo Blanch, 2013.

ORTEGA MARTÍNEZ, Jesús, “Sociedad de la información y Derechos Humanos de la Cuarta Generación. Un desafío inmediato para el derecho constitucional”, Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, 2004. Disponible en <https://archivos.juridicas.unam.mx/www/bjv/libros/4/1510/26.pdf>

Ponderación y equilibrio entre los derechos al olvido y de información, plantean expertos, Comunicado del INAI, no. INAI/226/16, 23 de agosto de 2016, disponible <http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-226-16.pdf>

Press Release Issued by the Article 29 Data Protection Working Party, Disponible en inglés, en http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20141126_wp29_press_release_ecj_de-listing.pdf

Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo de 27 de abril de 2016, 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Disponible en <https://eur-lex.europa.eu/eli/reg/2016/679/oj/spa>

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 2011

Reporte de transparencia de Google, disponible en:
<https://transparencyreport.google.com/eu-privacy/>

Resolución TD/266/2007 de la Agencia Española de Protección de Datos

SILBERLEIB, Laura, "El Derecho al Olvido y la persistencia de la memoria." Información, cultura y sociedad: revista del Instituto de Investigaciones Bibliotecológicas, no. 35 (2016):125-136. Redalyc, <https://www.redalyc.org/articulo.oa?id=263048647007>

SOLOVE, Daniel J.; SCHWARTZ, Paul M., Information Privacy Law, 4th Ed., Wolters Kluwer Law & Business.

TAFOYA HERNÁNDEZ, J. Guadalupe; CRUZ RAMOS, Consuelo Guadalupe, "Reflexiones en torno al Derecho al Olvido", Revista del Instituto Federal de Defensoría Pública del Consejo de la Judicatura Federal, Número 18, diciembre de 2014, Disponible en <https://www.ifdp.cjf.gob.mx/resources/revistas/Revista18.pdf>

Tesis 1a. CXLIX/2007, Tomo XXVI, Julio de 2007, Página 272. Semanario Judicial de la Federación y su gaceta. Vida privada e intimidad. Si bien son derechos distintos, ésta forma parte de aquélla.

Tesis 1a. CXLVIII/2007 Tomo XXVI, Julio de 2007, Página 272. Semanario Judicial de la Federación y su gaceta. Vida privada. El artículo 1o. de la ley sobre delitos de imprenta, al proteger el honor y la reputación frente a cualquier manifestación o expresión maliciosa, no excede el límite establecido por el artículo 7o. De la constitución federal.

Tesis 1a./J. 42/2007, Tomo XXV, Abril de 2007, página: 124. Semanario Judicial de la Federación y su Gaceta. Garantía a la tutela jurisdiccional prevista en el

artículo 17 de la constitución política de los estados unidos mexicanos. Sus alcances.

Tesis: 1a. CCXIV/2009, Registro:165823, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXX, diciembre de 2009, p. 277.

Tesis: I.10o.A.120 A (10a.), Registro 2020549, Semanario Judicial de la Federación, Décima Época, 06 de septiembre de 2019. Datos personales. La licencia de uso de un signo marcario relativo a la prestación del servicio de motor de búsqueda en internet concedida por una empresa extranjera en favor de una sociedad mercantil mexicana es apta para considerar la responsabilidad de ésta por el tratamiento de aquéllos conforme a la normativa constitucional y legal respectiva.

Tesis: I.10o.A.5 CS (10a.), Registro: 2020563, Semanario Judicial de la Federación, Décima Época, viernes 06 de septiembre de 2019. Protección de datos personales. Constituye un derecho vinculado con la salvaguarda de otros derechos fundamentales inherentes al ser humano.

Tesis: I.10o.A.6 CS (10a.), Registro: 2020564, Semanario Judicial de la Federación, Décima Época, viernes 06 de septiembre de 2019. Protección de datos personales. El deber del estado de salvaguardar el derecho humano relativo debe potencializarse ante las nuevas herramientas tecnológicas, debido a los riesgos que éstas representan por sus características.

Tesis: I.3o.C.695 C, Registro: 168944, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXVIII, septiembre de 2008, p. 1253. "Derecho a la intimidad. Su objeto y relación con el derecho de la autodeterminación de la información."

Tesis: I.5o.A.13 A (10a.), Registro: 2020767, Semanario Judicial de la Federación y su Gaceta, Décima Época, t. I.5o.A.13 A (10a.), Libro 71, Octubre de 2019, Tomo IV, p. 3640. Tribunal federal de justicia administrativa. Carece de

competencia para conocer de las demandas promovidas contra las resoluciones emitidas por el instituto nacional de transparencia, acceso a la información y protección de datos personales, al ser éste un organismo constitucional autónomo.

The Value of Personal Online Data European Union Agency for Cybersecurity, April 23, 2018, disponible en <https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data>

Treasury Targets Drug Trafficking Networks in Colombia and Mexico, Treasury US, Julio 15, 2020, disponible en <https://www.treasury.gov/press-center/press-releases/Pages/tg775.aspx>

TUDÓN MALDONADO, Martha A., “El Derecho al Olvido y lo que se pretende borrar”, Animal Político, México, 7 de febrero, 2020, disponible en: <https://www.animalpolitico.com/altoparlante/el-derecho-al-olvido-y-lo-que-se-pretende-borrar/>

USTARAN, Eduardo, “European Data Protection, Law and Practice”, International Association of Privacy Professionals (IAPP), 2018.

WARREN, Samuel D.; BRANDEIS, Louis D., The Right to Privacy, Harvard Law Review, Vol. 4, No. 5. (diciembre 15, 1890), pp. 193-220, disponible en https://www.jstor.org/stable/1321160?seq=2#metadata_info_tab_contents (URL permanente)



Anexos

ANEXO I

Preguntas frecuentes sobre las solicitudes europeas de privacidad relacionadas con la eliminación de resultados de la búsqueda

¿Cómo funciona el proceso de Google?

Las personas o sus representantes primero deben completar este [formulario web](#). La persona recibirá una respuesta automática en la que se le confirmará la recepción de la solicitud. Las solicitudes se evalúan una por una. En algunos casos, es posible que solicitemos que la persona nos proporcione más información. Una vez que tomemos una decisión, la persona recibirá un correo electrónico en el que se le informará nuestra decisión y, en caso de que no se elimine el contenido, se le proporcionará una breve explicación.

¿Quién puede solicitar una eliminación?

Las personas pueden solicitar la eliminación de resultados de la búsqueda de acuerdo con las leyes europeas de protección de datos. También está permitido realizar solicitudes en nombre de otra persona, siempre que el solicitante pueda demostrar que cuenta con una autorización legal para hacerlo.

¿Quién toma las decisiones sobre las solicitudes para eliminar contenido?

El personal de Google Inc. toma las decisiones pertinentes. Contamos con un equipo de revisores entrenados especialmente para este fin, cuyo centro principal se encuentra en Dublín, Irlanda. Nuestro equipo remite solicitudes a empleados superiores y abogados de Google para que emitan fallos sobre casos difíciles y complejos. Hasta el 1 de noviembre de 2015, poco más del 30% de las solicitudes se remitieron a una instancia superior para recibir una segunda opinión.

¿Cómo se evalúan las solicitudes?

Desarrollamos minuciosamente los criterios en consonancia con las [pautas del Grupo de trabajo del artículo 29](#). Después de que recibimos una solicitud a través de nuestro formulario

web, se realiza una revisión manual. No existen categorías de solicitudes que personas o máquinas rechacen de forma automática.

Nuestro proceso de evaluación consta de cuatro pasos:

1. ¿La solicitud contiene toda la información necesaria para que podamos tomar una decisión?
2. ¿La persona que presenta la solicitud tiene una conexión con un país europeo, como residencia o ciudadanía?
3. ¿Las páginas aparecen en los resultados de la búsqueda del nombre del solicitante y el nombre del solicitante figura en las páginas que se piden eliminar?
4. ¿La página que se solicita eliminar contiene información que es inadecuada, irrelevante, excesiva o que ya no se considera relevante, sobre la base de la información que proporciona el solicitante? ¿Existe un interés público de que esa información se mantenga disponible en los resultados de la búsqueda que se generan al buscar el nombre del solicitante?

Si una persona nos presenta una solicitud que no contiene información suficiente para que podamos tomar una decisión, es posible que solicitemos información suplementaria para respaldar nuestra evaluación.

Para demostrar el alcance de las solicitudes de eliminación, incluimos una sección de resúmenes de solicitudes en el Informe de transparencia.

¿Las páginas se eliminan completamente de los resultados de la búsqueda?

No. Las páginas solo se eliminan de los resultados en respuesta a consultas relacionadas con el nombre de una persona. Por lo tanto, si se aceptara la solicitud para eliminar un artículo de John Smith sobre su viaje a París, no se mostraría el resultado para las consultas relacionadas con [John Smith], pero sí se mostraría para una consulta como [viaje a París]. Eliminamos URL de todos los dominios europeos de Búsqueda de Google (google.fr, google.de, google.es, etc.) y usamos señales de ubicación geográfica para restringir el acceso a la URL desde el país de la persona que solicita la eliminación.

Por ejemplo, si elimináramos una URL como resultado de una solicitud de John Smith en el Reino Unido, los usuarios en esa ubicación no verían la URL en los resultados de la búsqueda para las consultas que incluyeran [John Smith] al buscar en cualquier dominio de Búsqueda de Google, incluido google.com. Por el contrario, los usuarios fuera del Reino Unido podrían ver la URL en los resultados al buscar [John Smith] en cualquier dominio no europeo de Búsqueda de Google.

¿Qué sucede si una persona no está de acuerdo con la decisión?

Si decidimos no eliminar una URL de los resultados de búsqueda, la persona puede acudir a una autoridad local con competencia en protección de datos para que revise nuestra decisión.

¿Se les informa a los webmasters que se elimina contenido?

Google tiene como política enviarles una notificación a los webmasters cuando se quitan las páginas de su sitio de nuestros resultados de búsqueda a causa de una solicitud legal. Lo hacemos para garantizar la transparencia. Para respetar la privacidad de las personas que solicitaron la eliminación, solo enviamos las URL afectadas, no el nombre del solicitante.

¿Los webmasters pueden cuestionar de alguna manera las decisiones?

Los webmasters que reciban nuestra notificación para que realicen eliminaciones a través de las Herramientas para webmasters de Google pueden solicitar que volvamos a revisar una decisión.

¿Este fallo también se aplica a otros servicios de búsqueda de Google como Búsqueda de imágenes?

Actualmente, nuestro proceso abarca la eliminación de resultados de nuestras propiedades de búsqueda, como Búsqueda de Google, Búsqueda de imágenes, Búsqueda de videos y Google Noticias.

¿Cuáles son algunos de los casos comunes de eliminación de páginas?

Algunos de los factores materiales más comunes que se tienen en cuenta al momento de decidir qué páginas eliminar incluyen:

- **Ausencia clara de interés público:** Por ejemplo, sitios agregadores con páginas que contienen información de contacto personal o la dirección, instancias en las que el nombre del solicitante no aparece más en la página y páginas que ya no se encuentran en línea (error 404).
- **Información confidencial:** Páginas con contenido que se relaciona únicamente con información sobre la salud, la orientación sexual, la raza, el origen étnico, la religión, la filiación política y la posición a nivel sindical de una persona.
- **Contenido relacionado con menores de edad:** Contenido relacionado con menores o delitos de menores que ocurrieron cuando el solicitante era menor.
- **Absoluciones, exoneraciones y condenas cumplidas por delitos:** Conforme a las leyes locales acerca de la rehabilitación de los delincuentes, tendemos a actuar en favor de eliminar el contenido relacionado con condenas que ya se cumplieron, acusaciones que se comprobaron que eran falsas en un tribunal o contenido relacionado con un delito penal del cual se absolvió al solicitante. También consideramos la antigüedad de este contenido y la naturaleza del delito en nuestro análisis.

¿Cuáles son algunos de los casos comunes en los que no se eliminan páginas?

Algunos de los factores materiales más comunes que se tienen en cuenta al momento de decidir qué páginas eliminar son:

- **Soluciones alternativas:** Hay otra vía para que el solicitante elimine esa página de nuestros resultados de la búsqueda. Por ejemplo, es posible que el solicitante haya publicado el contenido en un sitio que permite que los usuarios impidan la aparición del contenido en los resultados de la búsqueda. Cuando podemos, les proporcionamos información sobre estas herramientas a los solicitantes.
- **Razones técnicas:** Una URL incompleta o rota es un error técnico común. Algunas veces, los solicitantes nos piden que eliminemos páginas para una consulta que no coincide con su nombre o el de la persona que el solicitante afirma representar.

- **URL duplicada por la misma persona:** Un solicitante envía varias solicitudes de eliminación de la misma página para el mismo nombre.
- **Interés público importante:** Es posible que rechacemos la eliminación si determinamos que la página contiene información que es de gran interés público. Determinar si el contenido es de interés público es complejo y puede significar considerar diversos factores que incluyen, con carácter meramente taxativo, si el contenido se relaciona con la vida profesional del solicitante, un delito que se cometió en el pasado, un cargo político, su posición en la vida pública o si el contenido es de autoría del solicitante, se trata de documentos del gobierno o es de carácter periodístico.

¿Pueden proporcionar estadísticas más detalladas sobre la naturaleza de estas solicitudes y eliminaciones?

Proporcionamos estadísticas sobre la magnitud de nuestro proceso de eliminación (que se actualizan diariamente) desde octubre de 2014 en este [Informe de transparencia](#) y agregamos ejemplos anónimos de decisiones de eliminación para darle color. Los datos adicionales sobre factores materiales comunes se pueden descargar [aquí](#). Un informe más detallado sobre los datos del período 2014-2017 está disponible [aquí](#). Continuamos explorando formas de proporcionar más transparencia a las decisiones de eliminación de una manera operacionalmente eficiente y con debido respeto a la naturaleza confidencial y privada de las solicitudes.

¿Por qué algunos gráficos indican que las fechas de los datos solo llegan a enero de 2016?

En conformidad con un fallo de la corte de 2014, Google trabajó para implementar un proceso que evalúe las solicitudes de la forma más rápida posible. Dado que este era un proceso completamente nuevo, todavía no habíamos determinado qué información deseábamos recopilar sobre las solicitudes. Con el tiempo, ajustamos y mejoramos nuestros procesos y la cantidad de datos que registramos sobre cada solicitud. En enero de 2016, implementamos un nuevo proceso interno basado en nuestras experiencias hasta la fecha.

¿Cómo clasifican a un solicitante?

Las categorías de los solicitantes se usan con el objetivo de clasificar a las personas que envían solicitudes para eliminar contenido de Búsqueda, por ejemplo, si el solicitante es una persona privada, un menor, una entidad corporativa o una figura pública. Establecemos estas categorías con la información que proporciona el solicitante (p. ej., la razón por la que solicita la eliminación) y la información disponible al público, como el contenido en la URL.

¿Cuáles son las diferentes categorías para los solicitantes?

- **Entidad corporativa:** El solicitante se comunica en nombre de una empresa o una corporación.
- **Persona fallecida:** El solicitante se comunica en nombre de una persona fallecida.
- **Funcionario público:** El solicitante es un político o funcionario del Gobierno actual o anterior.
- **Menor:** El solicitante es menor a la edad de consentimiento sexual.
- **Figura pública que no pertenece al Gobierno:** El solicitante es conocido a nivel internacional (p. ej., es una actriz o un actor famoso), o cumple un papel importante en la vida pública de una región o área específica (p. ej., es una académica reconocida en su campo).
- **Persona privada:** No se aplica ninguna de las otras categorías a esta persona.

¿Cómo clasifican el contenido de la página?

Las categorías del contenido de la página clasifican el contenido que aparece en las páginas específicas enviadas en solicitudes relacionadas con el derecho al olvido. El contenido de la página se relaciona con la vida social del solicitante, es de su propia autoría o hace referencia a actos criminales. Cuando evaluamos una solicitud, revisamos el contenido en la URL para la que se solicitó su eliminación y asignamos la categoría correspondiente.

¿Cuáles son las diferentes categorías para el contenido de la página?

- **Crimen:** El contenido de la página hace referencia al solicitante en relación con actos criminales. Por ejemplo, el contenido se relaciona con una condena del solicitante, su testimonio en un juicio o su condición de víctima.

- **No se encontró el nombre:** No se puede encontrar ninguna referencia al nombre del solicitante en la URL indicada. Sin embargo, es posible que el nombre de la persona aparezca en la URL.
- **Información insuficiente:** No se categorizó el contenido de la página porque Google requiere más información para procesar la solicitud. Por ejemplo, el solicitante proporcionó una URL incompleta o no indicó una razón para la eliminación de una URL.
- **Varios:** El contenido de la página no corresponde a ninguna de las otras categorías de contenido.
- **Información personal:** El contenido de la página incluye la dirección personal del solicitante, su residencia u otra información de contacto; imágenes o videos de la persona; o demás información personal no confidencial.
- **Política:** El contenido de la página incluye críticas sobre las actividades políticas o gubernamentales del solicitante, o información que es relevante al perfil, la plataforma o la trayectoria política pública de la persona.
- **Información profesional:** El contenido de la página incluye la dirección de trabajo del solicitante, su información de contacto o información general sobre sus actividades comerciales.
- **Ofensas profesionales:** El contenido de la página hace referencia a actividades criminales o penales (crímenes, absoluciones o exoneraciones) específicamente relacionadas con un rol profesional.
- **Autoría propia:** El solicitante es el autor, total o parcial, del contenido de la página.
- **Información personal confidencial:** El contenido de la página menciona el estado médico, la orientación sexual, el credo, el origen étnico o la afiliación política del solicitante.

¿Cómo clasifican los sitios web?

Estas categorías clasifican el sitio web que aloja una página con una solicitud para su eliminación; p. ej., un sitio de noticias, una red social o un sitio gubernamental. Durante nuestra evaluación de una solicitud individual, evaluamos el sitio para determinar su categoría.

¿Cuáles son las diferentes categorías para los sitios web?

- **Directorio:** La página web se aloja en un sitio que funciona como un directorio o agregador de información, p. ej., direcciones postales o números de teléfono de empresas o personas.
- **Gobierno:** La página se aloja en un sitio web oficial del Gobierno; en un sitio que hace referencia o contiene registros legales, comerciales o gubernamentales; o en un sitio web que es el canal de medios oficial del Gobierno (tenga en cuenta que los medios públicos, como BBC o PBS, no se incluyen aquí).
- **Noticias:** La página se aloja en un sitio web de un tabloide o canal de medios no gubernamental.
- **Varios:** Las demás categorías no se aplican al sitio web que aloja la página.
- **Redes sociales:** La página es un perfil de una cuenta, una foto, un comentario o demás contenido alojado en el sitio de una red social en línea.

¿Por qué algunas URL con el contenido de la página "No se encontró el nombre" aparecen como eliminadas?

Si el nombre de un solicitante no aparece en el contenido de la página en cuestión, es posible que tomemos medidas para que esta página no se muestre en los resultados de la búsqueda para las consultas que incluyen el nombre de dicha persona.

¿Por qué algunos meses muestran un valor de "0" para el volumen de URL solicitadas?

Google no comenzó a registrar datos detallados sobre las URL hasta mediados de junio de 2014.

¿Dónde puedo obtener más información?

En julio de 2014, Google recibió una invitación para reunirse con el Grupo de trabajo del artículo 29 para analizar la implementación práctica. Anterior a la reunión, completamos un cuestionario en el que se detalla el proceso y la implementación, el cual publicamos [aquí](#). La decisión de la corte está disponible [aquí](#).

ANEXO II

Formulario para solicitar la retirada de información personal¹⁶⁶

Retirada en virtud de la ley de privacidad de la UE

Formulario para solicitar la retirada de información personal

Por motivos de privacidad, tienes el derecho a solicitar que se retire determinada información personal sobre ti.

Este formulario sirve para solicitar que retiremos de la Búsqueda de Google resultados específicos de consultas en las que se incluya tu nombre. Si quieres solicitar la retirada de información personal de otro producto de Google, envía una solicitud a través del formulario correspondiente, que puedes encontrar en nuestra página [Cómo retirar contenido de Google](#)

Por ejemplo, si quieres retirar información personal de Blogger, envía una solicitud a través del formulario de Blogger.

Cuando envías una solicitud, en Google buscamos el equilibrio entre los derechos a la privacidad de los usuarios afectados, el interés público que pueda tener esa información y el derecho de otros usuarios a distribuirla; por ejemplo, es posible que rechacemos retirar cierta información sobre estafas financieras, negligencias profesionales, condenas penales o conductas de funcionarios.

Para completar este formulario, necesitas una copia digital de un documento de identidad. Si envías una solicitud en nombre de otra persona, tienes que facilitar su documento de identidad.

* Campo obligatorio

TU INFORMACIÓN

País de origen *

Nombre legal completo *

Aunque envíes la solicitud en nombre de otra persona que te haya autorizado para representarla, debes indicar tu nombre. Si representas a otra persona, debes tener autoridad legal para actuar en su nombre.

¹⁶⁶ https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=637058001879032052-3333461258&rd=1

Nombre:

Apellidos:

Dirección de correo electrónico de contacto *

Actúo en nombre de... *

Si envías esta solicitud en nombre de otra persona, tienes que especificar tu relación con ella (por ejemplo, "padre" o "abogado"). Es posible que te solicitemos documentación que confirme que estás autorizado para representarla.

Yo mismo Cliente Familiar Amigo Otros

Tu relación legal con la persona en cuyo nombre presentas esta solicitud *

Adjuntar una copia legible de un documento que verifique la identidad de la persona en cuyo nombre se presenta la solicitud *

Para evitar que se envíen solicitudes de retirada de contenido fraudulentas procedentes de personas que se hacen pasar por otras, que intentan dañar a la competencia o que quieren eliminar información legal de forma inadecuada, tenemos que verificar la identidad de la persona en cuyo nombre se realiza la solicitud (la persona correspondiente). No es necesario que sea un pasaporte ni otro documento de identificación oficial. Puedes ocultar partes del documento que proporcionen (por ejemplo, el número de identificación), siempre que se pueda identificar a la persona correspondiente con el resto de la información. Asimismo, puedes ocultar cualquier fotografía presente en el documento de identificación, excepto si estás solicitando que se retiren páginas con fotografías de esa persona. Google LLC solo utilizará esta información para evaluar y documentar la autenticidad de tu solicitud y eliminará la copia en un plazo de un mes una vez cerrada la solicitud, a menos que la ley establezca lo contrario.

Para subir varios documentos a la vez, mantén pulsada la tecla Ctrl o Comando al seleccionar los archivos.

¿Has presentado una solicitud anterior?

Si tú (o la persona correspondiente) ya has solicitado que retiremos URLs con contenido similar, podremos ayudarte antes si, en lugar de enviarnos una notificación nueva, contestas a algún correo electrónico que te hayamos enviado a ti (o a la persona correspondiente).

Si prefieres enviarnos una notificación nueva, introduce el número de referencia de 14 dígitos que identifica tu solicitud anterior, con un formato similar a 1-1111000001111. Puedes encontrar este número en el asunto del correo electrónico que te enviamos como respuesta a tu anterior solicitud.

IDENTIFICA LA INFORMACIÓN PERSONAL QUE QUIERAS QUE SE RETIRE Y SU UBICACIÓN

Si esta notificación está relacionada con varios motivos que han sido objeto de una infracción, envía únicamente el primero aquí abajo. A continuación, haz clic en el enlace "Añadir un nuevo grupo" que aparece debajo de los cuadros de texto para añadir otro motivo.

Las URL del contenido que incluya la información personal que quieres retirar *

Haz clic [aquí](#) para obtener ayuda con la búsqueda de la URL.



Introduce una URL en cada línea (1000 líneas como máximo).

Motivo de la eliminación *

Para cada una de las URL que facilites, debes indicar lo siguiente:

- (1) cómo se relaciona la información personal identificada anteriormente con la persona en cuyo nombre presentas esta solicitud; y
- (2) por qué crees que esta información personal debe retirarse

Por ejemplo: "(1) Esta página está relacionada conmigo porque a, b y c. (2) Esta página debería retirarse porque x, y y z".

[Añadir un nuevo grupo](#) (10 grupos como máximo)

Nombre utilizado para realizar búsquedas *

Este debería ser el nombre que, si se utiliza como consulta de búsqueda, produzca los resultados que quieres eliminar del registro. Si quieres enviar varios nombres (por ejemplo, si tu apellido de soltera es diferente al que utilizas ahora), utiliza una barra diagonal ("/") para separarlos. Por ejemplo, "Ana García / Ana Díaz".

DECLARACIONES JURADAS

Lee las afirmaciones siguientes y marca las casillas para confirmar que estás de acuerdo.

Consiento que se procese la información personal que envío, como se describe a continuación: *

Google LLC utilizará la información personal que facilites en este formulario (como tu dirección de correo electrónico y todos los datos de identificación) y la información personal que envíes en otros mensajes para procesar tu solicitud y cumplir con nuestras obligaciones legales. Google puede compartir información de tu solicitud con las autoridades de protección de datos, pero solo si la solicitan para investigar o revisar una decisión que Google haya tomado. Esto suele ocurrir si te has puesto en contacto con la autoridad de protección de datos nacional en relación con nuestra decisión. Si, debido a tu solicitud, se han retirado URLs de nuestros resultados de búsqueda, Google puede facilitar información a los webmasters de dichas URL.

Ten en cuenta que si has iniciado sesión en tu cuenta de Google, podemos asociar tu solicitud a esa cuenta.

Declaro que la información de esta solicitud es precisa y que estoy autorizado para enviarla. *

Entiendo que Google no puede procesar mi solicitud si el formulario no se ha rellenado correctamente o si la solicitud está incompleta. *

FIRMA

Fecha de la firma: *

MM/DD/YYYY (por ejemplo, "12/19/2010")

Firma: *

por ejemplo, Juan Pérez
Al escribir tu nombre completo más arriba, nos proporcionas tu firma digital, que es legalmente vinculante del mismo modo que tu firma física. Ten en cuenta que tu firma debe coincidir exactamente con el nombre y los apellidos introducidos en la parte superior de este formulario web para que el envío se realice correctamente.

FORMATO DE SOLICITUD PARA EL DERECHO A SUPRESIÓN (DERECHO AL OLVIDO)

Es su derecho solicitarnos la supresión de cualquier dato personal que tengamos sobre usted en virtud del Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

La información proporcionada en esta solicitud únicamente será utilizada para identificar los datos personales que se desean suprimir y para dar respuesta a su solicitud. No está obligado a completar este formato para hacer la solicitud, sin embargo, este formato es de gran ayuda para procesar su solicitud de manera eficaz.

SECCIÓN 1: DATOS DE LA PERSONA QUE SOLICITA LA INFORMACIÓN

Nombre completo: _____

Dirección: _____

Teléfono de contacto: _____ Correo electrónico: _____



SECCIÓN 2: TITULAR DE LOS DATOS PERSONALES

Seleccione la opción más adecuada y posteriormente lea las instrucciones.

SÍ: Soy el titular. Adjunto fotocopia de mi identificación oficial (Por favor ir a la sección 4)

NO: Estoy actuando en representación del titular. Adjunto la autorización por escrito del titular de los datos, fotocopia de su identificación oficial y fotocopia de mi identificación oficial (Por favor ir a la sección 3)

Para asegurarnos de que estamos suprimiendo los datos personales de la persona correcta, le pedimos que nos proporcione una identificación oficial. En fotocopia o imagen escaneada (no envíe los originales) :

Identificación oficial:

- Pasaporte, licencia de conducir con foto, documento de identificación nacional, entre otros.

En caso de no poder validar su identidad, nos reservamos el derecho de negarnos a aceptar su solicitud.

SECCIÓN 3: DATOS DEL TITULAR (EN CASO DE SER DIFERENTES AL DE LA SECCIÓN 1)

Nombre completo: _____

Dirección: _____

Teléfono de contacto: _____ Correo electrónico: _____

SECCIÓN 4: MOTIVO DE LA SOLICITUD DE SUPRESIÓN

Dado a la naturaleza sensible de la supresión de datos personales, el artículo 17 del RGPD requiere que se cumplan ciertas condiciones antes de considerar una solicitud. Por favor indique el motivo por el que desea que se supriman sus datos.

Por favor seleccione el motivo:

- Considero que mis datos personales ya no son necesarios para los fines para los que fueron recopilados originalmente.
- Retiro el consentimiento para el tratamiento de mis datos personales.
- Me he opuesto al tratamiento de mis datos y el responsable no tiene interés legítimo para continuar el tratamiento.
- Siento que mis datos personales han sido tratados ilegalmente.
- Considero que están sujetos a una obligación legal de la Unión Europea o del Estado miembro que requiere la supresión de mis datos personales.
- Soy un niño, represento a un niño o era un niño al momento del tratamiento de mis datos personales y considero que se utilizaron para ofrecerme servicios de la sociedad de la información.



SECCIÓN 5: ¿QUÉ INFORMACIÓN DESEA SUPRIMIR?

Por favor incluya un anexo en el que describa la información que desea suprimir. Favor de proporcionar detalles relevantes que considere que puedan ayudarnos a identificar la información.

Considere que en ciertas circunstancias, suprimir información puede afectar negativamente la libertad de expresión, ya que se contradice una obligación legal, actúa contra el interés público en el área de la salud pública, actúa contra el interés público en el área de investigación científica o histórica, o prohíbe el establecimiento de una defensa legal o el ejercicio de otros reclamos legales, también es posible que no podamos suprimir la información que solicitó de conformidad con el artículo 17 (3) del RGPD, de ser el caso se le informará de inmediato y explicarán los motivos de la decisión.

Nos complace realizar la supresión de datos personales que ha solicitado, sin embargo, nos reservamos el derecho, de acuerdo con el artículo 12(5) del RGPD, para cobrar un "monto razonable" o negarnos a la solicitud si se considera "manifiestamente infundada o excesiva". Sin embargo, haremos todo lo posible para proceder con la solicitud de supresión de sus datos personales, si corresponde.

SECCIÓN 6: DECLARACIÓN

Considere que realizar declaraciones falsas puede constituir un delito.

Confirmando que he leído y entiendo los términos de este formulario y certifico que la información proporcionada en este formato de solicitud de supresión de datos personales es verdadera. Entiendo que es necesario que confirme mi identidad o la del titular de los datos y puede ser necesario que se me solicite más información para corroborar mi identidad o la del titular de los datos.

Firma: _____ Fecha: _____

Documentos que deben adjuntarse a este formato de solicitud:

- Identificación oficial del Titular (ver sección 2)
- Autorización de los padres o tutor legal, cuando el titular es menor de edad.
- Autorización del Titular para actuar en su representación (si aplica)
- Descripción de la información que se desea suprimir (ver sección 5)