Colección Ensayos para la Transparencia de la Ciudad de México 2013

Invitamos a los lectores a consultar la página Web del Instituto, desde la cual tendrán acceso a todas nuestras publicaciones.

www.infodf.org.mx

Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal

La Morena No. 865 Local 1, Col. Narvarte Poniente,
Del. Benito Juárez, C.P. 03020, México, Distrito Federal
"Plaza de la Transparencia"
Tel. 5636-4636 (5636INFO) | www.infodf.org.mx | oip@infodf.org.mx

ensayos 23 PARA LA TRANSPARENCIA DE LA CIUDAD DE MÉXICO

El derecho al olvido en relación con el derecho a la protección de datos personales.

Isabel Davara Fernández de Marcos

El Instituto de Acceso a la Información Pública del Distrito Federal (InfoDF) pone a su disposición, la Colección de Ensayos para la Transparencia de la Ciudad de México, esfuerzo editorial dirigido a generar reflexión y análisis sobre el conocimiento y práctica de la transparencia, el acceso a la información, la protección de datos personales y la rendición de cuentas, en un contexto complejo como el Distrito Federal, una de las ciudades más grandes del mundo.

Comprometido con la promoción de la cultura de la transparencia, el instituto, a través de su línea editorial Ensayos Científicos, impulsa el desarrollo de investigaciones acerca de estos componentes esenciales para el fortalecimiento de las democracias modernas, convocando a reconocidos investigadores y académicos a debatir y aportar ideas y experiencias, a través de este género que consideramos apropiado a los propósitos de divulgación del InfoDF.

Los ensayos pretenden ser puntos de partida para impulsar debates, documentar tendencias recientes, e incorporar análisis críticos y novedosos. Su estructura libre, su tratamiento sintético, la variedad temática, convierten al ensayo en un recurso pedagógico para inducir a todo público en el conocimiento y reflexión, que sin duda son necesarios para construir un pensamiento analítico en torno a estos nuevos conceptos que acompañan el fortalecimiento de las democrácias contemporáneas. Esperamos que los temas y el estilo personal de sus autores, inviten a la lectura y sobre todo, motiven su interés en participar en la discusión actual sobre estos temas y generar iniciativas que apoyen la consolidación de la cultura de trasnparencia en nuestra Ciudad de México.

23

EL DERECHO AL OLVIDO EN RELACIÓN CON EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

Isabel Davara F. de Marcos

infodf
Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal

Primera edición, Abril 2014
ISBN: 978-607-7702-04-7

ÍNDICE

ISABEL DAVARA
F. DE MARCOS

Doctora en Derecho y licenciada en Ciencias Económicas y Empresariales. Socia del despacho DAVARA ABOGADOS (www.davara.com.mx <http://www.davara.com.mx>), boutique legal especializada en Derecho de las TIC. Miembro del Consejo de la Sección de Ciencia y Tecnología, y presidenta del Comité de Comercio Electrónico para Latinoamérica en la American Bar Association.

Coordinadora del Diplomado de Derecho de las TIC en el ITAM nivel posgrado, y profesora de la misma institución; profesora invitada en diversas academias nacionales y extranjeras; conferencista y panelista en multitud de foros especializados en Derecho de las TIC nacional e internacionalmente, así como autora y coautora de numerosas obras, artículos y ensayos en la materia a nivel nacional e internacional.

Autora del blog sobre firma electrónica para Política Digital.

1. PLANTEAMIENTO[1]

Lo primero que me vino a la mente al comenzar este artículo fue el título "El derecho al olvido". ¿Podría haber tenido algún significado escribir sobre un tema así hace tan sólo unas décadas?, ¿qué implica necesitar que exista un derecho a ser olvidado o a olvidar?, ¿no debería ser algo que se diera sin más? y, en caso de que no sea así, ¿es posible exigirlo? o, mejor dicho, ¿es factible que en realidad se otorgue?

Parece que este tema no puede tener existencia sin hablar, a simple vista, de varias cuestiones interrelacionadas:

1. el tratamiento de información personal,
2. en grandes cantidades o por diferentes medios,
3. la dispersión de la información,

[1] Agradezco la ayuda de Ana Dorotea Vásquez Colmenares en el presente análisis.

4. el perfil obtenido o las consecuencias derivadas del tratamiento de la información personal,
5. la titularidad de la información personal, y
6. los diferentes derechos coexistentes (por ejemplo, derecho a la intimidad, al honor, a la propia imagen) y en conflicto (por ejemplo, libertad de expresión), así como los distintos ordenamientos aplicables.

Lo anterior, tan sólo como meros apuntes de aproximación introductoria pues, como veremos a lo largo de este breve estudio, existen muchos conceptos y temas involucrados.

Así, parece que debido al ingente volumen de información personal sometido a diversos tratamientos con diferentes herramientas, la persona, el individuo, se ve sujeto a la extracción de diferentes evaluaciones y consideraciones sobre su ser mismo como consecuencia de dicho tratamiento de información personal.

Esto es, hoy en día, más que ayer, y probablemente menos que mañana, se derivan acciones y decisiones del tratamiento de la información personal de los individuos. Cada vez más significativamente, en número y en calidad,[2] la persona ve cómo su información personal es tratada y evaluada en relación con un sinfín de actividades diversas: buscar empleo, solicitar un crédito, asistir a un centro educativo, realizar la compra semanal, son tan sólo ejemplos de la multitud de situaciones en las que la información personal se ve comprometida.[3]

[2] Y, dando un paso más allá, consideramos que hoy en día en realidad nuestra "identidad virtual" es incluso más importante, al menos cuantitativamente hablando, que nuestra única hasta el momento identidad física. Y así dice Rodotà: "Las tecnologías de la información y de la comunicación están rediseñando el mundo, las relaciones personales, sociales, políticas y económicas. Pero esta transformación tiene un precio. […] es justamente la información la que viene a constituir ahora la materia prima más importante y que, dentro de la información, los datos personales son especialmente preciados. […] nuestra propia vida está volviéndose hoy en día un intercambio continuo de informaciones […] la protección de datos asume una importancia creciente, que la conduce cada vez más hacia el centro del sistema político-institucional." Stefano Rodotà, *Tecnología y derechos fundamentales,* Agència Catalana de Protecció de Dades, 2004. Disponible en <www.apd.cat>. Consultado en diciembre de 2013.

[3] El valor de los datos personales es absolutamente innegable. De un lado, en términos

Pero, ¿qué se quiere decir con la expresión "derecho al olvido"? Arriesgándonos a realizar un símil un tanto complicado, especialmente si se toma en su exactitud, parece que estamos entrando en un apartado que antes se reservaba a las autoridades, cualesquiera que fuera su categoría, en relación con el derecho a tener un expediente "limpio", por ejemplo, en cuanto a los antecedentes de cualquier tipo (penales, crediticios, académicos). Claro, lo anterior, a pesar de que potencialmente podía ser más complicado, también era cierto que su ámbito de extensión o conocimiento era más controlado y controlable.

Es decir, antes, no hace mucho, el sujeto podía, hasta cierto punto y con cierta facilidad, controlar la expansión de su información personal; sin embargo, hoy esto se torna cada vez más difícil y, con ello, el perfil y la caracterización que en el futuro persigan al individuo se convierten en un tema de arduo control.[4]

Hasta la utilización masiva de la informática para dicho tratamiento, no se producía una intromisión tan importante y agresiva en la esfera personal e íntima de las personas.[5] Esta intromisión, que en algunos casos no tiene por qué ser negativa, ni mucho menos ilícita, se percibe como una amenaza potencial, desconocida. Además, la importancia del tratamiento por medios informáticos ha tenido una especial incidencia, pues las fronteras

de derecho de la personalidad, del individuo, y, de otro, en claros términos económicos. R. Posner, "The Economics of Privacy", *The American Economic Review*, vol. 71, núm. 2, mayo de 1981; A. D. Oliver Lalana, *Código invisible y pequeño gran hermano. Nuevas condiciones de posibilidad del derecho a la protección de datos*. Disponible en <http://www.unizar.es/fyd/prodatos/pdf/oliver_madrid02.pdf>. Consultado en diciembre de 2013.

[4] Como señala Aristeo García, la delimitación conceptual del derecho a la intimidad como facultad de aislamiento se ha convertido en un poder de control sobre las informaciones relevantes para cada sujeto. Y así, citando al famoso 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". 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] S. Bayens, "The search and seizure of computers: are we sacrificing personal privacy for the advancement of technology?", *Drake Law Review*, 2000; P. O'Connor, *Online Consumer Privacy*, Institut de Management Hotelier International at ESSEC Business School. Disponible en <http://cqx.sagepub.com/content/48/2/183.abstract>.

de tiempo y espacio, que protegían en gran manera la intimidad del individuo, se han difuminado sustancialmente, haciendo que la información personal se pueda tratar, comunicar, conservar, manipular, etc., de muy diferentes maneras, y donde la concepción cerrada y estática del derecho a la intimidad pasa a una abierta y dinámica, que implica el reconocimiento no sólo de un derecho sino, sobre todo, de la necesidad de nuevos mecanismos de protección.

Es por esto que surge, en mi opinión, con inusitada fuerza, el tema del "derecho al olvido" y, lo que es incluso más relevante para efectos prácticos, el cumplimiento práctico del mismo. Esto es, si probablemente puede llegar a darse cierto grado de consenso en cuanto al contenido y delimitación del derecho o, al menos, en relación con los límites más relevantes del mismo, parece que su control adolece de no pocas dificultades. Es decir, si bien podemos coincidir en que este derecho es una manifestación concreta y real del derecho fundamental a la protección de datos personales, parece que en su control en tiempo y lugar es en donde se encuentran más dificultades.

Además, este derecho puede ser visto desde una doble perspectiva:[6] por un lado, como un *derecho a ser olvidado* y, por otro, como un *derecho a olvidar*. Y ambas orientaciones están en cierto modo interrelacionadas, a modo de círculo vicioso, pues parece difícil olvidar si existe la posibilidad fáctica y real de ser recordado en cualquier momento. Así, el derecho a "olvidar" información personal que pueda ser perjudicial o tenga una connotación negativa para el individuo, de manera que el sujeto tenga la posibilidad de comenzar de nuevo, sin estar atado a un pasado que quiere dejar atrás y, por otro lado, pero estrechamente relacionado, el derecho a ser olvidado, expresado como un derecho de caducidad de la información personal de un individuo por el simple transcurso del tiempo, o bien porque la finalidad para la que se trataba ha dejado de existir.

Pero, para comenzar con la aproximación a este derecho, creemos que es importante empezar con el derecho a la protección de datos personales y a la autodeterminación informativa, por el que el titular de los

[6] Bert-Jaap Koops, *Forgetting Footprints, Shunning Shadows: A Critical Analysis of the "Right to Be Forgotten"*, SSRN Scholarly Paper, NY Social Science Research Network, Estados Unidos. Disponible en <http://papers.ssrn.com/abstract=1986719>.

datos personales, la persona física o individuo dueño de los mismos, es el único que tiene derecho a decidir quién, cómo, dónde, cuándo y para qué se tratan sus datos personales. Y, además, sin olvidar que ya hay quien apunta que el derecho al olvido no debería ser tutelado en relación con la protección de datos, sino con el derecho al honor o a la intimidad aunque, no obstante, lo que realmente ocurre es un tratamiento de datos personales, a pesar de que ese tratamiento pueda (o no) tener consecuencias o impactos en otros derechos. Y esto, en esencia, es la diferencia entre entender que el derecho a la protección de datos personales tiene una entidad individualizada e independiente,[7] sin necesidad de que existan otros derechos vulnerados.

Así pues, en el presente trabajo se realizará una aproximación al contenido del derecho al olvido, analizando de manera concisa diferentes puntos, entre los que podemos destacar su relación con el derecho a la protección de datos y la autodeterminación informativa, la incidencia de Internet y otras herramientas tecnológicas o, finalmente, el famoso "caso Google".

[7] La relevante sentencia del Tribunal Constitucional Español 292/00 del 30 de noviembre de 2000, como veremos más en detalle después, instaura jurisprudencialmente en España la autonomía e independencia del derecho fundamental a la protección de datos, diferenciándolo claramente de otros cercanos, como el de la intimidad.

2. EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y A LA AUTODETERMINACIÓN INFORMATIVA

El tratamiento de datos personales, y en consecuencia la necesidad de su regulación, no es algo etéreo o que pueda dejar indiferente a nadie. A diario se realizan multitud de diferentes tratamientos de datos personales sobre cada individuo que pueden pasar incluso desapercibidos, tanto para el que los realiza como para el que es sometido a los mismos (administrados, clientes, recursos humanos, etc.).

Se necesita cada vez más conocer a los destinatarios de productos y servicios, fabricados todos de manera muy similar, y la difícil competencia sólo encuentra dicha diferenciación en tanto se conoce al consumidor final. Y, dando un paso más allá, podemos afirmar que nuestra "identidad virtual" es incluso más importante, al menos cuantitativamente hablando,[8] que nuestra más tangible identidad física.[9]

[8] Stefano Rodotà, *op. cit.*

[9] En este sentido véase, entre otros, el documento de trabajo sobre servicios de autenticación en línea, WP 68, adoptado por el Grupo de Trabajo del 29 de enero de 2003. Disponible en <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp68_es.pdf>.

Esa identidad electrónica de la que hablamos se convierte entonces en un riesgo latente para el individuo, si existe un mal tratamiento en manos de terceros, bien sean empresas[10] o administración pública; por lo tanto, como decíamos, deviene imprescindible que se instrumenten soluciones jurídicas que protejan al titular de los datos contra esta intromisión ilícita en su privacidad.[11]

En México, en particular el derecho a la protección de datos personales, no fue reconocido constitucionalmente sino hasta 2009 con la reforma hecha a los artículos 6 y 16 en los cuales se incorpora éste a la lista de derechos fundamentales, señalando:

> **Artículo 6. [...]**
> II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y las excepciones que fijen las leyes.
> III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.
>
> **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 (ARCO), 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,

[10] Según una noticia del *New York Times*, los empresarios utilizan cada vez más las herramientas de Internet (como los buscadores o las redes sociales) para evaluar a un posible candidato: "For some, Online Persona Undermines a Résumé", *New York Times* del 11 de junio de 2006. Disponible en <http://www.nytimes.com/2006/06/11/us/11recruit.html?_r=1&pagewanted=all>. Consultado el 19 de agosto de 2013. Asimismo, véase el caso Leander relativo a un afectado rechazado para ocupar un puesto de trabajo a partir de un informe secreto desfavorable considerándole peligroso para la seguridad nacional en T. Freixes Sanjuán, "Obtención y utilización de datos personales automatizados", *Jornadas sobre el Derecho Español de la Protección de Datos Personales,* Madrid, Agencia de Protección de Datos, 28, 29 y 30 de octubre de 1996, pp. 159 a 162.

[11] Antonio Gómez-Robledo y Lina Ornelas Núñez, *Protección de datos personales en México: el caso del Poder Ejecutivo Federal*, México, Instituto de Investigaciones Jurídicas, 2006, p. 14.

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

A nivel federal, para el sector privado, la protección de datos personales está garantizada mediante la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en adelante, LFPDPPP)[12] y su normatividad de desarrollo, en las cuales se contemplan, además de los principios y tutela requeridos, los referidos derechos ARCO; para el sector público, también a nivel federal, rige la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en la que únicamente se prevén los derechos de Acceso y Rectificación.

A nivel local, en el Distrito Federal, tenemos que referirnos a dos normatividades: a la Ley de Protección de Datos Personales para el Distrito Federal[13] (LPDPDF), y a la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal[14] (LTAIPDF).

Así, según lo establecido por LPDPDF:

1. El artículo 5 habla de tres principios importantes para el ejercicio del derecho al olvido:

[12] El análisis de la protección de datos puede estructurarse en un triángulo cuyos tres vértices se denominarían principios, derechos y procedimiento, respectivamente. Así, diríamos que la protección de datos se compone de una serie de principios que, a modo de declaraciones programáticas, establecen los pilares en los que se basa la protección de datos. Los derechos, por su parte, representan la concreción subjetiva de ejercicio de esos principios, es decir, cómo el titular de los datos de carácter personal puede ejercer unos derechos que concretan los principios teóricos en los que se basa toda la normatividad. El procedimiento, finalmente, cerrando este triángulo ficticio, concreta la tutela pública a la que el individuo puede recurrir cuando se ve lesionado en el ejercicio de esos derechos como consecuencia de esos principios. Por otro lado, en el tratamiento de datos de carácter personal podemos distinguir tres fases claramente diferenciadas: la obtención de los datos, el tratamiento de los mismos y la utilización del resultado del tratamiento, y, en su caso, la transmisión de datos a un tercero. En cada una de esas fases tenemos que atender al respeto de todos los principios y derechos prescritos en la normatividad. De esta manera, si no se cumple con alguno, el tratamiento se convierte inmediatamente en ilícito. Véase a I. Davara F. de Marcos, *Hacia la estandarización de la protección de datos personales. Propuesta sobre una tercera vía o* tertium genus *internacional*, Madrid, Wolters Kluwer, 2011.

[13] *Gaceta Oficial del Distrito Federal*, 3 de octubre de 2008.

[14] *Gaceta Oficial del Distrito Federal*, 28 de marzo de 2008.

a) El principio de confidencialidad, que consiste en "garantizar que exclusivamente la persona interesada puede acceder a los datos personales o, en caso, el responsable o el usuario del sistema de datos personales para su tratamiento, así como el deber de secrecía del responsable del sistema de datos personales, así como de los usuarios". En este punto, podríamos decir que el hecho de que se le otorgue al titular de los datos la prerrogativa de que sea él únicamente quien tenga acceso a sus datos personales en poder del responsable, y que este último tenga un deber de secrecía respecto de éstos, habla de una disposición que el legislador presta a favor del ejercicio del derecho al olvido; esto es así ya que, siendo que los datos no son revelados a personas distintas del interesado y que solamente él puede disponer de ellos, será más sencillo para el titular ejercer su derecho de cancelación con la seguridad de que su información ha sido debidamente contenida y no cuentan con ella terceros indeseados por él.

b) El principio de disponibilidad: "los datos deben ser almacenados de modo que permitan el ejercicio de los derechos de acceso, rectificación, cancelación y oposición del interesado". Este principio da también mayor seguridad al titular de los datos, en tanto que le confirma que el responsable tiene almacenados sus datos de manera sistémica y ordenada, de modo que él podrá en todo momento saber qué datos tienen de él, rectificar los datos incorrectos, oponerse al tratamiento de los datos para ciertas finalidades y, más relevantemente para el tópico en cuestión, cancelar dichos datos, de modo que se eliminen de las bases de datos del responsable y el titular pueda "ser olvidado" dichos registros.

c) El principio de temporalidad, por virtud del cual "los datos personales deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los que hubiesen sido recolectados". Así, se obliga al responsable a que los datos personales sean destruidos una vez terminada la finalidad para la cual fueron recabados, o bien pasado un lapso determinado y razonable. Esto representa un punto eje del derecho que nos ocupa en el presente ensayo debido a que, justamente mediante el derecho al olvido, el

titular demanda que se elimine su rastro en el entorno de la información y su acceso.[15]

2. Por su parte, el artículo 19[16] de la LPDPDF establece el derecho de supresión por virtud del cual una persona física tiene derecho a que su información personal sea eliminada y, por lo tanto, deje de ser asequible, después de un cierto periodo de tiempo.

Por otro lado, la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal centra su objeto en la máxima publicidad de la información en posesión de las dependencias públicas del Distrito Federal, por lo que su orientación hacia la protección de datos personales es muy distinta, máxime cuando además ya se cuenta dentro del Instituto con la ley específica antes mencionada. En este sentido, el equilibrio y los límites de la protección de datos personales encuentran más restricciones frente a la publicidad y la garantía al acceso de la información.[17]

[15] En cuanto a los tipos de seguridad que se deben llevar para el almacenamiento de datos, la LPDPDF menciona que los responsables establecerán las medidas de seguridad técnica y organizativa para garantizar la confidencialidad e integralidad de los sistemas de datos personales que posean. En este sentido, se entiende que inclusive sobre los datos almacenados de forma electrónica o en la red, el responsable debe procurar mantener un control adecuado de éstos, así como las medidas de seguridad que eviten que la información sea publicada o compartida indiscriminadamente a terceros. De este modo, el derecho al olvido se facilita al titular una vez más ya que, al darse esta situación de vigilancia y transparencia, el titular de los datos podrá tener mayor certeza de que, al ejercer su derecho al olvido, se tiene idea y control del alcance que tuvieron sus datos publicados y de la eliminación de los mismos.

[16] **Artículo 19.** Los sistemas de datos personales que hayan sido objeto de tratamiento, deberán ser suprimidos una vez que concluyan los plazos de conservación establecidos por las disposiciones aplicables, o cuando dejen de ser necesarios para los fines por los cuales fueron recabados.
En el caso de que el tratamiento de los sistemas haya sido realizado por una persona distinta al ente público, el instrumento jurídico que dio origen al mismo deberá establecer el plazo de conservación por el usuario, al término del cual los datos deberán ser devueltos en su totalidad al ente público, quien deberá garantizar su tutela o proceder, en su caso, a la supresión.

[17] Así, los artículos 8, 9 y 38, por ejemplo, hacen excepciones en cuanto a la publicidad de los datos de los servidores públicos porque, aunque siguen siendo datos personales, en función del cargo que ostentan, la transparencia y la rendición de cuentas están por encima, en función del bien jurídico superior protegido en el caso.

Habiendo expuesto brevemente algunas de las disposiciones contenidas en la normatividad nacional, resulta pertinente dilucidar el contexto actual en el que nos encontramos.

Hoy en día, en un entorno donde las tecnologías de la información y la comunicación (TIC) han evolucionado rápidamente y en el cual hemos sido testigos de un amplio progreso tecnológico, sucede con gran facilidad que toda clase de información y datos, incluyendo los personales, tienen gran difusión y alcance masivos, y son asequibles a muchas más personas con mayor facilidad.[18]

Así, la gran expansión de Internet y de todo lo que ello conlleva, ha tenido como consecuencia el surgimiento de la necesidad de encontrar un nuevo punto de equilibrio entre la libertad que tienen las personas de difundir información y la autodeterminación informativa del individuo.

[18] La Resolución (73) del Comité de Ministros del Consejo de Europa específicamente señala los peligros que pueden surgir del aumento en el uso y la popularización de la tecnología y, en nuestra opinión, resume de manera excepcional todas las preocupaciones mencionadas. Así, dicha Resolución dice:
Las finalidades para las que los ordenadores se están utilizando en los sectores público y privado no son por sí mismas diferentes de las más tradicionales formas de almacenamiento y proceso de datos. Lo que diferencia a los ordenadores de los medios tradicionales de almacenamiento y proceso de datos es la extraordinaria facilidad con la que han superado de golpe toda una serie de problemas generados en el tratamiento de la información: el gran volumen de datos, las técnicas de su almacenamiento y recuperación, su transmisión por largas distancias, su correcta interpretación y, finalmente, la velocidad con la que todas estas operaciones se pueden desarrollar. En consecuencia, los ordenadores, la informática, permite que se almacenen, como bases de datos, o colecciones de datos, o redes integradas de esas colecciones de datos. Estos bancos de datos pueden proporcionar, de manera instantánea y a través de largas distancias, información masiva acerca de los individuos. A pesar de que algunos pocos rechazarían los grandes avances ofrecidos por la aplicación de estas técnicas de proceso electrónico de datos, existe una preocupación creciente en el público acerca de la posibilidad de un uso indebido de la información personal sensible almacenada electrónicamente. Por ejemplo, es mucho más difícil para un individuo tomar los pasos para proteger sus intereses personales frente a un sistema de información que frente a los tradicionales registros de datos. Además, en lo relativo a sus datos, que por sí mismos son inofensivos, pueden ser relacionados de tal manera que su disponibilidad se convierta en una amenaza a sus intereses privados. (Traducción y énfasis propios.)
Resolución R (73) 22 relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado. Adoptada el 26 de septiembre de 1973, en la 224ª reunión del Consejo de Ministros.

La legislación mexicana, al igual que la internacional, hace especiales y reiteradas referencias al derecho a la autodeterminación informativa, siendo éste precisamente el objeto principal de las normatividades en datos, tal y como señala la LFPDPPP:

> **Artículo 1.** La presente Ley es de orden público y de observancia general en toda la República y tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

A nivel internacional, y especialmente europeo, con la conocida sentencia del Tribunal Constitucional Federal Alemán (en alemán, *Bundesverfassungsgericht*) de 1983[19] sobre la licitud del tratamiento de los datos del censo de un ciudadano alemán, se abre un nuevo e importante camino, al menos doctrinal, en la protección de datos en Europa.[20]

[19] La ley alemana del Censo de Población de 1983 fue aprobada por el Bundestag el 4 de marzo de 1983. Se presentó un recurso de amparo constitucional el 5 de marzo de ese mismo año por parte de una ciudadana que reclamaba que la Ley del Censo lesionaba los derechos protegidos en los artículos 1, 2, 5 y 19 de la Ley Fundamental de Bonn, en particular el derecho al libre desenvolvimiento de la personalidad y a la dignidad humana, la libertad de expresión y las garantías procesales. El recurso dio lugar a una sentencia cautelar del Tribunal Constitucional del 13 de abril que concluía que existían fundamentos para la suspensión provisional de la vigencia de la ley hasta la resolución de fondo, que se produjo mediante la sentencia del 15 de diciembre de 1983 y que anula parcialmente la ley impugnada. Sentencia del Tribunal Constitucional Alemán del 15 de diciembre de 1983, *Boletín de Jurisprudencia Constitucional*, 1984, páginas 126 y ss.

[20] El artículo 8 de la Carta Europea de Derechos Fundamentales señala claramente:
Artículo 8
Protección de datos de carácter personal
1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

En esta sentencia se asienta el conocido principio a la autodeterminación informativa[21] que señala que el titular de los datos es el único que tiene derecho a decidir cómo, cuándo, dónde y por quién se tratan sus datos.[22]

Tal y como señaló ya en su día 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[23] sobre ella y respecto a quién y con qué objeto se transmite".[24]

---

21 Que la doctrina suele llamar, en un juego de palabras, "principio a la autodeterminación informática", aludiendo al tratamiento automatizado de los mismos.

22 El principio de la autodeterminación es sustancial y va más allá que el principio del consentimiento, como señala Davara Rodríguez: "Un primer comentario lleva a decir que no nos parece adecuado unir autodeterminación con consentimiento en la recogida del dato haciendo ver que tanto es el principio del consentimiento como el principio de autodeterminación. De otra forma creemos que se vaciaría de contenido al principio de la autodeterminación informativa que tiene una calidad superior y marca la línea de protección absoluta de los datos personales, ciñéndola a un acto de voluntad por su titular. Otra cosa es el consentimiento unido a la licitud de la toma del dato que solamente abarca una faceta de la autodeterminación en la línea bidireccional marcada en la relación entre el titular del dato y el titular del fichero. […] Sin embargo, la autodeterminación puede tener un componente unidireccional, mediante el que una parte, en ejercicio de su libertad, presenta un dato suyo permitiendo, o no, expresa o tácitamente, su recogida y tratamiento automatizado." (subrayado propio). Véase a M. A. Davara Rodríguez, "La teoría del consentimiento en la protección de datos personales: su implicación con la relación contractual", Encuentros sobre Informática y Derecho, Madrid, Universidad Pontificia Comillas, 1996, páginas 75 y ss.

23 Así, Adinolfi resalta que el elemento caracterizador de este derecho es la autonomía del consentimiento, esto es, la posibilidad que tiene el individuo de autorizar, bloquear, oponerse al tratamiento, rectificar, o bien, de quedarse indiferente respecto a las circulaciones de su información personal y, en este sentido, en la medida en que la información personal de los individuos puede ser descargada, consultada, seleccionada, compartida y registrada de diversos modos, se debe tener la posibilidad de decidir libremente sobre la información personal y tener una verdadera autonomía con respecto de dichos datos. Giulio Adinolfi, "Autodeterminación informativa. Consideraciones acerca de un principio general y un derecho fundamental", *Cuestiones Constitucionales*, núm. 17, México, Instituto de Investigaciones Jurídicas de la UNAM, 2007. Disponible en <http://www.ejournal.unam.mx/cuc/cconst17/CUC000001701.pdf>. Consultado en diciembre de 2013.

24 De Terwangne señala que se refiere a "la capacidad de elegir, de tomar decisiones informadas, en otras palabras, a mantener el control sobre diferentes aspectos de [la] vida". Cécile de Terwangne, "Privacidad en Internet y el derecho a ser olvidado/derecho al olvido", *Derecho y Política*, núm. 13, Catalunya, Universitat Oberta de Catalunya, 2012, pp. 53-66.

Además de lo anterior, es importante detenernos de nuevo para resaltar que el derecho a la protección de datos personales y a la autodeterminación informativa es un derecho independiente y autónomo, de tercera generación.[25]

Esta categoría de derechos se distinguen porque surgen como respuesta a la evolución social. Asimismo, otra característica que presentan es que, para que puedan ser ejercidos y respetados, es necesario el esfuerzo conjunto de todos los actores de la sociedad; esto es, el Estado, el individuo, y las entidades públicas y privadas. Por esto, su realización depende de un cierto consenso social en los niveles locales, nacionales e internacionales.[26]

Son, además, derechos colectivos o comunitarios (por ejemplo, derecho a la autodeterminación, a la paz, al desarrollo, a la democracia, a la integración, a recibir y producir información equitativamente, al medio ambiente sano y ecológicamente equilibrado, a beneficiarse del patrimonio común de la humanidad) que se encuentran, internacionalmente, en distintas etapas de desarrollo.

Son, en definitiva, derechos que por un lado implican una defensa frente al Estado y, por otro, se pueden demandar ante el mismo, que requieren de todos los actores sociales para su cumplimiento, plantean exigencias en el plano nacional y en el internacional, y encajan en el concepto moderno de "calidad de vida".[27]

El desarrollo tecnológico ha tenido una fuerte incidencia en el nuevo planteamiento de las relaciones de los seres humanos con su entorno y

[25] "Los derechos y las libertades de la tercera generación se presentan como una respuesta al fenómeno de lo que se ha denominado 'contaminación de las libertades' —pollution des libertés—, término con el que algunos sectores de la teoría social anglosajona hacen alusión a la erosión y degradación que aqueja a los derechos fundamentales ante determinados usos de las nuevas tecnologías." Aristeo García González, *op. cit*.

[26] Corte Suprema de Justicia - División de Investigación, Legislación y Publicaciones, *Protección de Datos Personales*, Paraguay, 2010.

[27] Disponible en <http://www.iepala.es/curso_ddhh/ddhh1518.htm> y <http://www.dlh.lahora.com.ec/paginas/judicial/PAGINAS/D.Humanos.15.htm>. Consultado en septiembre de 2009.

entre ellos mismos, viéndose necesariamente afectados, con ello, los derechos humanos. Es justamente el derecho que tienen las personas a que se protejan sus datos personales de las amenazas que presenta el avance de las nuevas tecnologías, lo que abre paso con mayor fuerza a la implementación del derecho a la autodeterminación informativa.[28]

La privacidad, como dijimos, no puede ser ya hoy entendida como el derecho[29] a ser dejado solo,[30] sino que conlleva el poder de controlar

[28] La mencionada Sentencia del Tribunal Constitucional 292/00 del 30 de noviembre instaura jurisprudencialmente en España, y se ha tomado como referencia internacional en nuestro entorno, la autonomía e independencia del derecho fundamental a la protección de datos, diferenciándolo claramente de otros cercanos, como el de la intimidad, y así lo señala en su Fundamento Jurídico Sexto: "el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado [...] atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer."

[29] Rodotà, distinguiendo entre vida privada (que se incluye en el título de la Directiva, entre otras cosas) y derecho a la protección de datos, indica que "Y es importante resaltar que, caso único en el entero texto de la Constitución Europea, al derecho a la protección de datos personales se dedica un artículo específico también en la primera parte (artículo 51). Este nuevo derecho fundamental no puede ser enmarcado en el esquema de 'ser dejado solo', sino que se concreta en la atribución a cada uno del poder de 'gobernar' la circulación de las informaciones que le conciernen. Se transforma así en elemento capital de la libertad del ciudadano en la sociedad de la información y de la comunicación. Esta distinción no es sólo un aspecto externo." Stefano Rodotà, *Democracia y protección de datos*. Disponible en <https://www.agpd.es/portalweb/canaldocumentacion/conferencias/common/pdfs/DemocraciaMadrid_mayo_05.pdf>.
Se crea así un nuevo modelo que, al reforzar la esfera privada, fortalece al mismo tiempo el peso del individuo en la esfera pública, constituyendo un elemento básico de la que podemos denominar nueva ciudadanía electrónica, donde el test de "impacto privacidad" es imprescindible para juzgar el efectivo nivel de democracia del sistema político en cuestión.

[30] En el conocido artículo de los Jueces del Tribunal Supremo, Samuel D. Warren y Louis D. Brandeis, de finales del siglo diecinueve, se explica la evolución de dicho derecho, apoyándose en un tratado muy renombrado sobre injurias de otro juez, llamado Cooley, donde defendía el derecho a "ser dejado en paz", y comienzan así a definir lo que en dichos ordenamientos se entiende la privacidad en la era moderna. Hemos extraído, y traducido, un párrafo que ejemplifica lo que venimos diciendo:
Las recientes invenciones y métodos de negocios llaman la atención sobre el siguiente paso que se tendrá que tomar en la protección de la persona, y para asegurar al individuo lo que el Juez Cooley denomina "el derecho a ser dejado solo".

la información personal[31] 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 control sobre los sujetos, públicos o privados, que disponen de sus datos personales. Se pretende proteger al titular de los datos, pues corre peligro de convertirse en un ciudadano de vidrio,[32] transparente a ojos de todos.[33]

Las fotografías instantáneas y las empresas periodísticas han invadido los sagrados recintos de la vida privada y doméstica; numerosos aparatos mecánicos amenazan haciendo predicciones como "lo que se susurre en los armarios será proclamado desde los tejados de las casas". Durante años ha habido un sentimiento de que la ley puede proporcionar algún remedio para la circulación no autorizada de retratos de personas; y el demonio de la invasión de la privacidad por los periódicos, sentido desde hace mucho tiempo, ha sido recientemente discutido por un capacitado escritor. Los factores alegados de algún caso notorio ante un tribunal menor en Nueva York hace unos meses, directamente implicaban la consideración del derecho a circular retratos; y la pregunta de si nuestro derecho reconocerá y protegerá el derecho a la privacidad a éste y otros respectos debe tenerse en consideración por nuestros tribunales pronto.
Véase "The right to privacy", *Harvard Law Review*, vol. IV, núm. 5, 15 de diciembre de 1890. Disponible con modificaciones en <http://www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html>. Consultado el 2 de julio de 2009.

Y el desarrollo posterior, en el ordenamiento jurídico estadounidense, ha tenido lugar gracias al desarrollo jurisprudencial, tal y como, por ejemplo, se resalta en la Sentencia del Tribunal Constitucional Español 290/2000, del 30 de noviembre: "Suele citarse una sentencia de 1965, dictada en Griswold *vs*. Connecticut, donde se consideró violado el derecho a la privacidad en el matrimonio, invocando al efecto las Enmiendas Primera (que se refiere a varios derechos, entre ellos el de libertad religiosa), la Enmienda Tercera (no alojar tropas sin el consentimiento del dueño de la casa), Enmienda Cuarta (inmunidad del hogar), Enmienda Quinta (garantías del imputado). Con estos derechos se argumentó que proporcionar información sobre el uso de contraconceptivos, que es lo que hacía el Sr. Griswold, director de una Liga de planeamiento familiar, conculcaba el derecho a la privacidad en el matrimonio. La Enmienda Novena, al dejar abierta la lista de derechos fundamentales, facilitó esta elaboración jurisprudencial de un derecho atípico."

31 C. Fried, "Privacy", *Yale Law Journal*, núm. 475, 1968.

32 La mencionada Sentencia del Tribunal Federal Alemán dice: "en virtud de esta evolución de los condicionamientos tecnológicos, es posible producir una imagen total y pormenorizada de la persona respectiva –un perfil de la personalidad- incluso en el ámbito de su intimidad, convirtiéndose así el ciudadano en «hombre de cristal»".

33 Rodotà indica que "el «hombre de vidrio» es una metáfora nazi, que refleja la idea de un Estado que puede adueñarse por entero de la vida de las personas, que frente a si no tiene ciudadanos sino súbditos". "Democracia y protección de datos", *Cuadernos de Derecho Público*, núms. 19-20, mayo-diciembre de 2003, Madrid, INAP.

En definitiva, como consecuencia de todo lo que hemos ido señalando, surge un nuevo derecho que es independiente y autónomo. Lo anterior es esencial, puesto que puede llegar a confundirse con otros tantos derechos relacionados, como el derecho a la intimidad o a la vida privada, por ejemplo.

Es absolutamente fundamental entender que este derecho surge como consecuencia del mero tratamiento de los datos personales de un individuo, sin que se necesite, para la existencia de este derecho, que se vea lesionado ningún otro derecho. Es decir, se protege a la persona frente al tratamiento ilícito de su información personal, sin que necesitemos que se cumpla cualquier otro requerimiento de cualquier otra infracción para que pueda existir la protección.

El tratamiento de datos personales de un sujeto es independiente en sí mismo y requiere una protección por sí misma. Reiteramos lo esencial del concepto: no es necesario que se vean involucrados otros derechos para que se proteja al sujeto.

Esto lo planteamos aquí porque, como veremos después, hay quien sostiene que el derecho al olvido tiene que tratarse en relación con el derecho al honor (o a otros semejantes como la imagen, por ejemplo), pero lo anterior sería dejar sin contenido, al menos en parte, al derecho a la protección de datos personales. Es decir, si bien es cierto que en muchos de los casos en los que se pretenda este derecho al olvido será como consecuencia de que el tratamiento de los datos ha provocado que se trate una información de la persona que ésta entiende como lesiva, en puridad no se necesita este condicionante para que el derecho a la protección de datos tenga lugar.

Esto es, el derecho a la protección de datos surge y se perfecciona por el mero tratamiento de los mismos, sin que sea necesario que dicho tratamiento vulnere algún otro derecho. Y, por lo tanto, aunque en la mayor parte de los casos parece razonable pensar que los titulares querrán que se “olvide” aquello que es “negativo” o “nocivo” para sus intereses, lo cierto es que la existencia del derecho a la protección de datos personales en sí evita que tengamos que entrar en subjetividades, y permite que el

titular esté protegido frente al mero tratamiento de sus datos personales, sin tener que entrar a demostrar si dicho tratamiento vulneró otros derechos subjetivos. Si el tratamiento es ilícito, en relación con lo previsto en la normatividad, la persona está protegida. Una vez que entendamos que es un derecho independiente, con total y propia entidad, no tendrá que relacionarse con ningún otro derecho para demostrar o exigir su tutela.

Como cierre de esta idea, por el momento, consideramos de excepcional interés resaltar diversos fragmentos de la relevante Sentencia del Tribunal Constitucional Español 292/00 del 30 de noviembre de 2000,[34] que instaura jurisprudencialmente en España la autonomía e independencia del derecho fundamental a la protección de datos, diferenciándolo claramente de otros cercanos, como el de la intimidad, señalando en su Fundamento Jurídico Sexto:[35]

> Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). **La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran**.

[34] Era consecuencia del Recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo, contra los artículos 21.1 y 24.1, y 2 de la LOPD.

[35] El resaltado es mío.

Continuando su razonamiento en el Fundamento Jurídico Sexto:

> 6. La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad [por todas STC 144/1999, de 22 de julio, FJ 8]. **En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado.** En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal [SSTC 134/1999, del 15 de julio, FJ 5; 144/1999, FJ 8; 98/2000, del 10 de abril, FJ 5; 115/2000, del 10 de mayo, FJ 4], es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos.
>
> [...]
>
> De ahí la singularidad del derecho a la protección de datos, pues, **por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad** que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal [STC 170/1987, del 30 de octubre, FJ 4], como el derecho al honor, citado expresamente en el art. 18.4 CE, e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona.
>
> (...)
>
> Pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE. Dicha peculiaridad radica en su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a

terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido [SSTC 73/1982, del 2 de diciembre, FJ 5; 110/1984, del 26 de noviembre, FJ 3; 89/1987, del 3 de junio, FJ 3; 231/1988, del 2 de diciembre, FJ 3; 197/1991, del 17 de octubre, FJ 3, y en general las SSTC 134/1999, del 15 de julio, 144/1999, del 22 de julio, y 115/2000, del 10 de mayo], **el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer.** A saber: **el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales** [STC 254/1993, FJ 7].

En definitiva, tal y como afirma rotundamente el Fundamento Jurídico Séptimo:[36]

> 7. De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos **consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.** Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos **se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular**.

[36] El resaltado es mío.

No obstante todo lo anterior, la STC mencionada no deja de señalar que este derecho fundamental, como cualquier otro, tiene también sus límites[37] en su Fundamento Jurídico Noveno:

> 9. En cuanto a los límites de este derecho fundamental no estará de más recordar que la Constitución menciona en el art. 105 b) que la ley regulará el acceso a los archivos y registros administrativos "salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas" [en relación con el art. 8.1 y 18.1 y 4 CE], y en numerosas ocasiones este Tribunal ha dicho que la persecución y castigo del delito constituye, asimismo, un bien digno de protección constitucional, a través del cual se defienden otros como la paz social y la seguridad ciudadana. Bienes igualmente reconocidos en los arts. 10.1 y 104.1 CE [por citar las más recientes, SSTC 166/1999, de 27 de septiembre, FJ 2, y 127/2000, de 16 de mayo, FJ 3.a; ATC 155/1999, de 14 de junio]. Y las SSTC 110/1984 y 143/1994 consideraron que la distribución equitativa del sostenimiento del gasto público y las actividades de control en materia tributaria [art. 31 CE] como bienes y finalidades constitucionales legítimas capaces de restringir los derechos del art. 18.1 y 4 CE.[38]

[37] Porque como dice en su Fundamento Jurídico Undécimo: "En el primer caso, regular esos límites es una forma de desarrollo del derecho fundamental. En el segundo, los límites que se fijan lo son a la forma concreta en la que cabe ejercer el haz de facultades que compone el contenido del derecho fundamental en cuestión, constituyendo una manera de regular su ejercicio, lo que puede hacer el legislador ordinario a tenor de lo dispuesto en el art. 53.1 CE."

[38] Respecto al artículo 105 b), véase a M. Lucas Durán, *El acceso a los datos en poder de la Administración Tributaria*, Pamplona, Aranzadi, 1997, páginas 265 y ss.

3. EL TRATAMIENTO DE DATOS PERSONALES POR MEDIOS ELECTRÓNICOS: LA RELEVANCIA ACTUAL Y PRÁCTICA DEL DERECHO AL OLVIDO

Si bien las tecnologías de la información y las comunicaciones –o en términos coloquiales o generalizadores, el uso de Internet– han traído consigo incontables beneficios, y ha cambiado la dinámica social mediante la cual nos comunicamos con otros y encontramos información de nuestro entorno, también es cierto que ha encerrado el riesgo implícito de la falta de control que tiene el usuario sobre la existencia y almacenamiento de su información personal y sobre el quién, cuándo y cómo ésta es consultada. Recordemos que todo lo que una vez ha pasado por la red, deja un rastro digital.[39]

[39] Así dijo la Comisionada del Instituto Federal de Acceso a la Información y Protección de Datos, Sigrid Arzt Colunga:
Ante el creciente uso de tecnologías mediante las cuales se transmiten millones de datos personales, el derecho al olvido puede considerarse como el derecho de las personas a eliminar o suprimir información que afecte su intimidad o su imagen, a fin de que aquellos datos que alguna vez fueron difundidos sean omitidos de la red.
En los casos de la información que existe en registros gubernamentales, dichos datos pueden ser eliminados cuando éstos ya no sean necesarios para la finalidad con que fueron recabados, o bien, cuando el periodo e utilidad ha concluido.
En Internet, el derecho a ser olvidado refiere a aquel que ampara a una persona para solicitar que los motores de búsqueda descarten su rastro o no los indexen en la red,

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. Así, en este punto, cabe resaltar lo mencionado en el Preámbulo de la LFPDPPP:

> […] La premisa básica detrás de la protección de los datos personales y de las regulaciones que gobiernan este derecho, debe ser la de la libertad de los individuos de controlar la forma en la que otros utilicen su información personal (derecho a la autodeterminación informativa). El tratamiento y utilización de los datos personales de un individuo, debe estar sujeto a reglas que aseguren que los mismos sean utilizados con fines legales y respetuosos del derecho fundamental de su protección.
>
> El derecho a la protección de datos personales, fundado en el control del individuo de la forma en que se utilizan por terceras personas, no depende del poder informático o del empleo de las nuevas tecnologías de la información y comunicaciones. Éstas son sólo herramientas que pueden ser utilizadas para su procesamiento, pero que pueden también proveer medidas de protección adecuadas y positivas que permitan a los individuos ejercer su derecho a elegir quiénes manejan, y cómo deben ser manejados sus datos personales.

a fin de asegurar conservar su imagen, su buen nombre y su dignidad, y evitar ser permanentemente objeto de agresiones, descalificaciones u ofensas.
El derecho al olvido se configura con la actualización de un dato o rectificación del mismo, la oposición a publicidad o publicación, así como a la cancelación permanente y definitiva si dicho dato rebasa los principios de la protección de datos personales (licitud, proporcionalidad, etc.).
Véase la ponencia "México, el derecho al olvido en internet: ejercicio de los derechos de cancelación y oposición, derecho al olvido *versus* derecho a la libertad de información, su incidencia en los medios de comunicación", XI Encuentro Iberoamericano de Protección de Datos, Cartagena, Instituto Federal de Acceso a la Información y Protección de Datos, octubre de 2013. Disponible en <http://www.redipd.org/actividades/encuentros/XI/common/Ponencias/P1_IFAI_MEXICO.pdf>.

> En este contexto, el Marco de Privacidad de APEC advierte sobre los riesgos de una legislación laxa en materia de privacidad en relación con la economía de un país: en la medida en que la recolección y manejo de datos personales es cada vez más fácil e indispensable para el crecimiento económico, los individuos comienzan a ser más recelosos para compartir su información, y pueden experimentar desconfianza sobre el uso que tendrá su información por parte de las entidades privadas que la recolectan.[40]

Así, podemos claramente hablar de un "efecto multiplicador" de Internet o de las tecnologías de la información y las comunicaciones en relación con el tratamiento de datos personales. En este contexto, cuando un usuario accede a Internet, datos como el idioma, los programas que se tienen instalados en el ordenador, el sistema operativo utilizado, entre otros, son enviados y recolectados por medio de la red. Esta información pueden ser datos personales que permiten identificar al usuario, según la definición contenida en el artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Y así, el usuario que navega por Internet está compartiendo, muchas veces sin conocimiento, sus datos personales.[41]

No hace falta que un usuario de Internet dedique horas a navegar, o que sea un adicto a las redes sociales para que cantidades grandes de sus datos estén alojados en la red. El simple correo electrónico es un claro ejemplo de esto: en nuestros correos electrónicos se archivan todos los mensajes que han sido enviados y recibidos desde años atrás, incluyendo los transmitidos mediante el servicio de chat.

---

40 Exposición de Motivos de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, LX Legislatura en la Cámara de Diputados del honorable Congreso de la Unión, 8 de diciembre de 2008.

41 En particular, un ejemplo de las herramientas de Internet que presentan un riesgo real para la privacidad son las llamadas "cookies". Las cookies son archivos que se mandan desde el sitio web que visita el usuario, y a través de los cuales se personalizan las páginas web que se visitan con posterioridad, pues accede a la información contenida en éstas sobre sus hábitos de navegación. En este sentido, la normatividad mexicana, y en concreto la federal aplicable al sector privado, presta especial atención a este respecto y a la necesidad de su concreción e información al titular.

A esto se suma la información almacenada en redes sociales,[42] donde se guardan fotos, conversaciones, archivos, publicaciones y cualquier intercambio de este tipo. Aun cuando no se realice un uso intensivo de Internet, o no se esté vinculado con ninguna red social, todas las búsquedas que se hacen mediante motores de búsqueda se guardan en un servidor para conformar, con esa información, un historial que permite crear un exhaustivo perfil de la persona con gran facilidad.[43]

---

42 Véase "Facebook quiere tu cara", <http://tecnologia.elpais.com/tecnologia/2013/08/30/actualidad/1377858949_296393.html>.
"Facebook sabe muchísimo de cada uno de sus usuarios: quiénes son sus amigos, familiares, los sitios a los que va, los productos que adora, los libros que lee o las películas que ve. Se declara abiertamente, forma parte del juego. Ahora quiere reconocer también a cada uno de sus clientes.
"En el nuevo documento con las normas de privacidad se explica qué podrá hacer la empresa con las fotos de perfil. Según esta propuesta, Facebook podrá analizar la imagen de perfil y usarla para sugerir etiquetas en otras fotos de la misma persona. La novedad estriba en que la sugerencia de etiquetas hasta ahora sólo se hacía basándose en fotos que ya tuvieran la etiqueta pero nunca tomando como modelo la imagen de perfil -la principal de cada miembro, que aparece junto a su nombre en cada una de sus acciones- que no tiene por qué tener una etiqueta.
"[...]
"Otro punto pendiente de aclarar es cómo usará la empresa los datos personales de cada miembro de la red con los anunciantes. Se limitan a zanjarlo con un "habrá más explicación". Hasta ahora necesitaban el permiso explícito para poner datos de un usuario en sus anuncios. El pasado lunes tuvieron que enfrentarse a un proceso judicial en el que se les pedían 15 millones de euros (20 millones de dólares), aunque inicialmente eran más de 110 (145 de dólares), por infringir esta norma en sus "historias patrocinadas", un formato publicitario que se presenta de manera muy similar al contenido generado por el usuario cuyos fines son comerciales.
"La demanda colectiva presentada en los juzgados de California argumentaba que los usuarios habían dado a 'me gusta' en una página de un producto y después vieron cómo se publicitaba esa acción sin su consentimiento. Desde el lanzamiento de este formato publicitario, hace 19 meses, Facebook se ha embolsado más de 176 millones de euros (234 millones de dólares) con este soporte."

43 Lo anterior, además, no se limita únicamente a la información que el usuario publica de sí mismo y que después termina en manos de un tercero. Diversos datos del titular pueden estar en línea luego de que un tercero los ha hecho disponibles, sin su consentimiento o conocimiento: si alguien "sube" una foto del usuario, si una entidad oficial publica en su portal una base de datos que contiene su nombre, si un medio de comunicación publica un artículo donde se incluyen sus datos, etc., existirá, sin siquiera saberlo el usuario, un gran cúmulo de sus datos disponibles en Internet. Puede parecer alarmante la idea de que cualquier información que "suba" el titular a Internet dejará un rastro permanente y será accesible para cualquier usuario, de manera que pueda almacenarla, copiarla, modificarla y volver a difundirla. Incluso si el titular mismo es quien proporciona esa información para su publicación, surge el cuestionamiento de si debe soportar que ésta tenga difusión perpetua. Esta cuestión se vuelve aún más relevante cuando existe información falsa o difamatoria sobre los titulares en noticias o blogs, sobre todo si lesiona la reputación del titular.

En especial, las redes sociales son *plataformas que permiten interactuar a los usuarios mediante el intercambio de diversos contenidos [como son] mensajes, archivos, imágenes, música y videos, entre otros.*[44] Hoy en día, las redes sociales son un medio cardinal de comunicación para el establecimiento de relaciones interpersonales entre sus usuarios. A través de ellas, los titulares de los datos personales publican información de ellos mismos, de manera que otros usuarios tengan acceso a ésta. Por el carácter universal de Internet, las redes sociales trascienden las fronteras territoriales y temporales, ya que permiten a cualquiera encontrar la información de otra persona, relativa a su pasado y su presente, en cuestión de segundos.[45]

En resumen, con carácter general, podemos decir que se han descrito dos dificultades ante las que se encuentra un usuario de Internet, con respecto del control sobre su información personal: 1) a quién se divulga la información, y 2) en qué momento se produce la divulgación.[46]

Con respecto al primer punto, existe el gran problema de controlar quién tiene acceso a la información de los titulares, pues si bien los usuarios pueden elegir en muchas ocasiones en un primer momento a quién le comparten sus datos (familiares, amigos, conocidos en un foro, miembros de un grupo de interés, etc.), la multitud de herramientas disponibles en el entorno electrónico dan la posibilidad a terceros desconocidos al individuo, de extraer dicha información de diferentes contextos y seleccionar qué información desea del individuo, y en consecuencia es sumamente complicado tener un control de quién conoce o tiene acceso a la información personal del usuario.

---

44 Lilibeth Álvarez Rodríguez, "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 <http://www.repositoriodigital.ipn.mx/bitstream/handle/123456789/3987/Memoria%204to%20Foro%20DHTIC%2015.pdf?sequence=1>.

45 Uno de los problemas que se han presentado en cuanto a las redes sociales es que varias de ellas se han mostrado renuentes a eliminar la información personal de los usuarios, incluso después de que éstos decidieron cancelar su cuenta. Por otro lado, hay casos en los que el administrador de la red social acepta dejar de publicar los datos personales del usuario que se sale del servicio, de manera que quedan inaccesibles, pero rechaza la idea de suprimirlos por completo.

46 Cécile de Terwangne, *op. cit*, p. 59.

La segunda dificultad se refiere al espacio temporal en el cual se divulga la información de la persona en la red, surgiendo así la cuestión de que si lo que una vez ha sido difundido debe permanecer disponible al público de manera indefinida. En ambas cuestiones, y especialmente en esta segunda, se materializa concretamente el tema que nos ocupa, esto es, el derecho al olvido.

El derecho al olvido y la cancelación

El concepto de 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. Las normas de protección de datos que plantean los antes mencionados derechos ARCO dan la posibilidad al titular de los datos de que su información contenida en bases de datos o, en términos generales, sometida a tratamiento, sea suprimida o cancelada.

En este tenor, 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,[47] contenidos en diversas legislaciones, entre ellas la mexicana.[48]

[47] Cuando se habla de derechos ARCO se está usando un acrónimo para referirse a los derechos de Acceso, Rectificación, Cancelación y Oposición.

[48] Normatividad para el Sector Privado:
El artículo 6, párrafo segundo, fracción II; el artículo 16, párrafo segundo; y el artículo 73 inciso XXIX-O de la Constitución Política de los Estados Unidos Mexicanos.
Ley Federal de Protección de Datos Personales en Posesión de Particulares (*DOF*, 5/07/2010).
Reglamento de la LFPDPPP (*DOF*, 21/12/2011).
Criterios Generales para la Instrumentación de Medidas Compensatorias sin la Autorización Expresa del Instituto Federal de Acceso a la Información y Protección (*DOF*, 18/04/2013)
Lineamientos para el Aviso de Privacidad (*DOF*, 17/01/2013)
Parámetros para el Correcto Desarrollo de los Esquemas de Autorregulación Vinculante (*DOF*, 16/07/2013).
Reglamento Interior del Instituto Federal de Acceso a la Información y Protección de Datos.
Recomendaciones en Materia de Seguridad de Datos Personales (*DOF*, 30/10/2013).

Normatividad para el Sector Público:
a) Administración Pública Federal.
El artículo 6, párrafo segundo, fracción II; el artículo 16, párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos.

Estos derechos permiten al titular de los datos exigir que se le informe qué datos tiene el responsable sobre él en sus bases de datos, oponerse a que sus datos sean tratados, solicitar la corrección de sus datos que obren en poder de otro y, finalmente, pedir que se cancelen (o, para efectos del tema que nos concierne, que se olviden) cuando resultare procedente; todo esto, con la necesidad de que su consentimiento informado haya sido obtenido previo al tratamiento de los mismos.[49]

De igual manera se produjo, a nivel europeo, en la Directiva de Protección de Datos,[50] y en la Propuesta del Reglamento General de Protección de Datos donde se habla en el artículo 17 de "Derecho al olvido y

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (*DOF*, 11/6/2002).
Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (*DOF*, 11/6/2003).
Lineamientos de Protección de Datos Personales (*DOF*, 3/9/2005).
Recomendaciones del IFAI de Seguridad para la Protección de Datos Personales.
Reglamento Interior del Instituto Federal de Acceso a la Información y Protección de Datos.
b) A nivel estatal tendremos que atender a lo dispuesto por la regulación de los organismos estatales de transparencia y acceso a la información pública. En concreto, para el Distrito Federal, la Ley de Protección de Datos Personales del Distrito Federal (*Gaceta Oficial del Distrito Federal*, 3 de octubre de 2008) y la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal (*Gaceta Oficial del Distrito Federal*, 28 de marzo de 2008).

49 "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 […] o ha expirado el plazo de conservación autorizado y no existe otro fundamento jurídico para el tratamiento de los datos; y
c) el interesado se opone al tratamiento de datos personales […]."

50 "[...] a los interesados les debe asistir el derecho a que se supriman y no se traten sus datos personales, en caso de que ya no sean necesarios para los fines para los que fueron recogidos o tratados de otro modo, de que los interesados hayan retirado su consentimiento para el tratamiento, de que se opongan al tratamiento de datos personales que les conciernan o de que el tratamiento de sus datos personales no se ajuste de otro modo a lo dispuesto en el presente Reglamento." Comisión Europea, Directiva de Protección de Datos, "Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos", Bruselas, 25 de enero de 2012.

a la supresión".[51] También la Agencia Española de Protección de Datos ha abordado asimismo el derecho al olvido desde la perspectiva de los derechos ARCO antes mencionados, asimilándose al derecho de cancelación.

En este sentido, no puede obviarse que lo anterior podría asimilarse al derecho del titular a que sus datos sean cancelados[52] (o, en su caso, a que el titular se oponga a dicho tratamiento), que sería sólo un ejercicio práctico para concretar dicho derecho, comprendería sin duda alguna el derecho al olvido, pues tal derecho provendría del bloqueo y posterior eliminación de sus datos personales. No obstante, la anterior afirmación tiene varias debilidades, entre las que, a simple vista, nos surgen las siguientes:

1. la cancelación (o la oposición) sólo procede ante el responsable y, en su caso, éste tendría que ver cómo comunicarla a los posibles terceros a los que haya transferido la información; y

2. la información puede haber entrado, como de hecho ocurre, en un sinfín de lugares y tratamientos, bajo diversos medios (por ejemplo, entorno electrónico, y en especial en Internet).

[51] Otro punto importante que se toca en el citado documento es la posibilidad de que los titulares revoquen su consentimiento al uso de sus datos personales, cuando éste hubiera sido concedido mientras el titular es menor de edad, ya que cuando no se tiene conciencia plena de los riesgos que pudiera implicar su tratamiento, se debe tener la opción de poder suprimir la circulación en Internet de dichos datos personales.

[52] En la propuesta del "Reglamento del Parlamento Europeo y del Consejo Relativo a la Protección de las Personas Físicas en lo que Respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos" (Comisión Europea. Reglamento del Parlamento Europeo y del Consejo Relativo a la Protección de las Personas Físicas en lo que Respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos. Bruselas, 25/1/2012, COM, 2012), se habla del derecho al olvido como derivado del derecho de cancelación de un dato personal, pero que también puede manifestarse en variantes de los derechos de rectificación y oposición. Así, el derecho al olvido está importantemente vinculado con la finalidad del uso del dato en cuestión ya que, una vez cumplido este objetivo, deja de ser legítimo su tratamiento. En este tenor, puede suceder que el dato deba ser borrado porque ha "expirado" su plazo de utilización (asemejándose al derecho de cancelación), o bien que el individuo, por su propia voluntad, objete este tratamiento y le haga saber de ello a quien los trata; en este sentido, se parece al derecho de oposición.

Así se ha visto concretado en el famoso "Caso Google" que veremos un poco más en detalle a continuación. Y, en este punto, coincidimos con Ricard cuando señala que:[53]

> **Por último, afirma que el derecho al olvido no encaja en los derechos de rectificación y cancelación en el caso concreto que se examina.** Sí lo haría en el de oposición, aunque no ampararía un interés meramente subjetivo del afectado. Las conclusiones confirman que las costuras de la directiva ya no pueden contener Internet, pero quienes crean que con ello se cierra un debate se equivocan de plano. **El olvido es una necesidad tan humana como el recuerdo.** En Internet la información banal, o la que da una falsa imagen sobre una persona, cercena su libertad. **Controlar nuestra información es también una garantía de libertad.**
>
> El tribunal puede que decida que los buscadores no están obligados a olvidar, pero deberá decirnos quién debe hacerlo y cómo debe hacerlo. Puede que el olvido pierda el caso, pero en el momento íntimo de quitarse la toga algún abogado murmurará… *Eppur si muove.*[54]

¿Derecho del titular u obligación del responsable del tratamiento?

A los responsables del tratamiento, como consecuencia directa del respeto al principio de finalidad,[55] se impone la obligación de cancelación (y posterior supresión, en su caso) de los datos, que lleva a la posibilidad del ejercicio del derecho al olvido, en los términos en que éste está planteado en relación con la normatividad de protección de datos personales.

---

53 El resaltado es mío.

54 Ricard Martínez, Las costuras de la privacidad. El caso Google *versus* AEPD evidencia graves carencias regulatorias de la UE en materia de protección de datos. Disponible en <http://sociedad.elpais.com/sociedad/2013/06/25/actualidad/1372191768_928841.html>.

55 Artículo 40 del Reglamento de la LFPDPPP, que establece que: "Los datos personales sólo podrán ser tratados para el cumplimiento de la finalidad o finalidades establecidas en el aviso de privacidad […]. 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."

No obstante lo anterior, ningún derecho puede ser absoluto. Y, por lo tanto, el llamado "derecho al olvido" tampoco puede serlo, y encuentra ciertos límites entre los que destacan aquellos que se refieren a que la conservación de los datos sea necesaria, por ejemplo: 1) para el ejercicio del derecho a la libertad de expresión;[56] 2) por motivos de interés público en el ámbito de la salud pública; 3) con fines de investigación histórica, estadística y científica; y 4) para el cumplimiento de una obligación legal de conservar los datos personales.[57]

En este punto, pudiera llegar a surgir un debate en cuanto a la efectividad que pudiera tener el derecho al olvido. Se podría argumentar, por un lado, que los responsables del tratamiento, refugiándose en las excepciones previstas, se excusaran de la obligación de cancelar los datos que obran en su poder y, por lo tanto, dejar de aplicar fácilmente el derecho al olvido. Por otro lado, se podría pensar que la aplicación rígida de este derecho conllevaría al desmantelamiento del contenido informático de Internet, como lo conocemos.[58]

---

56 "Así, igualmente señala Ricard, *op. cit.*:
Las conclusiones del abogado general en el caso Google *versus* AEPD evidencian graves carencias regulatorias de la UE en materia de protección de datos. El Tribunal de Justicia se situará frente al mismo abismo que el Supremo de Estados Unidos en el caso Reno *versus* ACLU, la necesidad de responderse qué es Internet y cómo abordar la regulación. La posición del abogado parte de algunas certezas. Establece que un buscador no encaja en la idea de prestador de servicios de la sociedad de la información —aunque sorprendentemente resuelva el caso aplicando criterios idénticos a los establecidos—, e indica que si cuenta con una empresa asociada que ofrece servicios vinculados rige el criterio de establecimiento.
Existe un ámbito de incertidumbre que hay que recorrer con prudencia. […] El abogado se enfrenta al vértigo de decidir si la actividad del buscador es legítima y tutelada por las libertades de expresión e información. Y considera que, al menos en un plano teórico, las libertades prevalecen frente a la privacidad."

57 Así lo ha dicho la Comisión Europea, *op. cit.*

58 El Supervisor Europeo de Protección de Datos (SEPD) ha planteado que se incremente la protección al derecho al olvido, o derecho a ser olvidado para garantizar que los datos personales de los titulares desaparezcan automáticamente de la red, después de un periodo determinado de tiempo, inclusive aunque los titulares interesados no tomaren medidas o no tuvieran conciencia de que sus datos personales habían sido almacenados. El criterio sobre el cual se basa este razonamiento es que un derecho al olvido más reforzado en el entorno digital que trajera consigo la eliminación automática de los datos personales de los titulares, permitiría que las personas tomaran control sobre el tratamiento que se le da a su información; si las personas ya no quisieran usar un servicio, o no quisieran que cierta información de ellas fuera pública, no deberían tener problemas para que dichos datos fueran eliminados, ya fuera mediante petición, o bien de manera maquinal, cuando haya transcurrido el

periodo de almacenamiento que el titular aceptó al proporcionar sus datos. Lo anterior equivaldría a aplicar a los datos personales una fecha de caducidad, después del cual su eliminación fuera instantánea, sin que fuera necesaria ningún tipo de ponderación o análisis caso por caso previo a la supresión. Si esto fuera así, la automaticidad de la supresión y, por lo tanto, de la prohibición del tratamiento ulterior, se traduciría en un derecho diseñado previamente para su cumplimiento, inclinándose la balanza a favor de los titulares de los datos personales, siendo éstos quienes tendrían el beneficio, sin siquiera tomar iniciativa o solicitarlo, de la protección de su información. Sin embargo, el problema no acaba cuando el administrador de la página donde, originalmente, el titular compartió sus datos, elimina la información del mismo, sino que es posible que, por el efecto multiplicador de Internet, esta información haya tenido una mayor difusión.

Véase Supervisor Europeo de Protección de Datos (SEPD), Un enfoque integral sobre protección de datos personales en la Unión Europea, Dictamen sobre la comunicación de la Comisión al Parlamento Europeo al Consejo, al Comité Económico y Social Europeo, y al Comité de las Regiones, Bruselas, 2011. Disponible en <http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_es.pdf>.

4. BREVE REFERENCIA A "EL CASO GOOGLE"

En relación con la información que puede existir de una persona en Internet, cabe preguntarse ante quién deben de ejercerse los derechos de oposición o cancelación: ante el administrador de la página web que originalmente capta y publica los datos, o frente al buscador que favorece su difusión. Esto es, ¿quién se toma como responsable del tratamiento?

Cuando un sitio web publica información, el buscador rastrea los datos presentes en la red y los organiza de manera que todo aquel que realice búsquedas de ciertas palabras clave, pueda acceder a ellos. Si llegara a presentarse el caso de que los datos publicados en el sitio web fueran ilegítimos o apócrifos, el titular debe tener la posibilidad de ejercer sus derechos de oposición o cancelación, tanto ante el responsable que edita y publica los datos, como ante el buscador; esto sigue el razonamiento de que el titular de los datos personales cuenta con el derecho fundamental de actuar frente a todo aquel que haya lacerado su esfera jurídica, como puede ser la lesión a su dignidad como persona.

Puede darse la situación en la cual el tratamiento inicial de los datos sea lícito, pero que la continuidad de su propagación y difusión lo convierta en ilegítimo. Asimismo, puede ocurrir que justamente el acceso facilitado por los enlaces que proporciona un buscador, aun en su carácter de prestador de servicios neutral, torne el tratamiento de los datos en desproporcionado y, por ende, se contraríe la normativa que regula su protección.

En abril de 2013 se iniciaron actuaciones previas de investigación al reconocido buscador "Google" en relación con su política de privacidad, por parte de la Agencia Española de Protección de Datos (AEPD).[59] El caso más conocido, el primero en llevar el derecho al olvido a los titulares de los periódicos, fue el de Mario Costeja, un ciudadano español que vio cómo en Google aparecía un anuncio de subasta por impago de un inmueble suyo y de su esposa. Eso fue hace 15 años, y él ya no es un moroso, ni está casado. En su pedido para que el buscador retirase el resultado que lo mencionaba, consiguió el apoyo de la AEPD, pero Google se negó a ello y recurrió al Tribunal de Justicia Europeo.

En ese momento comenzó un controversial debate en el cual se tocaban puntos como la competencia por razón de territorio de la AEPD sobre una empresa constituida en territorio estadounidense, así como en cuanto a si se tenía la facultad de requerir a Google para que excluyera de su buscador la información contenida en una página web administrada por un tercero.

Finalmente, la AEPD inició un procedimiento sancionador contra Google y Google Inc. dado que, previas investigaciones, se detectó la comisión de cinco infracciones a la ley española de protección de datos personales:

> 1. Google no informa claramente sobre el uso que va a hacer de los datos que recoge de los usuarios, por lo que éstos no pueden conocer de forma precisa qué fin justifica la recogida de sus datos personales ni la utilización que se hará de los mismos.

[59] Agencia Española de Protección de Datos, nota de prensa, 2 de abril de 2013. Disponible en <http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2013/notas_prensa/common/abril/130402_NP_Act_prev_Google.pdf>.

2. En el marco de la unificación de políticas de privacidad, es posible que Google pueda combinar la información personal de un servicio con la de otros y utilizarla para otras finalidades. La ausencia de información por parte de Google podría implicar que el tratamiento de datos que realiza fuera ilegítimo.

3. Google podría estar haciendo un tratamiento desproporcionado de los datos de sus usuarios, ya que en su política de privacidad advierte que podrá utilizar los datos recabados de forma ilimitada en todos sus servicios, presentes y futuros.

4. Google podría estar conservando los datos de sus usuarios por tiempo indeterminado o injustificado. La ley establece que los datos personales deben ser cancelados una vez que hayan dejado de ser necesarios o pertinentes para la finalidad para la que fueron recabados, y Google los mantiene más allá de estos plazos.

5. La AEPD considera que el ejercicio de derechos por parte de los usuarios podría verse obstaculizado e incluso impedido, ya que las herramientas que ofrece Google para ejercer los derechos de acceso, rectificación, cancelación y oposición se encuentran dispersas, no están disponibles para todos los usuarios, son incompletas y aparecen con denominaciones que no siempre se corresponden con la materia que se trata.[60]

Así, el criterio de fondo que siguió la AEPD es el plasmado en la normativa de protección de datos, en el cual se entiende que, sin perjuicio de su ponderación con otros derechos, la disponibilidad de los datos personales por parte de su titular y la autodeterminación informativa debe ser protegido, y aún con más vigor, cuando la publicación de estos datos lesione de manera directa su intimidad y dignidad como ser humano.

El Tribunal de Justicia Europeo, a la fecha de cierre de este artículo, no se había pronunciado aún sobre el particular, si bien las conclusiones del abogado general Niilo Jääskinen en junio de 2013, quisieron verse como presagio del "triunfo" de Google.

[60] Agencia Española de Protección de Datos, nota informativa, 20 de junio de 2013. Disponible en <http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2013/notas_prensa/common/junio/130620_NP_PS_GOOGLE.pdf>.

En la discusión también se debatía si con esta acción de suprimir o cancelar estos datos desde el buscador, se estaría violando el derecho del titular de la página web a la libertad de expresión, así como el derecho a la información de los usuarios de Internet.

Algunos argumentaron que la cancelación por parte de Google del acceso a dichas páginas web no sería violatorio de ningún derecho, ya que la cancelación de los datos vía el buscador no lesiona la libertad de expresión, pues no se está impidiendo con ello que la información sea publicada, sino que se está limitando, únicamente, su difusión indiscriminada.

En este sentido, una de las argumentaciones más fuertes de defensa del buscador fue que en realidad aquí es donde encuentra la diferencia entre el derecho de cancelación u oposición y la existencia de derecho alguno que se pueda esgrimir para exigir al buscador que retire o elimine enlaces.[61] Así, el abogado del Tribunal Europeo parece decir en sus conclusiones que una autoridad nacional de protección de datos "no puede requerir a un proveedor de servicios de motor de búsqueda en Internet que retire información de su índice".

Entre las cuestiones más relevantes que se espera defina el Tribunal Europeo en la futura sentencia están las siguientes:

1. *Si Google está sometido a la normatividad europea y española de protección de datos:* punto esencial, porque delimitaría "el ámbito de aplicación de la legislación"[62] y, por ende, si Google, o cualquier otra em-

[61] Aunque es cierto que Google sí lo hace si considera que ha contravenido sus políticas, o determinadas legislaciones, como la de propiedad intelectual.

[62] El concepto de soberanía nacional, tan asentado desde varios siglos atrás, se tambalea. Las fronteras, no sólo físicas, desaparecen. Los Estados se ven incapaces de mantener el control sobre las materias que antes les pertenecían casi sin excepciones. La territorialidad como determinante punto de conexión de aplicación de la ley y de la competencia de la jurisdicción ha dejado de ser eficiente en muchos casos. La idea de Estado en sí misma ha dado muchos cambios. Ya no puede, desde nuestro punto de vista, pretenderse continuar con ideas absolutistas de reinos totalmente independientes y difícilmente relacionados. En el entorno electrónico, especialmente las jurisdicciones competentes y las leyes aplicables se entrecruzan con facilidad, y es imprescindible contar con sistemas jurídicos y expertos que los apliquen y determinen cuáles son los puntos de conexión y los medios de resolución de dichos conflictos multijurisdiccionales. Si ya ni la idea de la soberanía nacional es intocable, sino que se tiene que pensar en la conjunción de otras circunstancias, habría que empezar

presa estadounidense, está sometida a la normatividad europea. En este sentido, las conclusiones del abogado general señalan que:

> Se lleva a cabo tratamiento de datos personales en el marco de las actividades de un "establecimiento" del responsable del tratamiento, en el sentido del artículo 4, apartado 1, letra a), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo del 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, cuando la empresa que provee el motor de búsqueda establece en un Estado miembro, con el fin de promover y vender espacios publicitarios en su motor de búsqueda, una oficina o una filial que orienta su actividad hacia los habitantes de dicho Estado.[63]

a pensar, desde nuestra perspectiva, en el posible cambio de las organizaciones gubernamentales y sociales de control de aplicación de la legalidad en el respeto a la privacidad hasta el momento, y su adaptación a las nuevas coordenadas.

[63] Cabe resaltar que la legislación mexicana aplicable a la iniciativa privada, de ámbito federal, establece, en el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares lo siguiente:
Ámbito objetivo de aplicación
Artículo 3. El presente Reglamento será de aplicación al tratamiento de datos personales que obren en soportes físicos o electrónicos, que hagan posible el acceso a los datos personales con arreglo a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.
No se aplicarán las disposiciones del presente Reglamento cuando para acceder a los datos personales, se requieran plazos o actividades desproporcionadas.
En términos del artículo 3, fracción V de la Ley, los datos personales podrán estar expresados en forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a una persona física identificada o persona física identificable.
Ámbito territorial de aplicación
Artículo 4. El presente Reglamento será de aplicación obligatoria a todo tratamiento cuando:
I. Sea efectuado en un establecimiento del responsable ubicado en territorio mexicano;
II. Sea efectuado por un encargado con independencia de su ubicación, a nombre de un responsable establecido en territorio mexicano;
III. El responsable no esté establecido en territorio mexicano pero le resulte aplicable la legislación mexicana, derivado de la celebración de un contrato o en términos del derecho internacional, y
IV. El responsable no esté establecido en territorio mexicano y utilice medios situados en dicho territorio, salvo que tales medios se utilicen únicamente con fines de tránsito que no impliquen un tratamiento. Para efectos de esta fracción, el responsable deberá proveer los medios que resulten necesarios para el efectivo cumplimiento de las obligaciones que impone la Ley, su Reglamento y demás disposiciones aplicables, derivado del tratamiento de datos personales. Para ello, podrá designar un

2. *Si Google es responsable de las eventuales lesiones que la difusión de información personal puede causar a los ciudadanos.* En este sentido, las conclusiones del Abogado General apuntan en la dirección de que Google sea un encargado del tratamiento, y no un responsable, porque no decide sobre la finalidad o uso de la información.

> Un proveedor de servicios de motor de búsqueda en Internet cuyo motor de búsqueda localiza información publicada o incluida en Internet por terceros, la indexa automáticamente, la almacena con carácter temporal y, por último, la pone a disposición de los usuarios de Internet, "trata" datos personales, en el sentido del artículo 2, letra b), de la Directiva 95/46 cuando esta información contiene datos personales.
>
> Sin embargo, no se puede considerar al proveedor de servicios "responsable del tratamiento" de tales datos personales, en el sentido del artículo 2, letra d), de la Directiva 95/46, a excepción de los contenidos del índice de su motor de búsqueda, siempre que el proveedor del servicio no indexe o archive datos personales en contra de las instrucciones o las peticiones del editor de la página web.

3. Y, finalmente, *si los ciudadanos pueden ejercitar sus derechos ante la Agencia Española de Protección de Datos y ante los tribunales españoles o han de acudir a los tribunales de EE.UU.*

---

representante o implementar el mecanismo que considere pertinente, siempre que a través del mismo se garantice que el responsable estará en posibilidades de cumplir de manera efectiva, en territorio mexicano, con las obligaciones que la normativa aplicable imponen a aquellas personas físicas o morales que tratan datos personales en México.
Cuando el responsable no se encuentre ubicado en territorio mexicano, pero el encargado lo esté, a este último le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III del presente Reglamento.
En el caso de personas físicas, el establecimiento se entenderá como el local en donde se encuentre el principal asiento de sus negocios o el que utilicen para el desempeño de sus actividades o su casa habitación.
Tratándose de personas morales, el establecimiento se entenderá como el local en donde se encuentre la administración principal del negocio; si se trata de personas morales residentes en el extranjero, el local en donde se encuentre la administración principal del negocio en territorio mexicano, o en su defecto el que designen, o cualquier instalación estable que permita el ejercicio efectivo o real de una actividad.

Por otro lado, una de las conclusiones más llamativas del Abogado General dice así:[64]

> Los derechos de cancelación y bloqueo de datos, establecidos en el artículo 12, letra b), y el derecho de oposición, establecido en el artículo 14, letra a), de la Directiva 95/46, no confieren al interesado el derecho a dirigirse a un proveedor de servicios de motor de búsqueda para impedir que se indexe información que le afecta personalmente, publicada legalmente en páginas web de terceros, invocando su deseo de que los usuarios de Internet no conozcan tal información si considera que le es perjudicial o desea que se condene al olvido.

64 "Todas estas cuestiones, que abordan además importantes aspectos de la protección de los derechos fundamentales, no han sido tratadas hasta ahora por el Tribunal de Justicia" recogiendo las cuestiones anteriormente mencionadas y sus conclusiones en tres apartados:
1. El ámbito territorial de aplicación de las normas de protección de datos de la Unión Europea. Es decir, si le es de aplicación o no a Google la normativa europea, se concluye que se considera de manera indiscutible a las filiales de Google ubicadas en la UE como "establecimiento" en el sentido del artículo 4, apartado 1, letra a), en un Estado miembro, con el fin de promover y vender espacios publicitarios en su motor de búsqueda, una oficina o una filial que orienta su actividad hacia los habitantes de dicho Estado.
2. La posición jurídica de un proveedor de servicios de motor de búsqueda en Internet a la luz de la Directiva, particularmente en términos de su ámbito de aplicación, es decir, la responsabilidad del buscador en el tratamiento de datos. No entiende que el buscador sea responsable del tratamiento pero sí que sus operaciones implican claramente un tratamiento de datos personales, señalando que "Un proveedor de servicios de motor de búsqueda en Internet no es el 'responsable del tratamiento' de datos personales en páginas web fuente de terceros".
3. La tercera cuestión referente al llamado derecho al olvido y a si los interesados pueden solicitar que algunos o todos los resultados de búsqueda que les conciernen no estén disponibles a través del motor de búsqueda, es decir, si se puede invocar al derecho generalizado al olvido sobre la base de la Directiva, se remarca que la Directiva no establece ningún "derecho al olvido" generalizado. Los derechos de oposición, supresión y cancelación de datos de la Directiva no se extienden a un derecho al olvido como el descrito en el auto de remisión, que recordemos señalaba que "el interesado pueda dirigirse frente a los buscadores para impedir la indexación de la información referida a su persona, publicada en páginas web de terceros, amparándose en su voluntad de que la misma no sea conocida por los internautas cuando considere que puede perjudicarle o desea que sea olvidada, aunque se trate de una información publicada lícitamente por terceros".
Estas conclusiones, aunque habrá que ver la sentencia definitiva, llegan en un momento en el que se está debatiendo el borrador del nuevo reglamento europeo [...].
Véase R. Valera, "Google 1-0 AEPD. Repetimos: 'Olvídense del olvido' ". Disponible en <http://www.eurovima.es/google-1-0-aepd-repetimos-olvidense-del-olvido>.

En este orden de cosas, como ya adelantábamos, hay quien se cuestiona[65] que en realidad cuando se habla de derecho al olvido no debería entroncarse bajo la protección de la normatividad de datos personales, sino más bien bajo la figura de otros derechos que, si bien pueden ser colindantes y a veces hasta confundibles, son independientes y autónomos. Así, se señala que deberían entrar en juego otras protecciones como las del derecho al honor y a la intimidad, por ejemplo.[66]

Asimismo, se han llegado a hacer estudios pronosticando que en el futuro se tendrá que "comprar" la privacidad en Internet, porque será muy costosa de mantener y, por lo tanto, se abrirá un nuevo mercado, y una nueva oportunidad de negocios para los que vean que pueden ganar por venderle a las personas su espacio de privacidad.[67]

---

65 Véase D. Maeztu, "Sobre las conclusiones del Abogado General en el caso contra Google". Disponible en <http://derechoynormas.blogspot.com.es/2013/06/sobre-las-conclusiones-del-abogado.html>.

66 No obstante lo anterior, parece que no tiene por qué ser incompatible. Es decir, derivado de un tratamiento de datos, que de hecho se da y que merece protección como tal, se pueden infringir otras normatividades. Y aunque parece que es bastante razonable que usualmente se quiere someter a este derecho al olvido a cuestiones desagradables o negativas, no podría ser imposible que se pretendiera que algo que normalmente se considere como positivo se desee igualmente que se olvide. Esto es, no debemos prejuzgar la intención del titular de los datos al ejercer sus derechos, puesto que ésta es independiente del ejercicio de los mismos.

67 "The World Wide Web has significantly reduced the costs of obtaining information about individuals, resulting in a widespread perception by consumers that their privacy is being eroded. The conventional wisdom among the technological cognoscenti seems to be that privacy will continue to erode, until it essentially disappears. The authors use a simple economic model to explore this conventional wisdom, under the assumption that there is no government intervention and privacy is left to free-market forces. They find support for the assertion that, under those conditions, the amount of privacy will decline over time and that privacy will be increasingly expensive to maintain. The authors conclude that a market for privacy will emerge, enabling customers to purchase a certain degree of privacy, no matter how easy it becomes for companies to obtain information, but the overall amount of privacy and privacy-based customer utility will continue to erode." VV.AA., The Customer Economics of Internet Privacy, Universidad de Maryland, *Journal of the Academy of Marketing Science*, octubre de 2002, núm. 30, pp. 455-464. Disponible en <http://jam.sagepub.com/content/30/4/455.abstract>.

5. ALGUNAS REFLEXIONES A MODO DE CONCLUSIÓN

El derecho a la protección de datos personales debe conseguir su categoría e independencia total. Desde nuestra perspectiva, se encuentra aún muy lejos de ser valorado en su magnitud. A pesar de ser un derecho elevado a la categoría de fundamental en muchos ordenamientos, aún no se puede decir que se encuentre en igualdad de condiciones, en la práctica al menos, respecto de los demás derechos fundamentales.

La privacidad es muy difícil de definir, y más a nivel internacional.[68] Sin embargo, el tratamiento leal y legal de la información personal es algo diferente. Parece que sobre lo que sí podemos llegar a un acuerdo es

[68] Méjan, parafraseando al juez Potter Stewart del Tribunal Supremo de Estados Unidos, que en 1964 declaró: "Quizá no se pueda definir la pornografía con toda claridad, pero la reconozco cuando la veo", señala lo siguiente: "En efecto, por ser un derecho fundamental del ser humano, todos tenemos una conciencia de a qué realidad nos referimos cuando hablamos de la esfera íntima y del derecho a la privacía, sin embargo, cuando se trata de dar una definición la empresa parece poco sencilla". L. M. Méjan, *El derecho a la intimidad y a la informática*, México, Porrúa, 1994, pp. 69 y ss.

sobre qué entendemos por licitud en el tratamiento de la información personal.[69]

Todo lo anterior incluso teniendo en cuenta que el derecho a la protección de datos de carácter personal es también un derecho fundamental autónomo e independiente en nuestro ordenamiento jurídico, y que se encuentra también así reconocido en muchas jurisdicciones internacionalmente.

Aun cuando los orígenes de las preocupaciones acerca de la privacidad pueden ser distintos social y culturalmente hablando, existe un mínimo entendimiento común acerca de lo que significa ser responsable. Parece que el punto clave reside en sustentar claramente la responsabilidad por el manejo de los datos, y máxime a nivel internacional. Así, uno de los puntos más sensibles es precisamente cómo controlar que quienes tratan datos responden del buen manejo de los mismos, de manera que el individuo pueda reclamar en caso de controversia y no se vea lastimado en sus derechos.

Podría parecer que lo del control y el derecho a la autodeterminación informativa total, si no se establecen los mecanismos y las alianzas de protección necesarios, es una quimera o una utopía.

Parece, sin ir más lejos, que precisamente el haz de facultades del titular para controlar[70] su información personal no es del todo comprehensivo; parece que, una vez que la información ha sido tratada y dispersada, especialmente por medios electrónicos, es difícil que desaparezca del todo; parece que es relativamente sencillo encontrar rastros de información personal que no deberían seguir siendo accesibles o, al menos, no tan fácilmente accesibles; y parece que el titular debe ser consciente de que una vez que su información ha sido tratada y dispersada, se vuelve muy difícil que sea olvidada, porque en realidad olvido equivale en cierta medida a "limpieza", a "eliminación".

[69] J. Bennet, Colin, "An Internacional Standard for Privacy Protection: Objections to the Objections", Workshop on *Freedom and Privacy by Design*, 2000.

[70] Se busca definir de manera clara qué es aquello que los responsables pueden hacer con ellos y, al mismo tiempo, se busca "que los titulares de los datos mantengan control de los mismos al poder definir, por medio de mecanismos específicos, si comparten sus datos personales y con qué fines lo hacen". Exposición Motivos LFPDPPP.

No es tanto que se olvide, sino que se destruya, que se elimine, porque el olvido implicaría una actuación activa por parte de un individuo pensante. En realidad se está buscando que se elimine una caracterización o una adjetivación determinada, que no debe existir ya, por las circunstancias concretas. Si en realidad se tratara de olvidar podríamos aún tener la esperanza de que no se pudiera retener la información por demasiado tiempo, o en condiciones óptimas, pues nadie sería capaz de recordarla durante todo el tiempo.

Y es precisamente en este punto donde este derecho independiente y autónomo encuentra su justificación. Lo que se persigue proteger es el tratamiento de la información personal *per se*. No es necesario que entren en juego otros condicionantes o que existan vulneraciones a otros derechos ya asentados o colindantes. Es por ese tratamiento que se genera una información de la persona sobre la que ésta demanda dicho derecho al olvido.

En realidad lo que se busca es que los tratamientos de una información determinada desaparezcan. El problema es que los tratamientos son innumerables –por no decir infinitos– y de una dispersión incontrolable; es decir, no sabemos ni dónde ni quién los realiza y, por ende, no podemos encontrar, a simple vista, un mecanismo legal y universal que garantice que se cumple con la eliminación, o con el "olvido". Y el problema también es que no son inocuos. Que la persistencia de dichos tratamientos, de dichas evaluaciones asociadas a las personas, conllevan la toma de decisiones sobre las mismas, de distinta envergadura. Es más, podríamos hasta pensar en la toma de decisiones sobre terceros que vengan como consecuencia del tratamiento de datos de un individuo.

Es por esto que el derecho al olvido, como una manifestación peculiar del derecho independiente y autónomo a la protección de datos personales y a la autodeterminación informativa, deviene en una problemática específica y particularmente preocupante para las legislaciones y políticas públicas actuales.

En definitiva, parece que hay que virar, como en muchas otras cuestiones fundamentales, a los básicos de la teoría y, en concreto, a la autodeterminación informativa, como señalaba el magistrado Benda.

Referencias bibliográficas

Adinolfi, Giulio, "Autodeterminación informativa. Consideraciones acerca de un principio general y un derecho fundamental", *Cuestiones Constitucionales*, núm. 17, México, Instituto de Investigaciones Jurídicas-UNAM, 2007. Disponible en <http://www.ejournal.unam.mx/cuc/cconst17/CUC000001701.pdf>. Consultado en diciembre de 2013.

Agencia Española de Protección de Datos, nota de prensa, 2 de abril de 2013. Disponible en <http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2013/notas_prensa/common/abril/130402_NP_Act_prev_Google.pdf>.

Agencia Española de Protección de Datos, nota informativa, junio de 2013. Disponible en <http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2013/notas_prensa/common/junio/130620_NP_PS_GOOGLE.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 <http://www.repositoriodigital.ipn.mx/bitstream/handle/123456789/3987/Memoria%204to%20Foro%20DHTIC%2015.pdf?sequence=1>.

Artz Colunga, S., "México, el derecho al olvido en Internet: ejercicio de los derechos de cancelación y oposición, derecho al olvido *versus* derecho a la libertad de información, su incidencia en los medios de comunicación", XI Encuentro Iberoamericano de Protección de Datos, Cartagena, Instituto Federal de Acceso a la Información y Protección de Datos, octubre de 2013. Disponible en <http://www.redipd.org/actividades/encuentros/XI/common/Ponencias/P1_IFAI_MEXICO.pdf>.

Bayens, S., "The search and seizure of computers: are we sacrificing personal privacy for the advancement of technology?", *Drake Law Review*, 2000.

Bennet, Colin J., An Internacional Standard for Privacy Protection: Objections to the Objections, Workshop on "Freedom and Privacy by Design", 2000.

Corte Suprema de Justicia-División de Investigación, Legislación y Publicaciones, *Protección de Datos Personales*, Paraguay, 2010.

Davara F. de Marcos, I., Hacia la estandarización de la protección de datos personales. Propuesta sobre una *tercera vía o tertium genus* internacional, Madrid, Wolters Kluwer, 2011.

Davara Rodríguez, M. A., "La teoría del consentimiento en la protección de datos personales: su implicación con la relación contractual", Encuentros sobre Informática y Derecho, Madrid, Universidad Pontificia Comillas, 1996, pp. 75 y ss.

De Terwangne, Cécile, "Privacidad en Internet y el derecho a ser olvidado/derecho al olvido", *Derecho y Política*, núm. 13, Cataluña, Universitat Oberta de Catalunya, 2012, pp. 53-66.

Documento de trabajo sobre servicios de autenticación en línea, WP 68, adoptado por el Grupo de Trabajo el artículo 29 el 29 de enero de 2003. Disponible en <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp68_es.pdf>.

Freixes Sanjuán, T., "Obtención y utilización de datos personales automatizados", Jornadas sobre el Derecho Español de la Protección de Datos Personales, Madrid, Agencia de Protección de Datos, 28, 29 y 30 de octubre de 1996, pp. 159-162.

Fried, C., "Privacy", *Yale Law Journal*, núm. 475, 1968.

García González, Aristeo, "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-UNAM.

Gómez-Robledo, Antonio y Lina Ornelas Núñez, *Protección de datos personales en México: el caso del Poder Ejecutivo Federal*, México, Instituto de Investigaciones Jurídicas, 2006, p. 14.

Koops, Bert-Jaap, "Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' ", *SSRN Scholarly Paper*, NY Social Science Research Network. Disponible en <http://papers.ssrn.com/abstract=1986719>.

Lucas Durán, M., *El acceso a los datos en poder de la Administración Tributaria*, Pamplona, Aranzadi, 1997, pp. 265 y ss.

Maeztu, D., *Sobre las conclusiones del Abogado General en el caso contra Google*. Disponible en <http://derechoynormas.blogspot.com.es/2013/06/sobre-las-conclusiones-del-abogado.html>.

Martínez, R., *Las costuras de la privacidad. El caso Google* versus *AEPD evidencia graves carencias regulatorias de la UE en materia de protección de datos*. Disponible en <http://sociedad.elpais.com/sociedad/2013/06/25/actualidad/1372191768_928841.html>.

Méjan, L. M., *El derecho a la intimidad y a la informática*, México, Porrúa, 1994, pp. 69 y ss.

O´Connor, P., *Online Consumer Privacy*, Institut de Management Hotelier International at ESSEC Business School. Disponible en <http://cqx.sagepub.com/content/48/2/183.abstract>.

Oliver Lalana, A. D., *Código invisible y pequeño gran hermano. Nuevas condiciones de posibilidad del derecho a la protección de datos*. Disponible en <http://www.unizar.es/fyd/prodatos/pdf/oliver_madrid02.pdf>. Consultado en diciembre de 2013.

Posner, R., "The Economics of Privacy", *The American Economic Review*, vol. 71, núm. 2, mayo de 1981.

Resolución R (73) 22 relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado. Adoptada el 26 de septiembre de 1973, en la 224ª reunión del Consejo de Ministros.

Rodotà, S., "Democracia y protección de datos", *Cuadernos de Derecho Público*, núms. 19-20, mayo-diciembre de 2003, Madrid, INAP.

Rodotà, Stefano, *Democracia y protección de datos*. Disponible en <https://www.agpd.es/portalweb/canaldocumentacion/conferencias/common/pdfs/DemocraciaMadrid_mayo_05.pdf>.

_____, *Tecnología y derechos fundamentales,* Agència Catalana de Protecció de Dades, 2004. Disponible en <www.apd.cat>. Consultado en noviembre de 2013.

_____, *Tecnología y derechos fundamentales,* Agència Catalana de Protecció de Dades, 2004. Disponible en <www.apd.cat>. Consultado en diciembre de 2013.

Supervisor Europeo de Protección de Datos (SEPD), "Un enfoque integral sobre protección de datos personales en la Unión Europea", Dictamen sobre la comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Bruselas, 2011. Disponible en <http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_es.pdf>.

Valera, R., "Google 1-0 AEPD. Repetimos: 'Olvídense del olvido' ". Disponible en <http://www.eurovima.es/google-1-0-aepd-repetimos-olvidense-del-olvido>.

VV. AA., "Facebook quiere tu cara", *El País*. Disponible en <http://tecnologia.elpais.com/tecnologia/2013/08/30/actualidad/1377858949_296393.html>.

VV. AA., "The Customer Economics of Internet Privacy", *Journal of the Academy of Marketing Science*, núm. 30, octubre de 2002, pp. 455-464, Universidad de Maryland. Disponible en <http://jam.sagepub.com/content/30/4/455.abstract>.

VV. AA., "The right to privacy", *Harvard Law Review*, vol. IV, núm. 5, 15 de diciembre de 1890. Disponible con modificaciones en <http://www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html>. Consultado en julio de 2009.

Colección Ensayos para la Transparencia de la Ciudad de México

2007

01 **La transparencia y los sujetos no obligados de la rendición de cuentas.** Alberto Aziz Nassif

02 **Archivos gubernamentales: un dilema de la transparencia**. José Antonio Ramírez Deleón

03 **Transparencia y control ciudadano: comparativo de grandes ciudades**. Irma Eréndira Sandoval

2008

04 **¿Por qué transparentar las actividades de cabildeo? El caso del Presupuesto de Egresos de la Ciudad de México.** Alejandra Betanzo de la Rosa

05 **Transparencia y procuración de justicia en el Distrito Federal.** Catalina Pérez Correa González y Alejandro Madrazo Lajous

06 **Acceso a la información y transparencia política en el Distrito Federal.** Issa Luna Pla

07 **El derecho de acceso a la información pública: una herramienta para el ejercicio de los derechos fundamentales.** Paulina Gutiérrez Jiménez

08 **Transparencia y medios de comunicación.** Marco A. Morales Barba

2009

09 **Hacia una nueva arquitectura de la información pública. Información pública y política social en el Distrito Federal.** Eduardo Bohórquez

10 **Legislar en la oscuridad. La rendición de cuentas en la Asamblea Legislativa del Distrito Federal.** Khemvirg Puente

11 **Construir obra pública, edificar ciudadanía.** Miguel Ángel Pulido Jiménez

12 **Las delegaciones y los servicios públicos: una mirada sobre lo que deberíamos saber.** Darío Ramírez Salazar y Gabriela Morales Martínez

2010

13 **Sindicatos y transparencia en la Ciudad de México.** Arturo Alcalde Justiniani

14 **Transparencia 2.0 Nuevos medios digitales y acceso a la información pública en el Distrito Federal, oportunidad para el empoderamiento ciudadano.** Octavio Islas y Mauricio Huitrón

15 **Transparencia y desarrollo urbano en el Distrito Federal.** Emilio de Jesús Saldaña Hernández

2011

16 **La libertad de expresión y el derecho a la información en México: un desafío de nuestros tiempos.** Emilio Álvarez Icaza Longoria

17 **Transparencia y procesos electorales.** Lorenzo Córdova Vianello

18 **Acceso a la información, periodismo y redes sociales, escenarios futuros.** Jenaro Villamil

19 **Transparencia, acceso a la información y participación social en la ciudad de México.** Ricardo Raphael

2012

20 **Acceso a la información y protección de datos personales en el ámbito de la justicia.** Miguel Carbonell

21 **Transparencia y gobierno abierto en el D.F., ¿Para qué?.** Haydeé Pérez Garrido

Instituto de Acceso a la Información Pública
y Protección de Datos Personales del Distrito Federal

Ensayo 23 El derecho al olvido en relación con el derecho a la protección de datos personales.

Abril 2014

xxxxxxxx xxxxxx xxxxxx
xxxxx xxxxxxxxxx xxxxxxx xxx
xxxxxxxx xxxxxxx xxxxxxxxxx xxxxxxxx
xxxxxxxx xxxxxxx xxxxx

El tiraje fue de 1,000 ejemplares impresos en papel bond de 90 grs. Y forros en couché de 250 grs. Fuentes tipográficas: (Calibri Regular, Calibri Bold, Calibri italic, Myriad ProRegular y Myriad ProSemibold)
Cuidado de la edición: Dirección de Capacitación y Cultura de la Transparencia