EL DERECHO AL OLVIDO Y A LA PROTECCIÓN DE DATOS PERSONALES EN URUGUAY

*PABLO SCHIAVI**

Resumen

Los desarrollos doctrinarios y jurisprudenciales sobre el "derecho al olvido" se encuadran en los permanentes desafíos que la actual era digital con una sociedad hiperconectada e hiperinformada le impone al Derecho y a las distintas regulaciones.

El "derecho al olvido" deber ser analizado en el contexto de la protección de datos personales en internet y en las redes sociales con especial acento en el necesario equilibrio entre modernización y garantía del derecho del ciudadano a preservar el control sobre sus datos personales y la aplicación de las nuevas tecnologías de la información.

El "derecho al olvido", en tanto proyección de los derechos de supresión y oposición de los datos, no deber ser interpretado como sinónimo de "borrar" o de "ocultar" determinada información referida a una persona, aunque su consagración apunta al derecho del titular del dato a que su información personal no permanezca de manera indefinida y permanente, y de fácil acceso, en las redes sociales e internet.

Debemos ser muy cuidadosos en señalar que el derecho al olvido no puede interpretarse como contrario a la transparencia aunque debemos trabajar en soluciones y fórmulas que nos permitan respetar el derecho de una persona a que sus datos no permanezcan en forma indefinida en internet vinculados a hechos o acontecimientos de su vida negativos e incluso positivos y que suponen una condena social permanente en las redes sociales e internet.

* Doctor en Derecho y Ciencias Sociales por la Facultad de Derecho de la Universidad de la República Oriental del Uruguay. Máster en Derecho Administrativo Económico por la Universidad de Montevideo (UM). Profesor Adjunto Grado 3 (I) de Derecho Público II y III (Derecho Administrativo y Derecho Procesal Constitucional, respectivamente) en la Facultad de Derecho de la Universidad de la República. Profesor Ayudante Grado 1 (I) de Derecho Público I Y III (Derecho Constitucional y Derecho Procesal Constitucional, respectivamente) en la Facultad de Derecho de la Universidad de la República. Profesor de "Información Pública y Datos Personales"; de "Protección de Datos Personales en Salud "E Salud"; y de "Protección de Datos Personales Tributarios y Bancarios" en el Máster de Derecho Administrativo Económico (MDAE) en la Facultad de Derecho en la Universidad de Montevideo. Profesor de "Datos Personales" en el Máster en Dirección de Empresas de Salud (MDES) en la Escuela de Negocios de la Universidad de Montevideo (IEEM). Profesor de "Derecho de la Información" y de "Investigación y Documentación" en la Facultad de Comunicación de la Universidad de Montevideo. Profesor Asistente de "Procedimientos Administrativos" en el Máster de Derecho Administrativo Económico (MDAE) en la Universidad de Montevideo. Diplomado en Desarrollo y Financiamiento de Infraestructuras por la Universidad Politécnica de Madrid. Certificado en Prevención del Lavado de Dinero y Financiamiento del Terrorismo por el Isede y la Facultad de Derecho de la Universidad Católica del Uruguay "Dámaso Antonio Larrañaga". Miembro del Instituto de Derecho Administrativo de la Facultad de Derecho de la Universidad de la República. Miembro Titular de la Asociación Derecho Público del Mercosur. Coordinador de Estudios de Derecho Administrativo de la Editorial La Ley Uruguay - Thomson Reuters. Coordinador Nacional por Uruguay de la Red Iberoamericana de Contratación Pública (REDICOP). Miembro de la Red Internacional de Bienes Públicos (RIBP). Asesor Director en la Oficina de Planeamiento y Presupuesto (OPP), Presidencia de la República, Uruguay. Consultor y Asesor Corporativo Data Privacy. Autor de libros y artículos sobre temas de su especialidad. **https://www.linkedin.com/in/pabloschiavi/**

Abstract

The doctrinal and jurisprudential developments on the "right to oblivion" are framed in the permanent challenges that the current digital era with a hyper-connected and hyper-formed society imposes on the law and the different regulations.

The "right to oblivion" should be analyzed in the context of the protection of personal data on the Internet and social networks with special emphasis on the necessary balance between modernization and guarantee of the right of citizens to preserve control over their personal data and the Application of new information technologies.

The right to oblivion, as a projection of the rights of suppression and opposition of the data, should not be interpreted as synonymous with "erasing" or "hiding" certain information related to a person, although its consecration points to the right of the Holder of the data so that your personal information does not remain indefinitely and permanently, and easily accessible, in social networks and the internet.

We must be very careful to point out that the right to forget can not be interpreted as contrary to transparency, although we must work on solutions and formulas that allow us to respect a person's right to have their data not remain indefinitely on the Internet linked to facts or Negative and even positive events of their life and that represent a permanent social condemnation in social networks and the internet.

We understand that the real problem that witnessing today is not that there is secret or confidential information, - always existed type- information to the extent it is logical that certain information is not publicly available; but lies mainly in the lack of foundation and motivation of such limits to public information, on the understanding that it is not enough to say we can not access certain information because it is secret or confidential, we have to say because it is secret, or confidential.

Palabras claves: Internet. Redes sociales. Derechos. Datos Personales. Derecho al Olvido. Regulación.

Keywords: Internet. Social networks. Rights. Personal information. Right to forget. Regulation

I) LA PROTECCIÓN DE LOS DATOS PERSONALES EN LAS REDES SOCIALES

El reconocimiento a las dimensiones internacionales de la protección de los datos personales en la era digital, la importancia de los desafíos a la protección de los datos personales de los más jóvenes en internet y la urgencia de elaborar marcos normativos que puedan orientar a los Estados y a las empresas en sus esfuerzos para responder a esos desafíos[1], es, hoy en día, objeto de múltiples debates, conferencias y seminarios en todo el mundo.

1 BERNIER, Chantal – *El Memorándum de Montevideo: un marco de referencia para la protección de los datos personales de los jóvenes en Internet en la región Iberoamericana;* Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes; Memorándum de Montevideo; Carlos G. Gregorio – Lina Ornelas, Compiladores; IIJusticia – Instituto de Investigación para la Justicia, IFAI –Instituto Federal de Acceso a la Información y Protección de Datos; México, 2011, p. 16.

Es un lugar común afirmar que hoy en día vivimos la era digital, en donde gracias al avance de las tecnologías de la información, el Internet se ha convertido en un medio de comunicación plenamente socorrido, al punto que forma parte ya del desarrollo de nuestras actividades cotidianas. Asimismo las redes sociales en Internet han devenido herramientas de comunicación multifuncionales, que nos permiten entrar en contacto con personas de todo el mundo y compartir experiencias de muy variado tipo en esta nueva aldea global: permiten obtener, almacenar y transmitir un sin número de datos, documentos, fotografías, videos, música, -entre otros-, y el acceso a éstos es tan sencillo con simplemente un clic[2].

La irrupción de las nuevas tecnologías de marcado carácter social – *blogs*, *wikis*, *podcast*, redes sociales, etc.- ha determinado un alto grado de interconectividad entre los usuarios de Internet lo que, dicho sea de paso, les permite intercambiar todo tipo de opiniones sobre diferentes productos y experiencias con otras personas[3].

La sociedad de la información y la comunicación necesariamente debe tener como su centro de atención a las personas; esto es, la aproximación a la sociedad de la información y la comunicación desde una perspectiva basada en "derechos" implica colocar la dignidad humana, el desarrollo humano y los derechos como ciudadanos globales y digitales por encima de las consideraciones tecnológicas o la relación comercial productor-consumidor. Más aún, implica educar en la ciberciudadanía y proteger en este ámbito a las niñas, niños y adolescentes para garantizar una navegación segura[4].

En la era electrónica existe una considerable preocupación por el impacto de internet en el derecho fundamental a la protección de datos personales[5].

Dada la gran cantidad de datos personales que los usuarios publican en sus perfiles, estos se convierten en auténticas "identidades digitales" que facilitan un rápido conocimiento de datos de contacto, preferencias y hábitos del usuario. El consentimiento que presta el usuario es válido en el momento en que decide aceptar, la política de privacidad y condiciones de uso de la plataforma que constan en el formulario de registro[6].

Quizás y más allá de consejos esenciales para proteger nuestros datos en Internet, a los cuales hemos hecho referencia, debemos tener presente que todo lo que se publica en *Facebook* como en *Twitter*, es en principio público, esto es, cualquier persona, en cualquier

2 PESCHARD MARISCAL, Jacqueline – *Protección de las niñas, niños y adolescentes en el ámbito digital: responsabilidad democrática de las instituciones de gobierno y de las agencias de protección de datos;* Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes; Memorándum de Montevideo; Carlos G. Gregorio – Lina Ornelas, Compiladores; II Justicia – Instituto de Investigación para la Justicia, IFAI –Instituto Federal de Acceso a la Información y Protección de Datos; México, 2011, p. 22.

3 LÓPEZ JIMÉNEZ, David – *La protección de datos de carácter personal en el ámbito de las redes sociales electrónicas: el valor de la autorregulación;* Universidad de Alcalá de Henares. Servicio de Publicaciones, 2009.

4 PESCHARD MARISCAL, Jacqueline – *Protección de las niñas, niños y adolescentes en el ámbito digital: responsabilidad democrática de las instituciones de gobierno y de las agencias de protección de datos;* Ob. Cit; pág. 22 y siguientes.

5 SCHIAVI, Pablo. – "*La protección de los datos personales en las redes sociales*"; en Estudios de Derecho Administrativo; 2013, Nº 7; Director Augusto Durán Martínez; Coordinador Pablo Schiavi; LA LEY URUGUAY; Montevideo, 2013; pág. 215 y siguientes.

6 SCHIAVI, Pablo. – "*La protección de los datos personales en las redes sociales*"; en Estudios de Derecho Administrativo; 2013, Nº 7; Ob. Cit.; pág. 215 y siguientes.

lugar del mundo en que se encuentre podrá acceder a lo publicado por ser parte de la famosa "comunidad *Facebook*" o de la "comunidad *Twitter*"; salvo que en el momento en que tiene lugar su registración en la red, se configuren restricciones de privacidad, permitiendo acceder a los contenidos, ya sean fotos, textos, videos, solamente a los llamados "amigos" -que se supone serian personas con las cuales nos vinculamos en la red social- en el caso de *Facebook*; o solamente en el caso de los llamados "seguidores" en el caso de *Twitter*[7].

II) EL DERECHO AL OLVIDO EN TIEMPOS DE "GOOGLE"

Hace un par de años – no muchos- para encontrar una noticia relacionada a un determinado hecho de cualquier tipo, a una determinada situación o a una determinada persona, siempre y cuando la noticia se hubiese publicado en algún medio de prensa escrito, teníamos que ir al "histórico" de Diarios y Revistas de la Biblioteca Nacional o en su defecto, averiguar qué día de la semana se había publicado la noticia en la versión impresa de un periódico para ir a comprar ese ejemplar a su Sede Central donde muy amablemente un empleado nos preguntaba cual era el día en que se había publicado el Diario para poder acceder a él.

Nadie en ese momento se imaginaba que hoy iba a existir "Google".

Hoy todo cambió.

Para siempre.

La viralización de información y de contenidos que se nutre de datos personales de todo tipo se ha potenciado sin límites en el día de hoy con la existencia de los llamados *"buscadores"* o *"motores de búsqueda"* en internet, como por ejemplo *"Google"* en el cual simplemente alcanza con poner nuestro nombre y se dispara una enorme cantidad de noticias y de imágenes que refieren a nuestra persona, en una especie de biografía pública, de fácil acceso, al alcance de todos y sin ninguna restricción.

Hoy en día, toda la información referida a personas, empresas, historial y todo lo que se nos pueda ocurrir está al alcance de todos de "manera permanente", en forma gratuita y disponible las 24 horas del día los 365 días del año.

De ahí que se ha impuesto la práctica llamada *"google tu nombre"* y los invito a hacerlo para ver toda información de cada uno que hoy en día está al alcance de cualquiera en internet.

Nos preguntamos ¿qué podemos hacer con todo esto? ¿Qué pueden hacer los titulares de los datos personales, las personas ante esta manipulación y accesibilidad irrestricta a información que concierne a cada uno, y que basta simplemente con que se haya publicado en alguna página web o en las distintas redes sociales.

Google es una compañía estadounidense fundada en septiembre de 1998 cuyo produc-

7 SCHIAVI, Pablo. – *"La protección de los datos personales en las redes sociales"*; en Estudios de Derecho Administrativo; 2013, Nº 7; Ob. Cit.; pág. 215 y siguientes.

to principal es un motor de búsqueda creado por Larry Page y Sergey Brin. El término suele utilizarse como sinónimo de este buscador, el más usado en el mundo. Para realizar la búsqueda, existen dos grandes opciones: elegir *"Buscar con Google"* para que el buscador presente todos los resultados que encuentre en Internet o seleccionar *"Voy a tener suerte"*, que lleva al internauta al primer resultado hallado[8].

De ahí la frase de *"googlea tu nombre"* para ver que arroja el buscador más potente del mundo sobre nuestro historial personal y profesional, ya que alcanza simplemente con que nuestro nombre figure en el sitio web de cualquier medio de prensa, así como de una Universidad, de una empresa pública, de una empresa privada, a modo de ejemplo, para que en apenas un segundo *Google* ponga a disposición toda esa información al mundo sin siquiera avisarnos o pedirnos nuestro consentimiento.

Y es en este mundo hiperconectado e hiperinformado donde surge la necesidad y donde se encuentra el fundamento del llamado "derecho al olvido".

Google no nos avisa quién nos buscó en la red, quien "googleo" nuestro nombre y tampoco nos pidió permiso para darle, para facilitarle toda la información relacionada a nosotros y que nos identifica en un par de segundos.

Esto tiene un alto impacto en el mundo de las relaciones laborales, y sobretodo en la búsqueda de empleos, donde puede afirmarse que ninguna empresa contrata personal sin realizar previamente un "perfil público" del candidato con toda la información que relacionada a él se encuentra en internet y en las redes sociales.

Y es en este mundo hiperconectado e hiperinformado – lo que no significa necesariamente "bien informado"- donde surge la necesidad y donde se encuentra el fundamento del llamado derecho al olvido.

Es un derecho nuevo, poco desarrollado y no recogido aún en forma específica en la legislación uruguaya.

Es un paso más en la reciente regulación del derecho a la protección de datos personales con los alcances que veremos a continuación.

Cuando hablamos de derecho al olvido nos referimos al derecho de toda persona, de todo titular de datos a que determinada información personal que la hace identificable (datos personales, datos sensibles, datos laborales, datos financieros datos de salud, entre otros) no permanezca en forma permanente y de manera indefinida en internet las 24 hs del día y los 365 días del año; información a la cual se accede fácilmente y sin ninguna restricción a través de buscadores o motores de búsqueda en plataformas digitales, sin mediar consentimiento ni notificación alguna al titular de los datos**.**

A tales efectos entendemos que podría configurarse el derecho al olvido cuando se trata de informaciones que lucen en uno o en varios sitios web o en bases de datos que refieren a datos personales o se relacionan con situaciones personales referidas a hechos reales de la vida de una persona, no necesariamente positivos, que por distintos motivos tomaron estado público y que fueron recogidas en portales por medios de comunicación o en cualquier otra plataforma digital con la nota esencial de que perduran de manera

8 http://definicion.de/google/

indefinida en el tiempo en internet, incluso una vez agotada la situación que dio origen a la noticia.

El derecho al olvido no implicaría en los hechos "borrar esa información" ni "tapar o ocultar esa información" sino que supone el derecho de la persona a no permanecer expuesta o vinculada de por vida a estos hechos en las redes sociales e internet, como si fuera una extensión, en el mundo de las redes sociales, de la pena sufrida – en caso de delitos a modo de ejemplo -ante los tribunales competentes de un determinado país.

¿Como sociedad somos conscientes de estos extremos?

¿Hemos discutido si queremos que información que nos pertenece permanezca de manera indefinida y permanente en las redes?

Esto es, una persona que fue condenada por determinado delito, que cumplió con la pena que se le aplicó, tiene derecho a que su nombre no permanezca asociado de por vida a tales hechos en las redes sociales y webs por la potencia de los buscadores o motores de búsqueda.

Ejemplos pueden ser muchos y muy variados y de toda índole. Por ejemplo personas vinculadas a tráficos de drogas; contrabando; lavado de activos entre otros delitos.

Pero también hay otro tipo de situaciones vinculadas a la vida laboral. Por ejemplo una persona que trabajo durante muchos años en un determinada empresa y su nombre sigue vinculado a dicha empresa aún luego de su egreso cualquiera sean las razones.

También son comunes en el ámbito laboral, personas que en búsqueda de nuevos empleos, se presentan a concursos para determinados puestos de trabajo y los resultados de las instancias de evaluación son publicados en sitios web con lo cual otras personas al "googlear" su nombre –por ejemplo sus jefes actuales- y van a tomar conocimiento que se presentaron para tal o cual empleo – distintos del empleo actual -

En Latinoamérica hay varios ejemplos en tal sentido, algunos con soluciones favorables a lo solicitado en relación al derecho al olvido y otros no.

Entre ellos está el caso de un ciudadano argentino que fue acusado por tráfico de drogas, lo que generó la publicación de una nota periodística. Años después, el hombre encontró el artículo e invocó el derecho al olvido para que fuera eliminado de internet, para lo cual inició una acción judicial tanto contra el diario como contra Google. La resolución del caso determinó que la noticia era real al momento de su publicación y se expresó en los términos correctos (aunque no hubo una sentencia), por lo cual su eliminación no era pertinente[9].

En Brasil se dio un caso similar, pero, en vez de tratarse de un sitio de noticias, el demandante cuestionó la publicación en un sitio estatal de una decisión judicial, a lo que se respondió que eliminar documentos de tal entidad atentaría contra las prácticas de transparencia del Estado. Al respecto, se explicó que existen estándares internacionales

9 DI CIOCO, Lucía. – "*Google: olvida mi nombre*"; http://www.cromo.com.uy/google-olvida-mi-nombre-n955589.

para garantizar el anonimato de los afectados en determinadas sentencias para preservar su nombre[10].

Otro fue el caso en Colombia de una señora que se presentaba como Gloria. La mujer había sido imputada en el año 2009 en un caso de trata de personas, cuando trabajaba en una agencia de viajes y vendía pasajes a una red de tráfico. Sobre esto salió una nota en el diario local El Tiempo, la cual fue hallada por Gloria en una búsqueda en Google, años después[11].

La Justicia determinó que el diario debía actualizar la noticia (según establece la norma de ese país sobre las noticias en línea), pero con el agregado de que el portal debía utilizar protocolos de exclusión. ¿Qué significa esto? Los motores de búsqueda usan programas automatizados (bots) para verificar y categorizar qué contenido, páginas y secciones de una web van a ser indexadas en los resultados. Al cambiar las listas de comandos se impide que ciertas URL sean encontradas e indexadas por los buscadores. De esta manera la noticia en la que se mencionaba a la mujer ya no aparece en los resultados de Google[12].

Esta obligación de los medios de actualizar las noticias en sus portales de internet no existe en la legislación uruguaya, que ni siquiera aborda estos temas.

Chile fue por la misma línea que Colombia: una sentencia de la Suprema Corte determinó que se debía eliminar del portal del diario La Tercera una noticia sobre un carabinero procesado por delitos de abuso sexual; esto incluyó a su buscador interno[13].

En Uruguay, si bien el derecho al olvido carece de una regulación propia y específica, podría considerarse comprendido en el régimen general de protección de datos personales consagrado en la Ley Nº 18.331 de 11 de agosto de 2008, modificativas y decretos reglamentarios.

La Ley consagra los derechos de los titulares de los datos, entre ellos, el derecho de toda persona para solicitar la rectificación, actualización, inclusión o supresión de datos personales que le corresponda incluidos en una base de datos, al constatarse error o falsedad o exclusión en la información de la que es titular.

En lo que refiere a la problemática que estamos estudiando referida al derecho al olvido, no necesariamente las solicitudes que se planteen en tal sentido pueden referir a informaciones que sean erróneas, falsas o parciales.

Seguramente sean verdaderas.

Y ahí se ubica el gran problema en torno al derecho al olvido, teniendo presente el indiscutible peso que tienen hoy las redes sociales y el internet, que nos permite hablar, sin lugar a dudas, de una doble condena en aquellos casos en los cuales determinada persona por ejemplo haya sido procesada por la Justicia competente y además el hecho o la situación que generó tal procesamiento tomo estado público y permanece en forma indefinida en internet y en las redes.

10 DI CIOCO, Lucía. – "*Google: olvida mi nombre*"; http://www.cromo.com.uy/google-olvida-mi-nombre-n955589.

11 DI CIOCO, Lucía. – "*Google: olvida mi nombre*"; http://www.cromo.com.uy/google-olvida-mi-nombre-n955589.

12 DI CIOCO, Lucía. – "*Google: olvida mi nombre*"; http://www.cromo.com.uy/google-olvida-mi-nombre-n955589.

13 DI CIOCO, Lucía. – "*Google: olvida mi nombre*"; http://www.cromo.com.uy/google-olvida-mi-nombre-n955589.

En caso de que no prospere tal solicitud, el titular de los datos podrá promover la acción de habeas data prevista en la Ley ante la Justicia Competente.

Asimismo, debe destacarse la existencia de la Unidad Reguladora y de Control de Datos Personales, encargada de controlar la observancia del régimen legal, en particular las normas sobre legalidad, integridad, veracidad, proporcionalidad y seguridad de datos, por parte de los sujetos alcanzados, pudiendo a tales efectos realizar las actuaciones de fiscalización e inspección pertinentes.

Asimismo, la Unidad recibe por ejemplo denuncias de particulares y solicita a los responsables de las bases de datos o titulares de sitios Web la eliminación de determinada información, disponiendo las medidas sancionatorias que pudieren corresponder.

Olvidar es humano. Pero –a pesar de que detrás de Google hay personas– el buscador más popular del planeta no olvida fácilmente, y mucho menos el resto de internet. Lo que se sube a la red es permanente, como así lo son también sus consecuencias. Ante esta realidad es que reacciona la ley del derecho al olvido, famosa en Europa por haber arremetido contra Google, pero en Uruguay, incluso en América Latina, es difícil encontrar consenso sobre el tema[14].

Europa se familiarizó con este concepto en 2014, cuando el Tribunal de Justicia de la Unión Europea decidió que Google debía brindar a los europeos la oportunidad de solicitar que sus servicios de búsqueda "olviden" la información que les concierne, especialmente si es perjudicial o inexacta. Desde entonces, según datos presentados por Deya en su ponencia, actualizados al pasado 4 de agosto, se presentaron más de 500 mil solicitudes para retirar determinadas URL de los índices de búsqueda de Google, de las cuales se atendió al 43%[15].

La nota de perjudicialidad es la clave para valorar si corresponde o no eliminar las referencias a hechos, situaciones o imágenes que hagan identificables a una persona y que surgen libremente de cualquier buscador en internet.

El derecho al olvido no es absoluto y para su ejercicio es necesario ponderar derechos y analizar caso por caso, coincidieron expertos en el foro *Derecho al olvido, tutela integral de la privacidad. Visión Iberoamericana*, organizado por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y el Senado de la República[16].

En el panel *"Las dimensiones del derecho al olvido"*, la comisionada María Patricia Kurczyn Villalobos destacó la importancia del ejercicio de este derecho en el ámbito laboral, debido a que frecuentemente los trabajadores que inician algún juicio en contra de su patrón son ingresados a las "listas negras", lo cual les dificulta encontrar un nuevo empleo y con ello se ven vulnerados otros de sus derechos. Expuso que las listas negras pueden representar para los trabajadores una "muerte laboral" porque se rompen todas las posibilidades de que la persona pueda desempeñar otra actividad cuando ha sido cesado o despedido de una fuente de empleo, vulnerando sus derechos al trabajo y a la

14 DI CIOCO, Lucía. – "*Google: olvida mi nombre*"; http://www.cromo.com.uy/google-olvida-mi-nombre-n955589.

15 DI CIOCO, Lucía. – "*Google: olvida mi nombre*"; http://www.cromo.com.uy/google-olvida-mi-nombre-n955589.

16 http://www.lja.mx/2016/08/derecho-al-olvido-absoluto-necesario-ponderar-otros-derechos/

igualdad. Kurczyn explicó que el derecho al olvido puede ser un medio para proteger al trabajador cuando al exigir el respeto a sus derechos y demandar a su empleador, es ingresado a las listas negras y desprestigiado, aún cuando se determine la existencia de una causa justificada para la demanda: "Los datos personales de los trabajadores y de los empleadores tienen exactamente el mismo valor porque son parte de la esencia del ser humano y no podemos distinguir en categorías ni en grados de más o de menos"[17].

Felipe ROTONDO, presidente de la Unidad Reguladora y de Control de Datos Personales de Uruguay, dijo que el derecho al olvido no es absoluto y que para hacerlo efectivo se deben considerar elementos, como la naturaleza de la información, el interés público, la manera de acceder a los datos y la incidencia de su difusión en el titular: "Priorizar un derecho no es hacerlo absoluto sino ver la situación en el caso concreto". Planteó que en Uruguay el derecho al olvido es una proyección de los derechos de supresión y oposición de los datos y se aprecia en cada caso una visión de derechos humanos", enfatizó[18].

Guillermo Antonio Tenorio Cueto, profesor de la Universidad Panamericana y director del Centro de Estudios del Tribunal Federal de Justicia Fiscal y Administrativa (TFJFA), aseguró que el ejercicio de este derecho depende de cada caso y que incluso servidores públicos y personalidades públicas, pueden ejercerlo."No todos los que sean personalidades públicas son susceptibles de no pedir ningún tipo de derecho al olvido; tienen un margen de posibilidades porque tanto servidores públicos como personalidades públicas tienen derecho a la vida privada y a la protección de su honor, más en todas aquellas actividades que no tienen nada que ver con lo público", subrayó[19].

Olivia Andrea Mendoza Enríquez, investigadora del Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (Infotec), afirmó que el ejercicio del derecho al olvido no se resuelve con reglas generales, debe existir una ponderación de derechos y un análisis caso por caso: "Los derechos que se verían afectados si se salvaguarda el derecho al olvido, de manera general, sin ponderar, es el derecho a la verdad, el derecho de acceso a la información y el derecho a la libertad de expresión, pero ojo, ningún derecho es absoluto"[20].

El panel fue moderado por el senador Zoé Robledo Aburto, quien dijo que debe haber un balance entre el derecho al olvido y los derechos a la verdad y a la memoria colectiva[21].

III) DERECHO AL OLVIDO Y DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

Puede definirse el derecho a la protección de datos personales "como la facultad o el poder que tienen las personas para actuar per se y para exigir la actuación del Estado o de quien tenga competencia para ello a fin de tutelar los derechos que pudieran verse

17 http://www.lja.mx/2016/08/derecho-al-olvido-absoluto-necesario-ponderar-otros-derechos/

18 http://www.lja.mx/2016/08/derecho-al-olvido-absoluto-necesario-ponderar-otros-derechos/

19 http://www.lja.mx/2016/08/derecho-al-olvido-absoluto-necesario-ponderar-otros-derechos/

20 http://www.lja.mx/2016/08/derecho-al-olvido-absoluto-necesario-ponderar-otros-derechos/

21 http://www.lja.mx/2016/08/derecho-al-olvido-absoluto-necesario-ponderar-otros-derechos/

afectados por virtud del acceso, registro o trasmisión a terceros de los datos que atañen a su personalidad[22]".

"En general se dice que el derecho a la protección de datos personales es un derecho nuevo", agrega DURÁN MARTÍNEZ, citando a Carlos E. DELPIAZZO, que lo llama *"novel derecho"*, razón por la cual, se le ha considerado un derecho de la tercera generación, subrayando que "si bien el derecho a la protección de datos es considerado hoy en día un derecho autónomo, es un derecho instrumental".

Sobre el punto destaca Carlos E. DELPIAZZO[23] que "la mayoría de la doctrina continental utiliza la expresión *"derecho a la protección de datos personales"* para designar el derecho bajo examen cuyo objeto es la tutela frente a la posible utilización no autorizada de los datos de la persona para confeccionar una información que, identificable con él, afecte a su entorno personal, familiar, profesional o social".

José Luis PIÑAR MAÑAS[24], Director de la Agencia Española de Protección de Datos, señala que "… El derecho fundamental a la protección de datos reconoce al ciudadano la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos. Ello supone que el desarrollo y la aplicación de las nuevas tecnologías ha introducido comodidad y rapidez en el intercambio de datos, lo que ha contribuido también al incremento del número de tratamientos de datos que se realizan cotidianamente. La bondad que aportan estas técnicas es indudable respecto del progreso de las sociedades modernas y de la calidad de vida de los ciudadanos, pero se hace necesario garantizar el equilibrio entre modernización y garantía de los derechos de los ciudadanos. Esta ponderación entre derecho del ciudadano a preservar el control sobre sus datos personales y la aplicación de las nuevas tecnologías de la Información, es el contexto en el que el Legislador consagra el derecho fundamental a la protección de datos de carácter personal".

Es precisamente en el equilibrio entre modernización y garantía de los derechos de los ciudadanos, en la ponderación entre derecho del ciudadano a preservar el control sobre sus datos personales y la aplicación de las nuevas tecnologías de la Información, donde ubicamos el derecho al olvido, en tanto forma parte en forma ineludible del derecho fundamental a la protección de los datos personales.

Con acierto señala Cristina VÁZQUEZ PEDROUZO[25] que "así como la transparencia se encuentra en el origen de las regulaciones sobre acceso a la información pública, el desarrollo de la informática y su aptitud abarcadora de grandes volúmenes de información en tiempos reducidos ha creado la necesidad de tutelar los datos personales".

22 DURÁN MARTÍNEZ, Augusto. – *"Derecho a la protección de datos personales y al acceso a la Información Pública. Hábeas Data. Leyes Nº 18.331 de 11 de agosto de 2008 y Nº 18.381 de 17 de octubre de 2008"*; 2ª Edición actualizada y ampliada; AMF; Montevideo, 2012; pág. 11 y siguientes.

23 DELPIAZZO, Carlos. – *"A la búsqueda del equilibrio entre privacidad y acceso"*; Instituto de Derecho Informático, Facultad de Derecho, Universidad de la República; Protección de datos personales y Acceso a la Información Pública. FCU - AGESIC; Montevideo, 2009, pág. 9 y siguientes.

24 PIÑAR MAÑAS, José Luis.- *"Guía del Derecho Fundamental a la protección de datos de carácter personal"*, (Agencia Española de Protección de Datos, 2004). La información de esta Guía puede ser ampliada en Servicio de Atención al Ciudadano: www.agpd.es.

25 VÁZQUEZ PEDROUZO, Cristina. – *"El régimen jurídico del acceso a la información pública y la protección de datos personales";* (Revista de Derecho y Tribunales, Nº 15, A.M.F., Montevideo 2011), pág. 61.

Debemos ser muy cuidadosos en señalar que el derecho al olvido no puede interpretarse como contrario a la transparencia aunque debemos trabajar en soluciones y fórmulas que nos permitan respetar el derecho de una persona a que su nombre no permanezca en forma indefinida en internet vinculados a hechos o acontecimientos de su vida a los cuales ya hemos hecho referencia y que no necesariamente están acompañados de una condena social permanente en las redes sociales e internet.

IV) LA PROTECCIÓN DE DATOS PERSONALES EN LA LEGISLACIÓN URUGUAYA

1.- Régimen general.

El artículo 1º de la Ley Nº 18.331 dispone expresamente que *"el derecho a la protección de datos personales es inherente a la persona humana, por lo que está comprendido en el artículo 72 de la Constitución de la República*[26]*"*.

Sin perjuicio de no trasladar a este trabajo los valiosos estudios de la doctrina nacional sobre el punto, si queremos destacar la conclusión a la que arriba Augusto DURÁN MARTÍNEZ[27] sobre el punto: "…la ley siguió aquí las más modernas tendencias que se han impuesto en el mundo, tanto en el ámbito internacional como en los más avanzados estados nacionales..."

En cuanto al ámbito subjetivo, el artículo 2º dispone que: "El derecho a la protección de los datos personales se aplicará por extensión a las personas jurídicas, en cuanto corresponda.

Por su parte, el artículo 3º regula el ámbito objetivo: "El régimen de la presente ley será de aplicación a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado.

No será de aplicación a las siguientes bases de datos: **A**. las mantenidas por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas; **B**. Las que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito[28]; **C**. A las bases de datos creadas y reguladas por leyes especiales".

---

26 **Constitución de la República, artículo 72º**. *"La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno".*

27 DURÁN MARTÍNEZ, Augusto. – *"Derecho a la protección de datos personales y al acceso a la Información Pública. …"*; Ob. Cit.; pág. 45 y siguientes.

28 **Dictamen del Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales (URCDP) Nº 3/2011 de 10 de febrero de 2011.** *"Los sistemas de circuito cerrado de televisión (CCTV) o videovigilancia que se encuentren instalados en las entidades financieras públicas o privadas, por imposición de la normativa del Ministerio del Interior y del Banco Central del Uruguay, en tanto se sustentan en razones de "seguridad pública", resultan exceptuados del régimen de la LPDP, al amparo de lo previsto en su artículo 3º literal B). Por tanto, no les asiste la obligación de inscripción ante la Unidad Reguladora y de Control de Datos Personales".*

En cuanto al alcance del derecho a la protección de datos apunta Carlos E. DELPIAZZO[29] que "cabe compartir de la enseñanza según la cual tres son las características básicas con las que se delimita el estudio de la llamada protección de datos: a) que los datos sean susceptibles de tratamiento de tratamiento o se encuentren en soporte susceptible de tratamiento; b) que haya la posibilidad de identificar el resultado del tratamiento de datos (la información como dato elaborado hacia un fin) con el titular; y, c) que el manejo o acceso a los datos se haga sin consentimiento del titular, independientemente de que tal manejo sea malintencionado o no."

Cristina VÁZQUEZ apunta que "cuando se habla de protección de datos personales, acuden inmediatamente las nociones de "intimidad" y "privacidad". El vocablo "privacidad" ha sido tomado por nuestra lengua, fundamentalmente del inglés "privacy" y del francés "privacité", recordando que "la Constitución no emplea las expresiones "intimidad" o "privacidad" pero las mismas se han incorporado en diversas normas de jerarquía legal o reglamentaria[30].

La ley uruguaya en su artículo 4º define al dato personal como "información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables[31,32,33].

2.- Principios generales

El Capítulo II de la Ley regula los principios generales a los cuales deberá ajustarse la actuación de los responsables de las bases de datos, tanto públicos como privados, y, en general, de todos quienes actúen en relación a datos personales de terceros.

El artículo 5 "Valor y fuerza[34] dispone que la actuación de los responsables de las bases de datos, tanto públicos como privados, y, en general, de todos quienes actúen en

29 DELPIAZZO, Carlos. – "*A la búsqueda del equilibrio entre privacidad y acceso*"; Ob. Cit; Montevideo, 2009, pág. 13 y siguientes.

30 VÁZQUEZ PEDROUZO, Cristina. – *"El régimen jurídico del acceso a la información pública y la protección de datos personales";* Ob. Cit.; pág. 65.

31 **Dictamen del Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales (URCDP) Nº 14/2009 de 25 de setiembre de 2009.** Ante una consulta presentada ante la URCDP, por la Unidad de Acceso a la Información Pública (UAIP) el Consejo Ejecutivo de la URCDP dictaminó que solicitud de correos electrónicos de estudiantes egresados de las Facultades pertenecientes a la Universidad de la República, por parte de un Consejero de la misma, no es conforme a Derecho "comenzando por destacarse que el correo electrónico contiene o es en sí mismo un dato personal, puesto que contiene "información... referida a personas físicas o jurídicas, determinadas o determinables" (art. 4 de la Ley Nº 18.331 de 11-08-2008)".

32 **Dictamen del Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales (URCDP) Nº 13/2009 de 25 de setiembre de 2009.** A juicio de la URCDP de que no caben dudas de que los datos biométricos son "datos personales", en tanto se los ubica perfectamente en la definición del artículo 4 literal D de la Ley Nº 18.331, y como tal, su registro y tratamiento deben cumplir con los postulados y principios de la citada Ley.

33 **Resolución Nº 04/009 de 14 de julio de 2009 (Expediente Nº 2009/001) del Consejo Ejecutivo de la Unidad de Acceso a la Información Pública (UAIP).** Debe entregarse a los concursantes toda la información discriminada y existente en los expedientes con excepción de: a) aquellos datos que nada hacen a la situación evaluada por ejemplo: estados civiles, documentos de identidad, direcciones postales y electrónicas, números de teléfono, y b) datos de carácter sensible como ejemplo las evaluaciones sicológicas".

34 **Dictamen del Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales (URCDP) Nº 10/2010 de 16 de abril de 2010.** La URCDP dictaminó que en la videovigilancia como toda grabación, captación, transmisión, conservación y almacenamiento de imágenes y en algunos casos de sonidos mediante la utilización de videocámaras u otro medio análogo., las imágenes y sonidos mencionados constituyen información personal y por tanto es de aplicación la LPDP y sus normas complementarias, deben observarse los principios de la protección de datos.

relación a datos personales de terceros, deberá ajustarse a los siguientes principios generales: **A**. Legalidad; **B**. Veracidad; **C**. Finalidad, **D**. Previo consentimiento informado; E. Seguridad de los datos ; **F**. Reserva; **G**. Responsabilidad.

Dichos principios generales servirán también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de las disposiciones pertinentes".

El principio de legalidad, recogido en el artículo 6º, preceptúa que la formación de bases de datos será lícita cuando se encuentren debidamente inscriptas, observando en su operación los principios que establecen la presente ley y las reglamentaciones que se dicten en consecuencia. Las bases de datos no pueden tener finalidades violatorias de derechos humanos o contrarias a las leyes o a la moral pública.

Por su parte el artículo 7º recoge el principio de veracidad al disponer que los datos personales que se recogieren a los efectos de su tratamiento deberán ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la cual se hubieren obtenido. La recolección de datos no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a las disposiciones a la presente ley. Los datos deberán ser exactos y actualizarse en el caso en que ello fuere necesario.

A su vez el principio de finalidad se explicita en el artículo 8º al señalar que los datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. Los datos deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados.

Especial consideración merece el tratamiento del principio del previo consentimiento informado consagrado en el artículo 9[35] de la Ley a estudio.

Al respecto debe apuntarse que el artículo 152 de la Ley Nº 18.719 de 27 de diciembre de 2010 da nueva redacción al inciso 2 y al literal E) del artículo 9 de la Ley Nº 18.331 de 11 de agosto de 2008.

La redacción vigente del artículo a estudio es: "Artículo 9º. Principio del previo consentimiento informado- El tratamiento de datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá documentarse.

El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 13 de la presente ley.

No será necesario el previo consentimiento cuando: **A**. Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de

35 **DICTÁMENES/Dictamen del Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales (URCDP) Nº 19/2010 de 27 de agosto de 2010.** La URCDP dictaminó que "no se deben comunicar los datos referidos a números de teléfono celular, por parte de Clearing de Informes a la Dirección General Impositiva". El Dictamen en estudio se enmarca en primer lugar, en el alcance de la comunicación de datos regulada en el artículo 17 de la Ley Nº 18.331, exigiendo para su legitimidad la conjunción simultánea de los siguientes requisitos, el interés legítimo del emisor y del destinatario de la comunicación, y el previo consentimiento del titular de los datos, salvo las excepciones establecidas en la norma.

comunicación; B. Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal, **C**. Se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento. En el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma; **D**. Deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento. **E**. *Se realice por personas físicas para su uso exclusivo personal, individual o doméstico.*

Por su parte el artículo 10 de la Ley a estudio consagra el principio de seguridad de los datos al disponer que el responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales.

En cuanto a la vulneración de la seguridad, el artículo 8º, establece "Cuando el responsable o encargado de la base de datos o tratamiento conozca de la ocurrencia de vulneraciones de seguridad en cualquier fase del tratamiento que realice, que sean susceptibles de afectar de forma significativa los derechos de los interesados, deberán informarles de este extremo".

El principio de reserva regulado en el artículo 11º preceptúa que aquellas personas físicas o jurídicas que obtuvieren legítimamente información proveniente de una base de datos que les brinde tratamiento, están obligadas a utilizarla en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad, estando prohibida toda difusión de la misma a terceros. Las personas que, por su situación laboral u otra forma de relación con el responsable de una base de datos, tuvieren acceso o intervengan en cualquier fase del tratamiento de datos personales, están obligadas a guardar estricto secreto profesional sobre los mismos (artículo 302 del Código Penal), cuando hayan sido recogidos de fuentes no accesibles al público. Lo previsto no será de aplicación en los casos de orden de la Justicia competente, de acuerdo con las normas vigentes en esta materia o si mediare consentimiento del titular. Esta obligación subsistirá aun después de finalizada la relación con el responsable de la base de datos.

Y finalmente la Ley en su artículo 12 regula el principio de responsabilidad al disponer que el responsable de la base de datos es responsable de la violación de las disposiciones de la presente ley.

3.- Derechos de los titulares de los datos

El Capítulo III de la Ley regula especialmente los derechos de los titulares de los datos, y también del emisor y del destinatario de los datos.

En tal sentido podemos destacar el "derecho de información frente a la recolección de datos" (artículo 13); el "derecho de acceso" (artículo 14); y el "derecho de rectificación, actualización, inclusión o supresión" (artículo 15)

El artículo 15 de la Ley en su nueva redacción, dispone: *"Artículo 15*[36]. Derecho de

36 La redacción original del inciso cuarto del artículo 15 de la Ley Nº 18.331 de 11 de agosto de 2008 (Publicada D.O. 18 ago/008 - Nº 27.549) era: No procede la eliminación o supresión de datos personales salvo en aquellos casos de: A) Perjuicios a los derechos e intereses legítimos de terceros. B) Notorio error o falsedad. C) Contravención a lo establecido por una obligación legal.

rectificación, actualización, inclusión o supresión.- Toda persona física o jurídica tendrá derecho a solicitar la rectificación, actualización, inclusión o supresión de los datos personales que le corresponda incluidos en una base de datos, al constatarse error o falsedad o exclusión en la información de la que es titular.

El responsable de la base de datos o del tratamiento deberá proceder a realizar la rectificación, actualización, inclusión o supresión, mediante las operaciones necesarias a tal fin en un plazo máximo de cinco días hábiles de recibida la solicitud por el titular del dato o, en su caso, informar de las razones por las que estime no corresponde.

El incumplimiento de esta obligación por parte del responsable de la base de datos o del tratamiento o el vencimiento del plazo, habilitará al titular del dato a promover la acción de habeas data prevista en esta ley.

Procede la eliminación o supresión de datos personales en los siguientes casos:

A. Perjuicios a los derechos e intereses legítimos de terceros.

B. Notorio error.

C. Contravención a lo establecido por una obligación legal.

Durante el proceso de verificación, rectificación o inclusión de datos personales, el responsable de la base de datos o tratamiento, ante el requerimiento de terceros por acceder a informes sobre los mismos, deberá dejar constancia que dicha información se encuentra sometida a revisión.

En el supuesto de comunicación o transferencia de datos, el responsable de la base de datos o del tratamiento debe notificar la rectificación, inclusión o supresión al destinatario dentro del quinto día hábil de efectuado el tratamiento del dato.

La rectificación, actualización, inclusión, eliminación o supresión de datos personales cuando corresponda, se efectuará sin cargo alguno para el titular."

Es precisamente en el ejercicio de este derecho, que en Uruguay, el titular podrá presentarse para solicitar su exclusión de determinada base de datos o motor de búsqueda en internet y en las redes sociales.

Creemos que necesariamente habría que contemplar en forma específica el derecho al olvido en nuestra legislación incorporando la nota de perjudicialidad a la que refiere el Derecho Europeo.

Debemos explorar los conceptos de perjudicialidad y de incidencia de la información para su titular a los efectos de valorar si corresponde o no acceder a una solicitud de eliminación de determinada información que es pública en internet y en las redes sociales.

Felipe ROTONDO sostiene que el derecho al olvido es una proyección de los derechos de supresión y oposición de los datos y se aprecia en cada caso una visión de derechos humanos", apuntando que la normativa uruguaya sobre derecho al olvido se aplica en casos en que los datos no son pertinentes para la información que se difunde, así como cuando caducaron o son falsos o tratados ilegítimamente. Además, agregó que

la ley uruguaya establece excepciones cuando la información tiene valor histórico, científico, cuando contribuye a la seguridad pública o por cumplimiento de obligaciones tributarias, entre otros motivos.

La norma, agrega ROTONDO, también establece que si el responsable de la publicación de la información se da cuenta de que esos datos son incorrectos, falsos o si ya no sirven a la finalidad para la cual se recolectaron, debe quitarlos sin que nadie lo solicite[37].

Además de la intimidad, el derecho a borrar información protege el derecho de las personas a olvidar el pasado, dijo el experto en protección de datos del Instituto de Internet de Oxford, Viktor Mayer Schonberger, al diario británico The Guardian. "La belleza del cerebro humano es que olvidamos, lo que nos permite pensar en el presente. Eso nos ayuda a tomar decisiones", agregó[38].

Es fundamental destacar la importancia de los llamados "protocolos de exclusión". Los portales deben utilizar protocolos de exclusión en la medida de que los motores de búsqueda usan programas automatizados (bots) para verificar y categorizar qué contenido, páginas y secciones de una web van a ser indexadas en los resultados. Al cambiar las listas de comandos se impide que ciertas URL sean encontradas e indexadas por los buscadores.

4.- La acción de protección de datos personales

En caso de que la solicitud de supresión y/o oposición de los datos ante el Responsable de la Base de Datos -ya sea pública o privada- o ante el Responsable del Buscador o motor de búsqueda en internet no prospere, el titular del dato personal podrá entablar la acción de protección de datos personales *"Habeas data"* ante la Justicia competente.

El Capítulo VIII de la Ley Nº 18331 en estudio consagra la acción de datos personales, regulando el procedimiento, la procedencia y competencia, la legitimación y el trámite de primera y de segunda instancia.

En tal sentido El artículo 37 "Habeas data" establece que "Toda persona tendrá derecho a entablar una acción judicial efectiva para tomar conocimiento de los datos referidos a su persona y de su finalidad y uso, que consten en bases de datos públicos o privados; y –en caso de error, falsedad, prohibición de tratamiento, discriminación o desactualización– a exigir su rectificación, inclusión, supresión o lo que entienda corresponder. Cuando se trate de datos personales cuyo registro esté amparado por una norma legal que consagre el secreto a su respecto, el Juez apreciará el levantamiento del mismo en atención a las circunstancias del caso".

En cuanto a la procedencia, el artículo 38 dispone que "El titular de datos personales podrá entablar la acción de protección de datos personales o habeas data, contra todo responsable de una base de datos pública o privada, en los siguientes supuestos: A.Cuando quiera conocer sus datos personales que se encuentran registrados en una base de datos o similar y dicha información le haya sido denegada, o no le hubiese sido proporcionada por el responsable de la base de datos, en las oportunidades y plazos previstos por la ley; B. Cuando haya solicitado al responsable de la base de datos o trata-

37 DI CIOCO, Lucía. – "*Google: olvida mi nombre*"; http://www.cromo.com.uy/google-olvida-mi-nombre-n955589.

38 DI CIOCO, Lucía. – "*Google: olvida mi nombre*"; http://www.cromo.com.uy/google-olvida-mi-nombre-n955589.

miento su rectificación, actualización, eliminación, inclusión o supresión y éste no hubiese procedido a ello o dado razones suficientes por las que no corresponde lo solicitado, en el plazo previsto al efecto en la ley.

El texto legal exige y presupone la previa denegatoria tanto del titular de la base pública como del titular de la base privada, por lo que la formulación de petición ante el responsable público o privado de la base de datos, y su denegatoria expresa, tácita o por razones que el interesado juzgue no amparadas por la ley, constituye precisamente una cuestión previa, sin la cual no podrá acudir a la vía jurisdiccional.

5.- La Unidad Reguladora y de Control de Datos Personales[39]

La Unidad Reguladora y de Control de Datos Personales, fue creada por el artículo 31 de la Ley Nº 18.381 como órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), dotado de la más amplia autonomía técnica[40].

Estamos ante un nuevo órgano desconcentrado, en este caso de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), dotado de la más amplia autonomía técnica, como ejemplo reciente de la modalidad de ejercicio del control del Estado a través de órganos desconcentrados en la órbita del Poder Ejecutivo[41].

La regulación, el funcionamiento, los procedimientos, los cometidos y las funciones así como la potestad sancionatoria del órgano de control están regulados en el Capítulo VII de la Ley (artículos 31 a 36)[42].

Debe destacarse especialmente que la Unidad está encargada de controlar la observancia del régimen legal, en particular las normas sobre legalidad, integridad, veracidad, proporcionalidad y seguridad de datos, por parte de los sujetos alcanzados, pudiendo a tales efectos realizar las actuaciones de fiscalización e inspección pertinentes.

Asimismo la Unidad recibe por ejemplo denuncias de particulares y solicita a los responsables de las bases de datos o titulares de sitios Web la eliminación de determinada información, disponiendo las medidas sancionatorias que pudieren corresponder.

V) REFLEXIONES FINALES

Hace un par de años – no muchos- para encontrar una noticia relacionada a un determinado hecho de cualquier tipo, a una determinada situación o a una determinada persona, siempre y cuando la noticia se hubiese publicado en algún medio de prensa escrito, teníamos que ir al "histórico" de Diarios y Revistas de la Biblioteca Nacional o en su defecto, averiguar qué día de la semana se había publicado la noticia en la versión

39 Sitio Web: http://www.datospersonales.gub.uy

40 SCHIAVI, Pablo. – "*El Control del Acceso a la Información Pública y de la Protección de Datos Personales en el Uruguay*", Universidad de Montevideo – Facultad de Derecho, Montevideo, 2012; pág. 129 y siguientes.

41 SCHIAVI, Pablo. – "*El Control del Acceso a la Información Pública y de la Protección de Datos Personales en el Uruguay*", Ob. Cit, pág. 129 y siguientes.

42 SCHIAVI, Pablo. – "*El Control del Acceso a la Información Pública y de la Protección de Datos Personales en el Uruguay*", Ob. Cit, pág. 129 y siguientes.

impresa de un periódico para ir a comprar ese ejemplar a su Sede Central donde muy amablemente un empleado nos preguntaba cual era el día en que se había publicado el Diario para poder acceder a él.

Nadie en ese momento se imaginaba que hoy iba a existir "Google".

Hoy todo cambió.

Para siempre.

Los desarrollos doctrinarios y jurisprudenciales sobre el "derecho al olvido" se encuadran en los permanentes desafíos que la actual era digital con una sociedad hiperconectada e hiperinformada le impone al Derecho y a las distintas regulaciones.

El "derecho al olvido" deber ser analizado en el contexto de la protección de datos personales en internet y en las redes sociales con especial acento en el necesario equilibrio entre modernización y garantía del derecho del ciudadano a preservar el control sobre sus datos personales y la aplicación de las nuevas tecnologías de la información.

El "derecho al olvido", en tanto proyección de los derechos de supresión y oposición de los datos, no deber ser interpretado como sinónimo de "borrar" o de "ocultar" determinada información referida a una persona, aunque su consagración apunta al derecho del titular del dato a que su información personal no permanezca de manera indefinida y permanente, y de fácil acceso, en las redes sociales e internet.

Debemos ser muy cuidadosos en señalar que el derecho al olvido no puede interpretarse como contrario a la transparencia aunque debemos trabajar en soluciones y fórmulas que nos permitan respetar el derecho de una persona a que sus datos no permanezcan en forma indefinida en internet vinculados a hechos o acontecimientos de su vida negativos e incluso positivos y que suponen una condena social permanente en las redes sociales e internet.

En Uruguay, si bien el derecho al olvido carece de una regulación propia y específica, podría considerarse comprendido en el régimen general de protección de datos personales consagrado en la Ley Nº 18.331 de 11 de agosto de 2008, modificativas y decretos reglamentarios.

La Ley consagra los derechos de los titulares de los datos, entre ellos, el derecho de toda persona para solicitar la rectificación, actualización, inclusión o supresión de datos personales que le corresponda incluidos en una base de datos, al constatarse error o falsedad o exclusión en la información de la que es titular.

En lo que refiere a la problemática que estamos estudiando referida al derecho al olvido, no necesariamente las solicitudes que se planteen en tal sentido pueden referir a informaciones que sean erróneas, falsas o parciales.

Seguramente sean verdaderas.

Y ahí se ubica el gran problema en torno al derecho al olvido, teniendo presente el indiscutible peso que tienen hoy las redes sociales y el internet, que nos permite hablar, sin lugar a dudas, de una doble condena en aquellos casos en los cuales determinada

persona por ejemplo haya sido procesada por la Justicia competente y además el hecho o la situación que generó tal procesamiento tomó estado público y permanece en forma indefinida en internet y en las redes.

La incorporación del derecho al olvido en nuestra legislación se impone, con especial énfasis en criterios de valoración y ponderación tales como la nota de perjudicialidad y la incidencia de la información para su titular, de modo de evitar, cuando corresponda una "doble" condena para una persona, la de la Justicia de su país y la permanente, libre, e irrestricta de internet y de las redes sociales.

Como sociedad debemos interrogarnos y preguntarnos ¿qué podemos hacer con todo esto? ¿Qué pueden hacer los titulares de los datos personales, las personas ante esta manipulación y accesibilidad irrestricta a información que concierne a cada uno, y que basta simplemente con que se haya publicado en alguna página web o en las distintas redes sociales?

El Derecho al olvido se vislumbra como un primer intento.

VI) BIBLIOGRAFÍA

BERNIER, Chantal.- *El Memorándum de Montevideo: un marco de referencia para la protección de los datos personales de los jóvenes en Internet en la región Iberoamericana;* Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes; Memorándum de Montevideo; Carlos G. Gregorio – Lina Ornelas, Compiladores; IIJusticia – Instituto de Investigación para la Justicia, IFAI –Instituto Federal de Acceso a la Información y Protección de Datos; México, 2011, p. 16.

DI CIOCO, Lucía. – "*Google: olvida mi nombre*"; http://www.cromo.com.uy/google-olvida-mi-nombre-n955589

DELPIAZZO, Carlos E.-"*De la publicidad a la transparencia en la gestión administrativa*", en Revista de Derecho de la Universidad de Montevideo (Montevideo, 2003), Año II, Nº 3, pág. 113 y siguientes.

DELPIAZZO, Carlos E.-"*Acerca del control social de la gestión pública*", Cita On Line https://online.unisc.br/seer/index.php/direito/article/viewFile/672/458.

DELPIAZZO, Carlos. – "*A la búsqueda del equilibrio entre privacidad y acceso*"; Instituto de Derecho Informático, Facultad de Derecho, Universidad de la República; Protección de datos personales y Acceso a la Información Pública. FCU - AGESIC; Montevideo, 2009, pág. 9 y siguientes.

DURÁN MARTÍNEZ, Augusto. – "*Derecho a la protección de datos personales y al acceso a la Información Pública. Hábeas Data. Leyes Nº 18.331 de 11 de agosto de 2008 y Nº 18.381 de 17 de octubre de 2008*"; 2ª Edición actualizada y ampliada; AMF; Montevideo, 2012; pág. 11 y siguientes.

LÓPEZ JIMÉNEZ, David.- *La protección de datos de carácter personal en el ámbito de las redes sociales electrónicas: el valor de la autorregulación;* Universidad de Alcalá de Henares. Servicio de Publicaciones, 2009.

PESCHARD MARISCAL, Jacqueline.- *Protección de las niñas, niños y adolescentes en el ámbito digital: responsabilidad democrática de las instituciones de gobierno y de las agencias de protección de datos;* Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes; Memorándum de Montevideo; Carlos G. Gregorio – Lina Ornelas, Compiladores; II Justicia – Instituto de Investigación para la Justicia, IFAI –Instituto Federal de Acceso a la Información y Protección de Datos; México, 2011, p. 22.

PIÑAR MAÑAS, José Luis.- "*Guía del Derecho Fundamental a la protección de datos de carácter personal",* (Agencia Española de Protección de Datos, 2004). La información de esta Guía puede ser ampliada en Servicio de Atención al Ciudadano: www.agpd.es.

SCHIAVI, Pablo. – "*La protección de los datos personales en las redes sociales*"; en Estudios de Derecho Administrativo; 2013, Nº 7; Director Augusto Durán Martínez; Coordinador Pablo Schiavi; LA LEY URUGUAY; Montevideo, 2013; pág. 215 y siguientes.

SCHIAVI, Pablo. – "*Procedimiento administrativo especial: ruta de acceso a la información pública"* en Estudios de Derecho Administrativo 2014- Nº 10; Director: Augusto Durán Martínez – Coordinador: Pablo Schiavi (La Ley Uruguay. Montevideo, 2014), pág. 399 y siguientes.

SCHIAVI, Pablo. – "*Estudios de Información Pública y Datos Personales",* Recopilación de trabajos de investigación de los cursos de postgrado 2014-2015. Coordinador. Universidad de Montevideo – Facultad de Derecho, Montevideo 2016.

SCHIAVI, Pablo. – "*Estudios de Información Pública y Datos Personales",* Recopilación de trabajos de investigación de los cursos de postgrado 2012-2013. Coordinador. Universidad de Montevideo – Facultad de Derecho, Montevideo 2014.

SCHIAVI, Pablo. – *Reflexiones a cinco años de la Ley de Acceso a la Información Pública en el Uruguay"* en Estudios de Derecho Administrativo Nº 9/2014 – Director Augusto DURÁN MARTÍNEZ, Coordinador Pablo SCHIAVI (La LEY URUGUAY. Montevideo, 2014), pág. 181 y siguientes.

SCHIAVI, Pablo. – "*El Control del Acceso a la Información Pública y de la Protección de Datos Personales en el Uruguay",* Universidad de Montevideo – Facultad de Derecho, Montevideo 2012.

VÁZQUEZ PEDROUZO, Cristina. – *"El régimen jurídico del acceso a la información pública y la protección de datos personales";* (Revista de Derecho y Tribunales, Nº 15, A.M.F., Montevideo 2011), pág. 61.

VÁZQUEZ, Cristina; SCHIAVI, Pablo. – "*Procedimientos Administrativos"* Tomo I Decreto 500/991 de 27 de setiembre de 1991 (LA LEY URUGUAY, Montevideo, 2013).

UNIDAD DE ACCESO A LA INFORMACIÓN PÚBLICA. Sitio Web: http://www.informacionpublica.gub.uy.

UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES. Sitio Web: http://www.datospersonales.gub.uy.