Los datos personales.
La supresión de datos, conocida como el "derecho al olvido"

Por Carlos Damián Becerra[1]

Resumen: *El presente artículo nos presenta una problemática actual, referida a la protección de los datos personales, en particular desarrollamos aspectos a tener en cuanta sobre su tratamiento antes, durante y después de su publicidad. Buscamos clarificar el marco normativo al cual se someten los datos de las personas y el alcance que poseen empresas y organismos oficiales, sobre los mismos, teniendo como base los principios que rigen dicho tratamiento. Abordamos, de manera particular el derecho a la supresión de aquellos datos, sobre los cuales decidimos que ya no deben ser públicos, en lo que se conoce como "derecho al olvido", y el "comportamiento jurídico" de las redes sociales respecto a ello.*

Palabras clave: Datos personales - redes sociales - derecho al olvido – intimidad - supresión de datos.

La protección de los datos

Al hablar sobre protección de datos personales, es importante definir qué se entiende y cuál es la finalidad como tal.

En ese sentido, se puede pensar que todo dato de carácter personal se asocia a toda información que se encuentra vinculada con toda persona física identificada o identificable.

Identificable, se entiende que todo individuo puede ser identificable en el caso de poder ser individualizado o reconocida su identidad con un identificador, es decir, un nombre, número identificatorio, datos de posicionamiento geográfico, identificador de línea etc. También se lo puede identificar por su condición física, genética, fisiológica, mental, económica, social etc.[2]

a) Definiciones para tener en cuenta:

i. Interesado: se entiende como toda persona física, identificada o identificable, es decir, que quedan excluidas las personas jurídicas.

ii. Seudonimización: se entiende a la técnica utilizada para que no pueda atribuirse a un interesado que un dato se encuentra asociado con él. De esta manera, se evita que el mismo pueda identificarse dentro de una base de datos con un número identificador.

iii. Tercero: toda persona física o jurídica, servicio u organismo distinto del interesado, del responsable del tratamiento, encargado de tratamiento, y personas autorizadas para tratar datos personales.

---

[1] Licenciado en Administración. Abogado. Especialista en Conducción de Organizaciones Militares Terrestres. Especialista en Estrategia Operacional y Planeamiento Militar Conjunto. Alumno en el Posgrado de Especialización en Inteligencia Estratégica, en el Centro de Altos Estudios Nacionales (C.A.L.E.N), Montevideo-Uruguay. Doctorando en Derecho en la UNLZ.

[2] Agencia Española de Protección de Datos. (2018). Entrada en aplicación del Reglamento de Protección de Datos de la Unión Europea.

iv. Responsable del tratamiento: persona física o jurídica que por sí misma o juntos con otros, determina las pautas en que se fijará el tratamiento.

v. Encargado del tratamiento: es la persona física o jurídica que realiza el tratamiento de datos personales y que se encuentra bajo el monitoreo o por cuenta del responsable del tratamiento.

vi. Tratamiento de datos: se entiende como todo proceso que se realizan sobre los datos personales de manera automatizada o no, para su recolección, registro, organización, entre otros.

vii. Consentimiento del interesado: se la conoce como toda expresión de voluntad, la misma es libre, determinada, comunicada, e incuestionable, en donde el individuo acepta que se le traten los datos personales, sea por una declaración realizada por el mismo o por una acción que confirme dicha aceptación. (SIGLO21, 2024)

La intimidad y su reconocimiento jurídico

La publicación de los juristas Louis Brandeis y Samuel Warren (1890) fue el antecedente de mayor importancia para darle la jerarquía normativa tiempo después a lo relativo al derecho a la privacidad, intimidad y protección de datos personales.

En efecto, dichos autores manifestaron que el derecho a la privacidad no se trata de un derecho ilimitado, sino que fija ciertos límites en lo que respecta a lo siguiente: a) no se limita la publicación de lo que posea un interés público o general; b) no se descarta la publicación de ciertos temas sobre hechos o situaciones relativas a instituciones o corporaciones públicas; c) no se considera ningún resarcimiento por violación de la intimidad en situación de que sea oral y que no refleje un daño; d) el derecho a la privacidad deviene con la exhibición de situaciones publicadas por el afectado o por su consentimiento (Saldaña, 2012).

El presidente Richard Nixon en 1974, adopto la Privacy Act, o ley de acto privado o privacidad, la cual hace hincapié al uso indebido de información sobre los individuos de parte de las autoridades de gobierno. En efecto, se puede observar cómo el país americano puso en foco la regulación del tratamiento de los datos, desde los organismos públicos y no tanto de lo privado, como ocurre en otros países o continentes donde se centran en lo público y privado.

Otra cuestión a tener en cuenta son los llamados torts[3], que hacen referencia a cuando un individuo genera un daño o pérdida a un tercero y, por lo tanto, se genera una indemnización por esa afectación. En este sentido, esta herramienta jurídica, permite que, en caso de infracción de la privacidad de los datos personales, pueda ejercerse el uso de esta figura para resarcir, en cierta forma, el daño causado. Lo que debe dejarse en claro es que, identificar a los responsables de esa violación puede llevar tiempo, debido a que muchas veces la afectación puede originarse de manera anónima en ambientes como internet.

Principio de integridad y confidencialidad y principio de responsabilidad proactiva.

[3] En derecho anglosajón (common law) (véase derecho consuetudinario), el tort ('agravio' o 'daño', en español) se entiende como una acción o inacción perjudicial en materia civil, distinto de un incumplimiento de contrato.

El principio de integridad se centra en garantizar la existencia de una adecuada seguridad en los procesos de tratamiento de datos, sobre todo para evitar que dichos datos sean afectados por un acceso no autorizado, se pierdan o se dañen. Es importante mencionar que la integridad, junto con la confidencialidad, disponibilidad y resiliencia son los pilares de la seguridad informática.

La confidencialidad es un principio que tiende a garantizar una adecuada seguridad en los procesos de tratamiento de datos; tiende a que un dato o información no sea revelado a terceros sin el consentimiento de su titular. (SIGLO21, 2024)

Se entiende la disponibilidad como aquella que permite acceder al dato en cualquier situación, siempre que autorizados para hacerlo. De esa manera, protege al dato de cualquier persona que no esté autorizada.

La responsabilidad proactiva:

En inglés, accountability, ya que tiende a que el responsable demuestre en todo momento que cumple con la normativa en materia de protección de datos. La responsabilidad es un elemento clave a la hora de que la autoridad de control haga una valoración de la multa que se va a imponer por alguna infracción cometida.

El Derecho a la supresión de datos personales

El derecho a la supresión de datos personales, también conocido como derecho al olvido, está establecido en el RGPD[4] y puede ser ejercido por el interesado. El responsable del tratamiento está obligado a suprimir los datos personales sin demora cuando se cumpla alguna de las siguientes circunstancias:

i. Los datos personales, luego de ser usados, ya no son necesarios para los fines tratados.

ii. El interesado retira el consentimiento en el que se basaba el tratamiento y no existe otro fundamento legal para dicho tratamiento.

iii. El interesado se opone al tratamiento de sus datos en virtud del artículo 21.1 y no prevalecen otros motivos legítimos para el tratamiento, o el interesado se opone al tratamiento en virtud del artículo 21.2[5] .

iv. Los datos personales han sido tratados con un fin ilícito.

v. Los datos personales deben ser eliminados con el objeto de cumplir con una obligación legal al responsable del tratamiento.

vi. Los datos personales fueron recogidos en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8.1[6] .

Este derecho permite que los individuos tengan el control sobre la supresión de sus datos personales en ciertas situaciones y establece excepciones en casos en los que

[4] El Reglamento general de protección de datos (RGPD), la Directiva sobre protección de datos en el ámbito penal y otras normas relativas a la protección de datos personales.

[5] Reglamento de la Unión Europea 679 de 2016 [Parlamento Europeo]. Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Art. 22. 27 de abril de 2016.

[6] Reglamento de la Unión Europea 679 de 2016 [Parlamento Europeo]. Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Art. 8. 27 de abril de 2016.

el tratamiento de datos es necesario por razones legales, de interés público o para el ejercicio de derechos fundamentales. (SIGLO21, 2024)

Un ejemplo de cómo se puede materializar el uso de este derecho: Si Ud publica sus datos o contenido en un sitio WEB, y luego de un tiempo determinado desea que sus datos sean eliminados, y que ya no tenga acceso el público en general, Ud podría ejercer el "derecho al olvido", en virtud del RGPD y solicitar al responsable del tratamiento que suprima esos datos personales.

El responsable del tratamiento, tras recibir la solicitud, deberá evaluar si se cumplen las condiciones establecidas en el RGPD para la supresión de los datos. Si los datos ya no son necesarios para los fines para los que fueron recogidos, si el consentimiento ha sido retirado y no hay otro fundamento legal para el tratamiento, o si existen otros motivos legítimos para la supresión, el responsable deberá eliminar los datos personales de manera oportuna y sin demora indebida.

Una vez que se haya llevado a cabo la supresión de los datos, la información personal dejará de estar disponible públicamente y no podrá ser encontrada a través de motores de búsqueda u otros medios. Esto permite a la persona ejercer su derecho al olvido y proteger su privacidad en línea. (SIGLO21, 2024)

Respecto de las redes sociales

Las redes sociales están sujetas a las disposiciones del RGPD y la LOPDGDD (Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales)[7] en lo que respecta a la protección de datos personales. Estas regulaciones establecen ciertas obligaciones y principios que las redes sociales deben cumplir para garantizar la privacidad y protección de los datos de sus usuarios. A continuación, se presentan algunos aspectos relevantes:

a) Consentimiento informado: las redes sociales deben obtener el consentimiento explícito y libremente dado por los usuarios antes de recopilar y procesar sus datos personales. El consentimiento debe ser específico, inequívoco y basado en información clara sobre cómo se utilizarán los datos.

b) Información transparente: las redes sociales están obligadas a proporcionar a los usuarios información clara y concisa sobre cómo se recopilan, utilizan y procesan sus datos personales. Esto incluye detalles sobre los fines del tratamiento, las categorías de datos recopilados, los plazos de retención, los destinatarios de los datos y los derechos de los usuarios.

c) Derechos de los usuarios: las redes sociales deben garantizar el ejercicio de los derechos de los usuarios, como el derecho de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición. Deben proporcionar mecanismos y procedimientos para que los usuarios puedan ejercer estos derechos de manera efectiva.

d) Seguridad de los datos: las redes sociales deben aplicar medidas técnicas y organizativas adecuadas para proteger los datos personales de los usuarios contra el acceso no autorizado, la pérdida o la alteración. También deben informar a los usuarios en caso de violaciones de seguridad que puedan afectar sus datos.

[7] Ley Orgánica 3 de 2018 [Felipe VI, rey de España]. Por la cual se establece la protección de datos personales y garantía de los derechos digitales. 5 de diciembre de 2018. BOE-A-2018-16673.

e) Transferencias internacionales de datos: si las redes sociales transfieren datos personales a países fuera de la Unión Europea, deben garantizar que existan garantías adecuadas para proteger esos datos, como cláusulas contractuales estándar o el cumplimiento de esquemas de certificación reconocidos

f) Responsabilidad y registro de actividades: las redes sociales son responsables del cumplimiento de las regulaciones de protección de datos. Deben llevar un registro de las actividades de tratamiento de datos que realizan y demostrar el cumplimiento de los principios y requisitos legales. (SIGLO21, 2024)

En España, se abordan varios aspectos relacionados con las redes sociales y los derechos digitales de los usuarios. Algunos puntos relevantes son los siguientes:

a) Derecho al olvido: La LOPDGDD reconoce el derecho al olvido digital, que permite a los usuarios solicitar la eliminación de información personal que ya no es relevante, precisa o actual, especialmente en el contexto de las redes sociales.

b) Derecho a la portabilidad de datos: los usuarios tienen derecho a solicitar a las redes sociales que transfieran sus datos personales a otro proveedor de servicios en un formato, cuando sea técnicamente posible.

c) Derecho a la intimidad y uso de dispositivos: la ley protege el derecho de los usuarios a la intimidad en el uso de dispositivos electrónicos y servicios de comunicaciones electrónicas, incluyendo las redes sociales. Se establecen garantías para prevenir accesos no autorizados a dispositivos y para proteger la privacidad en las comunicaciones.

d) Derecho a la desconexión digital: los trabajadores tienen derecho a la desconexión digital fuera de su horario laboral, lo que implica que no se les puede exigir responder correos electrónicos o mensajes relacionados con el trabajo durante su tiempo libre.

e) Derechos de los menores en línea: la ley presta especial atención a la protección de los derechos de los menores en el entorno digital. Se establecen medidas para garantizar su seguridad y privacidad en las redes sociales, incluyendo la necesidad de obtener el consentimiento de los padres o tutores legales antes de recopilar datos personales de menores.

Esta ley, también establece obligaciones para los proveedores de servicios en línea, incluyendo las redes sociales, en términos de seguridad de datos, notificación de brechas de seguridad, designación de delegados de protección de datos y cumplimiento de las disposiciones de la ley en materia de protección de datos. (SIGLO21, 2024)

Bibliografía y citas

- Agencia de Acceso a la Información Pública, (2022). Aportes, opiniones y comentariosrecibidos en el proceso de Elaboración Participativa de Normas con relación al anteproyecto deLey de Protección de Datos Personales.https://www.argentina.gob.ar/sites/default/files/anexo4.pdf
- ALTABIR, (s.f.). ¿Qué es el consentimiento del interesado? https://www.altabir.es/consentimiento-interesado-lopd/
- Ayudaley, (2020). Seguridad de la información: aspectos a

tener en cuenta.https://ayudaleyproteccion datos.es/2020/07/14/seguridad-de-la-informacion/

- Grupo ATICO34, (s.f.). Consentimiento expreso: qué es y cómo conseguirlo para el tratamientode datos de carácter personal. https://protecciondatos-lopd.com/empresas/consentimiento-expreso/
- Ley 25326 de 2000. Protección de datos personales. 30 de octubre de 2000.
- Ley Orgánica 3 de 2018 [Felipe VI, rey de España]. Por la cual se establece la protección de datos personales y garantía de los derechos digitales. 5 de diciembre de 2018. BOE-A-2018-16673.
- Lico, M. (s.f.). Breve estudio de los principios generales del Derecho y de los principios generalesdel Derecho aplicables y surgidos del Derecho Administrativo. Gobierno de Buenos Aires.https://buenosaires.gob.ar/procuracion-general/breve-estudio-de-los-principios-generales-del-derecho-y-de-los-principios
- Reglamento UE 679 de 2016. Protección de las personas físicas en lo que respecta altratamiento de datos personales y a la libre circulación de estos datos. 27 de abril de 2016
- SIGNATURIT, (2018). GDPR: ¿qué medidas de responsabilidad proactiva exige?https://blog.signaturit.com/es/gdpr-que-medidas-de-responsabilidad-proactiva-exige
- Agencia Española de Protección de Datos (AEPD) (2022). Guia para el ciudadano. Agencia Española de Protección de Datos. https://www.aepd.es/sites/default/files/2020-05/guia-ciudadano.pdf
- Agencia Española de Protección de Datos (AEPD) (2022). Guia sobre el uso de las cookies. Agencia Española de Protección de Datos. https://www.aepd.es/es/documento/guia-cookies.pdf
- Diario Oficial de la Unión Europea (2002). Directiva 2002/58/CE relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Recuperado https://www.boe.es/doue/2002/201/L00037-00047.pdf
- Diario Oficial de la Unión Europea (2002). Directiva 2002/22/CE relativa a las comunicaciones electrónicas y servicios. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32002L0022
- Diario Oficial de la Unión Europea (2016). Directiva 2016/679/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. https://www.boe.es/doue/2016/119/L00001-00088.pdf