EL DERECHO AL OLVIDO EN LOS TIEMPOS DEL INTERNET. (Segunda Entrega)

Por

Emilio Tafur Charun

1.-EXORDIO

Curaca Kong (719:2022) manifiesta que, "Ya con la llegada del internet, se ha dado paso a la llamada sociedad de la información o de la transparencia, que está caracterizada por el rol preponderante que tiene el uso de la información en nuestra vida diaria, ocupando muchos aspectos de nuestra vida como el social, político, financiero u otros. El internet es la columna de la sociedad de la información que permite el uso masivo de datos y, como decía Luis Mieres, el internet resulta ser el foro público en virtud del cual millones de personas se expresan, pero también se informan. En este, la información se ingresa de manera masiva cada microsegundo, ello se le conoce como "Big data", cuyo procesamiento precisa el uso de aplicaciones no convencionales".

Según Raffo Velásquez Meléndez (66:2025), "Las nuevas tecnologías plantean desafíos inéditos a la protección de la vida privada al generar riesgos sustantivos que trascienden los paradigmas tradicionales. La magnitud de los cambios es tal que los mecanismos previstos originariamente por el constituyente –como la telefonía fija, el telegrama o las cartas– han quedado obsoletos en términos prácticos, pese a regularse aún bajo el principio de la inviolabilidad de las comunicaciones".

De otro lado y como antecedente de la presente entrega escribimos un artículo intitulado "El Derecho Al Olvido. Pasarán más de mil años muchos más". Ella fue la primera entrega que sobre esta materia hicimos. Ahora bien, y a efectos de repasar el contenido de la entrega precedente hemos tomado en préstamo la reseña impecablemente escrita por el Doctor Mario Castillo Freyre, editor de la publicación del aludido artículo. La reseña que deviene en inmejorable, es como sigue:

“Se trata de una reflexión especialmente pertinente sobre el impacto de la era digital en la protección de los datos personales y en la construcción jurídica del llamado derecho al olvido📜

A lo largo del texto, el autor desarrolla con solvencia la tensión entre autodeterminación informativa e interés público, destacando que la protección de la privacidad no puede entenderse de manera aislada, sino en diálogo con otros derechos fundamentales, como la libertad de expresión y el acceso a la información. Asimismo, examina el alcance de la Ley N.º 29733, sus principios de finalidad y proporcionalidad, y los mecanismos administrativos y jurisdiccionales previstos para la tutela de los datos personales”🔎

Una lectura imprescindible para comprender, desde una perspectiva doctrinal y jurisprudencial, los alcances y límites del derecho al olvido en el ordenamiento peruano”.

2.- ELEMENTOS BASILARES

Y es que, como ya lo hemos indicado en la entrega precedente, el *quid* de esta materia en estudio es una confrontación entre dos derechos fundamentales que de este modo se encuentran en una relación de tensión: autodeterminación informativa, de un lado y del otro, la libertad de expresión junto con el derecho al acceso de la información. Resulta importante indicar que los Derechos a la libertad de expresión y a la información encuentran un respaldo imprescindible para así operar. Nos referimos al interés público. A través de la ponderación y razonabilidad que suponen la relación entre ambos derechos será la autoridad la que resuelva esta disyuntiva.

Sobre el particular, Velásquez Meléndez (68:2025) sostiene que, “Algunas veces puede justificarse el acceso y difusión de los datos alegando que su contenido atañe al interés público (como la revelación de hechos noticiosos, delitos u otros valores constitucionalmente superiores). En tales casos, la tutela formal basada en la ‘expectativa razonable de privacidad’ deberá ponderarse con dichos intereses contrapuestos. Este análisis determinará si la divulgación está constitucionalmente amparada por su contribución al interés público o si, por el contrario, prima el derecho a la intimidad por carecer de la información de interés público.”

El mismo autor (68:2025) se muestra añadiendo que, “Por tanto, cuando se pretende difundir información protegida por una ‘expectativa razonable de privacidad’, resulta imperativo realizar un juicio de ponderación para determinar la existencia de un interés público en ello. Si no existe, prevalecerá la protección formal del derecho a la intimidad, proscribiéndose su difusión (sin importar su contenido íntimo o no). Sin embargo, si se determina la existencia de un interés público en los datos obtenidos, se podrá difundir solo aquellos aspectos relevantes a dicho interés. Aquí, adquiere plena vigencia la dimensión material del derecho, que exige la exclusión de todo dato intrínsecamente íntimo, garantizando que la afectación a la privacidad no exceda lo indispensable para satisfacer el fin público legítimo perseguido.”

Entendemos que cuando este autor alude a 'expectativa razonable de privacidad' se está refiriendo a la "autodeterminación informativa".

Es de indicar que en la primera entrega nos hemos referido al Exp. Nº 03041-2021-PHD/T. Sobre este mismo caso el Tribunal Constitucional, a través de su Oficina de Información Institucional ha emitido con fecha 15-8-2022, una nota de prensa en la cual se precisa los alcances sobre el derecho al olvido y crea jurisprudencia a favor de la libertad de prensa. En su parte pertinente la nota de prensa precisa que "además que toda investigación contra una persona, en cualquier nivel, sobre presuntos vínculos con narcotráfico y el terrorismo goza de la más alta relevancia e interés público, y constituye, a todas luces, un hecho noticioso que debe ser objeto de escrutinio a través del ejercicio del derecho fundamental a la libertad de información.

Respecto al derecho al olvido, el TC señaló que no obstante ser un derecho fundamental, también está sujeto a restricciones o limitaciones derivadas de la necesidad de armonizar su contenido con otros derechos o bienes constitucionales, por lo que es posible sostener una tensión con el derecho fundamental a la libertad de información reconocido en el artículo 2 inciso 4 de la Constitución".

Según Alfredo Orlando Curaca Kong (721: 2022) en el Perú, contamos en sede administrativa con la Autoridad Nacional de Protección de Datos, que a nivel administrativo fue la primera en pronunciarse sobre el derecho al olvido varios años. Sus decisiones, como es lógico, también pueden ser cuestionadas en sede judicial a través de la vía contencioso administrativa, lo que permite que se toque el tema desde la justicia ordinaria. Empero, por otro lado, y como ya ha sido manifestado, existe también en nuestro país el Hábeas Data, que protege tanto el derecho de acceso a la información pública y el derecho de autodeterminación informativa y brinda, entre otros, la posibilidad de suprimir el dato cuando atenta contra derechos fundamentales, como ya se dijo.

El mismo autor (720:2022) cita a María Álvarez Caro, para quien el derecho al olvido deriva de los derechos a la intimidad y a la protección de datos personales, y "…podría definirse como el derecho a equivocarse *o a que una equivocación pasada no marque y determine la vida de un individuo que, por definición, no es otra cosa que un proceso evolutivo, una secuencia de aciertos y errores, siempre en proceso de conformación, de cambio y de evolución constante."* Añade, asimismo, que "Se conoce como derecho al olvido, a un interés jurídicamente protegido de los ciudadanos que consiste en lograr efectivamente que sus datos personales no sean localizados por los buscadores en la Red." En tal sentido, compartimos el criterio de que "*No se trata de exigir el borrado de los datos porque éstos no son exactos o ciertos, sino porque el titular de los mismos considera que le perjudican y estima asimismo que no existe ningún fin que legitime la disponibilidad de dichos datos por parte de terceros."* (Las cursivas son nuestras)

La autora citada refiere "(…) que no existe ningún fin que legitime la disponibilidad de dichos (sic) por parte de terceros". Como veremos *infra,* este aserto se relaciona con el principio de finalidad.

Por nuestra parte, creemos que el derecho al libre desarrollo de la personalidad y el derecho a un proyecto de vida se vincularían estrechamente al derecho de protección de datos y constituirían en buena cuenta, la *ratio* del reconocimiento de este en el ámbito del ordenamiento jurídico. Pero no solo eso. Debemos también tener en cuenta al Derecho al olvido. Queda claro que esto se configuraría cuando el banco de datos de que se trate contenga información derogatoria o vulneradora del titular del derecho. Información derogatoria o vulneradora que puede frustrar o echar a perder el libre derecho al desarrollo de la personalidad y al proyecto de vida del agraviado. De este modo, y esto lo decimos en condicional, el Derecho al olvido además de proteger al titular de la información de contenidos que sean inexactos, sea por ser agraviantes, falsos, desactualizados o extemporáneos, la autoridad competente debe también ocuparse de llevar a cabo un examen de idoneidad, necesidad, proporcionalidad y razonabilidad, para asegurar en alguna medida, que no se está afectando el Derecho a la autodeterminación informativa del titular de datos, y junto con tal derecho, el libre derecho de desarrollo de su personalidad y su proyecto de vida. Lo aquí dicho solo es un planteamiento o una postura por demás inocuo y, si se quiere, meramente provisional.

Así y, de una parte, el interés público en tanto extremo de esta confrontación con la autodeterminación informativa, encuentra, entre otros a los cuales ya hemos aludido, su elemento basilar en el artículo 1, *ab initio*, de Ley 27806 (Ley de Transparencia y Acceso a la Información pública). El texto de este artículo es como sigue: "La presente Ley tiene por finalidad promover la transparencia de los actos del Estado *y regular el derecho fundamental del acceso a la información* consagrado en el numeral 5 del artículo 2 de la Constitución Política del Perú." (Las cursivas son nuestras) En este contexto, según el artículo 2 numeral 5 de la Carta de 1993, "Toda persona tiene derecho a solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional." Como respaldo del interés público que gatilla la libertad de expresión y el Derecho al acceso de la información, encontramos el Decreto Legislativo 1353, Decreto Legislativo que crea la Autoridad Nacional de Transparencia y acceso a la Información Pública, Fortalece el régimen de protección de datos personales y la Regulación de la Gestión de intereses.

Según el artículo primero de La Ley 29733 (Ley de Protección de Datos Personales) en adelante la Ley, esta tiene por objeto garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen.

El artículo 18 de la Ley detalla prolijamente qué información debe proveer el titular del banco de datos al titular de los datos personales, información que resulta siendo fundamental, para que este último dé un consentimiento informado y reduciendo así la asimetría informativa que siempre resulta siendo inevitable. De este modo el artículo 18 de la Ley refiere que, "El titular de datos personales tiene derecho a ser informado en

forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados; quiénes son o pueden ser sus destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y, de ser el caso, del o de los encargados del tratamiento de sus datos personales; el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles; la transferencia de los datos personales; las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; el tiempo durante el cual se conserven sus datos personales; y la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello. Si los datos personales son recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones del presente artículo pueden satisfacerse mediante la publicación de políticas de privacidad, las que deben ser fácilmente accesibles e identificables. En el caso que el titular del banco de datos establezca vinculación con un encargado de tratamiento de manera posterior al consentimiento, el accionar del encargado queda bajo responsabilidad del Titular del Banco de Datos, debiendo establecer un mecanismo de información personalizado para el titular de los datos personales sobre dicho nuevo encargado de tratamiento. Si con posterioridad al consentimiento se produce la transferencia de datos personales por fusión, adquisición de cartera, o supuestos similares, el nuevo titular del banco de datos debe establecer un mecanismo de información eficaz para el titular de los datos personales sobre dicho nuevo encargado de tratamiento".

El artículo 19 de la Ley, por su parte, prescribe que, "El titular de datos personales tiene derecho a obtener la información que sobre sí mismo sea objeto de tratamiento en bancos de datos de administración pública o privada, la forma en que sus datos fueron recopilados, las razones que motivaron su recopilación y a solicitud de quién se realizó la recopilación, así como las transferencias realizadas o que se prevén hacer de ellos."

3.-DERECHO DE ACCESO A LA INFORMACION

Desarrollando esta normativa el artículo 7 de la Ley 27086 - Ley de Transparencia y Acceso a la Información Pública - preceptúa que, "Toda persona tiene derecho a solicitar y recibir información de cualquier entidad de la Administración Pública. En ningún caso se exige expresión de causa para el ejercicio de este derecho."

Igualmente, conforme al artículo 12.3 del Decreto Supremo 029-2021-PCM, reglamento del Decreto Legislativo 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital- "Los ciudadanos digitales tienen los siguientes derechos: a) Derecho fundamental a la igualdad, garantizando su libre, igualitario y no discriminado acceso, con especial incidencia en las poblaciones vulnerables, en atención a lo previsto en el artículo 2 numeral 2 de la Constitución Política del Perú*. b) Derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, y conforme a lo establecido en la Ley N.º 29733, Ley de Protección de Datos Personales y su Reglamento*. *c) Derecho fundamental de acceder a la información considerando lo establecido sobre el secreto bancario y la reserva tributaria de acuerdo con lo previsto en el artículo 2 numeral 5 de la Constitución Política del Perú y el artículo*

85 del Código Tributario. d) Derecho fundamental al honor y a la buena reputación, intimidad personal y familiar, en atención a lo previsto en el artículo 2 numeral 7 de la Constitución Política del Perú. (Las cursivas son nuestras).

Los literales f) y g) del artículo 24 del mismo reglamento preceptúan lo siguiente:

f) Conservación de la información. Se garantiza que las comunicaciones y documentos generados en entornos digitales, se conservan en las mismas o mejores condiciones que aquellas utilizadas por los medios tradicionales, de acuerdo con la normatividad de la materia.

g) Seguridad desde el diseño. Los servicios digitales se diseñan y desarrollan preservando la disponibilidad, integridad, confidencialidad de la información que gestiona y, cuando corresponda, la autenticidad y no repudio de la información proporcionada.

4.-LAS DOS CARAS DE JANO

Oscar Puccinelli (237:2016) sostiene que jurídicamente, uno de los aspectos más relevantes de este fenómeno se relaciona con el «derecho a la información», disciplina en la que chocan dos grandes principios: el de máxima publicidad, propio de las leyes de acceso a la información pública, y el de mínima divulgación, vigente en el plano del tratamiento de los datos personales. De este modo, como Jano, el derecho a la información tiene dos caras que miran hacia esos dos lados diametralmente opuestos, de modo que el operador jurídico se enfrenta a verdaderos dilemas a la hora de resolver conflictos donde ambos aspectos forman parte de un conflicto generado en un caso concreto, por ejemplo frente a la divulgación de información de interés público, que precisamente al ser puesta en conocimiento de terceros puede afectar severamente a derechos fundamentales de los involucrados en ella (v.gr., intimidad, dignidad, libertad, buen nombre, crédito, etc.).

El mismo autor (239:2016) señala que: «Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes *a los fines para los cuales hubiesen sido recolectados*» (El énfasis es nuestro)

5.-PRINCIPIO DE FINALIDAD

El artículo IX de la Ley, desarrolla sobre la materia de los principios rectores y dispone que, El titular del banco de datos personales, o en su caso, quien resulte responsable del tratamiento de datos personales***, debe cumplir con el régimen jurídico en materia de protección de los datos personales de acuerdo con los principios rectores establecidos en la Ley (…)*** (El énfasis es nuestro)

A su vez, el artículo 12 se refiere al valor de los principios. Tal precepto nos dice que, "La actuación de los titulares y encargados de tratamiento de datos personales y, en general, de todos los que intervengan con relación a datos personales, debe ajustarse a los principios rectores a que se refiere este Título. Esta relación de principios rectores es enunciativa. Los principios rectores señalados sirven también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de esta Ley y de su

reglamento, así como de parámetro para la elaboración de otras disposiciones y para suplir vacíos en la legislación sobre la materia."

El artículo 6 de la Ley define el principio de finalidad estableciendo que, "Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización".

Y esto nos da luces sobre la finalidad y función del agente que fuere pues estos dos elementos son imprescindibles para dar legitimidad y legalidad a la recolección de datos. Son auténticos principios rectores. Nos explicamos: el acto jurídico por el cual se recolectan los datos debe tener una finalidad y función que sean valiosas y así ser validados y acogidos por el ordenamiento jurídico. De otro modo, tal acto jurídico, al no tener un fin valioso y más aun pudiendo ser arbitrario por exceso de poder o por lo que fuera, debe ser descartado por ser ilegal e ilegitimo, y dado esto, el mismo ha de ser objeto de supresión en ejercicio del Derecho al olvido.

Sobre el mismo principio, el Artículo 6 del Reglamento de la Ley, Decreto Supremo N.º 016-2024-JUS, artículo que trata sobre consentimiento informado, señala en su numeral 6.2 que cuando los datos personales son obtenidos directamente del titular de los datos personales se le debe comunicar de forma clara, con lenguaje sencillo, cuando menos lo siguiente: (…)2. ***La finalidad o finalidades del tratamiento a las que sus datos son sometidos (…).*** Asimismo, según el artículo 1.1.2 *la solicitud del consentimiento debe estar referida a un tratamiento o serie de tratamientos determinados,* ***con expresa identificación de la finalidad o finalidades*** *para las que se recaban los datos.* Por su parte el artículo *10.2* determina que, "El titular de los datos personales puede negar o revocar su consentimiento al tratamiento de sus datos personales para ***finalidades*** adicionales a aquellas que dan lugar a su tratamiento autorizado (…)." El artículo 82.1 del mismo reglamento relieva la importancia del principio de finalidad al aludir a elementos del mayor sustrato en esta disciplina como son la Supresión o Cancelación. El texto pertinente prescribe que, "El titular de los datos personales puede solicitar la supresión o cancelación de sus datos personales cuando estos hayan dejado de ser necesarios o pertinentes para ***la finalidad*** para la cual hayan sido recopilados (…)". Más específico es el artículo 27.2 del mismo reglamento el cual refiere que, "***Los operadores de los servicios de comunicaciones o telecomunicaciones*** no pueden realizar un tratamiento de los citados datos personales para ***finalidades*** distintas a las autorizadas por su titular, salvo orden judicial o mandato legal expreso." (El énfasis es nuestro).

No obstante ello, el Artículo 7 de la Ley 27806 -Ley de transparencia y acceso a la información pública"-prescribe que "Toda persona tiene derecho a solicitar y recibir información de cualquier entidad de la Administración Pública. *En ningún caso se exige expresión de causa para el ejercicio de este derecho.* (El énfasis es nuestro)

De tal suerte, se dispone, como una presunción que bien puede ser *iuris tantum*, que el recojo de la información pública es en ejercicio legítimo y regular de un derecho. Y además estaremos, presuntamente, frente a una finalidad cuya consecución no agravia el ordenamiento jurídico. Todo lo contrario.

Resulta, así, aplicable y lo reiteramos, que según el artículo 1.1.2 del reglamento de la Ley, "*La solicitud del consentimiento debe estar referida a un tratamiento o serie de tratamientos determinados,* ***con expresa identificación de la finalidad o finalidades*** para las que se recaban los datos. Así como las demás condiciones que concurran en el tratamiento o tratamientos, sin perjuicio de lo dispuesto en el siguiente artículo sobre las características del consentimiento". (El énfasis es nuestro)

Al respecto, el artículo 18.4 del Decreto Legislativo 1412 -Ley de Gobierno Digital- dispone como obligación de la entidad a cargo de la custodia de la información el, "Facilitar el acceso a la información requerida por otra entidad de la Administración Pública, sobre los datos de las personas que obren en su poder y se encuentren en soporte electrónico, *únicamente para el ejercicio de sus funciones en el ámbito de sus competencias*.". Aquí tenemos otra alusión al Principio de finalidad. (El énfasis es nuestro)

En el sector público tenemos las siguientes entidades, entre otras, que bien pueden ser tenedores de información sensible: el Ministerio de Justicia y Derechos Humanos (MINJUSDH), la Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT), el Registro Nacional de Identificación y Estado Civil (RENIEC), la Superintendencia Nacional de Educación Universitaria (SUNEDU), el Ministerio de Educación (MINEDU), el Ministerio de Salud (MINSA), el Ministerio del Interior (MININTER), la Contraloría General de la República (CGR), el Organismo Especializado para las Contrataciones Públicas Eficientes (OECE) y el Poder Judicial (PJ).

6.-DERECHO DE TUTELA.

El artículo 10 de la Ley establece el Principio de disposición de recurso. Esto es, todo titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales.

El artículo 24*, ab initio*, de la Ley alude al "Derecho a la tutela". Esto es, "en caso de que el titular o el encargado del banco de datos personales deniegue al titular de datos personales, total o parcialmente, el ejercicio de los derechos establecidos en esta Ley, este puede recurrir ante la Autoridad Nacional de Protección de Datos Personales en vía de reclamación o *al Poder Judicial para los efectos de la correspondiente acción de hábeas data.* (El énfasis es nuestro)

Conforme al artículo 25 de la Ley, y esto resulta de la mayor importancia, "El titular de datos personales que sea afectado a consecuencia del incumplimiento de la presente Ley por el titular o por el encargado del banco de datos personales o por terceros, tiene derecho a obtener la indemnización correspondiente, conforme a ley".

El artículo 88.1 del reglamento prevé que, “El ejercicio de los derechos regulados por la Ley y el presente Reglamento se inicia con la solicitud que el titular de los datos personales debe dirigir directamente al titular del banco de datos personales o responsable del tratamiento”.

Más aun, de acuerdo con el artículo 88.2 del reglamento, “El titular del banco de datos personales o responsable del tratamiento debe dar respuesta, en los plazos previstos en el presente Reglamento, expresando lo correspondiente a cada uno de los extremos de la solicitud. Transcurrido el plazo sin haber recibido la respuesta el solicitante puede considerar denegada su solicitud.”

El artículo 88.3 del mismo reglamento, establece que, “La denegatoria o la respuesta insatisfactoria habilitan al solicitante a iniciar el procedimiento administrativo ante la Dirección de Protección de Datos Personales.”

El artículo 32.2 del Decreto Supremo 029-2021-PCM - Decreto Supremo que aprueba el Reglamento de la Ley de Gobierno Digital- es nítido cuando señala que, “Las entidades de la Administración Pública son responsables de la integridad, veracidad y actualización de la información, contenidos digitales y servicios digitales que presten a través de su respectiva sede digital”.

De modo previo y para justificar la participación de los administrados en lo que a custodia de datos se refiere, dentro del marco normativo aplicable, es de citarse el artículo 5.2 del Decreto Legislativo 1412, norma que aprueba la Ley de Gobierno Digital. El mencionado artículo precisa que, “El ejercicio de la identidad digital para el uso y prestación de servicios digitales *confiere y reconoce a las personas las mismas garantías que otorgan los modos tradicionales de relacionarse entre privados y/o en la relación con las entidades de la Administración Pública”.* (Las cursivas son nuestras)

Es por ello que se justifica y legitima la aplicación del Código Civil a efectos de interpretar el artículo 25 de la Ley.

Como refuerzo de lo dicho, el reglamento de la Ley, en diversos numerales de su artículo 4 determina el régimen de aplicación de la normativa materia de protección de datos personales:

4.3 La existencia de normas o regímenes particulares o especiales, aun cuando incluyan regulaciones o instituciones privadas a las que dichos regímenes se aplican del ámbito de aplicación de la Ley y del presente Reglamento.

4.4 Lo dispuesto en el párrafo precedente no implica la derogatoria o inaplicación de las normas particulares, en tanto su aplicación no genere la afectación del derecho a la protección de datos personales, sobre datos personales, no excluye a las entidades públicas o instituciones privadas a las que dichos regímenes se aplican del ámbito de aplicación de la Ley y del presente Reglamento.

Tal es el caso del Decreto Supremo 002-2009- MINAM que aprueba el Reglamento sobre transparencia, acceso a la información pública ambiental y participación y consulta

ciudadana en asuntos ambientales. El artículo 2 de este reglamento prescribe que, "Las disposiciones establecidas en el presente Reglamento son de aplicación obligatoria para el MINAM y sus organismos adscritos; asimismo, será de aplicación para las demás entidades y órganos que forman parte del Sistema Nacional de Gestión Ambiental o desempeñan funciones ambientales en todos sus niveles nacional, regional y local, siempre que no tengan normas vigentes sobre las materias reguladas en este Reglamento."

Se podrá notar que estamos ante una antinomia. Dos normas del mismo grado y cuyos contenidos colisionan frontalmente. Inclusive ambas normas invocan su supremacía cuando se configura tal supuesto. Nos parece que en este asunto ha de prevalecer la norma especial. Esto es, el Decreto Supremo 002-2009- MINAM.

6.1.-RESPONSABILIDAD CIVIL

De otro lado, este artículo 25 de la Ley es por demás interesante. Nos lleva a preguntarnos lo siguiente:

a) ¿Estamos frente a un incumplimiento de naturaleza contractual o extracontractual? ¿Cuál es su naturaleza en caso que el responsable haya delegado la función de custodia de datos en un tercero con el que tiene a su vez una relación laboral o una locación de servicios?
b) ¿Estamos frente a una responsabilidad objetiva o responsabilidad subjetiva?
c) ¿Puede obtenerse una indemnización de daños y perjuicios por la vía del habeas data?

Desarrollo:

a) En principio entendemos que estaremos ante un caso de responsabilidad contractual. El artículo 5 de la Ley preceptúa que, "Para el tratamiento de los datos personales debe mediar el consentimiento de su titular". Habrá una relación jurídica patrimonial entre el agraviado y el titular del banco de datos quien conserva la información. Estamos frente a una obligación de no hacer que nace de la voluntad. Queda claro: La obligación de no hacer, esto es, de abstenerse, nace de la Ley y de la voluntad (Nos referimos a la Ley 29733). El artículo 1 del reglamento de la Ley, alude al consentimiento para el tratamiento de datos personales. De acuerdo al artículo 1.1 el titular del banco de datos personales o quien resulte como responsable del tratamiento, debe obtener el consentimiento para el tratamiento de los datos personales, de conformidad con lo establecido en la Ley y en el presente Reglamento, salvo los supuestos establecidos en el artículo 14 de la Ley, pues en estos no se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento. Entre otros, tenemos el numeral 2 del mencionado artículo 14, que prevé: "Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público". Mas allá de lo previsto por el artículo 14 de la Ley, estaremos en suma en un caso de relación contractual con todo lo que ello supone. Y este último supuesto es ya de por sí importante, pues

permite con anticipación establecer v.g. una cláusula penal, lo que permite saber a cuánto aproximadamente, quizá, ascenderá la eventual indemnización por daños y perjuicios dada la inejecución de obligaciones. Pero dentro del supuesto que estamos tratando, conllevará la ejecución de obligaciones accesorias que tendrán la naturaleza de obligación de hacer. Así, por lo pronto, la obligación a cargo del titular del banco de datos de hacer su mejor esfuerzo para custodiar permanentemente la data (tratamiento), en este caso, ello demanda especial diligencia dado, supuestamente, el especial valor de ella. Esto es recogido por el artículo 9 de la Ley cuyo texto es: El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.
En lo referente a la participación de un tercero en la conservación y custodia de la información entendemos que se configurará una responsabilidad vicaria. Y decimos ello, a sabiendas que es un tipo de responsabilidad el cual el Código Civil es ubérrimo en su positivación. Así, tenemos los siguientes artículos del Código Civil en donde se alude a este tipo de responsabilidad:

Artículo 1325º.- El deudor que para ejecutar la obligación se vale de terceros, responde de los hechos dolosos o culposos de éstos, salvo pacto en contrario.

Artículo 1766º.- El locador debe prestar personalmente el servicio, pero puede valerse, bajo su propia dirección y responsabilidad, de auxiliares y sustitutos si la colaboración de otros está permitida por el contrato o por los usos y no es incompatible con la naturaleza de la prestación.

Artículo 1772º.- El contratista no puede subcontratar íntegramente la realización de la obra, salvo autorización escrita del comitente. La responsabilidad frente al comitente es solidaria entre el contratista y el subcontratista, respecto de la materia del subcontrato.

Artículo 1981º.- Aquél que tenga a otro bajo sus órdenes responde por el daño causado por este último, si ese daño se realizó en el ejercicio del cargo o en cumplimiento del servicio respectivo. El autor directo y el autor indirecto están sujetos a responsabilidad solidaria.

Pero la normatividad sobre la protección de datos, no es ajena a este asunto. Esto es, responsabilidad vicaria. El artículo 38, *ab initio,* del reglamento de la Ley se refiere a la responsabilidad del tercero subcontratado. El texto es así: “La persona natural o jurídica subcontratada asume las mismas obligaciones que se establezcan para el encargado del tratamiento en la Ley, el presente reglamento y demás disposiciones aplicables”.

También es de citarse el Artículo 33 del reglamento de la Ley. Este artículo indica que, “La persona natural o jurídica subcontratada asume las mismas obligaciones que se establezcan para el encargado del tratamiento en la Ley, el presente

Reglamento y demás disposiciones aplicables. Sin embargo, asume las obligaciones del titular del banco de datos personales cuando: 1. Destine o utilice los datos personales con una *finalidad* distinta a la autorizada por el titular del banco de datos o responsable del tratamiento; o, 2. Efectúe una transferencia, incumpliendo las instrucciones del titular del banco de datos personales, aun cuando sea para la conservación de dichos datos."

b) Para la dación del presente literal nos basamos en los siguientes artículos del Código Civil cuyo texto es como sigue:
Artículo 1969º.- Aquel que por dolo o culpa causa un daño a otro está obligado a indemnizarlo. El descargo por falta de dolo o culpa corresponde a su autor.
Artículo 1970º.- Aquel que mediante un bien riesgoso o peligroso, o por el ejercicio de una actividad riesgosa o peligrosa, causa un daño a otro, está obligado a repararlo.
Se trata, en efecto, de dilucidar si en la materia objeto de estudio y en caso de tratarse de una relación extracontractual, en el cual no se requiere el consentimiento del titular de los datos (art. 14 de la Ley), resulta aplicable el artículo 1969 (responsabilidad subjetiva) o el artículo 1970 (responsabilidad objetiva). En el caso de la responsabilidad contractual el tema es pacifico, y por ello no lo trataremos.
Creemos que el *quid* de este asunto radica en dilucidar los alcances del artículo 1970 el cual, como hemos visto e interpretado, importa que el actor que se beneficia mediante un bien riesgoso o peligroso, o por el ejercicio de una actividad riesgosa o peligrosa, causa un daño a otro, está obligado a repararlo.
Entonces, cabe preguntarse si la custodia de documentos o información sensible implica el uso beneficioso de un bien riesgoso o peligroso o también puede suponer el ejercicio de una actividad riesgosa o peligrosa. De darse ello estaríamos frente a una responsabilidad objetiva. En este contexto, no existe el deber de probar si el tenedor de la data actuó con culpa o dolo. Basta que se haya beneficiado del uso de un bien o actividad riesgoso o peligroso.
Dada la sofisticación de los motores de búsqueda de datos y la potencia que tienen los mismos para conservar la información y a la vez diseminarla y difundirla, creemos que estamos frente a un bien y actividad riesgoso y peligroso.
Pero no se puede generalizar, el Derecho al olvido no se reduce al uso del Internet y a combatir su mal uso, también importa el uso de bienes y actividades menos sofisticados y menos aún peligrosos o riesgosos.

Imaginemos una Municipalidad de Centro Poblado Menor. En este caso no habrá bien ni actividad peligrosa o riesgosa que se pueda invocar. De esta manera resultará aplicable el artículo 1969 del Código Civil. Esto es, responsabilidad subjetiva. Habrá entonces que probar que se actuó con dolo o culpa.

Reiteramos que otro supuesto donde no se configurará la necesidad de brindar consentimiento, y por ello, la responsabilidad será extracontractual, es lo previsto por el ya citado artículo 14 de la Ley.

6.2.-INDEMNIZACION

De otro lado, no hemos encontrado en el Nuevo Código Procesal Constitucional alusión alguna al derecho a una indemnización dentro del proceso de Habeas Data a favor del agraviado. Lo que sí hemos encontrado es un Fundamento Jurídico, el número 7, *in fine*, dado en una sentencia del Tribunal Constitucional cuando el marco normativo de los derechos constitucionales era diverso al vigente. *Sin embargo, el texto de tal fundamento jurídico es idéntico al artículo 25 de la Ley 29733.* (EXP. N.º 04387-2011-PHD/TC) (El énfasis es nuestro)

Reiteramos la cita del artículo 25 de la Ley:

"El titular de datos personales que sea afectado a consecuencia del incumplimiento de la presente Ley por el titular o por el encargado del banco de datos personales o por terceros, tiene derecho a obtener la indemnización correspondiente, conforme a ley".

Queremos dejar en claro que el Tribunal de Transparencia y Acceso a la Información Pública (TTAIP) , no indemniza por daños y perjuicios. A modo de digresión, es de precisar que de acuerdo al artículo 6 del Decreto Legislativo 1353, "El Tribunal de Transparencia y Acceso a la Información Pública es un órgano resolutivo del Ministerio de Justicia y Derechos Humanos que constituye la última instancia administrativa en materia de transparencia y derecho al acceso a la información pública a nivel nacional. Como tal es competente para resolver las controversias que se susciten en dichas materias. Depende administrativamente del Ministro y tiene autonomía en el ejercicio de sus funciones. Su funcionamiento se rige por las disposiciones contenidas en la presente Ley y en sus normas complementarias y reglamentarias".

Con todo, Alexander Rioja Bermúdez (2018) sostiene que, "***Aunque no es de recibo en nuestro ordenamiento,*** este tipo de hábeas data consiste en solicitar la indemnización por el daño causado con la propalación de la información." (El énfasis es nuestro)

6.3.-MAS SOBRE DERECHO AL OLVIDO

Volviendo ya de lleno a la regulación del Derecho al olvido, creemos que el mismo tiene su origen en el consentimiento que ha de prestar el titular de la información para el tratamiento de la misma por parte del titular del banco de datos. Pero aún más exacto y puntual es el artículo 20 de la Ley que trata sobre lo que se entiende por Derecho de actualización, inclusión, rectificación y *supresión* de data, se entiende. El texto del aludido artículo 20, *ab initio,* establece que, "El titular de datos personales tiene derecho a la actualización, inclusión, rectificación y ***supresión*** *de sus datos personales materia de tratamiento, cuando estos sean parcial o totalmente inexactos, incompletos, cuando se hubiere advertido omisión, error o falsedad, cuando hayan dejado de ser necesarios o*

pertinentes a la finalidad para la cual hayan sido recopilados o cuando hubiera vencido el plazo establecido para su tratamiento. El tercer parágrafo del mismo artículo establece que, "Durante el proceso de actualización, inclusión, rectificación o supresión de datos personales, el encargado de tratamiento de datos personales dispone su bloqueo, quedando impedido de permitir que terceros accedan a ellos. Dicho bloqueo no es aplicable a las entidades públicas que requieren de tal información para el adecuado ejercicio de sus competencias, según ley, las que deben informar que se encuentra en trámite cualquiera de los mencionados procesos. (El énfasis es nuestro)

Sin embargo, es de relievar que los casos de Derecho al olvido serán, en algunos supuestos, configuraciones de banco de datos personales "abierto", los que implican el uso de determinadas "fuentes de público acceso".

De otro lado, el artículo 28 de la Ley, relieva las obligaciones del titular y el encargado de tratamiento de datos personales, según sea el caso, y tienen, entre otras, las siguientes obligaciones: 7. ***Suprimir los datos personales objeto de tratamiento cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hubiesen sido recopilados o hubiese vencido el plazo para su tratamiento***, salvo que medie procedimiento de anonimización o disociación. Numeral 1. Efectuar el tratamiento de datos personales, solo previo consentimiento informado, expreso e inequívoco del titular de los datos personales, salvo ley autoritativa, con excepción de los supuestos consignados en el artículo 14 de la presente Ley. Entre los supuestos contenidos en el artículo 14 de la Ley, numeral 2, encontramos el siguiente texto: "Cuando se trate de datos personales contenidos o destinados ***a ser contenidos en fuentes accesibles para el público"*** (El énfasis es nuestro). Asimismo, el artículo 8 del reglamento de la Ley señala que, "Tratándose de datos sensibles, además del cumplimiento de los requisitos para el consentimiento válido, este debe ser otorgado por escrito, a través de su firma manuscrita, digital, electrónica o cualquier otra modalidad que garantice la voluntad del titular de los datos personales." Según el artículo III 6 del reglamento de la Ley son "Datos sensibles: aquella información relativa a datos genéticos o biométricos de la persona natural, datos neuronales, datos morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la afiliación sindical, salud física o mental u otras análogas que afecten su intimidad".

Como hemos visto, el artículo 28.7, *ab initio*, de la Ley es obligación del titular encargado del tratamiento de la información, "***Suprimir los datos personales objeto de tratamiento cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hubiesen sido recopilados o hubiese vencido el plazo para su tratamiento (…)".*** Al respecto Puccinelli (259:2016) afirma que, "Si un hecho no tiene relevancia histórica por la cual merezca ser resguardado de manera permanente, corresponde realizar un análisis cualitativo y evaluar si los hechos que se pretenden eliminar alcanzaron un determinado punto de saturación en su exposición pública, ya que, si así ha ocurrido, su difusión ulterior puede ser considerada excesiva, desproporcionada o injusta. Así, por ejemplo, las informaciones sobre hechos que no están vinculados a la comisión de

delitos y que se desean excluir del acceso público, que puede que ya no contengan alguna función social en términos de su potencial educativo, formativo o de protección terceros (v.gr., las informaciones relativas a solvencia patrimonial y crédito, que luego de transcurrido cierto tiempo que en promedio alcanza a los cinco años (…)". En lo que al factor tiempo se refiere, el mismo autor (248-249:2016) indica que "(…) para la mayoría de la doctrina el evento o contexto fáctico objeto del ejercicio de este derecho no debe ser actual o contemporáneo, porque en la esencia del derecho al olvido se encuentra el juego entre el tiempo y la memoria, de modo que se requiere la necesaria intervención del paso del tiempo, que permite determinar lo que puede ser olvidado y lo que es digno de ser recordado. La existencia de no contemporaneidad se basa en que los hechos que se manifiestan en el presente o en el pasado reciente no han sufrido un período de maduración que permita evaluar su relevancia pública y la importancia que estos eventos pueden tener para la comunidad. Así, eventos que, pese a su potencial negativo para la esfera privada, todavía pueden ser accesibles al público y transmitidos por terceros (v.gr., una condena penal o civil que dañe la reputación, pero todavía tiene relevancia, por ejemplo, para determinar la existencia o no de reincidencia).

Ahora bien, el tema de la privacidad y en general de la autodeterminación informativa, lo hemos hecho en buena cuenta, partiendo del supuesto en que estaríamos frente a un previo acuerdo de voluntades. Un acuerdo de voluntades que bien podrá ser un contrato por adhesión o a través de cláusulas generales de contratación. El artículo 5 de la Ley prevé que, "Para el tratamiento de los datos personales debe mediar el consentimiento de su titular." Sin embargo y para lo que nos interesa, asumimos y lo reiteramos, que con más frecuencia se aplicará el Derecho al olvido, y lo hallaríamos en las así llamadas "fuentes accesibles al público". El artículo 2.11 de la Ley se refiere a fuentes accesibles para el público. Esto es, bancos de datos personales de administración pública o privada, que pueden ser consultados por cualquier persona, previo abono de la contraprestación correspondiente, de ser el caso. Las fuentes accesibles para el público son determinadas en el reglamento.

El artículo 11 del reglamento de la Ley alude al tratamiento de los datos personales obtenidos a través de fuentes accesibles para el público. Así las cosas, el artículo 11.1 señala que, para los efectos de la Ley y el presente Reglamento, se consideran fuentes accesibles para el público, con independencia de que el acceso requiera contraprestación, las siguientes: 1. Los medios de comunicación electrónica, óptica y de otra tecnología, siempre que el lugar en el que se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general, salvo una norma determine lo contrario. 2. Las guías telefónicas, independientemente del soporte en el que estén a disposición y en los términos de su regulación específica. 3. Los diarios y revistas independientemente del soporte en el que estén a disposición y en los términos de su regulación específica. 4. Los medios de comunicación social. 5. Las listas de personas pertenecientes a grupos profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección postal, número telefónico, número de fax, dirección de correo electrónico y aquellos que establezcan su pertenencia al grupo. En el caso de colegios profesionales, podrán

indicarse además los siguientes datos de sus miembros: número de colegiatura, fecha de incorporación y situación gremial en relación al ejercicio profesional. 6. Los repertorios de jurisprudencia publicados conforme a ley. 7. Los Registros Públicos administrados por la Superintendencia Nacional de Registros Públicos - SUNARP, así como todo otro registro o banco de datos calificado como público conforme a ley. 8. Las entidades de la Administración Pública, en relación a la información que deba ser entregada en aplicación de la Ley N.º 27806, Ley de Transparencia y Acceso a la Información Pública. Tengamos presente este numeral 8 para efectos de realizar la interpretación que practicaremos *infra.*

El artículo 11.3 del reglamento de la Ley es nítido al precisar que, "El tratamiento de los datos personales obtenidos a través de fuentes de acceso público debe respetar ***los principios*** establecidos en la Ley y en el presente Reglamento." (El énfasis es nuestro)

El artículo 11.2 del reglamento de la Ley resulta controversial. El texto de este artículo es como sigue: "Lo dispuesto en el numeral 8 del presente artículo no implica que todo dato personal contenido en información administrada por las entidades sujetas a la Ley de Transparencia y Acceso a la Información Pública sea considerado información de fuente accesible para el público. *La evaluación del acceso a datos personales en posesión de entidades de administración pública se realiza atendiendo a las circunstancias de cada caso concreto, valorando la afectación probable a otros derechos fundamentales".* Debemos señalar que este artículo no es una novedad. Estaba recogido, con marcados matices, en el artículo 17.8 del antiguo reglamento de la Ley ya derogado. Esta norma prescribía que, "Las entidades de la Administración Pública, en relación a la información que deba ser entregada en aplicación de la Ley N.º 27806, Ley de Transparencia y Acceso a la Información Pública. Lo dispuesto en el numeral precedente no quiere decir que todo dato personal contenido en información administrada por las entidades sujetas a la Ley de Transparencia y Acceso a la Información Pública sea considerado información pública accesible. ***La evaluación del acceso a datos personales en posesión de entidades de administración pública se hará atendiendo a las circunstancias de cada caso concreto***." El autor del nuevo reglamento de la Ley no ha dejado sin efecto lo establecido en el artículo 17.8 que figuraba en el reglamento precedente, el cual creemos que podía, dada la discrecionalidad manifiesta y así determinada, llevar a arbitrariedades agraviando de esta manera al administrado y al interés general. Por ello y a efectos de haberse "reglado" en alguna medida tal abierta discrecionalidad, es que celebramos que el nuevo reglamento haya agregado para efectos de la dación de datos por la Administración que esta se realiza atendiendo a las circunstancias de cada caso concreto***, valorando la afectación probable a otros derechos fundamentales***. Es un avance. (El énfasis es nuestro)

De otra parte, resulta interesante aludir al artículo 82.1 del reglamento de la Ley conforme al cual, "El titular de los datos personales puede solicitar la supresión o cancelación de sus datos personales cuando estos hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hayan sido recopilados, cuando hubiere vencido el plazo establecido para su tratamiento, cuando ha revocado su consentimiento para

el tratamiento y en los demás casos en los que no están siendo tratados conforme a la Ley y al presente Reglamento. El artículo 82.2 precisa que "La solicitud de supresión o cancelación puede referirse a todos los datos personales del titular contenidos en un banco de datos personales o solo a alguna parte de ellos".

Según el artículo 84 del reglamento de la Ley, "La supresión no procede cuando los datos personales deban ser conservados en virtud de razones históricas, estadísticas o científicas de acuerdo con la legislación aplicable o, en su caso, en las relaciones contractuales entre el responsable y el titular de los datos personales, que justifiquen el tratamiento de los mismos."

Sobre el particular es de citarse a Puccinelli (249:2016) cuando manifiesta que, "Los hechos históricos tienen una relevancia social constante en el tiempo, trascienden los intereses individuales y su disponibilidad está en la esencia del derecho colectivo a la memoria, de modo que impide que juegue el interés individual en que resulten olvidados. Por ello, los eventos históricamente relevantes no son pasibles de ser alterados por la vía del derecho al olvido, por más que resulten altamente dolorosos para algunas de las personas involucradas en ellos (o para sus herederos) y haya transcurrido un largo tiempo desde la fecha de su ocurrencia (v.gr., crímenes de lesa humanidad, incluso para las víctimas).De este modo, además del transcurso de un espacio importante del tiempo respecto de esa información que causa un daño, debe ponderarse si existe alguna necesidad de permanencia del hecho en la memoria colectiva para su transmisión a todas las generaciones futuras (todo ello con independencia del malestar individual o colectivo que pueda provocar), y si tal necesidad de preservación histórica no es tal, puede dejarse en el olvido."

El artículo 87 del reglamento de la Ley versa sobre el Derecho al tratamiento objetivo de datos personales. Así, el numeral 1 del referido artículo establece que, "El titular del dato personal tiene derecho a no ser objeto de decisiones, automatizadas o no, que le produzcan efectos jurídicos, discriminación o le afecten de manera significativa incluyendo aquellas que se basen únicamente en tratamientos automatizados destinados a evaluar, analizar o predecir, sin intervención humana, determinados aspectos personales del mismo, en particular, su rendimiento profesional, situación económica, estado de salud, orientación o identidad sexual, fiabilidad o comportamiento, entre otros, debiéndose considerar las excepciones contempladas en el artículo 23 de la Ley." El artículo 23 de la Ley prevé que, "El titular de datos personales tiene derecho a no verse sometido a una decisión con efectos jurídicos sobre él o que le afecte de manera significativa, sustentada únicamente en un tratamiento de datos personales destinado a evaluar determinados aspectos de su personalidad o conducta, *salvo que ello ocurra en el marco de la negociación, celebración o ejecución de un contrato o en los casos de evaluación con fines de incorporación a una entidad pública, de acuerdo a ley, sin perjuicio de la posibilidad de defender su punto de vista, para salvaguardar su legítimo interés."* (Las cursivas son nuestras)

El artículo 87.2 dispone que, "Para garantizar el ejercicio del derecho al tratamiento objetivo, de conformidad con lo establecido en el artículo 23 de la Ley, cuando se traten

datos personales como parte de un proceso de toma de decisiones sin participación del titular de los datos personales, el titular del banco de datos personales o responsable del tratamiento debe informárselo a la brevedad posible, sin perjuicio de lo regulado para el ejercicio de los demás derechos en la Ley y el presente Reglamento".

6.4.- REMEDIOS: RECTIFICACION, SUPRESION, CANCELACION, REVOCACION Y OPOSICION

Aun cuando ya en alguna medida hemos elaborado *supra* sobre este asunto, en el presente trataremos algunos aspectos sobre el Derecho de tutela que quedaron pendientes.

Reiteramos que el artículo 10 de la Ley el mismo que establece el "Principio de disposición de recurso". Esto es, todo titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales".

El artículo 47 del reglamento de la Ley se refiere en lo que respecta a la titularidad para invocar, entre otros, el Derecho al olvido. Este artículo dispone que el eventual ejercicio de la acción es personal y luego sostiene que, los derechos de información, acceso, ***rectificación, cancelación, oposición*** y tratamiento objetivo de datos personales sólo pueden ser ejercidos por el titular de datos personales, sin perjuicio de las normas que regulan la representación. (El énfasis es nuestro)

El artículo 80.1 del reglamento de la Ley se refiere a la rectificación la cual se deslinda del derecho a la supresión o cancelación. El artículo citado prescribe que la rectificación, es el derecho del titular de datos personales para que se modifiquen los datos que resulten ser inexactos, erróneos o falsos.

Asimismo, según el artículo 10.1 del reglamento de la Ley, "El titular de los datos personales puede revocar su consentimiento para el tratamiento de sus datos personales en cualquier momento, *sin justificación previa* y sin que le atribuyan efectos retroactivos. Para la revocación del consentimiento se cumplen los mismos requisitos observados con ocasión de su otorgamiento, pudiendo ser estos más simples, si así se hubiera señalado en tal oportunidad." (Las cursivas son nuestras)

Por su parte, el artículo 10.2 del reglamento de la Ley refiere que, "El titular de los datos personales puede negar o revocar su consentimiento al tratamiento de sus datos personales para finalidades adicionales a aquellas que dan lugar a su tratamiento autorizado, sin que ello afecte la relación que da lugar al consentimiento que sí ha otorgado o no ha revocado. En caso de revocatoria, es obligación de quien efectúa el tratamiento de los datos personales adecuar los nuevos tratamientos a la revocatoria y los tratamientos que estuvieran en proceso de efectuarse, en el plazo que resulte de una actuación diligente, que no puede ser mayor a diez (10) días.

Conforme al artículo 10.3 del reglamento de la Ley, "Si la revocatoria afecta la totalidad del tratamiento de datos personales que se venía haciendo, el titular del banco de datos personales, encargado del tratamiento, o en su caso el responsable del tratamiento,

aplica las reglas de cancelación o supresión de datos personales." (El énfasis es nuestro)

Pero existe otro tema que se relaciona con el Derecho al olvido. El artículo 22 de la Ley trata sobre el Derecho de oposición. Así, dispone que, "Siempre que, por ley, no se disponga lo contrario y cuando no hubiera prestado consentimiento, el titular de datos personales puede oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En caso de oposición justificada, el titular o el encargado de tratamiento de datos personales, según corresponda, *debe proceder a su supresión, conforme a ley*". (Las cursivas son nuestras)

El artículo 86.1 reglamenta la Ley, restringiéndola en cuanto a su alcance, y alude al Derecho de oposición por parte del titular de datos personales. El artículo establece que este tiene derecho a oponerse en cualquier momento, a efectos de que no se lleve a cabo el tratamiento de sus datos personales o se cese en el mismo, ***cuando no hubiere prestado su consentimiento para su recopilación por haber sido tomados de fuente de acceso al público***. (El énfasis es nuestro)

Siempre sobre el Derecho a la oposición el artículo 86.2 refiere que, "*Aun cuando hubiera prestado consentimiento,* el titular de datos personales tiene derecho a oponerse al tratamiento de sus datos, *si acredita la existencia de motivos fundados y legítimos relativos a una concreta situación personal que justifiquen el ejercicio de este derecho.* (Las cursivas son nuestras)

Según el artículo 86.3, "En caso de que la oposición resulte justificada el titular del banco de datos personales o responsable de tratamiento debe proceder al cese del tratamiento que ha dado lugar a la oposición".

A su vez, el artículo 20 de la Ley establece el Derecho de actualización, inclusión, rectificación y supresión. El texto del artículo es como sigue: "El titular de datos personales tiene derecho a la actualización, inclusión, rectificación y supresión de sus datos personales materia de tratamiento, cuando estos sean parcial o totalmente inexactos, incompletos, cuando se hubiere advertido omisión, error o falsedad, ***cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados*** o cuando hubiera vencido el plazo establecido para su tratamiento. Si sus datos personales hubieran sido transferidos previamente, el encargado de tratamiento de datos personales debe comunicar la actualización, inclusión, rectificación o supresión a quienes se hayan transferido, en el caso que se mantenga el tratamiento por este último, quien debe también proceder a la actualización, inclusión, rectificación o supresión, según corresponda. Durante el proceso de actualización, inclusión, rectificación o supresión de datos personales, el encargado de tratamiento de datos personales dispone su bloqueo, quedando impedido de permitir que terceros accedan a ellos. Dicho bloqueo no es aplicable a las entidades públicas que requieren de tal información para el adecuado ejercicio de sus competencias, según ley, las que deben informar que se encuentra en trámite cualquiera de los mencionados procesos (…)". (El énfasis es nuestro)

Según el artículo III 3 del reglamento de la Ley se entiende por cancelación: La acción o medida que en la Ley se describe como ***supresión***, cuando se refiere a datos personales, que consiste en eliminar o suprimir los datos personales. (El énfasis es nuestro)

El artículo 82 del reglamento de la Ley versa sobre la supresión o cancelación. Así, según el artículo 82.1 el titular de los datos personales puede solicitar la supresión o cancelación de sus datos personales ***cuando estos hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hayan sido recopilados,*** cuando hubiere vencido el plazo establecido para su tratamiento, cuando ha revocado su consentimiento para el tratamiento y en los demás casos en los que no están siendo tratados conforme a la Ley y su Reglamento. Conforme al artículo 82.2, "La solicitud de supresión o cancelación puede referirse a todos los datos personales del titular contenidos en un banco de datos personales o solo a alguna parte de ellos." (El énfasis es nuestro)

Respecto a esto, Puccinelli (259:2016) comenta que, "Si un hecho no tiene relevancia histórica por la cual merezca ser resguardado de manera permanente, corresponde realizar un análisis cualitativo y evaluar si los hechos que se pretenden eliminar alcanzaron un determinado punto de saturación en su exposición pública, ya que, si así ha ocurrido, su difusión ulterior puede ser considerada excesiva, desproporcionada o injusta. Así, por ejemplo, las informaciones sobre hechos que no están vinculados a la comisión de delitos y que se desean excluir del acceso público, que puede que ya no contengan alguna función social en términos de su potencial educativo, formativo o de protección terceros (v.gr., las informaciones relativas a solvencia patrimonial y crédito, que luego de transcurrido cierto tiempo que en promedio alcanza a los cinco años (…)"

En cuanto al factor "tiempo", Puccinelli (248-249:2016) indica que, "(…) para la mayoría de la doctrina el evento o contexto fáctico objeto del ejercicio de este derecho no debe ser actual o contemporáneo, porque en la esencia del derecho al olvido se encuentra el juego entre el tiempo y la memoria de modo que se requiere la necesaria intervención del paso del tiempo, que permite determinar lo que puede ser olvidado y lo que es digno de ser recordado". El mismo autor continúa señalando que, "La existencia de no contemporaneidad se basa en que los hechos que se manifiestan en el presente o en el pasado reciente no han sufrido un período de maduración que permita evaluar su relevancia pública y la importancia que estos eventos pueden tener para la comunidad. Así, eventos que, pese a su potencial negativo para la esfera privada, todavía pueden ser accesibles al público y transmitidos por terceros (v.gr., una condena penal o civil que dañe la reputación, pero todavía tiene relevancia, por ejemplo, para determinar la existencia o no de reincidencia)". Puccinelli (243:2016), en fin, precisa que, "Las reglas establecen en definitiva un plazo de caducidad del dato negativo, que implica en los hechos «olvidar» hechos por el mero transcurso del tiempo, los cuales incluyen a información sobre deudas que pueden encontrarse vigentes por ser todavía exigibles conforme a la legislación de fondo, tal como surge de la de la interpretación dada por la Corte nacional en los casos «Nápoli»6 y «Catania»7."

El numeral 3 del ya citado artículo 82 del reglamento de la Ley prevé que dentro de lo establecido por el artículo 20 de la Ley y el numeral 3 del artículo III del mismo Reglamento, la presentación de la solicitud de supresión al responsable del tratamiento implica el cese en el tratamiento de los datos personales a partir de un bloqueo de los mismos en tanto se evalúe su posterior eliminación.

De otro lado, el artículo 83 del reglamento de la Ley establece que, "El titular del banco de datos personales o responsable del tratamiento debe documentar ante el titular de los datos personales haber cumplido con lo solicitado e indicar las transferencias de los datos suprimidos, identificando a quién o a quiénes fueron transferidos, así como la comunicación de la supresión correspondiente".

El artículo 61 del reglamento se refiere a lo que denomina "Carácter personal". En tal sentido prevé que, "Los derechos de información, acceso, rectificación, ***cancelación,*** oposición y tratamiento objetivo de datos personales sólo pueden ser ejercidos por el titular de datos personales, sin perjuicio de las normas que regulan la representación. (El énfasis es nuestro)

REFERENCIAS BIBLIOGRAFICAS

Curaca Kong, Alfredo Orlando. (2022) El derecho al olvido y su reconocimiento jurisprudencial. Comentarios a la STC 03041-2021-PHD/TC. En Revista Peruana de Derecho Constitucional N°14.

Puccinelli, Oscar. (2016) El «derecho al olvido» en el derecho a la protección de datos. Con especial referencia a su vigencia en Internet. En: Pensamiento Constitucional N° 21, 2016, pp. 235-251

Rioja Bermúdez, A (2018) "El hábeas data en la jurisprudencia del TC. Definición, alcances y tipología". Disponible en: Pasión por el Derecho, https://lpderecho.pe/habeas-data-jurisprudencia-tc-definicion-alcances-tipologia/

Velásquez Meléndez, R. (2025) Derecho Fundamental al Secreto e inviolabilidad de las Comunicaciones: Análisis Comparado de su Sentido y Contenido. En THĒMIS-Revista de Derecho 88. julio-diciembre 2025. pp. 65-88