IUS: Revista de investigación de la Facultad de Derecho
Vol. 9 Núm. 1 (2020): IUS - Revista de Investigación de la Facultad de Derecho, 83-100
SECCIÓN PRINCIPAL

EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN EL PERÚ: 27 AÑOS DESDE SU INCORPORACIÓN EN LA CONSTITUCIÓN POLÍTICA DE 1993

Milagros Olivos Universidad del Pacífico

Desde más de dos décadas que nuestro país reconoció, en la categoría de derecho fundamental, el derecho a la protección de datos personales, al incorporarlo en el artículo 2.6 de la Carta Constitucional de 1993. Pocos son los países en América Latina que han realizado dicho reconocimiento, y más aún han desarrollado un marco normativo que regula el régimen de la protección de datos personales. Hace no más de dos años (en septiembre del 2017) se introdujeron algunas reformas al régimen existente, las cuales vienen consolidándose a través de las orientaciones emitidas desde la autoridad de control. A continuación, se presenta desde perspectiva meramente descriptiva el camino que ha recorrido este derecho, desde su reconocimiento en la Constitución de 1993 hasta nuestros días, haciendo especial mención, no solo a las disposiciones normativas, sino especialmente a los pronunciamientos emitidos por el órgano garante sobre quien – en estos momentos- recae la gran responsabilidad de mantener la vigencia de este derecho.

PALABRAS CLAVES: Privacidad, Protección de Datos Personales, Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, seguridad de la información.

KEYWORDS: *Privacy, Protection of Personal Data, General Directorate of Transparency, Access to Public Information and Protection of Personal Data, information security.*

1. INTRODUCCIÓN : ALGUNOS “ANÉCDOTAS” HISTÓRICOS SOBRE LA PRIVACIDAD Y LA

PROTECCIÓN DE DATOS PERSONALES

La «privacidad» como concepto jurídico tiene sus orígenes en la práctica norteamericana de los años sesenta del siglo XX, en el reconocimiento de las facultades de protección de los ciudadanos frente a los informes de solvencia patrimonial. Aunque su conceptualización es más histórica que doctrinal, es importante resaltar –aunque sea a manera de anécdota- los aportes cognitivos que permitieron, desde ese entonces, la configuración de este derecho.

En 1967, uno de los más importantes estuvo bajo la autoría del profesor Alan Furman Westin quien define la «privacidad» como el derecho de la persona «*para controlar, editar, gestionar y eliminar la información acerca de ellos* [mismos] *y decidir cuándo, cómo y en qué medida la información se comunica a los demás*». También destacan los aportes de Thomas Cooley quiensu momento hiciese referencia al *theright to be letalone*, así como la contribución de Warren y Brandeis quien define *theright to privacy* (SALDAÑA, 2012, pp. 195-240). La fundación del concepto «derecho a la vida privada» finalmente aparece en estos últimos textos. (MURILLO DE LA CUEVA y PIÑAR MAÑAS,2009,pp. 82-85).

A pesar de las precisiones en los planteamientos con los que se configuraba un derecho que reclamaba tutela desde aquel entonces, las posiciones planteadas no obtuvieron una inmediata repercusión en las sentencias de los tribunales (SALDAÑA, 2012, pp. 195-240); aunque pronto, -cuando se vieron enfrentados con más frecuencia a casos en los que una persona se sentía agraviada por una publicación o fotografía indiscreta- optaron por un cambio de posición (CORRAL TALCIANI, 2000, pp. 51-79).

En 1983, fue el Tribunal Constitucional alemán quien, a través de una sentencia sobre la legalidad de un censo, reflejó los aportes de esa doctrina -en su mayoría norteamericana y en particular los aportes de Westin- y puso de relieve la importancia del control sobre la propia información. Se configuró así el derecho a la privacidad y a la protección de datos. A pesar que, en 1983, no existía ley o referencia normativa alguna sobre un derecho específico la Sentencia de la Primera Sala del Tribunal Constitucional Federal Alemán, del 15 de diciembre, 1983 (1, BvR 209, 269, 362, 420, 440, 484/83), sobre la base del derecho a la dignidad humana y al libre desarrollo de la personalidad, optó por defender la garantía y la continuidad las libertades básicas, consagradas con anterioridad, con la formulación de un nuevo derecho. (González, 2001, p. 9). Se llamó a este derecho: autodeterminación informativa. En la sentencia, se puso de manifiesto la necesidad de crear mecanismos jurídicos de protección de los datos personales frente a su uso, más que por su carácter estrictamente privado, por el peligro que supone la utilización que se haga de los mismos. (HEREDERO HIGUERAS, 1984, pp. 139-158)

El derecho a la protección de datos personales como derecho autónomo se fundamenta en dos conceptos: «intimidad» y «privacidad» (HERNÁNDEZ LÓPEZ, 2013, pp. 25 y ss.). La denominación como tal (derecho a la protección de datos personales) es utilizada en diversos instrumentos internacionales que han servido de referente, en los cuales se le ha llegado a considerar como un nuevo derecho, autónomo e independiente de otros derechos, diferenciándolo especialmente del derecho a la intimidad. (HEREDERO HIGUERAS, 1984, pp. 139-158). Precisamente esa es la razón por la que cada derecho tiene una regulación independiente, tal como sucede también en nuestra propia Carta de 1993.

Desde el punto de vista normativo, la regulación acerca de la protección de la información personal, registra su primer antecedente en la Declaración Universal de los Derechos Humanos de 1948, en cuyo artículo 12 se reconoce: «*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia (...)*». En 1966, el artículo 17.1 del Pacto Internacional de Derechos Civiles y Políticos hace lo propio y recoge también esa misma restricción. Ambos instrumentos son reflejo de las primeras intenciones de los Estados para proteger la privacidad de los ciudadanos prohibiendo cualquier injerencia arbitraria.

Asimismo, tras la sentencia del Tribunal Constitucional Alemán, el concepto que denominó «autodeterminación informativa», vuelve a ser recogido por el Tribunal Constitucional español en sus sentencias 290/2000 y 292/2000 del 30 de noviembre. En la primera, confirmando la constitucionalidad de la Ley Orgánica 5/1992 de 29 de octubre de Regulación del Tratamiento Automatizado de Datos de Carácter Personal y mantenida por la Ley Orgánica de Protección de Datos de Carácter Personal de atribuir la competencia exclusiva sobre los ficheros de titularidad privada a la Agencia Española de Protección de Datos (FERNÁNDEZ VILLAZÓN, 2016, pp. 408 y ss.). Con la segunda, declarando inconstitucional la comunicación de datos entre ficheros de las Administraciones Públicas cuando carezca de consentimiento del titular de los datos o de previsión legal; las limitaciones del artículo 24.2 de la norma española respecto del ejercicio de los derechos de acceso, rectificación y cancelación en los ficheros de titularidad pública; así como la previsión del primer apartado de ese mismo artículo 24 que excluía el deber de informar al afectado de la recogida de datos para esos mismos ficheros cuando impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas y cuando afecte a la persecución de infracciones administrativas.

De esta manera, el Tribunal Constitucional español no solo reconoce la existencia de un derecho al que llama «derecho a la protección de datos de carácter personal», sino que además lo diferencia del derecho a la intimidad (LOPEZ AGUILAR, 2017, pp. 557-581), distinguiéndolo por su funcionalidad, su objeto y su contenido. Señala, además, este Tribunal, que aun cuando comparten un objetivo común (ofrecer una eficaz protección constitucional de la vida privada personal y familiar), se distinguen porque el derecho a la protección de datos personales atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya regulación se establece por ley desarrollando su contenido y/o regulando su ejercicio.

Como referencia general, resulta pertinente citar la STC 292/2000 de 30 de noviembre de 2000 la cual desarrolla – desde el ordenamiento español- el contenido de este derecho. Al respecto el Tribunal señala que:

«7. [el derecho a la protección de datos de carácter personal] *consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos*» (STC 292/2000, 2000, p. 7).

Esta facultad que tienen las personas para proteger su información personal (que incluye nombre y apellido, número de documento, nacionalidad, sexo, estado civil, número de teléfono, número de celular, huellas digitales, dirección de correo electrónico, número de tarjeta de crédito o débito, número de cuenta bancaria, fotos, videos, publicaciones, ubicación espacial, actividades, opiniones, etc.) importa también la potestad para permitir o rechazar el uso de la información personal, de controlar la certeza de su contenido, el acceso por parte de terceros, y hasta la utilidad que pueda dársele sea con fines económicos, sociales o políticos. (GARCÍA MEXÍA, 2005, pp. 56-97). La doctrina que analiza este derecho reconoce que el individuo está investido de una facultad de control que puede ejercer respecto de sus datos proporcionados -de manera voluntaria o involuntaria- como resultado de su interacción en esferas de actuación pública o privada, en distintos lugares y/o en diferentes etapas de su vida (MURILLO y PIÑAR, 2009, p. 23).

Como resulta evidente, el tratamiento masivo de la información personal a nivel mundial se ha convertido en una práctica cotidiana del siglo XXI, planteando - al mismo tiempo- varios desafíos que al Derecho de nuestro tiempo le toca responder. Uno de esos desafíos es la búsqueda de una tutela eficiente que garantice la privacidad de los ciudadanos y la defensa del derecho a la protección de datos personales en todos los escenarios.

El desarrollo legal, jurisprudencial y doctrinal del derecho a la protección de datos personales tiene una larga data, y su evolución ha ido avanzando de forma progresiva. Nuestro país no ha sido ajeno a esta realidad. Desde 1993 este derecho fue reconocido expresamente en el catálogo de derechos fundamentales de la Constitución peruana.

Hoy han transcurrido más de 25 de años desde dicha incorporación, y poco más de 10 años desde que legislativamente se desarrolló su contenido. Desde entonces, su impulso –en distintas esferas- especialmente en estos últimos años ha sido importante. El trabajo de la entonces Autoridad de Protección de Datos Personales (APDP), actualmente absorbida por la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (DGTAIP), ha contribuido significativamente con este logro.

Las siguientes líneas tienen por objetivo mostrar -desde una perspectiva más descriptiva que prescriptiva- la ruta que ha seguido el régimen de la protección de este derecho en el ordenamiento jurídico peruano. Con un enfoque normativo se presenta cómo se ha definido este derecho en el ordenamiento jurídico peruano y cuáles son los cambios normativos que se han generado durante los últimos años. Para tal fin se han abordado sus definiciones, características y contenido que progresivamente han ido consolidándose a lo largo de estos años, especialmente a través de instrumentos de orientación que ha emitido la autoridad de control en el ejercicio de sus funciones. La exposición que a continuación se presenta se realiza – nuevamente preciso- desde una mirada normativa, describiendo su regulación, incluso desde antes de su incorporación como derecho fundamental en la Constitución de 1993 hasta la reseña de las reformas iniciadas, especialmente a partir del 2017.

2 . L A PROTECCIÓN DE DATOS PERSONALES EN EL ORDENAMIENTO JURÍDICO PERUANO : LA RUTA

2 .1. A ntes de la vigencia de la LPDP : la configuración de la « autodeterminación informativa » y su c reación a partir de los pronunciamientos del Tribunal Constitucional.

El artículo 6.2 de la Constitución Política del Perú de 1993 reconoce el poder de los ciudadanos de disposición sobre sus datos, de modo que, siempre mediando su consentimiento, éstos pueden disponer de los mismos. Algunos años después de este reconocimiento, el Tribunal Constitucional comenzó a desarrollar – a través de diversos pronunciamientos y al amparo de la vigencia del artículo 61.2 del Código Procesal Constitucional- lo que él mismo denominó el «derecho a la autodeterminación informativa» refiriéndose a lo largo de todas sus decisiones a su contenido. Al respecto el TC se expresa en los siguientes términos:

«[e]l derecho a la autodeterminación informativa consiste en la serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos. Se encuentra estrechamente ligado a un control sobre la información, como una autodeterminación de la vida íntima, de la esfera personal. Mediante la autodeterminación informativa se busca proteger a la persona en sí misma, no únicamente en los derechos que conciernen a su esfera personalísima, sino a la persona en la totalidad de ámbitos. […] En este orden de ideas, el derecho a la autodeterminación informativa protege al titular del mismo frente a posibles abusos o riesgos derivados de la utilización de los datos, brindando al titular afectado la posibilidad de lograr la exclusión de los datos que considera “sensibles” y que no deben ser objeto

de difusión ni de registro; así como le otorga la facultad de poder oponerse a la transmisión y difusión de los mismos» (STC recaída en el Expediente N° 04739-2007-PHD/TC, fundamentos jurídicos 2-4 y también STC recaída en el Expediente N° 0746-2010-PHD/TC, fundamento jurídico 4).

En complemento a lo anterior mediante STC recaída en el Expediente Nº 04739-2007-PHD/TC el Tribunal sostuvo que: «*El derecho a la autodeterminación informativa consiste en* […] *facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos. Se encuentra estrechamente ligado a un control sobre la información, como una autodeterminación de la vida íntima, de la esfera personal.*

En las diferentes sentencias promovidas en distintos momentos, la nomenclatura se mantiene. El TC reconoce que el derecho a la autodeterminación informativa es el que se encuentra previsto en el artículo 2.6 de la Carta de 1993. No hay más novedad respecto de su definición, tampoco en las resoluciones siguientes. Así pueden leerse la STS del 18 de enero del 2002 recaída sobre el Expediente Nº 0197-2000-HD/TC, STS del 29 de enero del 2003 recaída sobre el Expediente Nº 1797-2002-HD/TC, STS del 30 de mayo del 2011 recaída sobre el Expediente Nº 04227-2009-PHD/TC, STS del 21 de agosto del 2014 recaída sobre el Expediente Nº 02995-2013-PHD/TC, así como en la sentencia recaída – en esa misma fecha- sobre el Expediente Nº 02324-2013-PHD/TC, entre otros, las cuales uniformemente muestran esa misma precisión.

En esa misma línea, el Tribunal también se preocupó – durante esos mismos años – por delimitar el contenido de este derecho, que para el ordenamiento jurídico peruano de esa época resultaba absolutamente novísimo. Al respecto, el Tribunal precisó que este derecho comprende:

1. La capacidad de exigir jurisdiccionalmente el acceso a los registros de información, computarizados o no, cualquiera que sea su naturaleza, en los que se encuentren almacenados los datos de una persona. Según lo explica el propio Tribunal, tal acceso puede tener por objeto conocer el tipo de información que se encuentra registrada, la finalidad por la que se habría realizado dicho registro y las personas que habrían ordenado su realización, pudiéndose incluso hasta identificar quiénes serían los responsables de recabar dicha información.
2. La posibilidad de añadir información al registro, ya sea para que se actualicen los datos que se encuentran registrados, o bien para que se incluyan aquellos no registrados, pero que resultan ser necesarios para una referencia completa sobre la imagen e identidad de la persona afectada.
3. La posibilidad de corregir la información registrada (independientemente de la naturaleza de la misma, sea personal o familiar); y
4. La capacidad de impedir que la información personal registrada se difunda para fines distintos de aquellos que justificaron su registro o, incluso, hasta la posibilidad de cancelar aquella información que se desee esté almacenada. Esto último se encuentra también reflejado en la STS del 16 de noviembre del 2007 recaída sobre el Expediente Nº 03052-2007-PHD/TC, fundamento jurídico 3. Incluso antes de este pronunciamiento, el TC había asumido dicha posición en la ya citada STS del 18 de enero del 2002 recaída sobre el Expediente Nº 0197-2000-HD/TC en su Fundamento Jurídico Nº 4.

A través de sus decisiones, el TC definió el contenido del derecho a la autodeterminación informativa, utilizando la nomenclatura de sus homólogos europeos.Este avance resulta especialmente importante porque la ruta muestra que en el Perú -aun cuando únicamente se había logrado el reconocimiento constitucional de este derecho (avance tremendamente crucial, especialmente si se compara qué sucedía o sigue sucediendo en nuestros días en los otros países de América Latina) y no existía un órgano de control o una ley desarrollo-, se llenó de contenido a un derecho hasta entonces inexistente, no solo a nivel legislativo sino también a nivel social.

En este estadío, el Tribunal – bajo la misma nomenclatura - hace un aporte mayor. En una de sus resoluciones se preocupa por plantear las diferencias de este derecho con otros, como son la intimidad, el honor, la imagen; y llega incluso a reconocerle la categoría de derecho autónomo. Así, en su STS del 29 de enero del 2003 recaída sobre el Expediente Nº 1797-2002-HD/TC reconoce que el derecho del artículo 2.6 de la Constitución es un derecho nuevo e independiente. En su texto y a su línea, el TC – refiriéndose a estas diferencias - manifiesta lo siguiente: «[el derecho a la autodeterminación informativa] se distingue:

i) Del derecho a la identidad personal, esto es, del derecho a que la proyección social de la propia personalidad no sufra interferencias o distorsiones a causa de la atribución de ideas, opiniones, o comportamientos diferentes de aquellos que el individuo manifiesta en su vida en sociedad.

ii) Del derecho a la imagen, reconocido en el art. 2.7 de la CPP que protege, básicamente, la imagen del ser humano, derivada de la dignidad de la que se encuentra investido. En este contexto, el Tribunal señala que mientras que el derecho a la autodeterminación informativa garantiza que el individuo sea capaz de disponer y controlar el tipo de datos que sobre él se hayan registrado, a efectos de preservar su imagen derivada de su inserción en la vida en sociedad.

iii)Del derecho a la intimidad, es decir, del poder jurídico de rechazar intromisiones ilegítimas en la vida íntima o familiar de las personas; toda vez que el derecho a la autodeterminación informativa garantiza la facultad de todo individuo de poder preservarla controlando el registro, uso y revelación de los datos que les conciernen».

Explica el Tribunal que este derecho (autodeterminación informativa) tiene por objeto proteger la intimidad, personal o familiar, la imagen y la identidad, frente al peligro que representa el uso y la eventual manipulación de los datos. Y agrega que: «[…] n*o puede identificarse con el derecho a la intimidad, personal o familiar, ya que mientras éste protege el derecho a la vida privada, el derecho a la autodeterminación informativa busca garantizar la facultad de todo individuo de poder preservarla ejerciendo un control en el registro, uso y revelación de los datos que le conciernen* […]». (STC recaída en el Expediente Nº 04739-2007-PHD/TC, fundamento jurídico 2-4)

En los años siguientes, entre el 2012 y el 2014, se emitieron algunos otros pronunciamientos desarrollando durante esos años algunos lineamientos para su ejercicio legítimo. Así, por ejemplo, en la STS del 7 de agosto del 2014 recaída sobre el Expediente N° 02491-2013-PHD/TC el Tribunal señaló:

«*Se evidencia la lesión del derecho a la autodeterminación informativa del recurrente, pues su negativa no encuentra sustento en supuesto razonable alguno, dado que la información o datos que se han solicitado no evidencian requerimiento sobre datos sensibles de terceros o que se encuentren vinculados a información clasificada cuya restricción resultaría legítima en los términos que hoy regula el artículo 4° del Reglamento de la Ley de Protección de Datos Personales (Decreto Supremo N.° 003-2013-JUS), razones por las que corresponde estimar la demanda, y proceder a entregar el expediente administrativo que en copia fedateada fue incorporado como acompañado al presente proceso.*»

Particularmente en el año 2014, los pronunciamientos del TC van a orientarse de forma particular con las actividades que realizan las centrales de riesgo en lo que respecta al tratamiento de información personal.

2 .2. La LPDP y sus normas reglamentarias: Una breve descripción sobre el consentimiento y los otros principios sobre los que se fundamenta el régimen jurídico de la protección de datos

El 3 de julio del 2011, completando el reconocimiento que el Constituyente hizo en 1993, el Gobierno publicó en su Diario Oficial la Ley Nº 29733, Ley de Protección de Datos Personales (en

adelante, LPDP), y el 22 de marzo del 2013 mediante Decreto Supremo Nº 003-2013 se aprobó su Reglamento. La norma, luego de abordar un breve Título Preliminar (tan solo con 3 Disposiciones Generales), desarrolla hasta siete Títulos cuyo contenido da vida a este derecho. El texto se compone de 40 artículos y el Reglamento de 130, con un adicional de 3 Disposiciones Complementarias Finales y Transitorias.

Los derechos y las obligaciones derivadas, tanto de la LPDP como de su Reglamento, son variadas y algunas de ellas son particularmente complejas, especialmente si se tiene en cuenta que aquello que antes se podía hacer forma libre (y hasta indiscriminada) luego de la vigencia de la norma se tenía que contar – bajo determinados parámetros- con la autorización correspondiente.

Del análisis de la estructura lógica del contenido de la LPDP, sus obligaciones válidamente pueden encuadrarse en dos grandes grupos. Por una parte, aquellas referidas a los «bancos de datos personales» entendidos como contenedores de la información personal; y por otra, aquellas relacionadas con el «tratamiento de los datos» referida a la acción propia del titular, encargado y/o quien resulte responsable. De manera general pueden identificadas las siguientes obligaciones:

TRATAMIENTO DE DATOS PERSONALES	BANCOS DE DATOS PERSONALES
Hacer tratamiento previo consentimiento del titular de los datos. Permitir el ejercicio de los derechos de los titulares de los datos (Derecho de información, acceso, actualización, inclusión, rectificación y supresión, impedir el suministro, oposición, tratamiento objetivo y tutela). Respetar los principios: Legalidad, consentimiento, finalidad, proporcionalidad, calidad, seguridad, disposición de recurso, protección adecuada. Garantizar la protección de la información en las trasferencias nacionales y/o internacionales, implementando las medidas de seguridad que correspondan.	Inscribir el Banco de Datos ante el Registro Nacional de Protección de Datos Personales.Modificar y/o cancelar los Bancos de Datos inscritos, de ser el caso.Disponer de las medidas de seguridad necesarias para la custodia de la información.

Fuente: Elaboración propia

La LPDP recoge 9 principios para el tratamiento de los datos personales los cuales se utilizan como criterios interpretativos para resolver las cuestiones que puedan suscitarse en la aplicación de la propia Ley o de su Reglamento, así como de parámetro para la elaboración de otras disposiciones y para suplir vacíos en la legislación sobre la materia. En ese sentido, a continuación, se desarrollará de forma breve en qué consiste cada uno de dichos principios. Teniendo en cuenta que el propósito de estas líneas no es generar discusión, sino contribuir al conocimiento básico de este derecho, no se analizarán las cuestiones específicas y técnicas que pueden ser desarrolladas en otros escenarios. Veamos.

A nivel internacional, el régimen general de protección de datos personales reconoce como uno de los principios, sino el más importante: el consentimiento. La norma peruana no fue la excepción. El art. 5 de la LPDP y art. 7 de su Reglamento reconocen que antes de realizar cualquier tipo de tratamiento de datos personales debe mediar la autorización de su titular. De esta forma, el tratamiento de los datos personales será lícito solo cuando el titular del dato personal hubiere prestado un consentimiento libre, previo, expreso, informado e inequívoco, prescribiendo de forma expresa que no se admiten fórmulas de consentimiento en las que éste no sea manifestado de forma directa, como aquellas en las que se requiere presumir, o asumir la existencia de una voluntad que no ha sido expresa. Es decir, la norma no admite el consentimiento tácito. Más aún, cuando el tratamiento de datos incluye datos sensibles, el consentimiento debe realizarse –según lo exige la propia norma- por escrito. En complemento, el artículo 12° del reglamento desarrolla las características del consentimiento obtenido en entornos digitales, señalando en el numeral 3 que en estos casos también se considera expresa la manifestación consistente en “hacer clic”,

“cliquear” o “pinchar”, “dar un toque”, “touch” o “pad” y otros similares.

El Reglamento también desarrolla algunos aspectos importantes al respecto, entre los que destaca – por ejemplo- que, a efectos de demostrar la obtención del consentimiento en los términos de la LPDP, la carga de la prueba recae - en todos los casos - en el titular del banco de datos personales o quien resulte el responsable del tratamiento.

Fuente: Elaboración propia

Tanto la doctrina norteamericana de la protección de datos personales como la doctrina europea, reconocen que este principio es el eje sobre el cual se erige todos los demás principios y obligaciones que integran este derecho. Se trata de un punto de coincidencia importante que debe ser estudiado y analizado con rigurosidad y profundidad porque resulta ser el punto de convergencia de todas las legislaciones a nivel mundial.

No existe una sola legislación (independientemente de los matices que se le quiera otorgar) en las que no se requiera el consentimiento – como mínimo previo e informado –para cualquier tratamiento de datos personales. Es precisamente, a partir de este principio del cual se puede llegar a reflexionar en un régimen comunitario para la protección de la privacidad, especialmente en una sociedad como la actual donde las fronteras físicas resultan cada vez más insignificantes.

En el ordenamiento peruano, junto a este importante principio, se encuentran los siguientes:

1. Principio de finalidad en virtud del cual los datos personales deben ser recopilados para un propósito determinado, explícito y lícito; sin extender el tratamiento a otro fin que no haya sido establecida de manera inequívoca como tal al momento de su recopilación. En estos casos se encuentran excluidas las actividades de valor histórico, estadístico o científico, cuando se utilice para ello un procedimiento de disociación o anonimización. Según lo precisa la norma, la finalidad es determinada si ha sido expresada con claridad, sin lugar a confusión; y cuando -de manera objetiva- se ha especificado el objeto que tendrá el tratamiento de los datos personales. Asimismo, la propia norma resalta que cuando el tratamiento incluya datos personales sensibles, su creación solo puede justificarse si su finalidad, además de ser legítima, es concreta y acorde con las actividades o fines explícitos del titular del banco de datos personales. Este principio se encuentra recogido en el art. 6 de la LPDP y art. 8 del Reglamento.
2. Principio de proporcionalidad según el cual se exige que todo tratamiento de datos personales sea adecuado, relevante y no excesivo con la finalidad para la que estos hubiesen sido recopilados. Este principio se encuentra previsto en el art. 7de la LPDP.
3. Principio de calidad en virtud del cual los datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, deben ser actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados. Deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento. El principio de calidad puede encontrarse en el art. 8 de la LPDP y art. 9 del Reglamento.
4. Principio de legalidad, según el cual el tratamiento de los datos personales debe realizarse conforme lo establecido en la ley. En virtud de este principio está prohibida la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos. El art. 4 de la LPDP contiene la descripción de este principio.
5. Principio de seguridad de acuerdo con el cual se exige que quien resulte responsable del banco de datos personales (lugar donde se almacena la información, independientemente del soporte en que se encuentre) debe adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de la información. De acuerdo a lo prescrito en la

norma, 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. El art. 9 de la LPDP y art. 10 del Reglamento han previsto su alcance. Asimismo, el sentido de la norma exige que las medidas de seguridad estén orientadas a evitar cualquier tratamiento contrario a la Ley o al reglamento, tales como la adulteración, la pérdida, las desviaciones de información, intencionales o no, entre otros. La norma no hace ninguna distinción respecto del origen (humano o técnico) de los riesgos. En términos normativos, este principio resulta tan importante que incluso se desarrolla de forma amplia en el Capítulo V del Título III del Reglamento, a través del cual se detallan de forma específica las medidas de seguridad que deben cumplir tanto los bancos de datos personales, así como el tratamiento en general de la información personal.

6. Principio de disposición de recurso según el cual el 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 art. 10 de la LPDP ha previsto el reconocimiento de este principio - derecho.
7. Principio de nivel de protección adecuado, el cual se aplica para los supuestos de flujo transfronterizo de información (supuesto en el cual la información es enviada fuera del territorio nacional). En este caso, la norma exige a quien realiza el tratamiento brindar las garantías necesarias para la protección de la información en el país donde esta será enviada. Según el texto de la norma, dicho país debe tener un nivel suficiente de protección para los datos personales que se vayan a tratar o, por lo menos, equiparable a lo previsto por la norma peruana o equivalente a los estándares internacionales en la materia. Este principio se encuentra en el art. 11 de la LPDP y también se encuentra desarrollado en los estándares internacionales de la materia.

A modo de síntesis, en el siguiente cuadro se muestran los principios que sostienen el régimen de protección de datos personales:

Fuente: Elaboración propia

2.3. Avances en materia de protección de datos tras la vigencia de la LPDP y del reglamento

Con la dación de la LPDP y la publicación de su Reglamento, en el 2011 se creó el órgano garante del derecho a la protección personales, que hasta nuestros días –independientemente de su organización y estructura- resulta ser el principal protagonista de su desarrollo. En ese entonces, se creó la Autoridad Nacional de Protección de Datos Personales (APDP) inicialmente concebida como un órgano de línea adscrito al Despacho Viceministerial de Derechos Humanos y Acceso a la Justicia.

El trabajo realizado por la entonces Autoridad de Protección de Datos Personales entre el 2014-2016 puso de manifiesto un alto índice de afectación al derecho de protección de datos personales de los ciudadanos. Entre las afectaciones más recurrentes se aprecian las siguientes:

1. El tratamiento de datos personales para perfilamientos comerciales era realizado sin contar con el consentimiento de los titulares de la información personal.
2. El envío de la información personal fuera del territorio peruano no tenía si quiera la autorización correspondiente, es decir, el consentimiento del titular los datos.
3. Las transferencias a terceros de la información personal para la prestación de servicios complementarios también eran realizadas sin que el titular de los datos personales tuviera siquiera conocimiento sobre dicha situación.

El trabajo realizado por la entonces APDP fue, después de los aportes del Tribunal Constitucional, una de las principales fuentes desde donde se produjeron las caracterizaciones de este derecho. Ya en esta época el TC había delineado a través de su jurisprudencia el contenido del derecho (al que llamó autodeterminación informativa) y sus resoluciones habían resuelto controversias presentadas especialmente con la protección de la información financiera y previsional. Ahora, con la creación del órgano garante, se asumía la responsabilidad de alcanzar a la sociedad las directrices para convivir en un entorno donde era legítimo oponerse a cualquiera intervención arbitraria sobre la vida privada. La tarea no fue sencilla, pero se lograron importantes objetivos. (Más adelante, se hará referencia por lo menos a los objetivos normativos que tuvieron lugar durante la gestión de la entones APDP).

Luego de varios años, en el 2017 se creó la Autoridad Nacional de Transparencia y Acceso a la Información Pública, y «se fortaleció el régimen de protección de datos personales» existente hasta entonces, mediante la publicación del Decreto Legislativo N° 1353. En junio de ese mismo año se creó la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (DGTAIPD) quien inició formalmente sus funciones a finales de año. La DGTAIPD es el órgano de línea del Despacho Viceministerial de Justicia encargado de ejercer la Autoridad Nacional de Transparencia y Acceso a la Información Pública, así como de ejercer la Autoridad Nacional de Protección de Datos Personales. A su vez, esta Dirección se encuentra compuesta por tres Direcciones: Dirección de Transparencia y Acceso a la Información Pública, Dirección de Protección de Datos Personales y Dirección de Fiscalización e Instrucción.

Hoy, han transcurrido más de 25 años desde que este derecho fue incorporado en la Carta Constitucional de 1993, y durante este tiempo se ha logrado un especial y significativo desarrollo el cual se ve plasmado fundamentalmente en la labor del órgano garante. Es a través de ellos, como los ciudadanos y la sociedad en su conjunto pueden hacer efectiva la garantía, tutela y respeto de este derecho.

A continuación, expondré de la manera más descriptiva posible, los principales instrumentos que – en el ejercicio de sus funciones – ha emitido el órgano garante desde el inicio de sus actividades, a partir de los cuales se puede integrar y conocer el régimen peruano que rige la protección de datos personales en el Perú.

2 . 3. 1. Directiva de Seguridad de la Información Administrada por los Bancos de Datos Personales

Este documento ha sido conocido cotidianamente como «Directiva de Seguridad». Es un documento de naturaleza orientativa que buscaba facilitar el cumplimiento de las obligaciones relacionadas con la seguridad en el marco del tratamiento de los datos personales. El documento, que fue publicado por la APDP, condensa - de modo orientativo- las medidas (técnicas, organizativas y legales) que deben cumplir aquellas personas (naturales o jurídicas) que realicen tratamiento de la información personal.

Para su elaboración se utilizaron como criterios el tipo de banco de datos (lugar donde se almacenaría la información personal), el tipo de tratamiento que se iba a realizar (para determinar si algún supuesto incluía el tratamiento transfronterizo de la información), así como la categoría de la información personal que sería sometida a tratamiento (básicamente para identificar cuándo existía tratamiento de información sensible). Según el contenido de su texto, las características de los bancos de datos personales permitían realizar una clasificación de los mismo. Para tal fin, se buscó correlacionar la naturaleza del banco de datos con los riesgos que dicha naturaleza genera. Esto dio lugar a las obligaciones que el titular de los bancos de datos estaba obligado a cumplir a fin de garantizar su seguridad. Siguiendo este razonamiento, la Directiva identifica bancos de datos básicos, simples, intermedios, complejos y críticos, dependiendo – por ejemplo- el número de datos personales respecto de los cuales se realiza tratamiento, el tiempo durante el cual se realiza el tratamiento de la información, la naturaleza del titular del banco de datos, el periodo de

almacenamiento, entre otros.

Esta Directiva ha sido reconocida como una de las principales iniciativas que han tenido las autoridades iberoamericanas de protección de datos. Si bien el cumplimiento de la Directiva no fue (y hasta ahora no es vinculante) su observancia permite que los titulares de los bancos de datos conozcan de manera objetiva las obligaciones relacionadas con el principio de seguridad– y lo más importante – conozcan los mecanismos sugeridos para garantizar su cumplimiento. A pesar de haber transcurrido varios años desde su elaboración, su contenido se mantiene vigente, aunque su implementación sigue sin ser obligatoria. Esto último, fundamentalmente por dos razones; por un lado, por su propia naturaleza orientativa, y por otro, porque desarrolla únicamente las obligaciones derivadas del principio de seguridad, más no el resto de obligaciones contenidas, tanto en la LPDP como en el reglamento.

Esta Directiva, junto a otro material, se encuentra registrada en el portal web de la actual DGTAIP (https://www.minjus.gob.pe/material-informativo-dp/) y desde ahí se puede acceder fácilmente a su contenido.

2.3.2. Directiva sobre protección de datos personales en el marco de los procedimientos para la construcción, administración, sistematización y actualización de bases de datos personales vinculados con programas sociales y subsidios que administra el Estado.

Mediante Resolución Directoral N° 060-2014-JUS/DGPD publicada en el Diario Oficial “El Peruano” el 25 de julio del 2014 se aprobó la Directiva N° 001-2014-JUS/DGPD sobre la protección de datos personales en el marco de los procedimientos para la construcción, administración, sistematización y actualización de bases de datos personales vinculados con programas sociales y subsidios que administra el Estado.

El objetivo de la Directiva fue establecer las disposiciones generales para el tratamiento y la protección de datos personales en el marco de los programas sociales del Estado. Según dicha Directiva, el Ministerio de Desarrollo e Inclusión Social sería el encargado de garantizar los derechos de los titulares de los datos personales, así como de establecer las medidas de seguridad necesarias para la salvaguarda de la información personal.

Asimismo, con el fin de garantizar la transparencia y permitir la fiscalización, el numeral 6.6 de la Directiva legitimó la publicación de los nombres, apellidos, región y nombre del programa social que le corresponde a cada usuario. En este mismo numeral se precisó también, que el número del documento de identidad, así como el nombre del distrito y la provincia podía ser usados como criterios de búsqueda organizada para acceder a la información publicada.

La Directiva dejó abierta la posibilidad que la entidad encargada de la administración de los programas sociales pueda disponer la publicación en medios físicos de datos adicionales, a fin de garantizar la realización efectiva de sus prestaciones. En esta Directiva expresamente se reconoce, además, que dicha publicación debe realizarse siempre observando el principio de proporcionalidad.

Esta Directiva es especialmente importante porque pone de manifiesto los lineamientos que el propio Gobierno (a través del Ministerio de Inclusión Social y Desarrollo) tenía que prever para el tratamiento de datos a través de los programas sociales.

Aun cuando resulta claro que el Estado es uno de los principales hacedores de la información personal de los ciudadanos, y por lo tanto una Directiva de esta naturaleza es especialmente importante y útil; desde entonces no se ha generado un instrumento de similar naturaleza. Hoy, lo único que se advierte en las normas (y no solo en las relacionadas con tratamiento de los datos personales) es una lista más o menos exhaustiva que expone cuál es la normativa vinculada para el instrumento jurídico que se crea. Si bien dicha acción no es en ningún caso desdeñable, dada las

particularidades de cada caso, es importante que se brinden las orientaciones respecto del tratamiento de los datos personales y se procure, siempre y en todos los escenarios, garantizar la seguridad de los ciudadanos.

2.3.3. Decreto Legislativo N° 1353 que promovió l a creación de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales – DGTAIPD y otros cambios normativos

El 7 de enero del 2017, mediante la publicación del Decreto Legislativo N° 1353, se creó la Autoridad Nacional de Transparencia y Acceso a la Información Pública, y se fortaleció el régimen de protección de datos personales existente hasta entonces. En junio de ese mismo año se publicó el Decreto Supremo N° 013-2017-JUS el cual aprobó el Reglamento de Organización y Funciones del Ministerio de Justicia y creó la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (DGTAIPD). Ambos instrumentos normativos introdujeron algunas reformas legislativas:

La modificatoria permite que cuando no sea el titular del banco de datos personales quien realice el tratamiento de la información debe (siempre y bajo cualquier circunstancia) celebrar un contrato de encargo que permita definir con precisión cuál es el alcance de las obligaciones de quien realiza este tratamiento, así como la delimitación de sus responsabilidades.

En el primer caso, se exige que el titular del banco de datos asuma la responsabilidad que el encargo incluya como obligación establecer un **mecanismo de información personalizado para el titular de los datos personales sobre dicho nuevo encargado de tratamiento. En el segundo caso, se exige que el nuevo titular del banco de datos establezca un mecanismo de información eficaz para el titular de los datos personales sobre dicho nuevo encargado de tratamiento.**

1. **Se introdujo la figura del «encargado del tratamiento de datos personales»** reemplazando lo que decía el art. 2.6 de la LPDP que definía al «encargado del banco de datos personales». El cambio refiere queel **«encargado de tratamiento de datos personales» será «***Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice el tratamiento sin la existencia de un banco de datos personales*»; y agrega en el numeral siguiente que el «e**ncargo de tratamiento» será aquella «*e*ntrega por parte del titular del banco de datos personales a un encargado de tratamiento de datos personales en virtud de una relación jurídica que los vincula. Dicha relación jurídica delimita el ámbito de actuación del encargado de tratamiento de los datos personales».*
2. **Cambios en la regulación del «consentimiento» para el tratamiento de datos personales:** Se precisa que cuando el tratamiento de datos se realiza en el marco de una relación contractual (entiéndase para su ejecución) esta incluiría también las etapas pre contractuales, hasta la propia celebración del contrato. El texto de la modificatoria decía lo siguiente: *Art. 14. - No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos:[…] 5. Cuando los datos personales sean necesarios para la **preparación, celebración y**ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.*
3. **También se introducen nuevas excepciones a la obtención del consentimiento para el tratamiento de datos personales.** Se consideran tres nuevos supuestos en los cuales dicho tratamiento podía ser realizado sin mediar la autorización del titular: a) Cuando el tratamiento se realice para **fines vinculados al sistema de prevención de lavado de activos y financiamiento del terrorismo u otros que respondan a un mandato legal;**

b) Cuando el tratamiento sea realizado por empresas de un mismo grupo económico que comparte información aunque únicamente para fines de prevención de lavado de activos y financiamiento del terrorismo, y otros supuestos de cumplimiento regulatorio; y c) cu**ando el tratamiento se realiza en ejercicio constitucionalmente válido del derecho fundamental a la libertad de información.**

4. **Se introducen dos cambios interesantes sobre el contenido del «derecho de información»** del titular de los datos personales reconociendo que existe un nuevo deber de información al titular de los datos personales en dos supuestos: a) cuando se establezca vinculación con un encargado de tratamiento de forma posterior al consentimiento para el tratamiento de los datos; b) cuando se produzca una transferencia de datos, como resultado de una fusión, adquisición de cartera o supuestos similares.
5. Como complemento, **se precisan cambios respecto de la facultad supervisora y sancionadora de la Autoridad.** En ese sentido, modificando el art. 38 de la LPDP se precisa que esta puede ordenar la implementación de una o más medidas correctivas, con el objetivo de corregir o revertir los efectos que la conducta infractora hubiere ocasionado o evitar que ésta se produzca nuevamente. Asimismo, en el tercer párrafo se reconoce expresamente la responsabilidad objetiva de los administrados por el incumplimiento de obligaciones derivadas de las normas sobre protección de datos personales

Así también, en el 2018 se produjeron dos aportes importantes al régimen peruano de la protección de datos: por un lado, se publicó la Resolución Directoral N° 043-2018-JUS/DGTAIPD del 3 de julio del 2018 mediante la cual se aprobó un modelo de cláusula informativa sobre las circunstancias y condiciones del tratamiento de datos personales requeridas por el artículo 18 de la LPDP; y por otro, se publicó la Resolución Directoral N° 85-2018- JUS/DGTAIPD del 26 de noviembre del 2018 que aprobó la actualización de los formularios para el inicio de procedimientos ante la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales y sus unidades orgánicas. Estos nuevos formularios de inscripción de bancos de datos personales que fueron aprobados incluían la información necesaria para la comunicación de flujo transfronterizo, condensando en una sola solicitud procedimientos que antes se tramitaban de forma separada. Incluso primero se inscribía el banco de datos personales, para luego poder iniciar el procedimiento de comunicación de flujo transfronterizo.

De forma complementaria se publicó el Decreto Legislativo N° 1390 que modifica la ley N° 29571, Código de protección y defensa del consumidor en cuyo artículo 58 se lee: «*El derecho de todo consumidor a la protección contra los métodos comerciales agresivos o engañosos implica que los proveedores no pueden llevar a cabo prácticas que mermen de forma significativa la libertad de elección del consumidor a través de figuras como el acoso, la coacción, la influencia indebida o el dolo. En tal sentido, están prohibidas todas aquellas prácticas comerciales que importen:* [...] *e. Emplear centros de llamada (call centers), sistemas de llamado telefónico, envío de mensajes de texto a celular o de mensajes electrónicos masivos para promover productos y servicios, así como prestar el servicio de tele mercadeo, a todos aquellos números telefónicos y direcciones electrónicas de consumidores que no hayan brindado a los proveedores de dichos bienes y servicios su consentimiento previo, informado, expreso e inequívoco, para la utilización de esta práctica comercial. Este consentimiento puede ser revocado, en cualquier momento y conforme a la normativa que rige la protección de datos personales.* [...]»

En ese sentido, respecto del primer contacto de las empresas con los clientes,la Autoridad se pronunció en los siguientes términos: «… *Siempre consideramos admisible el primer contacto con los consumidores, siendo la forma eficaz de solicitar su consentimiento, y que el inconveniente no se generó por ese primer contacto, sino por las prácticas sistemáticas de acoso por parte de las empresas que nunca aceptaron un no como respuesta, no respetaron las franjas horarias adecuadas para estas llamadas, no implementaron sistemas para que el ciudadano pueda rechazar el uso de sus datos con fines publicitarios*»

Con este nuevo marco normativo, así como con el fortalecimiento del régimen de protección de

datos y la creación de la nueva autoridad en el 2019 se impusieron algunas sanciones importantes: i) Se sancionó a una compañía con una multa de 38.5 UIT por vulnerar su deber de confidencialidad al haber transmitido a otra compañía datos sensibles vinculados a la condición de portador de VIH de uno de sus pacientes; ii) Se impuso una multa de 30.25 UIT a otra empresa por haber solicitado exámenes de VIH de forma desproporcionada, a la luz de la finalidad perseguida para cubrir un puesto de trabajo.

2.3.4. Directiva N° 01-2020-JUS/DGTAIPD sobre el Tratamiento de Datos Personales mediante Sistemas de videovigilancia

El 10 de enero del 2020, mediante Resolución Directoral N° 02-2020-JUS/DGTAIPD se aprueba la Directiva para el Tratamiento de Datos Personales mediante Sistemas de Videovigilancia. El numeral 6.1 de esta Directiva señala que su aplicación está orientada al tratamiento de datos de personas captados a través de los sistemas de videovigilancia, el cual implicaba la grabación, captación, transmisión, conservación o almacenamiento de imágenes o voces, incluida su reproducción o emisión en tiempo real o cualquier otro tratamiento que permita el acceso a los datos personales relacionados con aquellos, para fines – entre otros - de seguridad y control laboral. De modo general, la Directiva señala que, en espacios públicos de uso privado, como establecimientos comerciales, restaurantes, lugares de ocio, entre otras, se deberá cumplir en estricto con el principio de proporcionalidad.

En buena cuenta, el objeto de esta Directiva ha sido brindar las disposiciones generales (a veces demasiado generales) para que los titulares de los bancos de datos o quienes sean los encargados del tratamiento cumplan con las disposiciones, tanto de la LPDP como de su Reglamento, incluidas sus modificatorias.

Lo más resaltante de la Directiva aparece en el numeral 6.11 que, luego de precisar que los accesos a las zonas videoviligadas deben tener un anuncio visible, señala la información mínima que este debe contener: i) Identidad y domicilio del titular del banco de datos personales, ii) Información para el ejercicio de los derechos establecidos en la LPDP. iii) Mecanismos de acceso del informativo adicional. Como complemento, la Directiva señala que dicho cartel debe ser de 297 x 210 mm, salvo que el espacio donde se vaya a ubicar el cartel no lo permita. En este último supuesto, este (el cartel) debe adecuarse al espacio disponible, de tal forma que cumpla su finalidad informativa.

Sin perjuicio de lo anterior, vale resaltar que respecto del tratamiento de la información personal y de la protección de la privacidad en entornos video vigilados, la Directiva hace algunas precisiones adicionales que es importante resaltar:

Vale recordar que el artículo 37 del Reglamento permite que el titular del banco de datos subcontrate, algunas actividades que impliquen tratamiento de datos, con terceros. En ese caso, de acuerdo con su artículo, el subcontratado debería asumir las mismas obligaciones que se establezcan para el titular del banco de datos, responsable o encargado del tratamiento. En el documento suscrito debe consignarse también el deber de confidencialidad en el que se determine la obligación de secreto entre las partes, a efectos de no divulgar la información, así como la prohibición de reproducir, modificar, publicar o difundir o transferir a terceros la información sin autorización expresa de la otra parte.

1. Se precisa que las imágenes y/o voces grabadas se pueden almacenar por un plazo de treinta (30) días y hasta un plazo máximo de sesenta (60), salvo disposición distinta en normas sectoriales.
2. Se señala que cuando videovigilancia utilizada importe que sea otra persona la encargada de la gestión (y esa gestión incluya tratamiento de datos personales) debe suscribirse un contrato, convenio o documento similar en el que se identifique el objeto, la duración, la naturaleza y finalidad del tratamiento, el tipo de datos y categorías de interesados, las obligaciones y derechos que correspondan, así como el destino de los datos al finalizar la

prestación.

3. Se exige que quien realice la gestión de los sistemas de videovigilacia deban contar con procedimientos de identificación y autentificación de usuarios; un inventario documentado de las cámaras u otros dispositivos de videovigilancia; un esquema y/o diagrama documentado de la arquitectura física y lógica del sistema; documentación respecto a la gestión de accesos, privilegios y verificación periódica de privilegios asignados; mecanismos de respaldo de seguridad de la información, así como con un procedimiento para la verificación de la integridad de los datos almacenados en el respaldo; y la implementación de las medidas de seguridad en caso de transporte de los sistemas cuando estos contienen información de carácter personal. El transporte debe ser autorizado por el titular del banco de datos personales; entre otras.

En la parte final, la Directiva contiene disposiciones específicas para sectores especiales como son las empresas del sistema financiero, las instituciones educativas y los centros laborales; así como un apartado especial dedicado al tratamiento de datos con otras tecnologías. Como reglas generales de estas disposiciones especiales, resalta la preminencia de los principios de finalidad, proporcionalidad y seguridad; así como la garantía de los derechos de información, acceso y cancelación.

2.3.5. Opinión Consultiva N° 32-2020-JUS/DGTAIPD que contiene pronunciamiento respecto del t ratamiento de datos de salud durante la pandemia en el ámbito laboral.

Desde finales del 2019 el mundo fue víctima de una de las epidemias más agresivas que va a recordar la historia. Dada la velocidad de propagación y letalidad, todas las actividades se paralizaron y progresivamente se ha instaurado un sistema de “nueva normalidad”.

Los Gobiernos adoptaron medidas de distinta índole para hacer frente a la epidemia, especialmente medidas relacionadas con la salud de la población. En Perú, mediante Resolución Ministerial Nº 239- 2020-MINSA del 28 de abril de 2020 se aprobó el documento técnico denominado “Lineamientos para la vigilancia de la salud de los trabajadores con riesgo de exposición a COVID-19” cuya finalidad fue contribuir a la prevención del contagio de dicha enfermedad en el ámbito laboral público y privado. En este documento se incluyeron instrumentos para el tratamiento de datos sensibles de los trabajadores.

En ese sentido, mediante Opinión Consultiva N° 32-2020-JUS/DGTAIPD del 5 de mayo del 2020, la Autoridad se pronunció respecto de la posibilidad que el empleador realice el tratamiento de datos personales sensibles referidos al COVID-19 de los trabajadores sin su consentimiento, aceptando dicho supuesto; siempre que el tratamiento se realice en el marco de la LPDP y de su Reglamento; y sobre todo tenga como finalidad garantizar la seguridad y salud en el trabajo evitando contagios de esta enfermedad en los centros laborales. Según lo manifiesta la Autoridad: «[…] *resulta lícito que el empleador implemente medidas preventivas dirigidas a detectar si alguno de sus trabajadores ha contraído el COVID-19, como, por ejemplo, la toma de su temperatura, pues un dato que arroje una situación anormal de salud, puede constituir un peligro para los mismos trabajadores, para el resto del personal o para otras personas relacionadas con el centro laboral; por ende, esta medida constituye un medio relacionado con la vigilancia de la salud de los trabajadores que, conforme a la Ley de Seguridad y Salud en el Trabajo, resulta obligatoria para el empleador*.[…]»

Es importante resaltar que la Autoridad también pone de manifiesto la necesidad que el empleador atienda principios que rigen el derecho de protección de datos personales, especialmente el de finalidad, proporcionalidad, calidad y seguridad, tal como se encuentran previstos en la LPDP y su Reglamento.

Aunque el fundamento legal que sirve para argumentar la posición asumida por la Autoridad se encuentra ampliamente detallada en el contenido de la Opinión Consultiva citada, parece suficiente

citar el artículo 14.6 de la LPDP que contiene la excepción a solicitar el consentimiento para el tratamiento de datos personales precisamente cuando se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional; o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud; o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados. (LPDP, artículo 14, numeral 6). En ese sentido, queda claro que para el tratamiento de datos en este contexto que nos toca vivir no requiere del consentimiento explícito del titular de los datos.

De esta manera el derecho a la protección de datos coexiste con la defensa y garantía de otros derechos, como el derecho a la salud y el bien común.

3. CONCLUSI ONES :

Hoy, las nuevas tecnologías se siguen desarrollando, y es un reto para la comunidad global gestionarla de forma que ofrezcan sus beneficios a la ciudadanía sin que lleguen a representar un peligro para la privacidad y seguridad. Han transcurrido varios años desde la vigencia de la LPDP y de su Reglamento; y muchos años más desde que este derecho fuera reconocido en la Carta Constitucional; y todavía existe un largo camino por recorrer. Los avances que se han logrado hasta nuestros días son el resultado del esfuerzo conjunto de quienes, desde diferentes escenarios, promueven y colaboran con la tutela de este derecho. Como se ha puesto de manifiesto antes, la auténtica garantía del derecho a la protección de datos personales, que tiene como fundamento la dignidad humana, se materializará solamente cuando: los Estados brinden los mecanismos y elementos necesarios para su protección; los ciudadanos se empoderen de sus facultades, exijan sus derechos y adopten una verdadera cultura de privacidad; y las empresas internalicen que la protección de la información personal no es una carga sino un compromiso.

El 28 de agosto del 2018 se presentó una importante iniciativa legislativa que contenía Proyecto de Ley que busca fortalecer la actual Autoridad Nacional de Transparencia y Acceso a la Información Pública. El objeto es crear un *Organismo Público Técnico Especializado con personería jurídica de derecho público interno con autonomía técnica, funcional, económica, administrativa y financiera*. En este se propone ampliar las competencias de la actual autoridad para elevarla a la categoría de “organismo técnico especializado”, previsto en la Ley Orgánica del Poder Ejecutivo, con rectoría en las materias de su competencia; y de esta manera fortalecer los mecanismos de garantía de este derecho.

A nivel de derecho comparado, nuestro país – aun con el tiempo transcurrido – todavía tiene un incipiente desarrollo. Los modelos de regulación, especialmente el modelo europeo que es el que inspira nuestro esquema regulatorio, ha protagonizado importantes reformas.

El 25 de mayo del 2016 entró en vigor el Reglamento General de Protección de Datos, el cual cambió sustancialmente el régimen hasta entonces aplicable en los países de la Unión Europea. La norma entró en vigor el 25 de mayo de 2018, y partía de una afirmación fundamental: «*El tratamiento de datos personales debe estar concebido para servir a la humanidad….*». Esta nueva regulación significó la creación de un nuevo esquema en el marco regulatorio, que hasta entonces existía en Europa, y que -en buena cuenta- era el modelo que había inspirado la regulación de varios países de América Latina. Se propuso, entonces, un cambio de paradigma; un cambio que ha buscado migrar del *régimen reactivo* a la *responsabilidad activa* a través de una filosofía preventiva; y que pone de manifiesto la necesidad de una rápida capacidad de adaptación a los nuevos retos que se presentan. La norma supone un mayor compromiso de las organizaciones, tanto públicas como privadas, con el derecho a la protección de datos; sin que esto signifique

necesariamente ni en todos los casos una mayor carga. En muchos casos será sólo una forma de gestionar la protección de datos distinta de la que se viene empleando ahora. Según el Considerando 2 y 3 del propio Reglamento europeo, lo que se busca es «*…contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas física*. »

A la luz de estos cambios normativos, el esquema regulatorio de la protección de datos personales ha variado significativamente de forma positiva en la Unión Europea, impactando no solo en el ciudadano sino también en las empresas y las administraciones públicas; y las ha llevado a crear sinergias especiales de colaboración para la tutela de este derecho. Nosotros no debemos ser ajenos a dichos cambios; especialmente por los avances que se han logrado. Hoy el desarrollo de la tecnología, el tratamiento masivo de la información personal, así como la crisis sanitaria que nos ha tocado vivir nos invita a reflexionar constantemente sobre la vigencia de este derecho; pero sobre todo nos invitar a ser conscientes que el tratamiento de datos personales debe estar concebido para servir a la humanidad y no a la inversa.

4. B IBLIOGRAFÍA DE REFERENCIA

1. ÁLVAREZ-CIENFUEGOS SUÁREZ, J. M. (1999). *La defensa de la intimidad de los ciudadanos y la tecnología informática.* Editorial Aranzadi.
2. BERNALES BALLESTEROS, E. (1999) *La Constitución de 1993. Comentarios.* 5º Edición. Editora RAO SRL.
3. CARNOY, M. (2000). *El trabajo flexible en la era de la información.* Alianza Editorial.
4. CASTELLS M. (2000). *La era de la información*, economía, sociedad y cultura. *La sociedad red*. Vol. 1. Editorial Alianza.
5. CORRAL TALCIANI, H. (2000) "Configuración jurídica del derecho a la privacidad I: Origen, desarrollo y fundamentos" en *Revista Chilena de Derecho*, Volumen 27, Nº 1.
6. CORRALES, M.; BARNITZKE, B y FORGÓ NIKOLAUS; BOUCHOUX, María Clara. (2011). *Aspectos Legales de la computación en la Nube: protección de datos y marco general sobre propiedad intelectual en la legislación europea*. Tomo I. Editorial Allbremática.
7. COSTA PICAZO, R. (trad.) (2001) *IBM y el Holocausto.* Editorial Atlántida.
8. CUKIER, K. (2014) *Losbig datayelfuturode losnegocios.* Editorial del BBVA.
9. EVANS, P. (2014) *Reinventarla empresaen la eradigital.* Editorial del BBVA.
10. FUNDACIÓN KONRAD ADENAUER STIFTUNG. (2009). *Jurisprudencia del Tribunal Constitucional Federal Alemán. Extractos de las sentencias más relevantes compiladas por JürgenSchwabe.* Editorial Fundación Konrad Adenauer.
11. GARCÍA MEXÍA (2005) *PrincipiosdeDerechodeInternet.*Editorial Tirant lo Blanch.
12. GONZÁLEZ, ENRIC (2001) "IBM, al servicio del holocausto: Un libro describe cómo el régimen de Hitler clasificó a sus víctimas con material de la firma estadounidense" en *Diario El País,* Ediciones El País S.L.
13. GONZÁLEZ, F. (2015) *Reinventar la empresa en la era digital.* Editorial BBVA, Madrid, 2015.
14. GOZAÍNI, O. (2001) *Habeas data protección de datos personales.* Editorial Rubinzal-Culzoni, Buenos Aires.
15. HERNÁNDEZ LÓPEZ, J. (2013). *El derecho a la protección de Datos Personales en la Doctrina del Tribunal Constitucional,* Editorial Thomson Reuters Aranzadi.
16. HERRÁN ORTIZ, A. (1998) *La violación de la intimidad en la protección de datos personales.* Editorial Dykinson.
17. KRESALJA, B.; OCHOA C. (2009) *Derecho Constitucional Económico.* Fondo Editorial de la Universidad Católica del Perú.
18. ISACA (2009) *Computación en la nube: Beneficios de negocio con perspectivas de seguridad, gobierno y Aseguramiento,* Editorial Isaca.
19. MARR, B. (2015). *Big Data: Using smart Big Data, Analytics and Metrics to Make Better*

Decisions and Improve Performance,Editorial Wiley.
20. PALMA ENCALADA, L. (2006) "El proceso de hábeas data en el diseño del Código Procesal Constitucional" en *El derecho procesal constitucional peruano. Estudios en Homenaje a Domingo García Belaúnde,* Tomo II,Editorial Grijley
21. PIÑAR MAÑAS, J.L. (2009) *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo.
22. PIÑAR MAÑAS, J. L. (2010) *¿Existeprivacidad?enProtecciónde datospersonales. C ompendiodelecturasylegislación*,Editorial Tiro Corto Editores.
23. PUENTE DE LA MORA, X. (2011) "Protección de datos personales en México ante el modelo norteamericano y el modelo europeo" en *Derecho y TIC 10.0,* Editorial Temis.
24. SALDAÑA, (2012) "The right to privacy". La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis" en *UNED,Revista de Derecho Político,* Nº 85.
25. WARREN, S. D. y BRANDEIS, L. D. (1890) "The right to privacy" en *Harvard Law Review*, Vol. IV, Nº 5, Washington, 1890.
26. Jurisprudencia del Tribunal Constitucional peruano:

1. STC del 29 de enero del 2003 recaída sobre el Expediente Nº 1797-2002-HD/TC
2. STC del 18 de enero del 2002 recaída sobre el Expediente Nº 0197-2000-HD/TC
3. STC del 16 de noviembre del 2007 recaída sobre el Expediente Nº 03052-2007-PHD/TC
4. STC del 24 de julio del 2012 recaída sobre el Expediente N° 00693-2012-PHD/TC
5. STC del 30 de enero del 2014 recaída sobre el Expediente N° 06227-2013-PHD/TC
6. STC del 7 de agosto del 2014 recaída sobre el Expediente N° 02491-2013-PHD/TC
7. STC del 23 de octubre del 2014 recaída sobre el Expediente Nº 03468-2013-PHD/TC
8. STC del 7 de agosto del 2014 recaída sobre el Expediente Nº 03700-2010-PHD/TC
9. STC del 18 de marzo del 2011 recaída sobre el Expediente Nº 0831-2010-PHD/TC
10. STC del 30 de mayo del 2011 recaída sobre el Expediente Nº 04227-2009-PHD/TC
11. STC del 21 de agosto del 2014 recaída sobre el Expediente Nº 02995-2013-PHD/TC
12. STC del 21 de agosto del 2014 recaída sobre el Expediente Nº 02324-2013-PHD/TC
13. Jurisprudencia del Tribunal Constitucional español
14. STC Nº 254/1993 del 20 de julio
15. STC Nº 143/1994 del 9 de mayo
16. STC Nº 11/1998 del 13 de enero
17. STC Nº 33/1998 del 11 de febrero
18. STC Nº 35/1998 del 11 de febrero

1. STC Nº 45/1998 del 24 de febrero
2. STC Nº 60/1998 del 16 de marzo
3. STC Nº 77/1998 del 31 de marzo
4. STC Nº 104/1998 del 18 de mayo
5. STC Nº 105/1998 del 18 de mayo
6. STC Nº 106/1998 del 18 de mayo
7. STC Nº 123/1998 del 15 de junio
8. STC Nº 124/1998 del 15 de junio
9. STC Nº 125/1998 del 15 de junio
10. STC Nº 126/1998 del 15 de junio
11. STC Nº 158/1998 del 15 de junio
12. STC Nº 198/1998 del 15 de junio
13. STC Nº 223/1998 del 15 de junio
14. STC Nº 30/1999 del 8 de marzo
15. STC Nº 44/1999 del 22 de marzo
16. STC Nº 45/1999 del 22 de marzo
17. STC Nº 202/1999 del 8 de noviembre
18. Resoluciones emitidas por la Autoridad Nacional de Protección de Datos Personales del Perú:

1. Resolución Directoral Nº 009-2015-JUS/DGPDP del 30 de abril del 2015
2. Resolución Directoral Nº 017-2015-JUS/DGPDP del 26 de junio de 2015 recaída sobre el Expediente Nº 001-2015-PS.
3. Resolución Directoral Nº 037-2015-JUS/DGPDP-DS del 14 de julio de 2011 recaída sobre el Expediente Nº 009-2015-JUS/DGPDP-PS.
4. Resolución Directoral Nº 025-2015-JUS/DGPDP del 16 de setiembre de 2015 recaída sobre el Expediente Nº 006-2015-PS.
5. Resolución Directoral Nº 026-2015-JUS/DGPDP del 16 de setiembre de 2015 recaída sobre el Expediente Nº 010-2015-PS.
6. Resolución Directoral Nº 028-2015-JUS/DGPDP del 21 de setiembre de 2015 recaída sobre el Expediente Nº 040-2015-PS.
7. Resolución Directoral Nº042-2015-JUS/DGPDP del 07 de diciembre de 2015 recaída sobre el Expediente Nº 028-2015-PS.
8. Resolución Directoral N° 101-2015-JUS/DGPDP-DS de fecha 30 de noviembre de 2015 recaída sobre el Expediente Nº 012-2015-JUS/DGPDP-PS.
9. Resolución Directoral N° 020-2016-JUS/DGPDP de fecha 232 de febrero de 2016 recaída sobre el Expediente Nº 025-2015-PS.
10. Resolución Directoral Nº 016-2016-JUS/DGPDP-DS del 18 de enero de 2016 recaída sobre el Expediente Nº 021-2015-JUS/DGPDP-PS.
11. Resolución Directoral Nº 025-2016-JUS/DGPDP-DS del 28 de enero de 2016 recaída sobre el Expediente Nº 031-2015-JUS/DGPDP-PS.
12. Resolución Directoral Nº039-2015-JUS/DGPDP del 07 de diciembre de 2015 recaída sobre el Expediente Nº 080-2015-PS.
13. Resolución Directoral N° 006-2016-JUS/DGPDP de fecha 22 de enero de 2016 recaída sobre el Expediente Nº 018-2015-PS.
14. Resolución Directoral Nº 028-2015-JUS/DGPDP del 21 de setiembre de 2015 recaída sobre el Expediente Nº 040-2015-PS.
15. Resolución Nª 022-2015-JUS/DGPDP de 30 de julio de 2015 recaída sobre el Expediente Nº 004-2015-PTT.
16. Resolución Nª 003-2015-JUS/DGPDP de 20 de febrero de 2015 recaída sobre el Expediente Nº 016-2014-PTT.

Citas