



LA PROTECCIÓN DE LA PRIVACIDAD COMO OBJETO DE TUTELA EN EL ORDENAMIENTO JURÍDICO PERUANO

Milagros Katherine Olivos Celis¹

INFORMACIÓN DEL ARTÍCULO

Historia del artículo:

Recibido el 1 de octubre de 2018

Aceptado el 1 de diciembre de 2019

Palabras claves:

Derechos fundamentales

Protección de datos personales

Autodeterminación informativa

Libertades económicas

RESUMEN

Las siguientes líneas proponen analizar –desde un enfoque descriptivo y crítico– la configuración legal de este derecho en el ordenamiento jurídico peruano. Esto se ha realizado teniendo como punto de partida las primeras conceptualizaciones teóricas y legislativas formuladas en los modelos tradicionales que han servido de inspiración a varios países latinoamericanos para legislar en la materia, junto a las razones que motivaron la redacción de la fórmula legislativa tal como se encuentra prevista en el art. 2.6 de la Carta Constitucional, permitiendo conocer el escenario en el que –diez años después– surge su ley de desarrollo con su posterior entrada en vigencia.

The Protection of Privacy as a purpose of guardianship in the Peruvian Legal System

ABSTRACT

Keywords:

Fundamental rights

Protection of personal data

Self-determination information

Economic freedoms

The following lines propose the analysis –from a descriptive and critical approach– of the legal configuration of this right in the Peruvian legal system. This has been done taking as a starting point the first theoretical and legislative conceptualizations formulated in the traditional models that have served as an inspiration to several Latin American countries to legislate on the matter, together with the reasons that led to the drafting of the legislative formula as stated in the art. 2.6 of the Constitution (1993). It allows knowing the background in which – ten years later – this law has been developed and entered into force.

¹ Máster en Derecho por la Universidad de Zaragoza, España Máster en Derecho y Empresa por la Universidad Católica Santo Toribio de Mogrovejo, Perú. e-mail: molivos@isdeh.org

1. A MODO DE INTRODUCCIÓN: LA NECESIDAD DE NO QUEDARNOS DETENIDOS EN EL TIEMPO

El uso de la información personal ha sido, desde épocas antiguas, una actividad característica de las sociedades. En las sociedades desarrolladas, el uso de los datos como insumo económico de gran valía, fue reconocido como una práctica ancestral que se revolucionó con la llegada de la tecnología. Así, los recientes avances provenientes, especialmente de la informática, superaron exponencialmente lo que en su época significó la escritura y la imprenta, permitiendo desarrollar hoy nuevas formas en la gestión de la información. Sin embargo, cuando este desarrollo aunado al tratamiento de la información personal comenzó a producir afectaciones en la vida privada de las personas, el Derecho vio la necesidad de responder a dicho fenómeno, promoviendo desde sus fundamentos normas para regularlo.

Sobre esto último, cabe recordar el Censo de Población que tuvo lugar en Alemania en 1933; a través del cual, bajo un disfraz de legitimidad y legalidad, y como una acción estadística racional y planificada, el Estado recopiló gran cantidad de información personal, que posteriormente sería utilizada para ejecutar uno de los mayores crímenes contra la humanidad durante la época del *holocausto nazi* (González, 2001). A pesar que la Ley que autorizaba la realización de dicho censo fue declarada inconstitucional en 1983 (Schwabe, 2009)², su ejecución permitió recoger una cantidad de información importante sobre judíos, gitanos y homosexuales, brindando a los *nazis* una importante herramienta de control social sobre la población. La información fue analizada a través de un procesador de datos que permitió confeccionar listas y automatizar la persecución,

especialmente de judíos, mediante la creación de grupos destinados a la deportación a los campos de exterminio (Costa, 2001)³. En la sentencia de 1983, el Tribunal Constitucional Federal Alemán 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 mismos⁴. Ésta, entre otras circunstancias, exigieron que el Derecho brinde respuestas y garantías para la protección y defensa de los ciudadanos, pues las circunstancias estaban poniendo en evidencia que el tratamiento masivo de los datos personales y el tráfico de los mismos constituían una amenaza al sistema de derechos fundamentales, haciendo vulnerables a las personas en su día a día (Remolina, 2012). Así, la protección de la privacidad nace como una respuesta a un problema real. “El riesgo inherente al manejo vertiginoso y no siempre bien intencionado de la información en un entorno en que las tecnologías evolucionan de una manera que la humanidad nunca antes conoció” (Quiroga, 2015, p.37).

Ante este contexto, los diferentes países del mundo adoptaron en su Derecho interno regulaciones específicas para protegerse de invasiones arbitrarias a esferas de la vida que solo les corresponden a las personas. Lo propio hicieron los diferentes organismos internacionales quienes mediante declaraciones y/o recomendaciones han puesto de manifiesto la necesidad de tomar decisiones para atender los riesgos generados por los avances de la tecnología, especialmente de la informática.

Existen dos importantes modelos que han concebido la protección y tutela de la privacidad como un bien jurídicamente tutelado. Por un lado el modelo europeo, con una tradición sumamente

² Sentencia de la Primera Sala del Tribunal Constitucional Federal Alemán, del 15 de diciembre, 1983 (1, BvR 209, 269, 362, 420, 440, 484/83).

³ Recientes publicaciones históricas han puesto de manifiesto que una de las empresas de tecnología más importante del mundo, IBM –denominada durante esa época *Deutsche Hollerith Maschinen GmbH (Dehomag)*– fue quien facilitó la

utilización sistemática de los ordenadores (procesadores de datos) por parte de los *nazis* para que pudieran identificar y detener de forma eficiente a judíos y otras minorías, para utilizarlos como esclavos y finalmente exterminarlos.

⁴ Sentencia de la Primera Sala del Tribunal Constitucional Federal Alemán, del 15 de diciembre, 1983 (1, BvR 209, 269, 362, 420, 440, 484/83), fundamentos jurídicos III y IV.

protectora y defensora de la información personal y precursora de su configuración como derecho fundamental con una configuración propia; y por otro lado, el modelo norteamericano, con una posición sumamente diferente, pues lejos de proteger la información personal como derecho fundamental establece el marco normativo para su libre circulación y fomento del comercio (Puente, 2011).

A diferencia de lo que, en su momento, sucedió en Estados Unidos y en los demás países de la Comunidad Europea, América Latina inició el desarrollo del camino de la protección de este derecho desde hace algunos años, y aunque con pasos significativos, su progreso todavía es inicial. Hoy, han transcurrido aproximadamente 35 años del surgimiento de las primeras normas para proteger la información personal, y desde entonces se ha forjado un intenso camino en su desarrollo.

Lamentablemente, el intento por conocer y regular el uso de la información personal, a fin de evitar intromisiones arbitrarias en la vida de los ciudadanos, ha ocasionado el surgimiento de distintos conceptos para referirse a un mismo fenómeno. En el Perú, lo que queda claro es que con la incorporación del artículo 2.6 en la Carta Constitucional en 1993, la dación de la Ley N° 29733, Ley de Protección de Datos Personales, la publicación y su posterior entrada en vigencia tras la emisión de su Reglamento en el 2013, y la creación del órgano garante (Autoridad Nacional de Protección de Datos Personales) que tutela este derecho, se colocaron los primeros cimientos para crear un sistema de protección y defensa este derecho.

Todavía queda un largo camino por recorrer; primero, para lograr un desarrollo tan significativo como lo han hecho el resto de países del mundo; y segundo para estar atentos a los avances que la tecnología genera, los cuales crecen de manera progresiva tan solo con el transcurrir del tiempo.

⁵ Hawking (2014) sostiene que «si miramos hacia el futuro, no hay límites a lo que podemos lograr en este campo. No hay ley física que impida que las partículas en un sistema de Inteligencia Artificial ser re-ordenen a sí mismas para realizar

No obstante, reconociendo la importancia del tema y el alcance global que se busca alcanzar, es necesario generar algunas reflexiones que puedan constituir un primer punto de partida en el estudio de este derecho. En ese sentido, a continuación, se presenta –desde un enfoque descriptivo y crítico– el análisis de la configuración de este derecho en el ordenamiento jurídico peruano. Esto se ha desarrollado teniendo como punto de partida las primeras conceptualizaciones teóricas y legislativas formuladas tanto en Estados Unidos como en Europa (especialmente en España), junto a las razones que motivaron a los legisladores a redactar la fórmula legislativa tal como se encuentra prevista en el art. 2.6 de la Carta Constitucional, permitiendo conocer el escenario en el que – diez años después– surge su ley de desarrollo con su posterior entrada en vigencia. Esto permitirá tener una apertura racional para las modificaciones estructurales y legislativas que sean necesarias.

2. EL USO DE LA INFORMACIÓN PERSONAL Y EL CONTEXTO HISTÓRICO DE SU PROTECCIÓN.

El desarrollo de la sociedad actual demanda, cada vez con mayor frecuencia, el uso de datos y más datos; tal es así que los procesos económicos de producción y distribución de bienes y servicios son inconcebibles en una sociedad tecnológicamente desarrollada sin antes conocer información sobre las preferencias, gustos, estadísticas, porcentajes, etc.

Hasta fines del siglo XIX no existía la vida privada como objeto de protección jurídica. Sin embargo, el avance de la ciencia y la tecnología, especialmente de la informática ha generado que, en nuestros días, esto ya no sea una novedad. Su desarrollo durante las últimas décadas ha cobrado cada vez mayor realce⁵. Sin embargo,

cálculos más complejos de los que somos capaces de hacer los seres humanos. Es perfectamente posible que se produzca un salto radical e inesperado (...)»

desde siempre, tanto el tratamiento de la información personal, así como la preocupación por su protección ha estado presente en el comportamiento social de todas las civilizaciones. Hernández (2013) haciendo referencia a los antecedentes históricos de las formas de protección de la información personal, señala que los ejemplos más antiguos que existen sobre este tema son el Juramento de Hipócrates (cuya vigencia se mantiene hasta la actualidad⁶) y el secreto de confesión (contenido en el IV Concilio de Letrán de 1215, y a través del cual se impuso a los ministros la obligación de guardar el secreto sacramental⁷).

Desde un enfoque jurídico, la historia también reporta manifestaciones que reflejaron el reconocimiento de la vida privada. En este contexto, la correspondencia y el domicilio constituyeron bienes de la persona dignos de protección jurídica, por lo que su inmunidad aparece como una figura penal típica que obedece al deseo de proteger al individuo frente a la amenaza que proviene del Estado (Corral, 2000). La ampliación de esta percepción (vida privada como un interés digno de protección) tiene su origen en el pensamiento de John Stuart Mill (1997), cuya doctrina intenta ofrecer una nueva visión sobre los límites del poder en un régimen democrático. En la teoría de Mill, la amenaza para los individuos ya no estaría en los abusos de un tirano o de una oligarquía, sino en el poder de las mayorías democráticas. De acuerdo con esta posición, era necesario respetar, no sólo la libertad de opinión sino también la libertad de conducta

que incluía el ámbito de su conciencia, sus pensamientos, sus sentimientos, expresiones, gustos y propósitos.

De acuerdo con la interpretación realizada por Corral (2000), en la doctrina de Mill, el ámbito de la vida libre se contrapone, ya no al poder del Estado o de la ley, sino al poder del control social, es decir, al poder de las masas. Sobre ello, se erige un derecho de propiedad entendido – en aquel entonces – como un ámbito propio en el cual nadie puede entrar sin permiso del titular⁸.

Entre las construcciones doctrinales respecto de la tutela de este derecho, destacan los aportes de Thomas Cooley quien en 1980 hizo referencia al «*the right to be let alone*» y la contribución de Warren y Brandeis «*The Right to Privacy*» (Warren y Brandeis, 1890). El establecimiento del concepto «derecho a la vida privada» se encuentra en estos últimos textos (Murillo y Piñar, s.f.). Sin embargo, a pesar de sus precisiones conceptuales, estos planteamientos no obtuvieron repercusión inmediata en las sentencias de los tribunales norteamericanos. La situación cambió cuando en los años siguientes, éstos deberían enfrentarse con más frecuencia a casos en los que una persona se sentía agraviada por una publicación o fotografía indiscreta (Corral, 2000). Así por ejemplo, en 1902 la Corte de Apelaciones de New York, en el caso *Roberson vs Rochester Folding Box Co.* resolvió la demanda del uso de una fotografía sin autorización del titular de la

⁶ «[...] De todo aquello que vea u oiga en la sociedad durante el ejercicio o de mi profesión, e incluso fuera de él, callaré lo que no necesita ser divulgado, considerando la discreción como un deber en semejante caso.» Cita de Hipócrates (Hersh, 1984)

⁷ «¡Qué cuidadosamente informarse acerca de la circunstancia del pecador y el pecado, para que con prudencia puede discernir qué tipo de consejos que debe dar y qué remedio a aplicar, utilizando diversos medios para curar a la persona enferma! Que se tome el máximo cuidado, sin embargo, no traicionar el pecador en absoluto por la palabra o signo, o de cualquier otra manera. Si el sacerdote necesita sabios consejos, que lo buscan con cautela, sin ninguna mención de la persona en cuestión. Por si alguien se atreve a revelar un pecado revelada a él en confesión, decreto que no es sólo para ser

depuesto de su oficio sacerdotal, sino también a ser confinado a un monasterio estrictas para hacer penitencia perpetua.» (IV Concilio de Letrán, 1215, Canon 21).

⁸ Esta suerte de intromisión no cesaría de diversificarse a lo largo de todo el siglo XX, con nuevos mecanismos de intrusión y difusión de lo privado: desde la interceptación de las comunicaciones telefónicas, pasando por la filmación, grabación y difusión televisiva, hasta el fichaje digital o la registración vía electrónica o cibernética. Durante esos años, la aparición de la fotografía, y con ella, el desarrollo de los medios de prensa y de comunicación masiva marcan un momento especial. Aparece entonces una forma de invasión en lo propio o personal que era desconocida: las historias e imágenes íntimas pueden llegar a ser fácilmente difundidas.

imagen⁹. En la decisión, el Tribunal declaró que el derecho a la privacidad no existía, y que la víctima no estaba protegida contra esa conducta. Esta decisión fue duramente criticada, hasta que la legislatura de New York aprobara un estatuto para prohibir el uso comercial de retratos o fotos de una persona sin su permiso. Tres años después, la Corte Suprema de Georgia, al resolver el caso *Pavensich Vs. New England Life Znsurance Co.* rechaza el precedente de Robertson y reconoce la existencia del «*right to the privacy*»; esto marca el comienzo de una nueva línea jurisprudencial (Corral, 2000).

Algunos años después, en 1967 aparece otro aporte cognitivo de especial relevancia, bajo la autoría del profesor Alan Furman Westin (1967)¹⁰. En su obra, Westin define la «privacidad» como 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.*». Importantes estudios de la doctrina comparada

⁹ En el caso el demandado había hecho uso de la fotografía de una mujer joven sin el consentimiento de ésta para anunciar harina.

¹⁰ Alan Furman Westin (1929–2013) fue profesor emérito de Derecho Público y Gobierno de la Universidad de Columbia, ex editor de las Revistas *Privacidad* y *American Business*; y ex presidente del Centro de Investigaciones Sociales y Jurídicas. Westin escribió grandes libros: «Privacidad, Confidencialidad y Libertad» en 1967; y «Bancos de datos en una sociedad libre» en 1972. Ambos libros fueron los primeros trabajos que motivaron la legislación sobre privacidad. Se especializó en el estudio del impacto de las tecnologías de la información en las operaciones gubernamentales nacionales y locales, a partir de la toma de decisiones para la atención al ciudadano y la libertad de la administración de la información. Sus planteamientos fueron traducidos en su libro «Tecnología de la Información en una democracia» publicado en 1971. En 1993, junto a Robert Belair, fundó el instituto «*Privacy & American Business*» que proporcionaba análisis en temas sobre privacidad y negocios. En el 2005, Westin recibió el Premio «Privacy Leadership Award» otorgado por la *International Association of Privacy Professionals*. Murió el 18 de febrero de 2013 en Nueva Jersey. (Scalet, 2003).

¹¹ El 15 de diciembre 1983, el Tribunal Constitucional alemán dicta su Sentencia sobre el Censo en la que se refleja aportes de la doctrina, en su mayoría norteamericana y en particular los aportes de Westin, que se habían producido en orden a destacar el control sobre la propia información en la configuración del derecho a la privacidad y a la protección de datos. El Tribunal

atribuyen a este autor la definición del concepto «*privacidad*» en términos de «*autodeterminación (self determination)*», concepto que más tarde fue expresamente asumido por el Tribunal Constitucional Federal Alemán en su Sentencia del 15 de diciembre de 1983 sobre el Censo de 1933¹¹. Una posición similar fue asumida por el Tribunal Constitucional español quien como consecuencia de sus razonamientos reconoce el derecho fundamental a la «*autodeterminación informativa*» basado en los derecho de la personalidad y con protección frente a la recogida, almacenamiento, utilización y transmisión ilimitada de información personal, garantizando a los individuos la facultad de decidir por sí mismos sobre su difusión y la utilización¹². Estas posiciones, también fueron utilizadas por el Tribunal Constitucional peruano, como más adelante veremos¹³.

En varios ordenamientos, este derecho se desarrolló tomando en cuenta sus características morfológicas y la técnica jurisprudencial de sus

Constitucional Alemán completó los derechos constitucionales de la personalidad a pesar de la inexistencia en la Ley Fundamental de 1949 de un derecho específico. Sobre la base del derecho a la dignidad humana y al libre desarrollo de la personalidad el Tribunal garantizó la continuidad de las libertades básicas, consagradas con anterioridad, con la formulación de un nuevo derecho, el derecho a la autodeterminación informativa. Cfr. MURILLO DE LA CUEVA, Pablo Lucas y PIÑAR MAÑAS, José Luis: *Ob. Cit.*; págs. 88–89. También puede consultarse la traducción de la Sentencia en HEREDERO HIGUERAS, M.: "La sentencia del Tribunal Constitucional de la República Federal Alemana relativa al censo de población de 1983" en *Documentación Administrativa*, N° 198, Madrid, 1984, págs. 139–158.

¹² La protección de datos personales, como una prerrogativa autónoma e independiente, devino de las STC 290/2000 y 292/2000, ambas del 30 de noviembre de 2000.

¹³ Similar posición fue asumida por el Tribunal Constitucional español quien como consecuencia de sus razonamientos reconoce el derecho fundamental a la «autodeterminación informativa» basado en el derecho de la personalidad y con protección frente a la recogida, almacenamiento, utilización y transmisión ilimitada de información personal, garantizando a los individuos la facultad de decidir por sí mismos sobre su difusión y la utilización. La protección de datos personales, como una prerrogativa autónoma e independiente, devino de las STC 290/2000 y 292/2000, ambas del 30 de noviembre de 2000.

Tribunales. En este contexto, en el derecho comparado – y especialmente en la doctrina – pueden encontrarse elaboraciones teóricas que buscan desde reconocer este derecho como una extensión del derecho a la intimidad, hasta formulaciones legislativas que han identificado a la privacidad como el bien jurídico autónomo que el derecho a la protección de datos personales busca proteger¹⁴.

En el ordenamiento jurídico peruano, la legislación que desarrolla el modelo de protección de este derecho emplea la denominación «*protección de datos personales*» para referirse a la protección de la vida privada. Así, el artículo 1 de la LPDP reconoce como su objeto de tutela la garantía del derecho fundamental previsto en el artículo 2.6 de la Constitución Política del Perú, e identifica a la privacidad como su objeto de tutela. Este conocimiento y reconocimiento supone un paso decisivo en toda sociedad que consolida los pilares fundamentales de un Estado Social y Democrático de Derecho: *la dignidad y la libertad* (Cano, 2009)¹⁵.

Finalmente, después de tiempo se ha reconocido normativamente el valor actual de la información personal y el derecho a la protección de los datos personales. Como ya se ha señalado, la mayor

parte de los derechos de los Estados Iberoamericanos reconocen este derecho, sea por referencia directa de su Constitución, o como consecuencia de las decisiones adoptadas por sus órganos judiciales.

3. LA PRIVACIDAD COMO OBJETO DE PROTECCIÓN EN EL ORDENAMIENTO JURÍDICO PERUANO Y EL DISEÑO DE SU FÓRMULA LEGISLATIVA

Varios ordenamientos jurídicos han optado por desarrollar este derecho en función de sus características morfológicas y la técnica jurisprudencial de sus Tribunales. Así, en el derecho comparado – muy especialmente en la doctrina – pueden encontrarse elaboraciones teóricas que buscan desde reconocer la protección de la vida privada como la extensión del derecho a la intimidad, y hasta formulaciones legislativas que han identificado a la privacidad como el bien jurídico autónomo que el derecho a la protección de datos personales busca proteger.

En muchos casos, la discusión se centraba en determinar el verdadero fundamento de la protección de este nuevo derecho. Por un lado, hay

¹⁴ Por un lado, se sostiene que se trata de un derecho derivado de otros derechos fundamentales preexistentes, como son el derecho a la intimidad personal y familiar. Por ejemplo, en nuestros días todavía es común encontrar doctrina que identifica ambos derechos o que reconoce el derecho a la protección de datos personales como una proyección del derecho a la intimidad. (García, s.f.). El autor citado sostiene: «El reconocimiento del derecho a la intimidad – en sus diversas manifestaciones – luego de lograr su consolidación como un derecho fundamental, ha ido alcanzando nuevos matices. (...) Por ello, el derecho a la intimidad ha tenido que ir redireccionando su ámbito de protección donde además de la facultad del individuo de rechazar las invasiones a su ámbito privado, ahora supone el reconocimiento de un derecho de control y acceso de sus informaciones, es decir de toda aquella información relativa a su persona. (...)» Por otro lado, hay quienes sostienen que se trata de un derecho nuevo y autónomo cuyo fundamento radica en el reconocimiento de la dignidad humana como valor supremo y fundamental en las sociedades democráticas. Esta discusión se ha presentado especialmente en España donde, en su momento, se analizó si el derecho a la protección de datos personales derivaba del

artículo 18.4 de la CE (Art. 18.4 de la CE.– *La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*), tal como lo sostiene la STC 290/2000 y 292/2000; o si, por el contrario, era un derecho cuyo fundamento se encontraba en el artículo 10.1 de la CE (Art. 10.1 de la CE.– *La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social.*) y, por tanto, se sustentaba en la dignidad de la persona o en el propio derecho a la intimidad reconocido en el art. 18.1 del mismo texto constitucional. (Art. 18.1 de la CE. – *Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*) Cabe resaltar que el derecho a la protección de datos personales no se encuentra en la relación de derechos de la CE. (Hernandez, 2013)

¹⁵ El autor y otros explican que si un ciudadano no sabe qué informaciones sobre su persona se han recogido y almacenado, ni qué uso se les va a dar, no puede actuar con la misma libertad, tanto en su vida privada como en su vida en sociedad, que si supiera qué datos se han recogido, y pudiera disponer y controlar el uso que se les va a dar.

quienes sostienen que se trata de un derecho derivado y análogo a otros derechos fundamentales preexistentes, como son el derecho a la intimidad personal y familiar¹⁶. Y por otro lado, hay quienes argumentan que se trata de un derecho nuevo y autónomo cuyo fundamento radica en el reconocimiento de la dignidad humana como valor supremo y fundamental en las sociedades democráticas.

Una posición interesante aparece en el profesor Alguacil (2001) quien al defender la extensión del derecho a la protección de datos personales para garantizar otros derechos de las personas, distinto del derecho al honor y a la intimidad, importa la admisión de un nuevo derecho, un derecho diferente al derecho a la intimidad, o que si se quiere, lo complementa.

En el Perú, la Carta constitucional no utiliza ninguna acepción concreta; sin embargo, el desarrollo jurisprudencial del Tribunal Constitucional peruano (siguiendo a su homólogo español) ha preferido utilizar la denominación de «autodeterminación informativa» precisamente para referirse al derecho contenido en el numeral 6 del artículo 2 de la Constitución del '93: *Toda persona tiene derecho a que los servicios informáticos computarizados o no, públicos o privados, no suministren información que afectan la intimidad personal y familiar.*

A pesar que el desarrollo legislativo y jurisprudencial de este derecho inició aproximadamente al promediar los años 50 del

siglo pasado, recién el Constituyente peruano del 1993, a pesar de las objeciones iniciales, asumió con responsabilidad la necesidad de reconocer y tutelar la defensa de la privacidad. El art. 2.6 de la CPP reconoce que toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

La incorporación de este artículo se aprobó en la 5° Sesión (matinal) realizada el 25 de enero de 1993. El debate fue dirigido por Congresistas Carlos Torres y Torres Lara, Enrique Chirinos Soto y Martha Chávez Cossío.

Según la información contenida en el Diario de Debates de la Comisión de Constitución y Reglamento, inicialmente se discutió si este derecho que se intentaba tutelar era suficiente como para merecer un artículo independiente en el catálogo de Derechos fundamentales de la Constitución. Al mismo tiempo se discutía sobre la posibilidad de incorporarlo como parte del art. 2.7 referido a la protección de la intimidad, o como parte del art. 2.10 referido al secreto de las comunicaciones¹⁷.

Para esto, resultan especialmente emblemáticos los cuestionamientos que se hacían los legisladores respecto del significado del objeto de la tutela de este derecho. En este punto, por ejemplo, la Congresista Chávez Cossio se planteaba las siguientes reflexiones:

¹⁶ Por ejemplo, en nuestros días todavía es común encontrar doctrina que identifica ambos derechos o que reconoce el derecho a la protección de datos personales como una proyección del derecho a la intimidad. García (s.f.) sostiene: «El reconocimiento del derecho a la intimidad – en sus diversas manifestaciones – luego de lograr su consolidación como un derecho fundamental, ha ido alcanzando nuevos matices. (...) Por ello, el derecho a la intimidad ha tenido que ir redireccionando su ámbito de protección donde además de la facultad del individuo de rechazar las invasiones a su ámbito privado, ahora supone el reconocimiento de un derecho de control y acceso de sus informaciones, es decir de toda aquella información relativa a su persona. (...)»

¹⁷ Por un lado, el congresista Cáceres Velásquez señaló «(...) propongo que el inciso, que está sustentado por la mayoría, se involucre dentro de lo que es el inciso 10), porque no pienso

que tenga el rango suficiente para constituir un inciso independiente de la Constitución.»; y por otro el Congresista Ferrero Costa sostenía: «En todo caso, si aceptáramos el criterio que sostiene Róger Cáceres, que tiene una duda cuyo origen solamente yo comparto, habría que ver si es que la información personal de carácter íntimo es más una cuestión de intimidad o privacidad o es, más bien, una cuestión de comunicación; porque nuestro inciso 10) trata básicamente de los papeles privados y de las comunicaciones, mientras que el problema de la intimidad personal está en el inciso 7). Le sugiero al Dr. Cáceres que, mientras vamos discutiendo este tema, analice lo que le estoy planteando: el problema de la intimidad personal en nuestra Constitución está, más bien, alrededor del inciso 7), y no alrededor del inciso 10).» (Congreso de la República, 1993).

«Nadie me puede exigir una información que yo misma he conseguido respecto de alguien. Por ejemplo, si como empleador yo sé que mi trabajador ha sufrido de tuberculosis, necesito tener esa información en mi archivo, porque eso va a determinar, por ejemplo, que no lo pueda mandar a trabajar en una obra submarina. Entonces, en todo caso, lo que podrían prohibirme es que yo proporcione esa información.¹⁸» (Congreso de la República, p.162)

En un sentido similar el Congresista Olivera Vega expresaba lo siguiente:

«[...] dentro de los alcances [...] de esta supresión de información de los servicios privados, también podría llegar a los medios de comunicación y sus unidades de investigación. Yo me pregunto si, dentro de este alcance, se podría llegar a que los medios de comunicación suprimieran todas las investigaciones o referencias a las actividades personales del señor Vladimiro Montesinos, por ejemplo; si invocando esto habría que anular cualquier tipo de referencia de un personaje que es público, tal como hasta lo han aceptado funcionarios públicos del servicio de inteligencia nacional, y, en general, de cualquier tema que la prensa o persona particular considere dentro de su libertad individual.» (Congreso de la República, p.162)

Ante esto, el Congresista Torres y Torres Larra aclara la discusión en los siguientes términos:

«Este inciso no intenta impedir que alguien tenga información, incluso secreta, sobre la situación de la persona; esto no es una limitación a eso. En consecuencia, en lo que respecta a los papeles privados, cualquier persona o entidad puede tener informaciones sobre la intimidad de otra persona, como la tiene un médico, un abogado, un confesor, un periodista; eso no está prohibido.

En este momento, lo que el derecho exige, de acuerdo a los cambios actuales, es prohibir que los sistemas informáticos —vale decir, computarizados— que manejen globalmente esta información puedan reproducirla nacional o

internacionalmente, con la enorme facilidad que los caracteriza. Como vemos, hay una gran diferencia entre el manejo privado que se puede hacer sobre información, también privada, y el concepto del uso masivo de esta información a través de los sistemas computarizados.» (Congreso de la República, p.162)

Frente a los cuestionamientos planteados se optó por reflexionar sobre si hay o no hay datos que deberían estar prohibidos poseer porque no guardan relación con la actividad que se desarrolla; y el Congresista Torres y Torres Lara terminó expresando

«El problema de la informática, señor Presidente, tiene varios aspectos. Uno de ellos ya lo hemos tratado: el acceso de la ciudadanía a la información. El otro gran pedido que se ha abierto en la comunidad mundial es porque algunas instituciones —sean públicas o privadas, secretas o no— negocian e influyen sobre la comunidad en general con los datos íntimos de las personas, lo cual va contra la dignidad de éstas. [...] No estamos inventando este derecho, sino que se ha recogido en los últimos diez años de las modificaciones constitucionales más modernas, como el caso de Brasil, que ha establecido precisamente el habeas data. [...] Esto quiere decir que nadie está en el derecho de ir contra la dignidad de una persona para que, a través de sistemas masivos de información, se generalicen informaciones que pertenecen solamente a su persona» (Congreso de la República, p.165)

Finalmente, tras estas discusiones, se incorpora a la Constitución Política de 1993 el art. 2.6 que reconoce la tutela de la privacidad como objeto del derecho a la protección de datos personales¹⁹. La discusión parlamentaria final se llevó a cabo en la 10^oB Sesión (Matinal) del 22 de febrero de 1993. Esto se registró en el Diario de Debate del Pleno, el Congreso Constituyente Democrático (Congreso Constituyente Democrático, 1998)

En este contexto, el Congresista Torres y Torres Lara volvió a resaltar la relevancia de la

¹⁸ Cfr. CONGRESO DE LA REPÚBLICA DEL PERÚ, "5^o Sesión (matinal) (162).

¹⁹ El texto fue aprobado por 8 votos a favor y 3 en contra. Posterior a ello, el texto constitucional pasó a debatirse en el Pleno del Congreso.

incorporación del reconocimiento de un derecho de esta naturaleza²⁰. Traducimos acá algunas cuestiones que parecen importantes:

«Se trata, igualmente, de una importante innovación que no contiene nuestra Constitución, y que sí la contienen algunas constituciones modernas, como la de Brasil, especialmente, y, de modo parcial, la de España o la de Portugal. [...] El poder, decíamos en nuestra anterior intervención, nace ahora de la información. Pero, ¿quién maneja la información, y cómo se maneja? Se maneja esta información, ahora, en un sistema diferente al tradicional. Cuando una persona podía acumular información en un cuaderno, en unos archivos, no tenía mayor efecto social; pero hoy, cuando la información se puede acumular a través de las computadoras, adquiere un poder incluso transnacional. [...] Como se ha analizado ampliamente en la filosofía y en la psicología modernas, quien conoce el secreto de otras personas tiene poder sobre ellas. Y aquí entramos en el tema de la intimidad personal. [...] Hemos analizado en la Comisión las enormes dificultades que implica esta nueva tecnología en la defensa de los derechos de la persona, y hemos llegado a la conclusión de que la obtención de la información y su conservación no es el problema fundamental, sino la comunicación de esta información. [...] En consecuencia, la protección que debe dar la Constitución es que nadie pueda transmitir informaciones que estén referidas a la intimidad personal a través de los medios comunes; [...] En otras palabras, se intenta, pues, establecer un derecho, un mecanismo para proteger al ciudadano del desarrollo de la informática, en el sentido de que la informática sirva para el desarrollo de la economía y para el desarrollo de los patrimonios, pero que no vaya contra la intimidad personal o familiar» (Torres, 1989, p. 112)

²⁰ Para profundizar en el análisis de los planteamientos transcritos puede consultarse TORRES Y TORRES LARA, Carlos: "Nociones preliminares sobre el Derecho de la informática y la informática jurídica", en *Revista Peruana de Derecho de la Empresa*, N° 32, Lima, 1989, págs. 49 –78; y MARCENARO FERS, R.: "El derecho a la intimidad y la informática" en *Revista*

Finalmente, tras del debate y de introducir algunas modificaciones al texto inicialmente propuesto se terminó aprobando por unanimidad la siguiente fórmula: «*Inciso 6. A que los servicios informáticos computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal o familiar.*»

En general, esto significa que el ordenamiento jurídico peruano reconoció la protección de los datos personales como derecho fundamental, con rango constitucional y separada de la protección de los derechos vinculados a la privacidad o intimidad desde 1993; acompañándola, además, de la correspondiente acción de garantía, a través del Habeas Data que conforme al artículo 200, de la propia Constitución que señala "*procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2, incisos 5 y 6 de la Constitución*".

Efectivamente, se trata de un derecho fundamental, un concepto lleno de contenido en sí mismo que, producto de un largo proceso de gestación, desarrollo y afirmación, ha ganado su autonomía en relación con otros derechos.

La doctrina peruana poco se ha preocupado sobre la denominación del derecho que se tutela a través del artículo 2.6 de la CPP. Sin embargo, de la transcripción de los textos contenidos en los Diarios de Debates parece ser que la intención del Constituyente era legislar un «derecho nuevo».

A pesar de ello, parece importante resaltar que la fórmula legislativa utilizada para redactar el art. 2.6 de la CPP tampoco resulta muy pacífica; pues el mismo texto constitucional señala que se trata de una «*protección ante el suministro de informaciones que afecten la intimidad personal y familiar*»; aun cuando dichos bienes jurídicos son tutelados por el artículo siguiente²¹. Más aun, la legislación se complementa con el texto contenido

Peruana de Derecho de la Empresa, N° 32, Lima, 1989, págs. 79 – 100.

²¹ Artículo 2.7 de la CPP. – Toda persona tiene derecho [...] Al honor y a la buena reputación, a la intimidad personal y familiar, así como a la voz y a la imagen propias. Toda persona afectada por afirmaciones inexactas o agraviada en cualquier

en el Código Procesal Constitucional que en su art. 61.2 expresa lo siguiente:

«El hábeas data procede en la defensa de los derechos constitucionales reconocidos por los incisos 5 y 6 del artículo 2 de la Constitución, en consecuencia toda persona puede acudir a dicho proceso para: [...] Conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentran almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicios o accesos a terceros. Asimismo, a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos fundamentales.».

De esta forma se separan los mecanismos de tutela de dos derechos que resultan marcadamente diferenciados. Esto sin duda, produce un mejor tratamiento en la configuración del derecho fundamental y completa lo normado en el texto Constitucional, otorgándosele a los ciudadanos una herramienta útil para que puedan protegerse.

4. ANÁLISIS DEL CONTENIDO DEL ARTÍCULO 2.6 DE LA CONSTITUCIÓN PERUANA Y SU TÉCNICA DE DESARROLLO A TRAVÉS DE LA LEY N° 29733, LEY DE PROTECCIÓN DE DATOS PERSONALES.

La amplia esfera donde interactúa el derecho contenido en el artículo 2.6 de la CPP permite reconocer múltiples ejes de acción, que en nuestro país se ha materializado, no solo desde los distintos pronunciamientos del Tribunal Constitucional (en el que se reconoce el «derecho

a la autodeterminación informativa»), sino con la dación y vigencia de la Ley de Protección de Datos Personales. Este derecho fundamental, reconocido y protegido con la Constitución de 1993 surge a fin de evitar una nueva forma de control oculto sobre la vida de los humanos por el abuso del poder informático. Este derecho, entre otras cosas, consiste en poder disponer de los datos de información propios y, por tanto, permitir o rehusar su uso, en controlar la veracidad de su contenido, el acceso a su conocimiento por parte de terceros, el uso que de ellos se haga con finalidades sociales, económicas y políticas, etc.

La interpretación doctrinal que analiza este derecho sostiene que el texto constitucional del artículo 2.6 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 (Morales, 2007). Esto último sucede porque tanto las personas naturales como jurídicas, públicas o privadas, con el fin de mejorar sus niveles de competitividad, utilizan con mayor frecuencia nuevos instrumentos que incrementan exponencialmente el uso, acceso y transferencia de información de distinta índole, especialmente aquella de tipo personal. Algunas manifestaciones de lo afirmado se reflejan, por ejemplo, en la gestión de procesos electorales a través de la biometría, monitoreo de pronósticos con imágenes satelitales, sucursales bancarias en teléfonos inteligentes, diagnóstico médicos con máquinas de alta especialización, la implementación de la historia clínica electrónica, entre varios otros (García, 2005).

En este quehacer cotidiano, las actividades económicas constituyen un ámbito de especial relevancia; y en este escenario, la persona –en su rol de agente económico– se encuentra particularmente expuesta a tratamientos relevantes de su información personal.

medio de comunicación social tiene derecho a que éste se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley.

Jurisprudencialmente, el Tribunal Constitucional desarrolló este derecho antes de la promulgación de LPDP, al amparo de lo prescrito por el Código Procesal Constitucional. Desde sus primeras resoluciones el Tribunal utilizó la denominación «autodeterminación informativa» para referirse al derecho reconocido en el art. 2.6 de la Carta Constitucional. La importancia de este reconocimiento radica en la decisión del propio Tribunal de diferenciarlo de otros derechos como son la intimidad, el honor, la imagen. El TC ha reconocido el *derecho a la autodeterminación informativa* como un derecho independiente (Sentencia Tribunal Constitucional, 29 de enero 2003), siguiendo las denominaciones propuestas en su momento por el Tribunal Constitucional Federal de Alemania y el Tribunal Constitucional español.

Una de las primeras sentencias que emitió el máximo intérprete de la Constitución se produjo tres años después de la incorporación del art. 2.6 en la CPP. Entonces el Tribunal delineó el contenido constitucional de este derecho en los siguientes términos:

«El hábeas data [como instrumento que tutela el derecho consagrado en el inciso 6 del artículo 2° de la Constitución] constituye un proceso al que cualquier justiciable pueda recurrir con el objeto de acceder a los registros de información almacenados en centros informáticos o computarizados, cualquiera sea su naturaleza, a fin de ratificar, actualizar, excluir determinado conjunto de datos personales, o impedir que se propague información que pueda ser lesiva al derecho constitucional a la intimidad.»

En el mismo sentido ha señalado que su protección comprende: i) La capacidad de exigir jurisdiccionalmente la posibilidad de acceder a los registros de información, computarizados o no, cualquiera que sea su naturaleza, en los que se encuentren almacenados los datos de una

persona. Explica el Tribunal que tal acceso puede tener por objeto que se permita conocer qué es lo que se encuentra registrado, para qué y para quién se realizó el registro de información, así como la (o las) persona(s) que recabaron dicha información. ii) La posibilidad de agregar datos al registro que se tenga, ya sea por la necesidad de que se actualicen los que se encuentran registrados, o bien con el fin de que se incluyan aquellos no registrados, pero que son necesarios para que se tenga una cabal referencia sobre la imagen e identidad de la persona afectada. iii) La oportunidad de rectificar la información, personal o familiar, que se haya registrado; impedir que esta se difunda para fines distintos de aquellos que justificaron su registro o, incluso, tiene la potestad de cancelar aquellos que razonablemente no debieran encontrarse almacenados (Sentencia Tribunal Constitucional, 16 de noviembre 2007, 3)²².

Resulta interesante observar que el TC, aunque utiliza la denominación *autodeterminación informativa*, se refiere al derecho contenido en el artículo 2.6 de la CPP; incluso antes de la promulgación de la LPDP, configurando y delimitando su contenido.

Su jurisprudencia ha hecho referencia, entre otras cosas, a diferenciar a uno y otros derechos aparentemente similares. Al respecto ha señalado que «la autodeterminación informativa» se diferencia:

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

²² Antes de este pronunciamiento, el TC había asumido dicha posición en el ya citado STC del 18 de enero del 2002 recaída

sobre el Expediente N° 0197-2000-HD/TC, fundamento jurídico N° 4.

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 (Sentencia Tribunal Constitucional, 18 de enero 2002, 3)²³.

Explica el TC que este derecho 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 a través de los ordenadores electrónicos.

Entre el 2012 y el 2014 el Tribunal Constitucional, emitió algunos pronunciamientos sobre controversias relacionadas con el – utilizando su denominación original– derecho a la autodeterminación informativa (Sentencia Tribunal Constitucional, 24 de julio 2012, 6)²⁴.

Los pronunciamientos obtenidos durante esos años hacen referencia a algunos lineamientos para

el ejercicio legítimo del derecho que el TC denominó autodeterminación informativa, aun cuando sino porque además durante estos años ya empezaban los esbozos legislativos de una ley sobre la materia. De hecho, en algunos pronunciamientos se hace referencia a dicha norma. 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.(2013, 5)²⁵»

De forma particular, en el año 2014 el Tribunal comienza a brindarle mayor contenido al derecho

²³ En complemento a lo anterior mediante sentencia recaída en el Expediente N° 04739–2007–PHD/TC el Tribunal ha sostenido que: «El 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; por tanto, no 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 [...]. 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.»

²⁴ «El derecho a la autodeterminación informativa también supone que una persona pueda hacer uso de la información privada que existe sobre ella, ya sea que la información se encuentre almacenada o en disposición de entidades públicas, o sea de carácter privado. En ese sentido, parece razonable afirmar que una persona tiene derecho a obtener copia de la información particular que le concierne, al margen de si ésta se encuentra disponible en una entidad pública o privada». En ese sentido el Tribunal advierte que la entrega de la información solicitada por la recurrente resulta parcial y por lo tanto se evidencia la afectación del derecho de acceso a la autodeterminación informativa, por lo que corresponde estimar la demanda. (Fundamentos jurídicos N° 6–9).

²⁵ Con similares referencias, se resuelve en la STC del 21 de agosto del 2014 recaída sobre el Expediente N° 02995–2013–PHD/TC, STC del 21 de agosto del 2014 recaída sobre el Expediente N°02324–2013–PHD/TC; y en la STC del 23 de junio de 2014 recaída en el Expediente N° 03025–2013–PHD/TC.

que sigue denominando *autodeterminación informativa* y emite algunos pronunciamientos especialmente importantes²⁶ relacionadas con las actividades que realizan las centrales de riesgo en lo que respecta al tratamiento de información personal.

En el mismo sentido, el TC plantea también algunos lineamientos importantes. Tal es el caso de la STS del 23 de octubre del 2014 recaída en el Expediente N° 03468-2013-PHD/TC, en la cual el Tribunal sostuvo: «*La entidad o banco de datos encargada de resguardar datos personales no tiene la obligación de crear o generar información con la cual no cuente*». En este caso el Tribunal evidenció que la petición del recurrente no se encontraba destinada a acceder a información preexistente, sino que pretendía la emisión de certificados de discapacidad que aún no han sido aún elaborados, situación que no lesionaba derecho a la autodeterminación informativa invocado. Asimismo, el Tribunal – citando la LPDP recuerda al recurrente su derecho para solicitar el acceso al citado documento conforme lo dispone el artículo 19° de la Ley de Protección de datos personales.

5. LA PROTECCIÓN, DEFENSA Y GARANTÍA DE LA PRIVACIDAD EN EL PERÚ A TRAVÉS DE LA LPDP: ALGUNAS REFLEXIONES EN TORNO A LA REAL EXISTENCIA DE UN SISTEMA DE PROTECCIÓN.

El artículo 2.6 de la CPP de 1993 reconoce como objeto de tutela, la protección de la privacidad. Los mecanismos de defensa de este derecho se han desarrollado a través de la LPDP y de su respectivo Reglamento, cuya vigencia empezó desde julio del 2011.

²⁶ Recuérdese que a partir del 2011, el art. 2.6 de la CP de 1993 fue desarrollado con la promulgación y vigencia de la Ley N° 29773, Ley de Protección de Datos Personales y su Reglamento, cuyo contenido será desarrollado en los apartados siguientes.

²⁷ En adelante DCF.

²⁸ Dicha disposición señalaba: «La presente Ley entra en vigencia conforme a lo siguiente: 1. Las disposiciones previstas

El 3 de julio del 2011 se publicó en el Diario Oficial *El Peruano* la Ley N° 29733, Ley de Protección de Datos Personales, en cuya 12° Disposición Complementaria Final²⁷ se regularon los aspectos relacionados a su vigencia²⁸. Tal como puede leerse del texto de la norma, la primera parte de la 12° DCF señalaba que las obligaciones vigentes al día siguiente de la publicación de la norma eran:

- Título II referido al tratamiento de datos personales y el consentimiento, obligaciones sobre el flujo transfronterizo, seguridad en el tratamiento de los datos personales, confidencialidad de los datos personales;
- Art. 32° (primer párrafo) referido a la creación de la Autoridad Nacional de Protección de Datos Personales (APDP);
- 1° DCF que trata sobre la elaboración del reglamento a través de una comisión presidida por la APDP;
- 2° DCF referida a la elaboración de la directiva de seguridad de la información;
- 3° DCF que reconoce el plazo de adecuación para los documentos de gestión y del Texto Único de Procedimientos Administrativos del Ministerio de Justicia;
- 4° DCF que introduce las modificaciones a las leyes existentes a efectos de su adecuación a la LPDP;
- 9° DCF referido a la no afectación de facultades de la administración tributaria;
- 10° DCF sobre el financiamiento.

En complemento a ello, el segundo numeral de dicha disposición precisaba que el resto de obligaciones resultarían exigibles 30 días hábiles después de la publicación del Reglamento, el cual tenía un periodo de 120 días para elaborarse (Art. 1° DFC). Y adicionalmente, la 5° DFC de la misma LPDP señalaba que los bancos de datos personales preexistentes a la vigencia de la norma tenían que

en el Título II, en el primer párrafo del artículo 32 y en las primera, segunda, tercera, cuarta, novena y décima disposiciones complementarias finales rigen a partir del día siguiente de la publicación de esta Ley. 2. Las demás disposiciones rigen en el plazo de treinta días hábiles, contado a partir de la publicación del reglamento de la presente Ley.»

esperar el *plazo de adecuación* que sería definido también en el reglamento²⁹, sin perjuicio de las obligaciones derivadas del artículo 29°.

Fundamentalmente, dicho artículo 29° contiene la obligación de inscribir los Bancos de Datos Personales ante el Registro Nacional de Protección de Datos Personales, señalando su finalidad, identidad, así como el domicilio de su titular o del encargado, de ser el caso³⁰. Ahora, al no encontrarse contenida en ninguna de las referencias de la primera parte de la 12° DFC, su vigencia tendría que esperar los 30 días hábiles posteriores a fecha de la publicación del reglamento³¹, es decir su cumplimiento sería exigible a partir del 8 de mayo del 2013.

Y esto significaba; primero, que una parte de las obligaciones contenidas en la LPDP entraron en vigencia al día siguiente de la publicación de la ley, y las demás entrarían en vigencia 30 días después de la publicación del Reglamento. Segundo, que los bancos de datos preexistentes a la vigencia de la ley tendrían un «plazo de adecuación», que sería determinado por el Reglamento y contado desde la publicación de éste. Tercero, que era obligación de los ciudadanos (o por lo menos de quienes están relacionados con las cuestiones jurídicas de la actividad empresarial) conocer cuál era el alcance, exigencias y limitaciones de la norma; y, evidentemente, cómo afectaba dicha regulación a las empresas (tanto del sector público, como del sector privado). Más aún cuando ésta norma materializaba uno de los derechos fundamentales contenidos en la Constitución Política del Perú de 1993, el derecho a la privacidad. (Art. 2 inc. 6 de la CPP)³². Hasta aquí, es posible esquematizar lo antes referido de la siguiente manera:

²⁹ 5° DFC de la LPDP.– «Los bancos de datos personales creados con anterioridad a la presente Ley y sus respectivos reglamentos deben adecuarse a esta norma dentro del plazo que establezca el reglamento. Sin perjuicio de ello, sus titulares deben declararlos ante la Autoridad Nacional de Protección de Datos Personales, con sujeción a lo dispuesto en el artículo 29.»

³⁰ Literalmente, el referido artículo señala: «La creación, modificación o cancelación de bancos de datos personales de administración pública y de administración privada se sujetan a lo que establezca el reglamento, salvo la existencia de

Cuadro N° 01 Vigencia de la Ley de Protección de Datos Personales en el Ordenamiento Jurídico peruano (Parte I)

3 de julio del 2011	4 de julio del 2011	3 de julio del 2011 + 120 días hábiles
Publicación de la LPDP	Vigencias de las primeras obligaciones	Vigencia de las demás obligaciones
	(Principio de aplicación inmediata)	(Principio de aplicación inmediata)
	Tratamiento de datos personales y el consentimiento	El resto de obligaciones de la LPDP tendría que esperar 30 días contados desde la publicación del Reglamento.
	Flujo transfronterizo	
	Seguridad en el tratamiento de los datos personales	
	Confidencialidad de los datos personales	
	Creación de la APDP	
	Elaboración del reglamento	
	Elaboración de la directiva de seguridad de la información	
	Adecuación de procedimientos del Ministerio de Justicia	
	Codificaciones a las leyes existentes a efectos de su adecuación a la LPDP;	
	Las facultades de la administración tributaria	
	El financiamiento	

Fuente: Elaboración propia

Tal como lo ordenaba la 1° DCF de la LPDP, para la elaboración del Reglamento se constituyó una comisión multisectorial presidida por la Autoridad

disposiciones especiales contenidas en otras leyes. En todo caso, se garantiza la publicidad sobre su existencia, finalidad, identidad y el domicilio de su titular y, de ser el caso, de su encargado.»

³¹ Según lo disponía el numeral 2 de la 12° DFC.

³² Denominado por el Tribunal Constitucional como «derecho a la autodeterminación informativa». El Tribunal Constitucional definió este derecho en su sentencia de fecha 29 de enero de 2003 en el Expediente N° 1797-2002-HD/TC, en el marco de un proceso de hábeas data.

de Protección de Datos Personales, la cual tuvo un plazo de 120 días hábiles para concluir su encargo³³.

El 22 de marzo del 2013 el Diario Oficial «El Peruano» publicó el Decreto Supremo N° 003-2013 mediante el cual se aprobaba el reglamento de la Ley N° 29733, Ley de Protección de Datos Personales. El artículo 3° de dicho Decreto Supremo señalaba que la vigencia del reglamento sería treinta (30) días hábiles posteriores a su fecha de publicación, es decir el 8 de mayo del 2013. Esto implicaba también que en esa misma fecha se activarían las disposiciones de la LPDP que esperaban la reglamentación³⁴.

No obstante, el reglamento también tenía sus propias disposiciones para la vigencia de algunas obligaciones. En primer lugar señalaba que el «plazo de adecuación» para los bancos de datos personales preexistentes a la vigencia de la norma era de dos (2) años, sin perjuicio – claro está – de la obligación de registro contenida en el artículo 29° de la ley³⁵. Y en segundo lugar precisaba que la facultad sancionadora de la Dirección General de Protección de Datos Personales, en relación a los bancos de datos personales preexistentes a la vigencia del reglamento estaba suspendida hasta el vencimiento del plazo de adecuación de los dos (2) años concedido por el mismo reglamento³⁶. Y ¿qué sucedería con las demás facultades de la APDP y el resto de disposiciones del reglamento? El artículo 3° del Decreto Supremo que aprueba el reglamento señalaba que éste en su conjunto entraba en vigencia 30 días después de su publicación; por lo que debería interpretarse que

³³ 1° DCF de la LPDP.- Para la elaboración del proyecto de reglamento, se constituye una comisión multisectorial, la que es presidida por la Autoridad Nacional de Protección de Datos Personales. El proyecto de reglamento es elaborado en un plazo máximo de ciento veinte días hábiles, a partir de la instalación de la comisión multisectorial, lo que debe ocurrir en un plazo no mayor de quince días hábiles, contado a partir del día siguiente de la publicación de la presente Ley.

³⁴ El segundo numeral de la 12° DFC señalaba que las disposiciones de la LPDP (no especificadas en el numeral 1) regirían en el plazo de treinta días hábiles, contado a partir de la publicación del reglamento de la Ley.

³⁵ 1° DC del reglamento.- Adecuación de bancos de datos personales. En el plazo de dos (2) años de la entrada en vigencia

la única salvedad era el «plazo de adecuación» contenido en la 1° DCF.

Cuadro N° 02 Vigencia de la Ley de Protección de Datos Personales en el Ordenamiento Jurídico peruano (Parte II)

22 de marzo de 2013	22 de marzo de 2013	8 de mayo de 2015
<ul style="list-style-type: none"> • Publicación del Reglamento 	<ul style="list-style-type: none"> + 30 días hábiles = 8 de mayo de 2013 • Vigencia de las disposiciones de la LPDP que esperaban reglamentación. (Aplicación suspendida) Vigencia del Reglamento (Principio de aplicación diferida) Artículo 3° del Decreto Supremo N° 003-2013 mediante el cual se aprobaba el Reglamento. 	<ul style="list-style-type: none"> • Vigencia de las obligaciones respecto de los bancos de datos personales preexistentes a la vigencia de la norma. <p>Plazo de adecuación: 2 años, contados desde la vigencia del reglamento.</p>

Fuente: Elaboración propia

Transcurridos los 30 días hábiles posteriores a la publicación del reglamento, casi la totalidad de la normativa respecto de la protección de datos personales estaría vigente; especialmente aquella relacionada con el tratamiento de los datos personales y todo lo que ello implicaba.

En ese sentido, en la medida que las obligaciones resultaban predicables del tratamiento de datos, 30 días hábiles posteriores a la publicación del reglamento eran exigibles aquellas disposiciones

del presente reglamento, los bancos de datos personales existentes, deben adecuarse a lo establecido por la Ley y el presente reglamento, sin perjuicio de la inscripción a que se refiere la 5° DCF de la Ley N° 29733, Ley de Protección de Datos Personales.

³⁶ 2° DC del reglamento.- Facultad sancionadora. La facultad sancionadora de la Dirección General de Protección de Datos Personales, en relación a los bancos de datos personales existentes a la fecha de la entrada en vigencia del presente reglamento, queda suspendida hasta el vencimiento del plazo de adecuación establecido en la Primera Disposición Complementaria Transitoria.

respecto de los principios, el consentimiento, el ejercicio de los derechos de los titulares de los datos, la transferencia de la información. Y con referencia a las obligaciones que recaen sobre los bancos de datos, únicamente eran exigibles las obligaciones relacionadas con la inscripción del Banco de Datos ante el Registro Nacional de Protección de Datos Personales.

Por tanto, las medidas de seguridad necesarias para la custodia de la información, era lo que quedaba sujeto al «plazo de adecuación» de dos (2) años siempre que los bancos de datos hayan sido creados antes de la vigencia de la norma, esto es, antes del 8 de mayo del 2013.

La diferenciación inicialmente planteada sobre las obligaciones respecto de los bancos de datos personales, como contenedor de la información personal; y del tratamiento de los datos personales, como acción propia del titular, encargado y/o responsable, explicaría también el sentido del «plazo de adecuación» contenido en la 5° DFC de la Ley y la 1° DC del reglamento; entendiéndose que aquello que se encontraba suspendido eran las obligaciones respecto de los bancos de datos personales preexistentes a la vigencia de la norma, y que el reglamento determinó el periodo de dos (2) años; más no las obligaciones generadas por el tratamiento de la información personal.

¿Cuáles son esas obligaciones? Hasta este análisis se han logrado determinar tres obligaciones concretas: 1. Inscribir el Banco de Datos ante el Registro Nacional de Protección de Datos Personales. 2. Modificar y/o cancelar los Bancos de Datos inscritos, de ser el caso. 3. Disponer de las medidas de seguridad necesarias para la custodia de la información. Las dos primeras obligaciones se encuentran estrechamente vinculadas, por lo que es concretamente la tercera la que entrará en vigencia después del 8 de mayo del 2015 y comenzará a ser exigible por parte de la Autoridad Nacional de Protección de Datos Personales, la APDP.

De lo antes descrito se deriva la pregunta final ¿Qué sucedería el 8 de mayo del 2015? Por un lado, habrá vencido el «plazo de adecuación» para los

bancos de datos personales creados con anterioridad a la vigencia de la norma; y por otro, con el vencimiento de dicho plazo también entrará en vigencia la facultad sancionadora de la APDP respecto de estos bancos de datos.

Esta regulación creó para los peruanos un nuevo paradigma, fortaleciendo no solo la garantía de un derecho constitucionalmente reconocido, sino además la materialización de un derecho indispensable para esta nueva era de la tecnología y la informática, propia del siglo XXI.

Sin embargo, dada la naturaleza de este – para nosotros– nuevo régimen, rápidamente el sector empresarial cuestionó su poca flexibilidad en algunos casos y su excesiva rigurosidad en otros; subordinando –en su mayoría– la defensa de un derecho fundamental a distintas valoraciones, especialmente de índole económica (Galvez, 2015). Uno de los primeros cuestionamientos que surgieron, al publicarse la Ley estuvo relacionado con los gastos que generaría a las empresas su adecuación, pues se consideró que la regulación era excesiva y se convertiría en un importante sobre costo para los negocios.

En ese sentido – a criterios de quienes argumentan en contra de esta ley– resultaba poco coherente exigir obligaciones que demandaban un incremento de costos en las transacciones, desaceleración de la economía, ausencia de inversiones, dificultades para el desarrollo de los negocios, además de situaciones que afectan, en general, la libertad de empresa (Gálvez, 2015). Por tanto, argumentando y sosteniendo que durante los últimos años ha sido intención del Gobierno reactivar el crecimiento económico, se consideró que una ley de esta naturaleza limitaba las actividades comerciales, pues lo que antes era lícito hacerlo libremente; ahora *hay que pedir permiso* (Quiroga, 2014, p– 84). Y esto es así porque, tras la entrada en vigencia de la LPDP y su reglamento, las empresas no podrán utilizar deliberadamente la información personal que tengan en su poder.

Bajo el argumento de que las normas sobre protección de datos personales conspiran contra el deseo de incentivar que las empresas compitan

por mejorar el diseño de los productos o servicios para ganar al consumidor; parece haberse olvidado que para un Estado de Derecho como el nuestro resulta altamente cuestionable que la garantía de un derecho fundamental dependa de la valorización económica que pueda hacer un empresario (Quiroga, 2015). Más aun cuando la Carta Fundamental del Perú reconoce que Perú se rige por los estándares de un modelo económico constitucional que exige la sinergia entre las libertades económicas y el respeto a la dignidad humana, poniendo en evidencia que los derechos fundamentales no se encuentran aislados en el ordenamiento, sino que concurren creando una influencia recíproca que contribuye incluso a delimitar sus contenidos.

No cabe duda que en pleno siglo XXI, los «datos personales» se han convertido en la nueva «moneda de cambio». Hoy, las empresas buscan reunir, a toda costa, diferente tipo información que les permita diseñar sus estrategias comerciales, desarrollar mejor su producto, optimizar sus servicios, fortalecer su competitividad y destacar en el mercado. Así, por ejemplo, se recopilan datos relacionados con los ingresos, la salud, la familia, gustos, preferencias, costumbres, etc.

El trabajo realizado por la Autoridad de Protección de Datos Personales (en lo sucesivo APDP) entre el 2014–2016 ha puesto de manifiesto un alto índice de incumplimiento a la norma. Entre las infracciones más recurrentes se aprecian las siguientes: (i) Tratamiento de datos para perfilamientos comerciales sin consentimiento de los titulares de los datos personales³⁷. (ii) Envío de información personal fuera del territorio peruano sin la autorización correspondiente ³⁸. (iii) Transferencias a terceros de la información personal para la prestación de servicios complementarios³⁹.

³⁷ Al respecto puede consultarse la Resolución Directoral N°039–2015–JUS/DGPDP del 07 de diciembre de 2015 recaída sobre el Expediente N° 080–2015–PS; Resolución Directoral N° 006–2016–JUS/DGPDP de fecha 22 de enero de 2016 recaída sobre el Expediente N° 018–2015–PS.

³⁸ Al respecto puede consultarse la Resolución Directoral N° 028–2015–JUS/DGPDP del 21 de setiembre de 2015 recaída sobre el Expediente N° 040–2015–PS.

A pesar de la identificación de dichos problemas, desde entonces hasta hoy poco parece haberse avanzado. Recientemente, el 6 de enero del 2017, a través del Decreto Legislativo N° 1353 se creó la Autoridad Nacional de Transparencia y Acceso a la Información Pública, y se modificó la Ley N° 29733, Ley de Protección de Datos Personales, presentándose algunos cambios en nuestro sistema de protección; sin embargo, la vigencia de las modificatorias que dicha norma desarrolló se encuentran suspendidas hasta que se apruebe su reglamentación y se produzca la modificación del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos. Hasta ahora la garantía de la defensa y protección de la privacidad parecen haberse detenido en el tiempo.

6. CONCLUSIONES

La regulación respecto del tratamiento de los datos personales, tal como sucede en todos los países del mundo, tiene impacto tanto sobre las entidades del sector público como las empresas del sector privado. No obstante, el *enforcement* normativo de la ley peruana es probablemente uno de los desafíos más importantes que deben afrontarse. La causa de esto es variante, pero dos factores pueden identificarse como los principales motivos. Por un lado el desconocimiento de la ley, y por otro la escasa cultura que tienen los ciudadanos respecto de la protección de su privacidad. El mayor cuestionamiento que ha recibido el estado peruano respecto de este tipo de regulación se ha gestado en el sector empresarial, quienes han recibido de forma negativa las exigencias derivadas de la normatividad vigente. Sin embargo, parece haberse olvidado que para un Estado Social y Democrático de Derecho el nuestro

³⁹ Al respecto puede consultarse la Resolución N° 022–2015–JUS/DGPDP de 30 de julio de 2015 recaída sobre el Expediente N° 004–2015–PTT; Resolución N° 003–2015–JUS/DGPDP de 20 de febrero de 2015 recaída sobre el Expediente N° 016–2014–PTT.

resulta altamente cuestionable que la garantía de un derecho fundamental dependa de la valorización económica que pueda hacer un empresario. Más aun cuando la Carta Fundamental del Perú reconoce que Perú se rige por los estándares de un modelo económico constitucional que exige la sinergia entre las libertades económicas y el respeto a la dignidad humana.

Bibliografía

- Álvarez, J. M. (1999). *La defensa de la intimidad de los ciudadanos y la tecnología informática*. Pamplona, España: Aranzadi.
- Bernales, E. (1999). *La Constitución de 1993. Comentarios*. 5° Edición, Lima, Perú: Editora RAO SRL.
- Bustamante, R. (2010) *Entre la moral, la política y el derecho: el pensamiento filosófico y jurídico de Gregorio Peces-Barba*. Madrid, España: Dykinson.
- Carnoy, M. (2000) *El trabajo flexible en la era de la información*. Madrid, España: Alianza Editorial.
- Castells, M.: *La era de la información, economía, sociedad y cultura. La sociedad red*, Vol. 1. Editorial Alianza, Madrid, 2000.
- Castelló, A. (2010) *Estrategias empresariales en la web 2.0. Las redes sociales online*. Alicante, España: Editorial del Club Universitario.
- Corrales, M.; Barnitzke, B.; Forgó, N.; 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, Buenos Aires, Argentina: Editorial Allbremática.
- Costa, R. (trad.) (2001), *IBM y el Holocausto*. Buenos Aires, Argentina, Editorial Atlántida.
- Cukier, K. (2014) *Los big data y el futuro de los negocios*. Madrid, España: Editorial del BBVA.
- Evans, P (2014) *Reinventar la empresa en la era digital*. Madrid, España: Editorial del BBVA.
- Fundación Konrad Adenauer Stiftung (2009). *Jurisprudencia del Tribunal Constitucional Federal Alemán. Extractos de las sentencias más relevantes compiladas por Jürgen Schwabe*. México D.F., México, Editorial Fundación Konrad Adenauer.
- García, M. (2005). *Principios de Derecho de Internet*. Valencia, España: Tirant lo Blanch.
- González, E. (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*. New York, USA: Ediciones El País S.L.
- González, F. (2015). *Reinventar la empresa en la era digital*. Madrid, España: Editorial BBVA.
- Gozaíni, O. (2001). *Habeas data protección de datos personales*. Buenos Aires, Argentina: Editorial Rubinzal-Culzoni.
- Hernández, J. (2013). *El derecho a la protección de Datos Personales en la Doctrina del Tribunal Constitucional*, Madrid, España: Editorial Thomson Reuters Aranzadi.
- Herrán, A. (1998) *La violación de la intimidad en la protección de datos personales*. Madrid, España: Editorial Dykinson.
- Kresalja, B.; Ochoa, C. (2009). *Derecho Constitucional Económico*. Lima, Perú: Fondo Editorial de la Universidad Católica del Perú.
- Isaca (2009). *Computación en la nube: Beneficios de negocio con perspectivas de seguridad*,

- gobierno y Aseguramiento*, Illinois, USA: Editorial Isaca.
- Marr, B. (2015). *Big Data: Using smart Big Data, Analytics and Metrics to Make Better Decisions and Improve Performance*, Indianápolis, USA: Editorial Wiley.
- Piñar, J. (2009). *El derecho a la autodeterminación informativa*, Madrid, España: Fundación Coloquio Jurídico Europeo.
- Palma, 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, (pp. 673-681). Lima, Perú: Editorial Grijley.
- Piñar, J. (2010) *¿Existe privacidad? En Protección de datos personales. Compendio de lecturas y legislación*, Ciudad de México, México: Editorial Tiro Corto Editores.
- Puente, X. (2011) "Protección de datos personales en México ante el modelo norteamericano y el modelo europeo" en *Derecho y TIC 10.0*, (pp. 335-366) Bogotá, Colombia: Editorial Temis.
- Alguacil, J. (2001). La libertad informática: aspectos sustantivos, y competenciales (SSTC 290/2000 y 292/2000). *Revista Teoría y Realidad Constitucional*, N° 7, pp. 365-985.
- Cano, P. (2009). La protección de datos personales en Iberoamérica. *Anuario Facultad de Derecho de la Universidad de Alcalá II*, pp. 515-549.
- Chirinos, D; Albán, J. (2015). Ley de protección de datos personales: ¿Cuán protegidos estamos? *Revista Semana Económica*, SE N° 1491, pp. 21-22.
- Corral, H. (2000). Configuración jurídica del derecho a la privacidad I: Origen, desarrollo y fundamentos. *Revista Chilena de Derecho*, Volumen 27, N° 1, pp. 51-79.
- González, A. (1993). Comentario a la S.T.C. 254/1993, de 20 de julio. Algunas reflexiones en torno al artículo 18.4 de la Constitución y la protección de los datos personales. *Revista Vasca de Administración Pública*, N° 37, pp. 227-270.
- Gálvez, V. (2014). Ley de protección de datos personales: ¿Cuánto le costará a las empresas? *Revista Semana Económica*, SE N° 1450, pp. 4 - 6.
- García, A. (s.f.). La protección de datos personales: Derecho fundamental del siglo XXI. Un estudio comparado. *Boletín Mexicano de Derecho Comparado*, Año XL, N° 120, pp. 743- 778.
- Herdero, Manuel (s.f.). La sentencia del Tribunal Constitucional de la República Federal Alemana relativa al censo de población de 1983. *Documentación Administrativa*, N° 198, pp. 139-158.
- Iglesias, C. (2012). Derecho e información. *El profesional de la información*, N° 5, V. 21, s/e, pp. 449-452.
- Marcenaro, R. (1989). El derecho a la intimidad y la informática. *Revista Peruana de Derecho de la Empresa*, N° 32, pp. 79 - 100.
- Martínez, R. (2007). El derecho fundamental a la protección de datos: perspectivas. *Revista de Internet, Derecho y Política*, N° 5, pp. 47-61.
- Morales, Juan. (2005). Privacidad de la intimidad personal y familiar. *La Constitución comentada*, pp. 81-116.

- Ornelas, L.; Higuera, M. (2013). La autorregulación en materia de protección de datos personales: la vía hacia una protección global. *Revista de Derecho, comunicaciones y Nuevas Tecnologías*, N° 9, pp. 5– 30.
- Quiroga, J. (2014). La protección de datos personales: a propósito del caso datosperu.org. *Revista La Ley, el ángulo legal de la noticia*, diciembre 2014, pp. 84–85.
- Quiroga, J. (2015). Sobre el desinterés y el desconocimiento de una Ley: La Protección de Datos Personales: ¡Bienvenidos al tema! *Revista La Ley, el ángulo legal de la noticia*, mayo 2015, pp. 37–41.
- Red Iberoamericana de protección de datos, (2006) *Autorregulación y protección de datos personales*, pp. 1–9.
- Remolina, N. (2012). Aproximación constitucional de la protección de datos personales en Latinoamérica. *Revista Internacional de Protección de Datos Personales*, pp. 1–13.
- Remolina, N. (2012), Insuficiencia de la regulación Latinoamericana frente a la recolección internacional. *Quaestiones Disputatae 2*, pp. 179–226.
- Riascos, L. (2008). La informática jurídica documental, los datos personales informatizados, el *thesauro* jurídico y el documento jurídico electrónico. *Ensayos jurídicos de derecho informático*, pp. 1–22.
- Saldaña, M. (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. *UNED, Revista de Derecho Político*, N° 85, pp. 195–240.
- Torres, C. (1989). Nociones preliminares sobre el Derecho de la informática y la informática jurídica. *Revista Peruana de Derecho de la Empresa*, N° 32, pp. 49 –78.
- Vásquez, J. (2013). Horizontes y desafíos de Internet de las cosas. *Revista Cambio: 19 ensayos fundamentales sobre cómo internet está cambiando nuestras vidas*, pp. 9–24.
- Warren, S.; Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, Volumen IV, N° 5, pp. 193–220.
- STC del 29 de enero del 2003 recaída sobre el Expediente N° 1797–2002–HD/TC
- STC del 18 de enero del 2002 recaída sobre el Expediente N° 0197–2000–HD/TC
- STC del 16 de noviembre del 2007 recaída sobre el Expediente N° 03052–2007–PHD/TC
- STC del 24 de julio del 2012 recaída sobre el Expediente N° 00693–2012–PHD/TC
- STC del 30 de enero del 2014 recaída sobre el Expediente N° 06227–2013–PHD/TC
- STC del 7 de agosto del 2014 recaída sobre el Expediente N° 02491–2013–PHD/TC
- STC del 23 de octubre del 2014 recaída sobre el Expediente N° 03468–2013–PHD/TC
- STC del 7 de agosto del 2014 recaída sobre el Expediente N° 03700–2010–PHD/TC
- STC del 18 de marzo del 2011 recaída sobre el Expediente N° 0831–2010–PHD/TC
- STC del 30 de mayo del 2011 recaída sobre el Expediente N° 04227–2009–PHD/TC
- STC del 21 de agosto del 2014 recaída sobre el Expediente N° 02995–2013–PHD/TC

STC del 21 de agosto del 2014 recaída sobre el
Expediente N° 02324-2013-PHD/TC