PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ESCUELA DE POSGRADO

COMPLIANCE LABORAL EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

TRABAJO DE INVESTIGACIÓN PARA OPTAR EL GRADO ACADÉMICO DE MAGÍSTER EN DERECHO DE LA EMPRESA

AUTOR:

TRILLO VIGIL CAROL FIORELLA

ASESOR:

DEBENEDETTI LUJÁN BRUNO EDOARDO

Lima, Perú

Setiembre, 2019

DEDICATORIA

''No es posible convertirnos en lo que queremos ser permaneciendo siempre en lo que somos''. Esta frase se traduce al ánimo de superación, entrega y compromiso que asumí hace unos años atrás como profesional y como madre.

Una dedicatoria especial para mi hijo Milan, quien fue mi mayor motivación durante todo este emprendimiento. Y a mi esposo Diego, ya que a pesar de todos los obstáculos inimaginables, junto con Milan, me dieron la fortaleza para superarlos y poder decir al fin ¡Lo logramos!

RESUMEN EJECUTIVO

La rápida evolución tecnológica y la globalización traen como principal consecuencia resaltar la relevancia de la información en diversos sectores. Sin duda, las empresas no se encuentran exentas a esta realidad, planteándoles nuevos retos con relación a la protección de datos personales (en adelante PDP) dentro del marco de las relaciones laborales.

Por ello, el tema de PDP dentro del marco de la prestación laboral cobra mucha relevancia en el área del *compliance* laboral-por ser la PDP uno de sus ámbitos de actuación- en donde sus sistemas de gestión de cumplimiento sirven no solo para prevenir y gestionar incumplimientos laborales; sino también, para afianzar las buenas prácticas empresariales.

En este contexto, la normativa de PDP en el Perú (Ley No. 29733 y su reglamento) se convierte en el principal instrumento jurídico que toda empresa debe observar, conocer y cumplir.

No obstante, se evidencia la posibilidad de las empresas de incurrir en malas prácticas en materia de PDP en el ámbito de las relaciones laborales, motivado por el incumplimiento de la normativa aplicable en PDP y por no asumir un compromiso voluntario relacionado a la autorregulación, a la efectiva gestión de riesgos y al cumplimiento normativo laboral.

Por ello, para lograr una mejor comprensión de nuestra problemática referida anteriormente, se utiliza la metodología del método comparado y riesgos legales. Con el análisis de casos nacionales y extranjeros, se logra evidenciar la problemática existente en cada caso, y del mismo modo, se logra establecer diversas propuestas alternativas con el fin de que las empresas puedan mitigar o prevenir los riesgos que podrían acarrearles perjuicios legales, económicos y reputacionales; y de esta manera, fomentar las buenas prácticas empresariales.

Por último, resulta importante que las empresas incorporen dichos sistemas de gestión, en donde la PDP sea un componente relevante en dicho sistema, y por ende, en la cultura de cumplimiento empresarial. De esta manera, el *compliance* laboral sería considerado como un cambio en la filosofía de toda empresa, primando el compromiso por parte de estas de cumplir con sus obligaciones y promover una cultura de cumplimiento normativo en esta materia, en donde la ética y la responsabilidad social empresarial sean los principales ejes rectores.

ÍNDICE

CAPÍTULO I: INTRODUCCIÓN

1.1 Planteamiento del tema y problema

El mundo está en constante cambio y el Derecho como ciencia debe permanentemente ajustarse a los preceptos y a las necesidades de las diferentes sociedades. Actualmente, un verdadero reto que enfrentan las empresas es la nueva era vinculada con la protección de los datos personales lo cual representa un gran desafío dentro de las relaciones laborales.

En este sentido, la PDP es un asunto jurídico en donde la intimidad y el tratamiento de datos emergen como uno de los temas de gran envergadura, provocando un gran número de divergencias jurisprudenciales con relación a la potestad de fiscalización del empresario debido a que las nuevas avances en el campo tecnológico posibilitan nuevas formas de intromisión en esta área protegida que no se habían propuesto con anterioridad (TOLEDO, 2010, p. 38-39).

Con relación a lo anterior, podemos resaltar que nuestro TC en varios pronunciamientos ha señalado que el empleador no se encuentra habilitado para intervenir los correos electrónicos de sus empleados porque lesiona el derecho al secreto de las comunicaciones e intimidad, y que además, dichos correos carecen de valor probatorio para acreditar faltas laborales. En adición, señala que el empleador sólo estaría habilitado a acceder a tales correos mediante un mandato judicial motivado. En contraposición, el TC español mediante sentencia 170/2013, entiende que al ser el correo electrónico una herramienta de trabajo, su uso por parte de los trabajadores se encuentra limitado. Del mismo modo, el Tribunal Europeo de Derechos Humanos posee el mismo criterio, ya que mediante la sentencia del 12 de enero del 2016 (Caso Burbulescu vs Rumanía), estableció que el empleador tiene derecho a fiscalizar y controlar el correo electrónico debido al carácter estrictamente profesional que posee el mismo.

El tema que abordaremos en el presente trabajo de investigación ha cobrado mucha relevancia en el área del *compliance* o cumplimiento normativo dentro de las organizaciones, convirtiéndose este último en un imprescindible empresarial tanto a nivel internacional como nacional, ya que el Perú no ha sido ajeno a éste.

En este orden de ideas, se ha reconocido la estrecha relación del *compliance* con la función de prevenir y gestionar los riesgos de no cumplimiento de los deberes intrínsecos y extrínsecos de una organización (SOLÍS, 2007, p.78), siendo una de sus

metas principales identificar, manejar y mitigar los riesgos de una manera rentable (TARANTINO, 2008, p.193).

Es notorio que hoy en día se sigue asociando el término *compliance* al área penal, ya que en el ordenamiento de varios países se ha introducido la responsabilidad de las personas jurídicas en esta rama. Sin embargo, se ha constatado que el disponer de protocolos, procedimientos y modelos organizativos que delimiten el grado de cumplimiento normativo en la empresa ya no es netamente propio del orden penal, ya que este sistema de vigilancia ha ganado igual presencia en su vertiente laboral (Rojas, 2017, p. 2).

Así, en el campo jurídico laboral, el *compliance* laboral se refiere a la función corporativa de gestionar y prevenir los riesgos vinculados a un eventual incumplimiento laboral dentro de una organización, en donde dichos riesgos de cumplimiento o *risk compliance* se centran no sólo en las sanciones legales, sino también en las pérdidas económicas y reputacionales que podría sufrir la persona jurídica como consecuencia de su falta de capacidad en el cumplimiento de las regulaciones, leyes vigentes, códigos de conducta y normas de la buena práctica (Rojas, 2017, p.2).

Entendemos, pues, que el *compliance* laboral pretende ser una nueva herramienta para las empresas capaz de tratar la normativa laboral que subyacen en las mismas, siendo un sistema no solo de gestión del funcionamiento de las empresas y el cumplimiento de la legislación laboral, sino también de creación de una nueva cultura empresarial. Así las cosas, resulta importante contar con esta herramienta frente a la minimización de los riesgos y a la implantación de un código ético en las empresas que trate diferentes áreas de incidencia laboral (Rojas, 2017, p. 24-27).

En este sentido, una de las áreas de actuación que debe abarcar el *compliance* laboral es el de la PDP, en donde sus sistemas de gestión de cumplimiento sirvan no sólo para prevenir y gestionar incumplimientos laborales, sino también para afianzar –como parte de la responsabilidad social de las corporaciones- las buenas prácticas laborales sobre la base de un desarrollo continuo y cumplimiento ético y responsable del bloque normativo laboral y de PDP que toda empresa está obligada a conocer, observar y cumplir (Rojas, 2017, p. 26).

Por ello, el cumplimiento normativo puede ser utilizado como una estrategia preventiva para las empresas frente a los riesgos laborales que puedan surgir, siendo sumamente relevante no solo que sus programas de cumplimiento sean monitorizados de forma permanente y continua; sino también, que éstos sean diseñados bajo una serie de

pautas a tomar en cuenta, como por ejemplo, el hecho de contar con responsable de cumplimiento (Sánchez, 2017).

Con relación al problema, podemos afirmar que la rápida evolución tecnológica, la globalización y el aumento de producción normativa hacen que se incremente el riesgo legal para las empresas en materia de PDP. Bajo esta óptica, la necesidad de cumplir con la normativa está intrínsecamente ligada a la actividad empresarial, y por ende, a las relaciones laborales.

Cabe resaltar que nuestra investigación estará centrada en analizar aquellas relaciones laborales cuyos agentes puedan tener una intervención y responsabilidad frente al tratamiento y manejo de los datos personales dentro del marco laboral, a saber:

(i) En primer lugar, se encuentran las relaciones entre el empleador y el empleado, que pueden ir desde el momento de seleccionar al personal hasta el inicio del contrato y el desarrollo de la prestación de trabajo. En estas relaciones se puede recoger gran información de los empleados que puede afectar a su esfera personal y profesional. Por ello, es una responsabilidad de las empresas salvaguardar los datos de índole personal de sus empleados.

(ii) En segundo lugar, se encuentran las relaciones entre los empleados y/o el empleado con el tercero vinculado a la empresa, como es el caso del cliente. Es indudable que el trabajador puede también intervenir en el tratamiento de los DP, y a pesar de ser la empresa quien responda frente a las acciones del trabajador con relación a la violación de alguna obligación en esta materia, puede el empleador imponer alguna sanción de índole laboral u optar por el término del contrato de trabajo de acreditarse el incumplimiento. Por ello, es responsabilidad de las empresas clarificar a sus empleados sobre las políticas y deberes en materia de PDP, con el fin de evitar algún incumplimiento.

En esta línea, si existiese un incumplimiento- en las obligaciones de los empleadores y en los deberes de los empleados con relación a esta materia- y máxime si no existiese un adecuado sistema de gestión y prevención de riesgos en esta específica incidencia laboral, las personas jurídicas se verían menoscabadas no sólo legal, sino también, económica y reputacionalmente.

Con todo lo anterior, podemos afirmar que la problemática que enfrentan las empresas es su posibilidad de incurrir en malas prácticas en esta materia, no solo por incumplir

con la normativa aplicable, sino también, por no asumir un compromiso voluntario relacionado a la efectiva gestión de los riesgos, la autorregulación y el cumplimiento normativo.

Un ejemplo de ello es el caso de la empresa Domiruth Travel Service S.A.C., el cual se encuadra en la relación laboral de empleador –empleado, en donde el primero detentó responsabilidad en el tratamiento de datos frente al segundo (titular).

En el año 2015, la referida empresa solicitó exámenes médicos pre ocupacionales, así como la prueba del VIH, a uno de sus postulantes para el puesto de trabajo de ‘’Ejecutivo de producto Receptivo’’. El denunciante que ejercería dicho puesto se encargaría de brindar información a los clientes sobre viajes y/o cotizaciones. Cabe resaltar que si bien la Dirección de PDP consideró que la finalidad era legítima (Artículo 6 LPDP)- la recopilación de los datos del denunciante era necesaria para que la empresa lo evalúe para la selección a un puesto de trabajo-, se contravino con el *principio de proporcionalidad* (artículo 7 de la LPDP)-brindar un dato sensible no proporcional para con el fin de evaluarlo en el proceso de selección del puesto de trabajo para una actividad que no implica un riesgo laboral- y con el *principio de seguridad* –al no contar con las medidas legales, organizativas y técnicas que garanticen su seguridad-, colocando en un estado de indefensión al titular de los datos.

En otras palabras, de acuerdo a la normativa laboral, esta prueba sólo puede solicitarse en casos de actividades de alto riesgo, relacionadas con los centros penitenciarios o el sector salud. Así, la Autoridad Nacional de PDP entendió que la actividad que realizaría el postulante no estaba encuadrada en ninguno de los dos sectores mencionados, resultando desproporcional solicitar la prueba del VIH como parte de las evaluaciones médicas previas al proceso de contratación. Por ello, al vulnerarse los principios de proporcionalidad y seguridad en el tratamiento de los DP del denunciante, se tipificó la conducta como ‘’grave’’ (Artículo 39, numeral 2)-con relación al primero y ‘’leve’’ (Artículo 132, numeral 1, Reglamento de la LPDP)-con relación al segundo, imponiéndose a la empresa una multa de 30.25 UIT y 1.31 UIT, respectivamente.

Con relación a lo anterior, se puede confirmar la falta de capacidad de la empresa de cumplir con las normas vigentes y la carencia de un sistema que gestione y prevenga los riesgos ante el incumplimiento laboral. De esta manera, podemos inferir que la empresa se vio perjudicada en tres aspectos: (i) legal -al incurrir en un incumplimiento con la normativa laboral y de PDP, la empresa se vio envuelta en un procedimiento administrativo sancionador-, (ii) económica -la empresa sufrió un perjuicio económico al estar en la obligación de pagar las multas establecidas en la Resolución Directoral No.

04-2018-JUS; y (iii) reputacionalmente- al mediatizarse el caso se pudo formar una opinión negativa por parte del público que utilizaba el servicio turístico de Domiruth Travel Service S.A.C.

1.2 Hipótesis de investigación y metodología

La existencia de posibles malas prácticas en materia de PDP pueden traer consigo un panorama de difícil gestión, resultando indiscutible que exista una obligación de cara a las empresas sobre la implementación de programas de cumplimiento normativo laboral, independientemente de su magnitud y actividad a nivel geográfico, con el propósito de prever riesgos legales derivados de algún incumplimiento normativo producidos concretamente en el marco de las relaciones de trabajo.

Por ello, el reto que tienen las empresas es evitar que existan malas prácticas con relación al tratamiento de los DP en el marco de las relaciones laborales, resultando relevante que éstas cuenten con herramientas idóneas capaces no sólo de verificar el cumplimiento normativo; sino también de mitigar los riesgos y de implantar un código ético que trate esta área de incidencia laboral de PDP.

En adición a ello, es importante que se incorpore un sistema de gestión de cumplimiento normativo laboral, en donde la PDP sea un componente relevante en dicho sistema, y por ende, en la cultura de cumplimiento empresarial. De esta manera, el *compliance* laboral sería considerado como un cambio en la filosofía de toda empresa, primando el compromiso por parte de estas de cumplir con sus obligaciones y promover una cultura de cumplimiento normativo en esta materia, en donde la ética y la responsabilidad social empresarial sean los principales ejes rectores.

En este sentido, el *compliance* laboral se revela, pues, como un instrumento eficaz, capaz de asegurar una óptima vigilancia y cumplimiento por parte de las organizaciones no sólo de las normas laborales nacionales, sino también de las normas y estándares internacionales existentes en el ámbito laboral, tales como los Convenios de la OIT en materia de derechos humanos sociales, el Libro Verde de la Comisión Europea y la Norma SA 8000 en el ámbito de la responsabilidad social empresarial (Rojas, 2017, p. 4).

En adición, la metodología que se utilizará para entender la problemática establecida será mediante el método comparado y riesgos legales.

Mediante el método comparativo pretendemos cotejar la normativa nacional e internacional que evidencian notas similares o diferenciales en materia de PDP, con el objetivo de realizar una valoración e interpretación de la normativa nacional (Carta

Magna, Ley No. 29733 y su reglamento); así como de la normativa internacional (Reglamento General de Protección de Datos para los países de la Unión Europea).

Asimismo, pretendemos cotejar la jurisprudencia nacional e internacional, lo cual ha significado un notorio avance en materia de PDP en el marco de prestación laboral. Cabe mencionar que dentro de los casos tratados en el derecho comparado, debemos resaltar el remarcable trabajo de España en esta materia, máxime en el campo laboral, en donde se destaca el uso de las nuevas tecnologías, como los correos electrónicos.

Por último, mediante los riesgos legales se identificará el impacto que podría tener el no cumplir con la normativa de PDP en el marco de las relaciones de trabajo o con el hecho de no haber implementado un correcto sistema de detección, gestión y prevención de riesgos a tiempo. Por ello, resulta importante identificar, analizar y valorar los riesgos dentro de una empresa, ya que solo así se podrán tomar las decisiones correctas en la materia que nos atañe.

1.3 Objetivos

- Establecer la relevancia de incorporar un sistema de gestión de cumplimiento normativo laboral, en el cual la PDP sea un componente relevante en dicho sistema y en la cultura de cumplimiento de toda empresa.
- Proponer mecanismos de cumplimiento normativo laboral en materia de PDP, con el objetivo de evitar o minimizar los riesgos, como por ejemplo: implementación de políticas relacionadas a la PDP, establecimiento de acuerdos de confidencialidad, establecimiento de medidas se seguridad idóneas y eficaces para evitar pérdidas o filtraciones de la información de los titulares de los datos, entre otras.
- Analizar la normativa nacional e internacional; así como los casos tratados en el Perú y en el derecho comparado sobre el proceder en materia de PDP.

CAPÍTULO II: ESTADO DEL ARTE

Actualmente vivimos inmersos en la nueva era de las telecomunicaciones, en donde el intercambio y el manejo de DP se han transformado en una práctica frecuente en los diferentes sectores económicos y sociales, lo cual puede traer consigo una serie de riesgos para la intimidad en diversos sectores, sobretodo, para el sector empresarial.

Así, el uso y tratamiento de datos personales en el seno de las empresas dentro del marco laboral es una realidad que ninguna empresa puede ignorar, máxime que el vertiginoso desarrollo tecnológico y la globalización plantean nuevos desafíos para la PDP.

Bajo esta óptica, las organizaciones se ven cada vez más obligadas a cumplir con la normativa vigente en materia de PDP, la cual no solo aplica para las relaciones que se desarrollan en el ámbito laboral; sino también, garantiza y regula el derecho de PDP del empleador, empleado y de cualquier tercero vinculado a la empresa.

Por ello, con el fin de evitar sanciones legales o económicas resulta importante que las empresas no sólo cumplan a cabalidad con la normativa vigente, sino que ponderen el hecho de implementar un sistema de gestión de cumplimiento normativo laboral, en donde se dote de mecanismos de protección a los titulares de los DP y en donde la PDP sea el componente relevante en dicho sistema y en la cultura de cumplimiento de cada empresa.

El estado del arte que se realizará en el presente trabajo de investigación se dividirá en dos ámbitos. El primero estará referido a la PDP y su marco jurídico nacional. El segundo estará referido al cumplimiento normativo y a la gestión de riesgos; abordando específicamente la gestión del riesgo laboral; así como el sistema de cumplimiento normativo laboral vinculado al incumplimiento de las normas en PDP dentro del marco de las relaciones de trabajo.

2.1 Protección de datos personales y marco jurídico nacional

2.1.1 Protección de datos personales

A partir de la proclamación de la Carta de Derechos Fundamentales de la UE, se concibió a la PDP –en su artículo 8- como un derecho fundamental, independiente y autónomo del derecho a la intimidad (Remolina, 2015, p. 5).

En este sentido, el jurista italiano Stefano Rodotà entiende que la PDP es un derecho fundamental, el cual se formaliza en la potestad que se le confiere a cada persona con el poder de gobernar su propia información (Rodotá, 2003, p. 17).

El derecho anteriormente mencionado se puso de manifiesto en la constitución de distintos países latinoamericanos[1]; sin embargo, tuvo un reconocimiento jurisprudencial preliminar en Alemania (Eguiguren, 2015, p. 132).

En palabras de Bru, este derecho fue el resultado jurisprudencial de la necesidad de un tratamiento masivo de datos, el cual se proyectó con la sentencia del Tribunal Constitucional Federal Alemán de 1983[2] al establecer que el individuo tiene la facultad de decidir por sí mismo y dentro de los límites que entienda conveniente (2007, p. 81), convirtiéndose esta en una referencia para que la mayoría de los países reconozcan una PDP de cada individuo.

En este sentido, circunscribiéndonos al caso peruano, la doctrina constitucionalista tiene posturas contrarias con relación a la PDP. Así, una parte de la doctrina entiende que este derecho es conocido como el de ‘’autodeterminación informativa’’ o ‘’libertad informática’’, el cual brinda protección al titular frente a eventuales riesgos derivados de utilizar los datos. Bajo esta perspectiva, si el titular fuese afectado, este tendría el derecho de excluir los ‘’datos sensibles’’, así como el derecho a oponerse frente a la difusión y transmisión de los mismos. (Eguiguren, 2015, p. 132).

Esta postura es secundada por Bru, quien entiende que la autodeterminación informativa es similar al derecho de PDP, el cual constituye una garantía individual que permite al titular llevar el seguimiento y control de los DP registrados en fuentes informáticas, siendo la naturaleza jurídica del derecho a la PDP: personal, innato, subjetivo, inherente a la persona, intransmisible, irrenunciable, imprescriptible e indisponible (2007, p. 81).

En adición, Eguiguren entiende que el derecho constitucional a la autodeterminación informativa posee dos dimensiones: (i) La primera es la dimensión negativa y se refiere a la potestad del titular del derecho de prohibir la difusión, transmisión y registro de datos

[1] Para profundizar sobre el tema ver Remolina, 2015, p. 6-11.

[2] La sentencia del 15 de diciembre de 1983 falló con relación a la Ley del Censo de la población germana, anulando tres preceptos de dicha ley por considerarse inconstitucionales, entre ellos los relativos a los DP del censo estatal con los de los padrones. Los simpatizantes del movimiento de los ´´verdes´´ interpusieron recurso de legalidad sobre la referida Ley por entender que era contraria a los derechos de las personas respecto a la transmisión de datos entre el Estado, regiones y ayuntamientos. Cabe mencionar que esta sentencia europea es el primer antecedente que legitima la existencia del derecho a la autodeterminación informativa como un derecho autónomo.

de carácter sensible. (ii) La segunda es la dimensión positiva y se refiere a la potestad de ejercer el control (propio del titular) sobre los datos que a él le concierne. Dentro de esta dimensión se encuentra el derecho de actualizar, inspeccionar, verificar y corregir los datos; así como el derecho de cancelar toda aquella información concerniente a los datos sensibles que no deben ser difundidos o registrados (2015, p. 133).

Por otro lado, otra parte de la doctrina entiende que el derecho a la PDP ha sido configurado en nuestra Carta Magna de 1993 dentro del derecho fundamental de la autodeterminación informativa, el cual autoriza al titular de datos a oponerse a que se suministren informaciones que puedan afectar su integridad personal y familiar (Zegarra, 2011, p. 1).

Anudado a ello, debemos estacar ciertas investigaciones españolas con relación a este derecho, ya que la ley peruana en PDP está inspirada en el ordenamiento jurídico español.

Así, una de las investigaciones (Martínez, 2007) se enfoca en estudiar a la PDP como un derecho fundamental de la legislación española y varias interrogantes vinculadas con este derecho. En este sentido, se considera que el derecho a la PDP tiene perfiles muy definidos (Martínez, 2007, p. 51-52). Por un lado, establece que la concepción del derecho fundamental a la PDP precisa al dato personal como la información relacionada a persona identificable no teniendo importancia su naturaleza pública o privada. Por otro lado, desde la óptica de la aplicación de las normas sobre PDP, el elemento básico radica en una definición determinante: el tratamiento. Ambos conceptos (dato y tratamiento) se proyectan sobre el derecho fundamental a la PDP hasta lograr obtener un modelo bien definido.

Otra de las investigaciones españolas considera que la PDP es un asunto jurídico actual en el que la disparidad entre el tratamiento de datos y la libertad informativa junto con la intimidad y la libertad de expresión, surge como uno de los más grandes temas de nuestro tiempo (Toledo, 2010, p. 38).

Con relación a lo anterior, debemos hacer énfasis en considerar a la PDP como un tema relevante en el ámbito de toda empresa, ya que estas están obligadas a cumplir con los principios y lineamientos relacionados con el tratamiento de los datos personales.

Así, se considera que la PDP es necesaria desde dos ópticas: legal (cumplir con la normativa vigente) e interna (dentro de las relaciones laborales y de empresa – empleados, clientes, proveedores, etc.). El deber de cumplir con la normativa en esta materia está ligada con la actividad empresarial, ya que representan un activo relevante

en el día a día. Asimismo, los autores entienden que una de las implicaciones más graves asociados al incumplimiento de la normativa en esta materia son los riesgos económicos y de imagen. (Santos, López & Tejedor, 2005, p. 20).

Por todo lo anterior, resulta relevante tratar el marco jurídico nacional en materia de PDP, destacando el desarrollo que ha tenido el Art. 2 numeral 6 de la Carta Magna- aprobado por la Ley 29733- ley que tiene por propósito brindar garantía a una serie de derechos de los individuos, como el derecho a la información, acceso, rectificación, cancelación u oposición. Para ello, dicho cuerpo normativo establece un mínimo de obligaciones y requisitos que deberán cumplir los titulares de los bancos de datos (Minjus, 2013), los cuales se verán a detalle en el siguiente acápite.

2.2.2 Marco jurídico nacional

Antes de la entrada en vigencia del cuerpo normativo en materia de PDP, el Perú solo contaba con normas sectoriales que regulaban el secreto bancario o el de las telecomunicaciones; es decir, el país no contaba con una regulación que brindara un protección integral a los datos personales (Montezuma, 2010, p.1).

Por su parte, Eguiguren entiende que una de las limitadas novedades positivas de la Carta Magna de 1993 en materia de derechos fundamentales, fue la introducción del reconocimiento del derecho a todo individuo a ejercer dominio sobre el registro, difusión y tratamiento de sus DP. De esta manera, el artículo 2 numeral 6 del texto constitucional establece que los servicios informáticos, sean computarizados o no, privados o públicos, no deben proporcionar información que vulnere la intimidad en la esfera personal ni familiar. Desde ese reconocimiento pasaron varios años antes de dictar normas que regulen este derecho constitucional, destacando la Ley 29733 (en adelante LPDP), cuya publicación fue el 3 de julio del 2011, y el reglamento de la misma, aprobado por el DS 003-2013-JUS, cuya publicación fue el 22 de marzo del 2013. (2015, p.132)

En este orden, desde la publicación de la Ley 29733, el Perú cuenta con una legislación específica en materia de PDP. Esta ley junto con sus normas reglamentarias aprobadas por el DS 003-2013-JUS, proporcionan el marco normativo que regula las obligaciones y los derechos aplicables al tratamiento de DP mediante dos ejes rectores: la protección y garantía del adecuado ejercicio de los derechos del titular de los DP y el cumplimiento de las obligaciones a cargo de las entidades que incurren en el tratamiento de DP.

Así pues, se considera que las normas relacionadas con la PDP (Ley 29733 y su reglamento) constituyen un gran avance en el desarrollo y promoción en esta materia en el territorio nacional, ya que por primera vez se implementaron medidas

acondicionadas al aumento de los bancos de datos personales y al avance tecnológico. De esta manera, se presenta las principales disposiciones exigidas por la ley y el reglamento, las cuales están dirigidas a las personas jurídicas privadas y públicas y a las naturales que poseen banco de DP (Gamarra, 2015).

Sobre este punto, Zegarra (2011) considera que la LPDP no solo regula los alcances del derecho reconocido en nuestra Carta Magna, sino también, diferentes situaciones que pueden presentarse en el tratamiento de los DP, tanto en el ámbito de la Administración Publica (en sus tres niveles de gobierno) como en el ámbito privado.

Con relación a lo anterior, Eguiguren (2015, p.133-134) entiende que el principal objeto de la ley en esta materia es regular los sistemas relacionados al archivo, almacenamiento, registro, sistematización y transmisión de datos personales, los cuales pueden estar contenidos en registros, bases de datos o bancos a cargo de entidades privadas o públicas, con el fin de brindar protección al derecho fundamental establecido en el Art. 2, numeral 6 de la Carta Magna.

Por su parte, el artículo 3 de la LPDP señala que será de aplicación los DP que estén destinados a ser contenidos o estén contenidos en banco de DP que sean administrados por entidades del sector público o privado en el territorio nacional, resaltando que los datos sensibles tienen una protección especial. Del mismo modo, el mismo artículo señala los tipos de archivos, registros o banco de datos donde no estará aplicada la LPDP.

Sobre este punto, Eguiguren (2015, p. 135) señala como regla general que la legislación sobre PDP será de aplicación a todos los bancos o registros que se establezcan en cualquier tipo de actividad económica; administrados por entidades privadas o públicas, a excepción de que el titular sea una persona natural-para su uso privado- o una entidad pública, solo cuando sean estrictamente indispensables para cumplir con sus competencias institucionales, en materias de seguridad jurídica, defensa nacional, entre otras.

Anudado a ello, es importante resaltar las definiciones más relevantes contenidas en la Ley 29733. Un primer término que debemos abordar es el relacionado con datos personales. En la legislación peruana, este es definido como toda información con relación a una persona que la identifica mediante medios que pueden ser razonablemente utilizados (numeral 2.4 LDPD). Por su parte, en el artículo 2.4 del reglamento complementa esta definición, señalando que se trata de información alfabética, numérica, fotográfica, gráfica, de sonido o de cualquier otro tipo, relativo a la persona que la permite identificar a través de medios utilizados de forma razonable.

Sobre este punto, debemos hacer hincapié en que la legislación española presenta un alto grado de similitud con el concepto de dato personal establecido en la normativa peruana, por ende, resulta interesante hacer mención al análisis realizado al respecto en el trabajo de investigación de Toledo.

Así, el concepto de dato de carácter personal que se establece en la Ley Orgánica española en materia de PDP es muy amplia, poseyendo dos elementos primordiales: (i) objetivo: la información y (ii) subjetivo: concerniente a la persona física. Asimismo, considera que tendrán el carácter de dato personal, no solo el nombre, apellido, etc.; sino también, sonidos, imágenes y voces (así también lo considera el reglamento de la LPDP peruana) (Toledo, 2010, p. 39).

Un segundo término que debemos abordar es el relacionado con los datos sensibles. El numeral 2.5 de la LPDP lo define como DP compuestos por los datos biométricos que pueden identificar por sí al titular, datos aludidos a ingresos económicos; origen étnico y racial; convicciones religiosas, políticas, morales o filosóficas; información relacionada a la salud o a la vida sexual y afiliación sindical. A su vez, el reglamento en su numeral 2.6 lo define como aquella información concerniente a DP relativos a las características morales, emocionales o físicas; hechos de su vida familiar y afectiva; los hábitos personales o cualquier información que afecte su salud física u otras análogas que afecte la intimidad.

Un tercer término que debemos abordar es el relacionado con el tratamiento de datos (Art. 2.17), en donde es definido como cualquier operación o procedimiento técnico (automatizado o no) que permite recopilar, registrar, organizar, almacenar, conservar, elaborar, modificar, extraer, consultar o cualquier otra forma, que permita acceder, correlacionar o interconectar los datos de carácter personal.

Otras definiciones importantes contenidas en la Ley 29733 es el relacionado con las obligaciones y derechos relacionados con la materia.

Con relación a la obligación de registro de los bancos de datos, la ley establece en el artículo 29 que la creación, cancelación y modificación del banco de DP, sean administradas por entidades privadas o públicas, se sujetarán a lo dispuesto por el reglamento, salvo que exista disposición especial en otra ley. Con el fin de facilitar la publicidad de la existencia de los bancos de DP, el artículo 34 de la ley dispone la creación del Registro Nacional de PDP, que estará a cargo de la Autoridad Nacional de PDP. En dicho registro deben inscribirse los bancos de datos a cargo de entidades privadas o públicas. Por ende, todos los titulares de los bancos de datos que no se

encuentren apartados del ámbito de aplicación de la ley, estarán obligados a declararlos y registrarlos ante la Autoridad Nacional.

En este punto, se debe de precisar algunas consideraciones que se hace al respecto. Como bien establece el artículo 34 de la LPDP, las personas que poseen bancos de datos personales deben inscribirse como tales, es decir, como titulares de los bancos. En este sentido, según el Texto Único de Procedimientos Administrativos del MINJUS, el registro de banco de datos se realiza completando un formulario oficial con carácter de declaración jurada. Sin embargo, antes de completar dicho formulario, debe hacerse una evaluación sobre si la persona cuenta con un banco de datos y si estos califican como personales de acuerdo a lo estipulado por la ley. Luego de ello debe identificarse: (i) los datos de las personas naturales que se encuentran en el banco; (ii) el uso para lo que se destina dicha información; (iii) la manera en que se obtuvo la información; entre otros. En otras palabras, en la práctica la entrega del formulario exige un análisis profundo de la información que posee el titular del banco de datos (Gamarra, 2015).

Con relación a la obligación de obtener el consentimiento del titular, el Art. 5 de la ley establece el principio del consentimiento, implicando que para el tratamiento de los DP debe existir una autorización del titular. En el mismo sentido, el numeral 13.5 de la LPDP establece que los DP solo pueden ser tratados con el consentimiento de su titular, salvo que exista una ley que autorice al respecto. Además, resalta que dicho consentimiento debe ser previo, informado, expreso e inequívoco. Por su parte, el reglamento en su artículo 14 señala que si los datos son sensibles el consentimiento deberá ser otorgado por escrito, sin embargo, existen excepciones estipuladas en el mismo artículo.

Sobre este punto, Gamarra (2015) entiende que el núcleo sobre el que se basa la PDP es el consentimiento. Ahora bien, la adecuación a este principio implica que todos los titulares de los bancos que realicen tratamiento de DP y que no tengan la autorización de los titulares de los datos, están obligados a regularizar dicha situación contactando a cada titular de los datos con el fin de obtener su consentimiento. Esto conllevará a recurrir a canales de correo electrónico, llamadas y/o visitas a domicilio que permitan obtener la autorización. De no cumplirse con todo lo anterior, se estará frente a una afectación a la normativa de DP. Sin embargo, esta regla presenta excepciones de acuerdo al artículo 14 de la ley.

Con relación a la obligación de implementar mecanismos para el ejercicio de los derechos ARCO (actualización, rectificación, cancelación y oposición estipulados en el Título III de la ley) se considera que las organizaciones deben implementar plataformas acordes con el objetivo de que los dueños de los datos puedan plantear solicitudes para

ejercer los derechos mencionados. Esto se traduce a implementar un canal de atención por escrito y otros canales informativos como el telefónico. Asimismo, se recomienda que en el caso de las grandes empresas, sería conveniente designar funcionarios que se ocupen de tramitar las solicitudes y crear un procedimiento de atención interno. Esto último es importante debido a que la atención de las solicitudes debe ser en un plazo no mayor a 20 días hábiles según cada tipo solicitud (Gamarra, 2015).

Sobre este punto, debemos resaltar que el cumplimiento con esta obligación es sumamente relevante para los sistemas de *compliance* laboral dentro del marco de las relaciones laborales de toda empresa, ya que lo que se busca es evitar incumplir con la normativa en PDP. Siendo así, tales sistemas están encaminados no solo con cumplir con los plazos para responder a las solicitudes respectivas que haga cada titular de los datos, sino también, a brindar a los trabajadores una serie de facilidades para el ejercicio de sus derechos ARCO.

Con relación a la implementación de medidas de seguridad, Gamarra (2015) considera que esta podría ser la medida que involucre un mayor costo. Según el artículo 16 de la ley, los titulares de los bancos de DP deberán acoger medidas organizativas, técnicas y legales tendentes a garantizar la seguridad. Así, el reglamento en sus artículos 39, 40 y 41 especifican las exigencias en materia de seguridad. Es decir, las medidas de seguridad que exige la ley y el reglamento poseen tres ejes de implementación: (i) seguridad informática, (ii) seguridad física y (iii) adecuación organizacional.´

Ahora bien, dentro del marco de las relaciones laborales, existen obligaciones que las empresas deben considerar para administrar su base de datos con la información personal de sus empleados de acorde a la normativa vigente en la materia, a saber: (i) efectuar el tratamiento de los datos con el previo consentimiento de los trabajadores o familiares, documentando tal consentimiento; (ii) informar de forma previa a los trabajadores la finalidad con la que se solicitan o recopilan sus datos; (iii) recopilar datos veraces, exactos y necesarios; (iv) utilizar los datos con el fin con el que fueron recopilados; (v) permitir a los empleados o sus familiares ejercer los derechos de actualización, acceso, rectificación, supresión, bloqueo y oposición; (vi) garantizar la seguridad y confidencialidad de la información. (Zubiaté, 2011)

Por otra parte, con relación a los derechos del titular de los DP, se establecen en la normativa los siguientes: (i) El derecho a ser informado: El artículo 18 de la LPDP establece que antes de que los datos sean recopilados, el titular debe ser informado, sobre la finalidad de su tratamiento; (ii) El derecho de acceso: El artículo 19 de la ley reconoce el derecho al titular de solicitar y obtener la información que se encuentre

registrada sobre él o es objeto de tratamiento; (iii) El derecho de actualizar, incluir, rectificar y suprimir los datos: El artículo 20 de la LPDP regula estos derechos cuando sean inexactos, falsos, errados o incompletos; (iv) El derecho de impedir que los datos sean suministrados: El artículo 21 de la LPDP establece este derecho cuando con ello se vulnere sus derechos fundamentales; (v) Derecho a la oposición: El artículo 22 LPDP confiere al titular el derecho de oponerse al tratamiento de sus DP, cuando no se haya consentido su tratamiento o cuando existan razones fundadas o legítimas de una situación personal en concreto; (vi) Derecho a la tutela: El artículo 24 de la LPDP establece que si el titular o encargado de la base de datos deniegue el ejercicio de algunos de los derechos reconocidos al titular de los DP, la ley habilita a obtener tutela por la vía administrativa o judicial; (viii) Derecho a la indemnización: En caso de que exista un incumplimiento a la normativa de PDP, el titular de los DP tendrá el derecho a ser indemnizado.

En adición a ello, es importante resaltar la investigación de Zubiaté con relación a la PDP -específicamente la PDP de los trabajadores- reconociendo su plena aplicación en el ámbito laboral, específicamente, con relación al tratamiento que los empleadores realicen respecto a la información de carácter personal de sus trabajadores que se encuentran almacenadas.

En este sentido, con relación al régimen jurídico sobre la PDP de los trabajadores, la LPDP y su reglamento buscan garantizar el adecuado tratamiento de los DP y sensibles almacenados en una base de datos, cuya administración este a cargo de entidades públicas o privadas (Zubiaté, 2011).

Con relación a lo anterior, Zubiaté (2011) resalta dos situaciones: (i) La primera se refiere al contrato de trabajo. En el escenario del contrato laboral se puede identificar fuentes en donde se encuentra almacenada la información personal de los trabajadores y sus familiares que son administradas por sus empleadores o por terceros privados o públicos, como los sistemas de almacén manejados por los cazatalentos, las páginas en línea que contienen los cv de los candidatos. (ii) La segunda se refiere a las relaciones de trabajo privadas, en estas los empleadores tienden a recopilar, almacenar y conservar datos de sus trabajadores. Por ejemplo, los archivos que los empleadores administran por cada trabajador, en donde se registra toda la información que se obtiene de él durante la duración de su contrato de trabajo. Otras fuentes que almacenan información de los trabajadores son los registros de accidentes de trabajo y las planillas de remuneraciones. En este sentido, la información contenida en las fuentes de almacenamiento anteriormente mencionadas permite identificar de forma potencial a

cada trabajador. Por ello, un mal manejo de la información podría vulnerar derechos fundamentales de los trabajadores como el de la intimidad personal y familiar.

De la revisión de la literatura podemos encontrar las siguientes conclusiones:

Con relación a la PDP, se ha considerado que a pesar de que este derecho surgió a partir del derecho a la privacidad y la vida íntima, hoy en día se le considera como un derecho independiente (Remolina, 2012), consustancial a la nueva era del avance de las nuevas tecnologías que hacen cada vez más endeble las informaciones de las personas.

En este sentido, la sentencia alemana logró la configuración del derecho a la intimidad como expresión del derecho a la autodeterminación informativa, estableciendo que el individuo tiene la facultad de decidir básicamente por sí mismo y dentro de los límites que estime conveniente con relación a situaciones concernientes a su vida personal (Bru, 2007).

Así las cosas, el derecho a la PDP es un derecho fundamental independiente, enmarcado dentro del derecho fundamental de la autodeterminación informativa (Zegarra, 2011).

Con relación al marco jurídico nacional, se considera que la normativa peruana en PDP posee una naturaleza jurídica de desarrollo constitucional (Eguiguren, 2015 & Zegarra, 2011). Su fin es ofrecer seguridad jurídica y garantías suficientes para la PDP.

Esta normativa sobresale no solo por su notorio avance en esta materia (Gamarra, 2015), sino también, por asumir los estándares internacionales sobre PDP y privacidad, incorporando en nuestro ordenamiento una serie de principios y reglas aplicables al tratamiento de datos y a la gestión y registro de bases de datos, tanto en el ámbito privado como público.

En adición, dicha normativa ha regulado los mecanismos relacionados al consentimiento, seguridad, confidencialidad, entre otros (Ley 29733 y su reglamento).

Por todo lo expuesto, se resalta que la normativa peruana de protección de datos personales, vertebrada por la Ley 29733 y su reglamento, constituyen el principal instrumento jurídico en esta materia. Por ende, las empresas deben estar direccionadas no solo a cumplir con la normativa en materia de PDP, sino también en asumir de forma voluntaria los compromisos vinculados con el cumplimiento normativo o *compliance laboral*, siendo una de sus principales áreas de actuación de incidencia laboral la PDP.

Dicha herramienta de gestión y prevención se tratará de forma general y específica en el siguiente acápite.

2.2 Cumplimiento normativo y gestión de riesgos

2.2.1 Cumplimiento normativo

El origen del *compliance* puede situarse en la década de 1960, cuando la US Securities and Exchange Commission[3] detectó que más de cuatrocientas compañías estadounidenses fueron partícipes de pagos ilícitos a partidos políticos o funcionarios del gobierno en el extranjero (Espinoza, 2017, p. 5).

Ante dicho contexto, el Senado aprobó en 1977 el Foreign Corrupt Practices Act[4], la cual incluyó disposiciones anti-soborno y prohibiciones de pagos ilícitos a funcionarios extranjeros.

Años después, surgió el Comité de Organizaciones Patrocinadoras de la Comisión Treadway[5]. En 1992, dicho comité puso en conocimiento una guía de referencia incorporado para el control interno de las empresas, el cual fue aprovechado como modelo para implementar, diseñar, dar seguimiento y evaluar lo controles internos (Espinoza, 2017, p. 6).

Posteriormente, en el año 2002, tras los nuevos escándalos desatados en Estados Unidos, se emitió la Ley Sarbanes. En este aspecto, varios casos fueron claros ejemplos para deducir que era necesario internalizar la cultura de cumplimiento normativo en las empresas, y además, fortalecer una efectiva supervisión de los programas de prevención interno (Espinoza, 2017, p.6).

[3] Es también conocida como SEC, fue creada en 1934 por la Ley de Intercambio de Valores. La SEC es una agencia de los EE.UU. cuya responsabilidad principal es brindar protección a los inversionistas, velar por el íntegro desarrollo de los mercados de valores y por el fiel cumplimiento de las legislaciones federales de los valores. Además de la Ley de 1934, la SEC se encarga de hacer cumplir otras legislaciones como la de Valores de 1933, Fideicomiso de 1939, la Sarbanes-Oxley de 2002, entre otras.

[4] También conocida como FCPA, traducida al español como la Ley de Prácticas Corruptas en el Extranjero. Fue aprobada en 1977 por el Congreso estadounidense para sancionar el soborno tendente a influenciar las decisiones de empleados públicos. En el caso que una empresa violase la referida ley, la acción sería considerada como delito y sancionada de manera civil y penal, lo cual podría ser aplicable a las empresas y particulares.

[5] COSO (Committee of Sponsoring Organizations of the Treadway) es una comisión constituida voluntariamente por delegados de cinco organizaciones del sector privado en EEUU como resultado de la existencia de malas prácticas empresariales. Los informes más relevantes publicados por la comisión son: COSO I y COSO II.

En este sentido, la referida ley constituyó un verdadero giro en los *compliance programs*, ya que a partir de esta legislación, las obligaciones se hicieron cada vez más rigurosas en esta materia (Fortuny, 2014).

En el ordenamiento jurídico peruano, debido a los nuevos casos de corrupción empresarial desatados en nuestro continente[6], el *compliance* se vio introducido -por las autoridades gubernamentales- con el objetivo de normalizar la función del complimiento normativo a nivel empresarial (Espinoza, 2017, p.7).

Por ello, el 21 de abril del 2016, se aprobó la Ley No. 30424, la cual tiene por fin reglamentar la responsabilidad administrativa de las personas jurídicas únicamente por el delito de cohecho activo[7] a nivel transnacional. Posteriormente, el Decreto Legislativo No. 1352 amplía el número de delitos, estableciendo, en adición, los delitos de cohecho activo genérico y específico, lavado de activos y financiamiento de terrorismo.

Después de abordar el anterior preámbulo histórico, resulta relevante abordar el concepto del término anglosajón *compliance* o también conocido como cumplimiento normativo. Así pues, existen diferentes definiciones del referido término: el *Black Law Dictionary*, por ejemplo, simplemente lo define como ‘’sumisión; obediencia; conformidad’’; la Enciclopedia Internacional de Ciencias Sociales y del Comportamiento afirma que ‘’para que la ley sea efectiva en el cumplimiento de su papel de minimizar la ocurrencia de conductas socialmente perjudiciales, las personas deben cumplir con los dictados de la ley, es decir, la ley debe ser obedecida’’. Desde esta óptica y utilizando estas definiciones como base, se considera al *compliance* como el cumplimiento de obligaciones específicas codificadas en un instrumento internacional a través de cualquiera de las medidas de implementación a nivel nacional (Thomann, 2011, p.22).

Por su parte, la Norma ISO 19600[8], define al *compliance* como el resultado de que una empresa ejecute sus obligaciones legales y sus compromisos asumidos de manera voluntaria, tales como estándares de buen gobierno corporativo, de comportamiento ético, entre otros.

[6] Uno de los casos más actuales de corrupción corporativa en América Latina es el relativo a la empresa Odebrecht, el cual fue parte de la operación Lava Jato. El escándalo, aunque comenzó siendo parte de la red de lavados de Petrobras, terminó por convertirse en uno propio debido a la magnitud de los sobornos y el despliegue a nivel mundial. Los sobornos entre los años 2001 al 2016 alcanzaron los 788 millones de dólares, destinados a políticos, partidos, y otros intermediarios en países de América Latina.

[7] Artículo 397-A del Código Penal Peruano.

[8] La Norma ISO 19600 (2015) es una norma de relevancia internacional, la cual ha contribuido con dotar a las empresas de un sistema de gestión de cumplimiento normativo con el fin de eludir los diferentes riesgos que se producen por no cumplir con la norma.

Sobre este punto, la Organización Mundial de Compliance entiende al *compliance* como la agrupación de buenas prácticas y procedimientos adoptados por las empresas con el fin de clasificar e identificar los riesgos legales y operativos que afrontan y establecer una serie de mecanismos destinados a prevenir, gestionar, controlar y reaccionar frente a los mismos (Cámara Guatemalteca de la Construcción, 2018).

En otros términos, el cumplimiento normativo puede ser definido como una función independiente que mediante políticas y procedimientos adecuados es capaz de detectar y gestionar el riesgo de incumplimiento de las obligaciones intrínsecas y extrínsecas que posee una empresa (Solís, 2007, p. 78).

Desde otra arista, se considera que el *compliance* es un concepto que actúa de acuerdo con las leyes, regulaciones, estándares, protocolos y especificaciones establecidas. El problema crítico se relaciona con el costo de incumplimiento, que puede ser civil, penal, reputacional, financiero o de mercado (Tarantino, 2008, p. 21-22).

En esta línea, con relación a la doble función que posee el *compliance*, Clavijo señala que, en primer término, este cuenta con una función de prevención. Esta función está conformada por una serie de medidas organizativas y de vigilancia interna de la empresa, con el fin de que esta no cometa infracciones legales. Es decir, lo que se busca es evitar infracciones que pueda cometer, de forma individual, un trabajador de la empresa, y además, aquellas infracciones derivadas de la organización defectuosa de la actividad que realiza. En segundo término, tenemos a la función de confirmación del derecho. Esta función consiste en establecer una serie de mecanismos con el fin de que se detecten la existencia de irregularidades dentro de la organización, y en el caso que de demostrarse su existencia, se ponga en conocimiento ante la autoridad que corresponda (2014, p. 631).

Pues bien, el *compliance*- relacionado con la acción de prevenir y gestionar los riesgos en el ámbito penal- es de suma importancia para las empresas, ya que con esta herramienta estas serían capaces de fomentar una ‘’verdadera cultura ética empresarial’’ -la cual va más allá de cumplir con las regulaciones- proveyéndose de procedimientos, protocolos y modelos en materia de *compliance* legal en general, y no sólo con la legalidad penal, cobrando relevancia en los diferentes campos jurídicos (Rojas, 2017, p. 25). Es decir, el *compliance* es el cumplimiento de todo el ordenamiento jurídico para evitar responsabilidades administrativas, penales y civiles (Bacigalupo, 2016, p. 4).

Cabe mencionar que la gestión y prevención de incumplimientos normativos debe entenderse del grupo de normas externas o internas, es decir, no solo con las normas

de carácter imperativo (hard law), sino también de aquellas que sean de cumplimiento voluntario (nacionales o internacionales), tales como las recomendaciones o estándares que tengan reconocimiento internacional (soft law), adquiriendo las organizaciones un pacto innegable con la cultura de cumplimiento ético (Rojas, 2017, p. 25). En este aspecto, el *compliance* sería considerado más que una herramienta de buen gobierno corporativo: una nueva filosofía para las corporaciones (Bacigalupo, 2016, p.4).

Por otro lado, no cabe duda que el *compliance* ha ganado relevancia en los diferentes campos jurídicos, ya que se ha constatado que el disponer de protocolos, procedimientos y modelos organizativos que delimiten el grado de cumplimiento normativo en la empresa ya no es netamente propio del orden penal, ya que este sistema de vigilancia ha ganado igual presencia en su vertiente laboral (Rojas, 2017, p. 2).

De esta manera, dentro del marco de la norma laboral, el *compliance* laboral o cumplimiento normativo en el ámbito laboral puede ser definido como la función corporativa capaz de prevenir y gestionar los riesgos relacionado a un incumplimiento laboral eventual en el seno de las organizaciones. Siguiendo esta aproximación conceptual, el riesgo de cumplimiento se basaría no sólo en los riesgos legales, sino también, en los riesgos económicos y reputacionales como consecuencia de la falta de capacidad de la empresa para cumplir con las regulaciones, leyes, códigos de conducta y normas de las buenas prácticas (Rojas, 2016, p.2).

Desde otra perspectiva, el *compliance* laboral es considerado como un modelo capaz de tratar de forma global las normas laborales-voluntarias u obligatorias-que subyacen en una empresa. Dicho modelo no solo permitirá minimizar riesgos, sino también implantar un código ético que sepa tratar diferentes áreas laborales, tales como: prevención de riesgos, condiciones de trabajo, acoso laboral, protección de datos, entre otras (Pañella, 2018).

Anudado a ello, se ha considerado que los programas de cumplimiento normativo laboral deben englobar distintas áreas de actuación, entre las que destacan: igualdad y no discriminación; condiciones de trabajo; nuevas tecnologías de la información y comunicación en el ámbito laboral; PDP y propiedad intelectual; prevención de delitos en el ámbito laboral; prevención de riesgos laborales, seguridad y salud en el trabajo, etc. (Rojas, 2016, p. 3).

Con relación al área de actuación de protección de datos, debemos hacer hincapié que resulta necesario establecer una cultura de *compliance* o cumplimiento normativo que

se relacione con el compromiso de la empresa respecto a la PDP, con el fin de que se vean mermados los riesgos de incumplimiento que se podrían producir en esta materia.

Por ello, los sistemas de *compliance* laboral son considerados como una herramienta esencial para prevenir y gestionar los incumplimientos laborales, basándose en el cumplimiento de la normativa laboral vigente y en el aseguramiento de desarrollar buenas prácticas laborales, siendo todo esto parte de la responsabilidad social empresarial (Rojas, 2017, p. 26).

Cabe mencionar que la efectividad de los sistemas de gestión de *compliance* laboral que se implementen vendrá determinado por la necesidad de auto-cumplimiento de las normas internas previamente aprobada en la empresa. De no ser el caso, el mencionado sistema no tendría suficiente legitimidad moral ni jurídica para exigir a sus empleados los diferentes deberes que hayan sido previamente comunicados (Rojas, 2017, p. 27).

Así, el logro de las políticas relacionadas al *compliance* laboral está en el cambio de criterio basada en la interiorización y en hacer propia la responsabilidad social corporativa y la cultura de cumplimiento ético en el comportamiento de todos los trabajadores (Baltar & Cuenca, 2018).

Sobre este punto, se entiende que la aplicación de un programa de *compliance* laboral se habrá logrado en el momento que dicha herramienta haya contado con la complicidad de todos los actores de la empresa- empleador y empleados. Este es el momento cúspide en donde se habrá alcanzado un sistema integral que creará una nueva cultura empresarial basada en el cumplimiento normativo, la igualdad y el bienestar laboral (Pañella, 2018).

2.2.2 Gestión de riesgos

La gran parte de las actividades humanas están expuestas al riesgo. En el caso de la actividad empresarial, existen un sin número de riesgos que pueden controlarse mediante la utilización de ciertas medidas de prevención (Zurita, 2015, p.18).

Según lo señalado por Banks, el riesgo puede afectar a todas las áreas de la actividad personal y corporativa. Bajo esta óptica, este puede ser definido como la incertidumbre que rodea el resultado de un evento futuro (2002, p.1).

Desde otra óptica, se considera que el riesgo está siempre vinculado a la incertidumbre integrada a un evento futuro. En el ámbito empresarial, el riesgo se singulariza por ser una eventualidad que puede ocurrir o no, y si llegara a presentarse, afectaría el cabal

cumplimiento de los lineamientos propios de una organización (Londoño & Núñez, 2010, p. 39).

De forma similar, el riesgo es definido como la probabilidad de que un evento ocurra, y de ser así, afecte el cumplimiento de los objetivos (Mejía, 2006, p. 32).

En este contexto, a pesar de que los riesgos empresariales pueden asumir muchas formas, en la presente investigación nos centraremos en abordar específicamente el riesgo legal.

En este sentido, debemos partir con la idea de que el riesgo legal está incluido dentro del riesgo operativo[9], ya que los procesos de una empresa deben estar en concordancia con la legislación y el marco contractual en el que se desenvuelve (Zurita, 2015, p. 29).

Sobre este punto, la doctrina legal europea está de acuerdo en que no existe una definición común de riesgo legal. Los autores Miscenic y Raccah entienden que desde el punto de vista de la ciencia legal, el riesgo legal no existe porque el núcleo de la ley debe ser predecible, por ende, la introducción del riesgo en la ley implicaría un juicio de valor que se opone a las amenazas y la seguridad. Sin embargo, entienden que la ciencia jurídica puede replantear el riesgo legal como un metalenguaje para describir y analizar el propósito, así como el impacto de la ley en diferentes componentes de la sociedad (2016, p. 4).

No obstante a lo anteriormente mencionado, el riesgo legal puede ser definido como el riesgo financiero o de reputación que puede resultar de la falta de conocimiento, de la falta de comprensión o de la ambigüedad respecto a la forma en que las leyes y regulaciones se aplican a la empresa, sus relaciones, procesos, productos y servicios (Whalley & Guzelian, 2017, p. 23).

Cabe destacar que el significado de riesgo legal trasciende las repercusiones estrictamente legales, incluido el riesgo de enjuiciamiento, acción reglamentaria, reforma legal, reclamos o la pérdida de derechos de propiedad contractuales o de propiedad intelectual. Esta definición tiene tanto significado práctico como la base de cualquier sistema de administración de riesgo legal y significado cultural para enmarcar la cultura corporativa en torno al derecho y la ética (Weinstein & Wild, 2013, p. 92).

[9] También llamado riesgo operacional. Este es definido como la ‘’posibilidad de que ocurran pérdidas como resultado de los procesos inadecuados, fallas de personal o de la tecnología de información o a eventos externos’’ (Acuerdo internacional de Basilea II)

Por su parte, el Comité de Supervisión Bancaria de Basilea define al riesgo legal como la probabilidad a que una empresa sea multada, sancionada u obligada a pagar daños punitivos como producto de acuerdos privados entre las partes (Zurita, 2015, p. 30).

Desde otro enfoque, el concepto de riesgo legal puede ser categorizado en dos: (i) El directo, se refiere a la posibilidad de pérdidas debido al incumplimiento de las leyes que afecta a los contratos y (ii) el indirecto, se refiere a que el riesgo legal crece con la incertidumbre sobre la normativa, leyes y acciones legales aplicables (Mahler, 2009).

Ahora bien, una herramienta de relevancia y de valor para la administración empresarial es el de la gestión de los riesgos.[10]

En este orden, para administrar y controlar los riesgos, las empresas deben esforzarse por utilizar todas las herramientas y enfoques disponibles, con el objetivo de minimizar la posibilidad de que ocurran pérdidas inaceptables (Banks, 2002, p.1)

En otras palabras, las empresas activas que toman riesgos deben tratar de utilizar enfoques tanto cuantitativos como cualitativos para ayudarlos a manejar sus exposiciones. De esta manera, la gestión cuantitativa del riesgo se basa en modelos matemáticos y técnicos para identificar, cuantificar y gestionar las exposiciones, es un enfoque importante para el control de riesgos. Sin embargo, la gestión de riesgos cualitativa se centra principalmente en la experiencia, el juicio y el sentido común, representa un segundo enfoque importante (Banks, 2002, p.1).

Así pues, algunas empresas prefieren los enfoques cuantitativos sobre los procesos cualitativos, mientras que otras prefieren un enfoque cualitativo. En algunos casos las empresas confían en ambos métodos. De hecho, el enfoque ‘’combinado’’ puede ser el mejor, ya que el proceso de riesgo verdaderamente efectivo se basa en las fortalezas de las técnicas cuantitativas y cualitativas para superar las deficiencias y debilidades individuales que caracterizan a cada disciplina (Banks, 2002, p.1).

En esta línea, COSO (2004) establece que la gestión de riesgos parte del supuesto de que las empresas existen con el fin de generar valor. En este sentido, el desafío de toda empresa es definir cuánta incertidumbre es capaz de aceptar frente a lo cual la gestión

[10] ISO 31000 es la norma internacional sobre la gestión de riesgos. Esta norma es de gran ayuda para las empresas con relación al análisis y evaluación de riesgos. Recoge una serie de buenas prácticas que proporcionan la eficiente gestión de los riesgos a todos los niveles, especialmente, operativo, de gobierno y a nivel de confianza de las partes interesadas. Además, esta norma incorpora una serie de principios del riesgo como factor clave del éxito en el diseño, implementación, operación, mantenimiento y mejora de un sistema de decisión de riesgos; sin embargo, el más relevante es el principio de la generación de valor.

de riesgos permite un manejo eficaz de los riesgos y las oportunidades con el fin de mejorar la capacidad de generar valor.

Así pues, la gestión de riesgos es definido como el proceso de gestionar la incertidumbre que surge en el curso normal de las actividades, incluidas las relacionadas con los negocios (Banks, 2012, p. 1).

Por otro lado, la norma internacional ISO 31000 define al proceso de gestión de riesgos como la aplicación sistemática de políticas tendentes a identificar, analizar, evaluar, tratar, dar seguimiento y revisar el riesgo.

En adición a lo anterior, es importante mencionar los modelos más relevantes de la gestión del riesgo.

Por una parte, se encuentra el ISO 31000 o ‘’Gestión de riesgos - principios y directrices’’ (2009). Según Whalley y Guzelian, la referida norma describe la gestión de riesgos como un proceso de cinco tareas secuenciales complementadas con dos actividades continuas que rodean el ejercicio de gestión de riesgos. Las cinco tareas de gestión de riesgos secuenciales son: (i) Establecer el contexto. El estándar puede aplicarse en muchos contextos. En los negocios, por ejemplo, el contexto sería la empresa en su conjunto e incluiría áreas específicas de riesgo tales como riesgo operacional, riesgo de crédito, riesgo de mercado y riesgo legal; (ii) Identificar el riesgo. La segunda tarea es establecer dónde existen riesgos en su contexto definido. Para el riesgo legal, se tendrá que identificar cuáles de sus prácticas comerciales, productos o servicios podrían resultar en pérdidas financieras o de reputación; (iii) Analizar. La tercera tarea es estimar el impacto de los riesgos en su capacidad para lograr sus objetivos. Especificar el tipo de impacto y nivel que le interesa es una parte clave de este paso; (iv) Evaluar. Cuando se haya identificado y analizado sus riesgos, se debe comparar y contrastar los impactos potenciales y priorizar los riesgos para el tratamiento de acuerdo con su impacto potencial relativo; (v) Tratar. La quinta y última tarea es implementar controles que minimicen o eliminen el riesgo por completo (2017, p. 55).

Ahora bien, las dos actividades que se debe realizar a lo largo del proceso son: (i) En un primer término, la actividad de monitoreo y la revisión continua. Es decir, se debe controlar el riesgo y asegurar que se está gestionando de acuerdo con el plan de tratamiento. (ii) En segundo término, la actividad de comunicación continua y consulta. También se debe verificar los riesgos nuevos y emergentes; así como reunirse regularmente con las partes interesadas para volver a analizar y reevaluar la cartera de riesgos legales y mantener el registro de riesgos legales relevante para las actividades actuales (Whalley y Guzelian, 2017, p. 55).

Por otra parte, se encuentra el modelo de gestión de riesgos COSO (2004). Según Whalley y Guzelian, este adopta un enfoque ligeramente diferente a la norma ISO. En lugar de centrarse en un tipo de riesgo específico, revisa todos los riesgos pertenecientes a la empresa e identifica ocho componentes de administración que gestionan colectivamente su exposición a diferentes riesgos, a saber: (i) Entorno interno. Este se refiere a los valores y políticas y cómo afectan las decisiones de riesgo; (ii) Establecimiento de objetivos. Resulta muy importante articular los objetivos que la empresa quiere lograr; (iii) Identificación de riesgos. Es importante enumerar los eventos que podrían afectar la capacidad de la empresa para lograr sus objetivos; (iv) Evaluación de riesgos. En este punto se debe estimar la probabilidad de que ocurra el evento y cuál sería el impacto que tendrá en el caso de que ocurra; (v) Respuesta de riesgo. En este punto es muy importante tomar la decisión con relación a lo que la empresa hará en respuesta al riesgo potencial; (vi) Actividades de control. Es decir, describir las políticas y los procedimientos que necesita implementar para garantizar que se lleve a cabo la respuesta seleccionada; (vii) Información y comunicación. Se debe capturar y comunicar información relevante que afecte las decisiones y actividades de gestión de riesgos, y por último, (viii) Seguimiento. Es de suma relevancia evaluar continuamente si las actividades de administración de riesgos que se implementó son efectivas y si los nuevos eventos y riesgos podrían afectar su capacidad para alcanzar sus objetivos (2017, p. 56).

Ahora bien, desde una perspectiva laboral y de incertidumbre legal, la gestión del riesgo legal laboral[11] está basado en la identificación y análisis de los riesgos legales laborales cuyo fin primordial es su minimización (Montenegro, 2016, p.31).

En esta misma línea, es importante resaltar que el Oficial de Cumplimiento (como figura primordial de los sistemas de gestión de *compliance)* estará obligado a atender los deberes laborales que puedan ser aplicables a la empresa (Rojas, 2017, p. 27).

Para ello, en palabras de Rojas, es necesario que se siga con los siguientes pasos: Primero, se debe proceder a identificar los riesgos potenciales que podría tener una organización por posibles incumplimientos laborales. En esta etapa no sólo se deberá tener presente el cumplimiento de las obligaciones laborales de *hard law* (convenios, reglamentos, leyes, entre otros), sino también normas de voluntario cumplimiento, y por ende, no vinculantes emitidas por alguna organización internacional (ISO, OCDE, OIT, entre otras) en materia de responsabilidad social corporativa y buenas prácticas laborales. Segundo, una vez que se ha realizado la primera etapa, se deberá hacer una

[11] Ver Montenegro, 2016, p. 31-32.

clasificación de los riesgos laborales de acuerdo a su impacto y probabilidad. Tercero, se deberá diseñar y ejecutar protocolos y mecanismos de control al interior de la empresa, como el canal de denuncias interno, el cual deberá estar vinculado a una normativa básica aprobada por la empresa, como el Código Ético o de Buenas Prácticas. Por último, el sistema de gestión deberá contener mecanismos de seguimiento, evaluación y monitoreo, con el fin de reaccionar y corregir a tiempo las posibles deficiencias que podría poseer el propio sistema de gestión (Rojas, 2017, p. 27).

De la revisión de la literatura podemos encontrar las siguientes conclusiones:

El breve preámbulo histórico que se ha desarrollado sobre el cumplimiento normativo es importante para comprender su origen, evolución y la indudable necesidad de crear un sistema de gestión capaz –en la medida de lo posible- de evitar la comisión de delitos.

El *compliance* o cumplimiento normativo se refiere a todas las medidas preventivas, organizativas y técnicas tendentes a asegurar que una empresa cumpla con el marco normativo, los códigos éticos, los compromisos con terceros (clientes, proveedores) y las buenas prácticas. Su doble funcionalidad se basa en la prevención y confirmación del derecho (Clavijo, 2014).

En el ámbito jurídico laboral, el *compliance* también juega un papel importante, ya que sus sistemas de gestión son herramientas fundamentales para la gestión y prevención de incumplimientos laborales (Rojas, 2017).

Con relación a la gestión de riesgos, las empresas deben esforzarse por utilizar todas las herramientas y enfoques disponibles (Banks, 2002), ya que el objetivo primordial de la gestión de riesgos es el control. Para ello, se han diseñado diferentes modelos de gestión de riesgos, tales como ISO 31000 y COSO, los cuales deben ser analizados de acuerdo a su aplicación para una u otra empresa.

En cuanto a la gestión del riesgo legal laboral, se debe tomar en consideración lo siguiente: a) Identificar el riesgo, es decir, identificar los riesgos potenciales que podría tener una organización por posibles incumplimientos laborales; b) Clasificar el riesgo, es decir clasificar los riesgos laborales de acuerdo a su impacto y probabilidad; c) Diseñar y ejecutar, es decir se deberá diseñar y ejecutar protocolos y mecanismos de control al interior de la organización, como el canal de denuncias interno; d) Dar seguimiento, es decir, el sistema deberá contener mecanismos de seguimiento, evaluación y monitoreo, con el fin de reaccionar y corregir a tiempo las posibles deficiencias que podría poseer el propio sistema de gestión (Rojas, 2017).

Por todo lo expuesto, podemos afirmar que estamos ante el análisis de diferentes campos jurídicos –protección de datos y cumplimiento normativo (gestión de riesgos) -, que sin duda se encuentran plenamente complementados entre sí.

Si las empresas adoptasen los sistemas de *compliance* en materia de PDP se generaría una sinergia indiscutible con relación al alcance de diversos objetivos, sobretodo, que las empresas sean capaces de gestionar, prevenir, minimizar o evitar los diversos riesgos que podrían enfrentar en caso de no haber implementado a tiempo tales sistemas.

En este sentido, es sumamente importante que las empresas ponderen la relevancia de incorporar sistemas de gestión de cumplimiento normativo laboral, en donde la PDP sea el principal componente en dicho sistema y en la cultura de cumplimiento.

Por ende, uno de los objetivos de este trabajo de investigación –además de establecer la importancia de la incorporación del sistema de gestión en las empresas- es proponer diferentes mecanismos de cumplimiento normativo laboral en materia de PDP, previo a esto se abordarán las secciones relacionadas a la problemática y discusión, las cuales serán detalladas en el próximo capítulo.

CAPÍTULO III: PROBLEMA DE INVESTIGACIÓN

En el capítulo 1 del presente trabajo de investigación se estableció someramente la problemática existente en nuestra temática objeto de estudio. En síntesis, dicha problemática se traducía en la posibilidad de las empresas de incurrir en malas prácticas en materia de PDP en el ámbito de las relaciones laborales, motivado no solo por el incumplimiento de la normativa aplicable con relación a sus obligaciones-tanto de los empleadores y/o empleados en esta materia- sino también por las empresas no asumir un compromiso voluntario relacionado a la efectiva gestión de los riesgos, la autorregulación y el cumplimiento normativo en esta específica incidencia laboral.

Por otro lado, en el capítulo 2, se estableció que actualmente resulta sumamente importante que las empresas no desconozcan la PDP dentro del marco las relaciones laborales, con el fin de evitar eventuales perjuicios legales, económicos y reputacionales, ya que éstas se encuentran cada vez más constreñidas a cumplir con la normativa aplicable en este ámbito. Por ello, con el fin de desarrollar el presente problema de investigación en relación al estado del arte, el mismo se dividió en dos partes; la primera, abordó todo lo relacionado con la PDP y su marco jurídico nacional; la segunda, estuvo referida al cumplimiento normativo y a la gestión de los riesgos (riesgo laboral y su sistema de cumplimiento normativo laboral).

Con el balance integral de ambos capítulos, debemos adicionar que para comprender nuestra problemática se dispuso que se utilizará la metodología del método comparado y riesgos legales, en donde, mediante la primera, se pretende cotejar la normativa y la jurisprudencia nacional e internacional en materia de PDP, significando un notorio avance en esta materia dentro del marco de la prestación laboral; y mediante la segunda, se pretende identificar el impacto que podría tener el no cumplir con la normativa de PDP en el marco de las relaciones de trabajo o con el hecho de no haber implementado un correcto sistema de detección, gestión y prevención de riesgos a tiempo.

Tal como fue mencionado anteriormente, nuestra investigación se centra en analizar aquellas relaciones laborales cuyos agentes puedan tener una intervención y responsabilidad frente al tratamiento y manejo de los datos personales, resultando ilustrativo destacar ciertos casos peruanos y extranjeros en donde se puede visualizar las malas prácticas de algunas empresas en esta materia, los cuales han sido resueltos mediante diversas resoluciones directorales y/o sentencias emanadas de los diferentes tribunales.

La relevancia de la selección de los casos que serán abordados en los próximos párrafos radica en que no solo se encuentran enmarcados dentro de la materia de PDP en el marco de las prestaciones laborales, sino también, permiten una notoria identificación de las obligaciones que deberían cumplir los diferentes agentes con relación al tratamiento de datos dentro del ámbito laboral. En suma, con el desarrollo de dichos casos seleccionados, resulta posible establecer variadas propuestas alternativas con el fin de mitigar o prevenir los riesgos que podrían acarrear perjuicios legales, económicos y reputacionales de cara a las empresas; y de esta manera, fomentar no solo las buenas prácticas empresariales, sino además, motivar a éstas a que asuman un compromiso voluntario relacionado a la efectiva gestión de los riesgos, la autorregulación y el cumplimiento normativo en materia de PDP.

3.1 Caso Asociación Pastoral de Servicios Good Hope: Contravención al principio de proporcionalidad

El primer ejemplo de lo antes mencionado es el caso relacionado a la Asociación Pastoral de Servicios Médicos Asistenciales Good Hope de la Iglesia Adventista del Sétimo Día, el cual se encuadra en la relación laboral de empleador –empleado, en donde el primero detentó responsabilidad en el tratamiento de datos frente al segundo (titular).

En el año 2015, la Dirección de Supervisión y Control inició un procedimiento sancionador a la referida Asociación por realizar un tratamiento desproporcional de la información personal de sus postulantes de trabajo al requerirles, al momento de postular, que declaren su religión; así como el tratamiento desproporcional de la información personal referida al sacramento religioso del bautizo de sus trabajadores. El 24 de mayo del 2016, mediante la Resolución Directoral No. 158-2016, se sancionó a la referida Asociación con una multa ascendente a 8 UIT por haber realizado un incorrecto tratamiento de los DP de los postulantes y trabajadores de la entidad. Esto se configuró como una contravención al artículo 7 de la LPDP (Principio de Proporcionalidad) y se consideró como una infracción grave (literal a, numeral 2 del Art. 38 LPDP).

No obstante a esto, la referida Asociación apeló el 6 de julio de 2016 la mencionada Resolución Directoral alegando que ésta se dedica al servicio de salud dirigida por la Iglesia adventista, siendo necesario contar con la información relacionada al perfil profesional y espiritual de los trabajadores, ya que la finalidad de la institución es brindar asistencia social pastoral médica con el fin de contribuir con el desarrollo del ser humano

basado en principios y fines espirituales de la Iglesia Adventista del Séptimo Día, resultando relevante para la institución religiosa conocer este tipo de información.

El 19 de agosto del 2016, mediante Resolución Directoral No. 065-2016, se estableció que la información referida al bautizo o religión es calificada como datos sensibles que requieren un consentimiento por escrito, y en su defecto, pueda efectuarse cuando una ley así lo autorice. En adición, se señaló que existe una protección del ejercicio de la libertad religiosa amparada por el Artículo 9 de la Ley 29635 y en el tercer párrafo del Artículo 3 de su reglamento. Finalmente, se argumentó que la empresa no indicó en su partida electrónica que los fines de atención de los servicios de salud estén referidos exclusivamente a las personas que pertenezcan a dicha entidad, es decir, que compartan la misma religión, sino que hace referencia a la prestación de los servicios de salud a toda la comunidad en general. Por todo ello, se dictaminó infundado el recurso de apelación, ya que la entidad vino realizando un tratamiento desproporcional de la información relacionada a la religión de los trabajadores y los postulantes a los puestos de trabajo, puesto que recopiló datos sensibles que son excesivos a la finalidad de cumplir con la gestión de recursos humanos como el acceso al empleo o el desarrollo propio de las actividades laborales.

En este caso en concreto, es preciso señalar que el poder de dirección propio del empleador tiene ciertos límites, como es el caso de los derechos fundamentales del empleado. Por ello, el hecho de que una persona sea parte de alguna relación laboral, esto no podría interpretarse como un abandono o atenuación de dicho derecho por parte del trabajador cuando efectivamente éste quiera ejercerlo. Es claro que antes o durante la relación laboral, la empresa no puede establecer que para tener acceso a un puesto de trabajo o desarrollar una actividad laboral, resulte necesario tener un determinado credo religioso, ya que se estaría vulnerando con el derecho a la libertad religiosa, salvo de que en los estatutos o normas internas de la empresa se estipule que ésta tenga una determinada ideología o tendencia religiosa (Ulloa, 2002, p. 543-544).

3.2 Caso Supermercados Peruanos S.A.: Recopilación y flujo transfronterizo de datos sin previa información

Otro ejemplo nacional lo constituye el caso de Supermercados Peruanos S.A.[12], por incurrir en infracciones contrarias a la LPDP. En el año 2016, la referida empresa hizo una recopilación de datos de sus clientes, sin haber una información previa a éstos con relación a los destinatarios de su tratamiento, omitiendo, en adición, las medidas de

[12] Si bien se ha iniciado un procedimiento sancionador en este caso en particular, la Resolución Directoral no ha sido publicada aún en la página web de la Autoridad Nacional de Protección de Datos Personales por estar aún en trámite y no haber adquirido firmeza.

seguridad respectivas. Asimismo, Supermercados Peruanos S.A. realizó una transferencia de DP de sus clientes fuera del territorio peruano, omitiendo la debida comunicación a la Autoridad Nacional de Protección de Datos Personales (APDP) al respecto.

Por ello, en el año 2018, la APDP consideró iniciar un procedimiento administrativo sancionador y multar a la empresa con 8.5 UIT -equivalente a S/.33,575.00 -por incurrir en las infracciones antes referidas.

En este caso en concreto, Supermercados Peruanos S.A. debió de obtener el consentimiento del titular de DP (los clientes), ya que según lo que se establece en el Art. 18 de la normativa peruana sobre PDP, dicho titular tiene el derecho a ser informado de forma detallada y previa a la recopilación de sus datos sobre: (i) la finalidad para la que sus DP serán tratados; (ii) los destinatarios que tendrán su información; así como la identidad del titular o el encargado de su tratamiento; (iii) la transferencia de sus DP; (iv) las consecuencias de negarse o no a proporcionar sus DP; (v) el tiempo durante el cual se conservarán sus DP; entre otros.

Asimismo, el Art. 16 de la LPDP establece que el titular del banco de DP está obligado a adoptar medidas técnicas, organizativas y legales que tiendan dar garantía a su seguridad y evitar su pérdida, alteración u acceso no autorizado. Es importante resaltar que existe una directiva de seguridad realizada por la APDP en donde se establecen los requisitos y condiciones que deben reunir los bancos de DP en materia de seguridad.[13]

Ahora bien, con relación al flujo transfronterizo, el Art. 15 dispone que el titular y el encargado del banco de DP debe realizar el flujo de dichos datos solo si el país destinatario posee niveles de protección acordes con la normativa peruana en materia de PDP. En el caso de Supermercados Peruanos, no hubo una comunicación a la APDP con relación a la salida del territorio peruano de dichos datos, obviando su debido registro en el Registro Nacional de PDP.

Sobre este punto, podemos inferir que este caso se encuadraría dentro de la relación empleado-cliente, teniendo el primero responsabilidad sobre el tratamiento de datos frente al segundo. No obstante, la empresa también tuvo responsabilidad, ya que como titular del banco de DP debió de establecer las medidas de seguridad necesarias para brindar garantía a la información de sus clientes. De esta forma, si bien la empresa Supermercados Peruanos S.A. fue quien recibió la sanción por parte de la APDP debido

[13] Para ampliar el tema de seguridad en materia de PDP, ver https://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-de-Directiva-de-Seguridad.pdf

a las infracciones antes referidas, quien ostentó también la responsabil5idad frente a esta situación fue el área de marketing al recopilar DP de clientes sin un consentimiento previo; así como del encargado del banco de datos al no comunicar a la APDP del flujo transfronterizo de DP de los clientes. En la mayoría de los casos, estos encargados suelen ser empleados de la empresa; así como los proveedores que le dan el servicio a Supermercados Peruanos S.A. con relación al tratamiento de datos, los cuales suelen ser nacionales y/o extranjeros, como por ejemplo Amazon Web Services Inc. de los Estados Unidos.

3.3 Caso Cotronic S.A.: Cesión de datos personales sin consentimiento

Por otra parte, un caso de derecho comparado lo constituye la sentencia No. STS 609/2015, del 12 de noviembre del 2015, emitido por el Tribunal Supremo Sala de lo Civil de Madrid. En el año 2011, un ex trabajador interpuso una demanda en contra de la empresa Cotronic S.A. (sub contratista de Telefónica S.A.) por verse vulnerados ciertos derechos como la imagen, honor y PDP.

En el año 2009, Cotronic S.A. optó por despedirlo por supuestamente haber cobrado una suma de dinero a un cliente por algo que debía ser gratuito. Luego del hecho, el ex trabajador tuvo varias entrevistas laborales en el sector de telecomunicaciones, pero sin suerte. Sin embargo, una de las empresas que estaba interesada en la contratación de éste, le manifestó que era imposible contratarlo, ya que su ex empleadora lo incorporó a un fichero, el cual calificaba al personal como conflictivo.

En primera y segunda instancia, su demanda fue desestimada. No obstante, en casación el Tribunal Supremo estableció que el punto neurálgico era verificar el alcance de la comunicación de datos del ex trabajador, es decir, si efectivamente la empresa Cotronic S.A. comunicó datos a la empresa Telefónica S.A. referidos al cese de la actividad laboral, específicamente la incorporación en su ‘’lista negra’’[14] (fichero de trabajadores conflictivos), lo cual no sólo afectaba la intimidad del ex trabajador; sino también su futuro laboral.

Sobre este punto, el demandante presentó diversos indicios probatorios de que se había producido una conducta lesiva a sus derechos fundamentales (testimonio de uno de los miembros del comité de la empresa Telefónica quien declaró la existencia de un fichero de empleados conflictivos; el hecho de que el demandante luego de su despido estuvo

[14] En la Sentencia No. 609/2015, en su página 6, numeral 4, se define a las ‘’listas negras’’ como ficheros de DP formados mediante la recopilación y transmisión de cierta información relativa a un determinado grupo de personas, elaborada de conformidad con determinados criterios que suelen implicar efectos adversos y perjudiciales para las personas incluidas en las mismas.

imposibilitado en verse contratado por otras empresas del rubro de telecomunicaciones y el hecho de que no pudo ser contratado por ninguna empresa. La última empresa con quien tuvo una entrevista lo sometió a un examen médico). Sin embargo, la empresa demandada (teniendo la obligación de carga probatoria) no presentó la prueba relacionada con el contenido de la comunicación que hizo llegar a la empresa Telefónica S.A.

Por ello, la Corte Suprema estableció que sí hubo una existencia de cesión de datos personales, los cuales fueron susceptibles de obstaculizar el acceso al empleo del ex trabajador.

En este sentido, podemos afirmar que la controversia del caso se basó en el hecho de que el trabajador tras acudir a varias entrevistas de trabajo no conseguía ser contratado por encontrarse en un fichero específico destinado a advertir a otras empresas sobre trabajadores que eran considerados conflictivos, detentando la empresa demandada responsabilidad frente al tratamiento de los datos del ex trabajador, incluso después de terminado su vínculo laboral.

Con la casuística nacional y comparada en los párrafos precedentes, podemos afirmar que existe una problemática traducida en el incumplimiento de la norma aplicable en materia de PDP dentro del marco de la relación laboral, observándose las siguientes relaciones: (i) en el primer caso relación empleador-empleado, (ii) en el segundo caso relación empleado-cliente; y (iii) en el tercer caso relación empleador-empleado. En este sentido, en cada una de dichas relaciones se ven reflejadas las distintas responsabilidades de los agentes frente a los titulares de los datos personales, viéndose mermado el derecho fundamental de PDP con la comisión de las distintas infracciones.

Es por ello que en el siguiente capítulo se examinarán los resultados obtenidos en nuestra investigación con el marco conceptual referido y se calificará dichos resultados en función de lo establecido en nuestra hipótesis.

CAPÍTULO IV: DISCUSIÓN

Con el desarrollo de nuestra problemática en el capítulo precedente, podemos afirmar que todas las empresas anteriormente referidas están direccionadas, de cierto modo, a gestionar datos de carácter personal y sensible, siendo indiscutible que todas éstas se encuentren obligadas a realizar una correcta gestión y tratamiento de la información.

Como bien afirman Santos, López & Tejedor, el deber de cumplir con la normativa en materia de PDP se relaciona con la actividad empresarial, ya que resulta sumamente necesario desde dos perspectivas: (i) legal -cumplir con la normativa vigente- e (ii) interna -dentro de las relaciones laborales- (2005, p. 20).

En este sentido, es importante nuevamente recalcar que como resultado de la aplicación de la normativa en materia de PDP, el empleador debe estar sujeto a cumplir con una serie de obligaciones, tales como: (i) efectuar el tratamiento de los datos con el previo consentimiento de los trabajadores o familiares, documentando tal consentimiento; (ii) informar de forma previa a los trabajadores la finalidad con la que se solicitan o recopilan sus datos; (iii) recopilar datos veraces, exactos y necesarios; (iv) utilizar los datos con el fin con el que fueron recopilados; (v) permitir a los empleados o sus familiares ejercer los derechos de actualización, acceso, rectificación, supresión, bloqueo y oposición; (vi) garantizar la seguridad y confidencialidad de la información (Zubiaté, 2011).

Sin perjuicio de lo anterior, el empleado también debe estar sujeto a cumplir con los deberes que se derivan de la referida normativa, ya que en el desempeño de sus funciones, éste puede realizar el tratamiento de DP. Así, el Art. 17 de la LPDP establece que quien tenga una intervención en el tratamiento de los DP, debe tener el deber de confidencialidad y secreto con relación a los DP que conozca, subsistiendo dicha obligación aún después de finalizada la relación laboral que se tenga con el titular del banco de DP (como es el caso de las empresas).

Por ello, se pone de manifiesto la relevancia del *''compliance''* laboral como una herramienta para las empresas capaz de tratar la normativa laboral, siendo un sistema no solo de gestión del funcionamiento de las empresas y el cumplimiento de la legislación laboral, sino también de creación de una nueva cultura empresarial (Rojas, 2017, p. 24-27).

En este sentido, la importancia de implementar –por parte de las empresas- programas de cumplimiento normativo laboral radica en el hecho de que no solo se minimicen los posibles riesgos legales; sino también, garanticen los correctos niveles de protección,

prevención y gestión de contingencias laborales, específicamente los relacionados a los DP de los trabajadores, clientes y otras partes interesadas.

De acuerdo a Sánchez, el diseño de un programa de cumplimiento normativo laboral debe estar encaminado a: (2017, p. 1)

- **Concientizar a la empresa sobre el hecho de la importancia de disponer de un programa de cumplimiento normativo laboral.** Esto se basa en el hecho de que las empresas deben ser conscientes de los beneficios que se pueden derivar del referido programa. Es decir, el hecho de implementar un sistema de gestión laboral no solo servirá para eludir sanciones administrativas; sino también, para crear una verdadera cultura de cumplimiento.

- **Realizar una identificación y evaluación de los posibles riesgos laborales que puede poseer la empresa a nivel de no cumplimiento.** Este es el punto de inicio a la acción preventiva de toda empresa. Según Sánchez, esto se podría lograr –por ejemplo-con la evaluación del Convenio Colectivo.

- **Brindar un adecuado tratamiento de los riesgos.** Se debe hacer hincapié en que no todos los riesgos son iguales. En el caso de que existan riesgos más considerables, se debe hacer un tratamiento a través de mecanismos de prevención, con el fin de evitar que se produzcan en un futuro.

- **Identificar otros posibles riesgos laborales.** Es decir, junto con las obligaciones de toda empresa (jornada laboral, remuneración, etc.); existen otros aspectos relacionados con la tecnología. Es decir, las empresas se encuentran obligadas a entender, por ejemplo, el hecho de carecer de una política de control de las cuentas electrónicas de los empleados.

- **Gestionar los riesgos que se hayan detectado.** Con todos los pasos anteriores, la empresa debe contar con un código de conducta, o también llamado código ético. Estos instrumentos son claves y necesarios en los programas de cumplimiento. Además, surgen como producto de un proceso de autorregulación voluntaria de las propias empresas y establecen un conjunto de criterios y valores de conducta dirigidos a los directivos, empleados y otras partes interesadas, como es el caso de los clientes y proveedores (Crespo, 2016, p. 37).

- **Informar a los empleados sobre lo que se está haciendo.** La empresa debe de informar a su personal sobre las políticas, herramientas y mecanismos que se van a utilizar en el manejo de PDP. Es indudable que esta comunicación conllevará a que los mismos empleados colaboren con el diseño de dichas políticas.

- **No vulnerar ningún derecho fundamental debido a la aprobación de la normativa de la empresa.** La empresa debe estar clara que el hecho de aprobar alguna normativa interna no debe de vulnerar los derechos fundamentales, como el de la intimidad. Según Sánchez, definir una política religiosa no es tarea fácil, ya que con ello se pueden atropellar las creencias religiosas de algunos trabajadores.

- **Poseer un responsable de cumplimiento multidisciplinar.** En palabras de Sánchez, contar con expertos que dominen materias específicas (laboral, medioambiental, etc.), representa una pauta importante, sobre todo, para las grandes empresas.

- **Dotar de canales de denuncia como mecanismo de control de la empresa.** Con el fin de darle eficacia a los programas de cumplimiento, es clave que las empresas cuenten con canales de denuncia que permitan a los directivos, trabajadores y terceros ajenos, denunciar hechos que puedan ser contrarios a la ley y a los principios éticos y de comportamiento que se estipulen en el código de conducta de cada empresa.

- **Establecer un régimen disciplinario para refrenar conductas delictivas.** La empresa debe clarificar a sus empleados sobre las consecuencias que podrían derivarse de algún incumplimiento con relación a la normativa en PDP.

En adición a ello, podemos agregar que un mecanismo que las empresas deben de implementar para llevar a cabo una correcta gestión y tratamiento de los DP son las medidas de seguridad en los bancos de DP. La propia normativa aplicable en esta materia (Art. 17 LPDP) dispone que para los fines de tratamiento, le corresponde al titular del banco de DP implementar las medidas organizativas, técnicas y jurídicas para preservar la confidencialidad y evitar cualquier tratamiento o acceso no autorizado, pérdida u alteración.

Cabe resaltar que las medidas que se adopten en cada organización, van a depender del tamaño y tipo de empresa y de las características de la información[15].

De acuerdo a la Directiva de Seguridad de la APDP, las medidas organizativas que podría adoptar una empresa consisten en: (i) desarrollar una estructura organizacional con roles y responsabilidades de acuerdo a la proporcionalidad de los datos a proteger, (ii) documentar los compromisos respeto a los principios de la norma, (iii) dar un seguimiento de control y registro de los operadores de acceso al banco de DP, con el fin de poder identificar al personal con acceso en determinado momento, (iv) realizar una revisión periódica sobre la efectividad de las medidas de seguridad adoptadas y registrar dicha verificación al banco de DP, (v) desarrollar un programa de creación de conciencia y entrenamiento en materia de PDP, por mencionar algunas (Minjus, 2013, p. 21).

Asimismo, según los lineamientos consignados en la referida Directiva, las medidas técnicas que podría adoptar una empresa consisten en: (i) gestionar y usar las contraseñas cuando el tratamiento se realice a través de medios informáticos, como por ejemplo, solicitar a los usuarios que mantengan sus contraseñas en secreto o que el servidor de autenticación almacene las contraseñas de manera cifrada, (ii) revisar y registrar- al menos semestralmente, los privilegios de acceso a los DP, los cuales deben de corresponder al personal autorizado, (iii) proteger el banco de DP contra acceso físico no autorizado mediante algún mecanismo de bloqueo, (iv) el titular del banco de DP (o quien éste designe) debe permitir o no el acceso de usuarios que realicen tratamiento de DP, lo cual debe estar registrado, entre otras (Minjus, 2013, p. 22-26).

En esta misma línea, las medidas legales que establece la Directiva de Seguridad de la APDP están basadas en: (i) mantener los formatos de consentimiento para el tratamiento de DP, adecuados y conforme al fin para la cual son acopiados, (ii) adecuar los contratos del personal y de terceros, manteniendo actualizado un documento de

[15] De acuerdo a los lineamientos de la Directiva de Seguridad de la APDP, existe una clasificación de categorías en el tratamiento de DP, a saber: **1.- Básico:** En esta categoría los bancos de DP no deben de contener información de más de 50 personas, no incluyen datos sensibles y su titular es una persona natural; **2.- Simple:** En esta categoría los bancos de DP no deben de contener información de más de 100 personas, no incluyen datos sensibles y tienen como titular a una persona natural o jurídica; **3.- Intermedio:** En esta categoría los bancos de DP deben de contener la información de hasta 1000 personas, pueden incluir datos sensibles y tiene como titular a una persona natural o jurídica; **4.- Complejo:** En esta categoría los bancos de DP pueden incluir datos sensibles y tiene como titular a una persona jurídica o entidad pública; **5.- Crítico:** En esta categoría los bancos de DP sirven para el tratamiento de DP cuya finalidad tiene el soporte de una norma, pueden incluir datos sensibles y tiene como titular a una persona jurídica o entidad pública.

compromiso de confidencialidad con relación al tratamiento de los DP (Minjus, 2013, p. 22).

En adición a todas las medidas de seguridad antes indicadas, debemos hacer énfasis a lo referido por Pañella con relación a cómo lograr una correcta aplicación de un programa de cumplimiento normativo laboral: esto se alcanzará sólo en el momento en que dicha herramienta haya contado con la complicidad de todos los actores de la organización, siendo éste el momento cúspide en donde se habrá alcanzado un sistema integral que creará una nueva cultura empresarial basada en el cumplimiento normativo, la igualdad y el bienestar laboral (2018).

Asimismo, resulta importante reiterar que nuestra investigación se centra en analizar aquellas relaciones laborales cuyos agentes puedan tener una intervención y responsabilidad frente al tratamiento y manejo de los datos personales dentro del marco laboral, a saber:

(i) En primer lugar, se encuentran las relaciones entre el empleador y el empleado, que pueden ir desde el momento de seleccionar al personal hasta el inicio del contrato y el desarrollo de la prestación de trabajo. En estas relaciones se puede recoger gran información de los empleados que puede afectar a su esfera personal y profesional. Por ello, es una responsabilidad de las empresas salvaguardar los datos de índole personal de sus empleados.

(ii) En segundo lugar, se encuentran las relaciones entre los empleados y/o el empleado con el tercero vinculado a la empresa, como es el caso del cliente. Es indudable que el trabajador puede también intervenir en el tratamiento de los DP, y a pesar de ser la empresa quien responda frente a las acciones del trabajador con relación a la violación de alguna obligación en esta materia, puede el empleador imponer alguna sanción de índole laboral u optar por el término del contrato de trabajo de acreditarse el incumplimiento. Por ello, es responsabilidad de las empresas clarificar a sus empleados sobre las políticas y deberes en materia de PDP, con el fin de evitar algún incumplimiento.

Bajo esta óptica, procederemos a analizar cada caso abordado en el capítulo 3 de nuestro trabajo de investigación, y según corresponda, enmarcarlos dentro de la división de relación laboral expuesta en el párrafo anterior. De igual forma, se buscará proponer diferentes mecanismos de cumplimiento normativo laboral en materia de PDP para cada

caso en particular, con el fin de minimizar, prevenir y evitar los riesgos legales, y fomentar así, las buenas prácticas empresariales.

4.1 Propuestas

El primer caso abordado en el capítulo 3 está relacionado con la Asociación Pastoral de Servicios Médicos Good Hope de la Iglesia Adventista del Sétimo Día. El referido caso se fundamentó en el incumplimiento por parte de la referida Asociación con la normativa de PDP por contravenir con el artículo 7 de la LPDP (Principio de proporcionalidad) al requerirles, tanto a los nuevos postulantes como a sus colaboradores, declarar su religión y el hecho de si habían recibido el sacramento del bautizo, realizándose así un tratamiento desproporcional de su información personal (considerados como datos sensibles), estando enmarcado dentro de la relación laboral empleador-empleado, teniendo el primero responsabilidad en materia de PDP frente al segundo.

Sin embargo, para la Iglesia Adventista era necesario contar con la información relacionada al perfil profesional y espiritual de los trabajadores, ya que la finalidad de la institución era brindar asistencia social pastoral médica con el fin de contribuir con el desarrollo del ser humano basado en principios y fines espirituales de la Iglesia Adventista del Séptimo Día, resultando relevante para la institución religiosa conocer este tipo de información.

No obstante, podemos afirmar que en este caso en concreto existe un incumplimiento con el marco regulatorio de PDP y con ciertos estándares establecidos en la misma norma, como es el caso de los principios de proporcionalidad y finalidad. Ante este panorama, resulta sumamente necesario que lo antes referido se vea mitigado con el establecimiento de un sistema de cumplimiento normativo laboral, y de esta forma se vea minimizado el riesgo derivado del incumplimiento de la normativa de PDP, en este caso específico, con el artículo 7 de la LPDP, el cual afirma que todo tratamiento de DP debe ser relevante, adecuado y no debe extra limitarse a la finalidad con la cual han sido recopilados.

Por ello, con el fin de evitar estas infracciones a la normativa de PDP y de fomentar las buenas prácticas empresariales, podemos establecer algunas propuestas que son relevantes para la gestión, minimización y prevención de riesgos, resultando útiles para futuros casos:

Primero: El programa de cumplimiento normativo laboral debería estar direccionado en que la Institución tenga en claro que antes o durante la relación laboral, ésta no puede establecer que para tener acceso a un puesto de trabajo o desarrollar una actividad

laboral, resulte necesario tener un determinado credo religioso, siendo la única excepción a esta regla que los estatutos o normas internas de la empresa estipulen que ésta tenga una determinada ideología o tendencia religiosa.

De acuerdo a lo mencionado en el párrafo anterior, debemos resaltar que la referida excepción está contenida en el tercer párrafo del artículo 3 del Reglamento de la Ley de la Libertad Religiosa aprobado mediante DS No. 010-2011-JUS. Así pues, este párrafo establece que el acceso al empleo no puede ser restringido por motivos religiosos, excepto que la entidad (al ser parte de una entidad religiosa), haya dispuesto previamente en sus estatutos que su ámbito de actuación está designado solo a aquellos que sean parte de dicha entidad o se hayan comprometido a respetar los principios que ésta posee.

En el caso de la Iglesia Adventista, no se especificaba nada en su partida electrónica, es decir, no se indicó en ésta que los fines de atención de los servicios de salud estén referidos exclusivamente a las personas que pertenezcan a dicha entidad (que compartan la misma religión), sino que hace referencia a la prestación de los servicios de salud a toda la comunidad en general (DGPDP, 2016, p.7).

En adición, la Iglesia Adventista realizó un tratamiento no proporcional de la información relacionada a la religión de los postulantes a los puestos de trabajo y los postulantes, ya que se hizo una recopilación de los datos sensibles que son excesivos a la finalidad de cumplir con la gestión de RRHH, es decir, acceder al empleo o desarrollar propiamente las actividades derivadas de la relación laboral (DGPDP, 2016, p.7).

Segundo: El programa de cumplimiento normativo laboral debería estar encaminado a no vulnerar ningún derecho fundamental debido a la aprobación de alguna decisión interna de la empresa.

En este caso en concreto, es preciso señalar que el poder de dirección propio del empleador tiene ciertos límites, como es el caso de los derechos fundamentales del empleador (Sánchez, 2017, p.1). Es claro que antes o durante la relación laboral, la empresa no puede establecer que para tener acceso a un puesto de trabajo o desarrollar una actividad laboral, resulte necesario tener un determinado credo religioso, ya que se estaría vulnerando con el derecho a la libertad religiosa, salvo de que en los estatutos o normas internas de la empresa se estipule que ésta tenga una determinada ideología o tendencia religiosa (Ulloa, 2002, p. 543-544).

Tercero: El programa de cumplimiento normativo laboral que se incorpore debería de observar la normativa en materia de PDP y su reglamento. En adición, en este caso en

concreto se debe observar la Ley 29635 y su reglamento que brinda protección al ejercicio de la libertad religiosa.

Así pues, además del artículo 7 de la LPDP, es preciso hacer mención a algunos artículos relacionados con el caso. En este primer ejemplo, se estableció que la información referida al bautizo o religión es calificada como datos sensibles que requieren un consentimiento por escrito, y en su defecto, pueda efectuarse cuando una ley así lo autorice. Por ello, debe de cumplirse cabalmente con el artículo 13 numeral 1, el cual dispone que el tratamiento de DP debe realizarse con pleno respeto de los derechos fundamentales de sus titulares y de los derechos que la legislación de PDP ampara. Además, el artículo 13 numeral 5, establece que los DP solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto. El consentimiento debe ser previo, informado, expreso e inequívoco. Por su parte el artículo 13 numeral 6 dispone que en el caso de datos sensibles, el consentimiento para efectos de su tratamiento, además, debe efectuarse por escrito. Aun cuando no mediara el consentimiento del titular, el tratamiento de datos sensibles puede efectuarse cuando la ley lo autorice, siempre que ello atienda a motivos importantes de interés público.

Cuarto: El programa de cumplimiento normativo laboral debería de considerar pertinente que se incorporen políticas relacionadas a la protección de datos personales, específicamente, las relacionadas a brindar protección a los datos sensibles de sus colaboradores- como es el caso del credo religioso- con el fin de tratar dicha información de manera lícita, adecuada y transparente.

Quinto: El programa de cumplimiento normativo laboral debería de incorporar medidas de seguridad, específicamente legales, de cara al titular del banco de datos (en este caso, la Institución Adventista). Como una medida legal podría adoptarse el mantener los formatos de consentimiento para el tratamiento de DP, adecuados y conformes al fin para lo cual son copiados, tal y como lo establece la Directiva de Seguridad del MINJUS. Por ejemplo, en el caso de la Institución Adventista debería de constar por escrito el consentimiento del titular de DP (postulante o colaborador) con relación a informar sobre su credo religioso, siempre y cuando en el estatuto de la empresa se establezca que la misma posee una determinada ideología o tendencia religiosa. Solo en este caso el titular del banco de datos (Institución Adventista) estaría en la obligación de incorporar como medida legal el mantener los formatos de consentimiento adecuado y conformes al fin para los cuales son copiados.

Por otro lado, otro caso nacional abordado en el capítulo 3, lo constituye la empresa Supermercados Peruanos S.A (2016), el cual se encuadra dentro de la relación laboral

empleado-cliente (teniendo el primer agente responsabilidad frente al segundo), en donde también podemos encontrar un deficiente cumplimiento de la normativa de PDP. Este caso se fundamentó en varias infracciones: (i) recopilación de datos de sus diferentes clientes por el área de marketing con el fin de mejorar sus ventas, sin existir un previo consentimiento ni información sobre los destinatarios de su tratamiento (ii) ausencia de la adopción-por por parte del titular del banco de datos (Supermercados Peruanos S.A.)- de medidas de seguridad con el fin de garantizar la seguridad de los datos y evitar futuras pérdidas y alteraciones, (iii) transferencia de los DP de sus clientes fuera del territorio peruano, no siendo comunicado a la APDP ni informado a los clientes sobre sus destinatarios.

En este sentido, podemos afirmar que en este caso en concreto existen ciertas infracciones contrarias a lo establecido por la LPDP y a ciertos estándares establecidos en la misma norma, como es el caso del principio de consentimiento, el principio de seguridad y el principio de nivel de protección adecuado. Ante este panorama, resulta necesario que lo antes referido se vea mitigado con el establecimiento de un sistema de cumplimiento normativo laboral, el cual debe estar direccionado a minimizar o evitar los riesgos que se deriven del incumplimiento de la LPDP.

Por ello, con el fin de evitar estas infracciones a la normativa de PDP y de fomentar las buenas prácticas empresariales, podemos establecer algunas propuestas que son relevantes para este caso en concreto, a saber:

Primero: El programa de cumplimiento que se incorpore debe de observar la normativa en materia de PDP y su reglamento. Así pues, de acuerdo a cada infracción cometida en el presente caso, la empresa debió:

(i) Tratar los DP de sus clientes con el previo consentimiento de los mismos, además, dicho consentimiento debe ser informado, expreso e inequívoco (Artículo 13.5 LPDP y Artículos 11 y 12 del Reglamento).

(ii) Garantizar el derecho de los titulares de DP (clientes) de ser informados en forma detallada, sencilla y previamente a la recopilación de los DP, sobre la finalidad para la cual su información será tratada; así como quienes son o serán sus posibles destinatarios (Artículo 18 LPDP).

(iii) Adoptar las medidas de seguridad (técnica, organizativa y/o legal) que garanticen la seguridad de la información y eviten su alteración, pérdida o tratamiento no autorizado (Artículo 16 LPDP).

(iv) Realizar el flujo transfronterizo de DP de sus clientes solo si el país destinatario mantiene los mismos niveles de protección que establece la

LPDP. Ahora bien, en caso de que dicho país no cuente con el mismo nivel de protección, el emisor debe garantizar que el flujo de DP se efectúe de acuerdo a la normativa vigente en PDP (Artículo 15 LPDP).

Segundo: El programa de cumplimiento normativo laboral debería de gestionar los riesgos que se hayan detectado (Sánchez, 2017, p. 1), en este caso en concreto, los riesgos legales al incumplirse con la normativa en materia de PDP. De esta forma, la empresa puede adoptar un instrumento clave para su referido programa de cumplimiento, como es el caso del código de conducta. Según lo mencionado por Crespo, la adopción de dicho instrumento resulta del proceso de autorregulación voluntaria de las propias empresas y establecen un conjunto de criterios y valores de conducta dirigidos a los directivos, empleados y otras partes interesadas, como es el caso de los clientes y proveedores (2016, p. 37).

En el caso de Supermercados Peruanos, la empresa ya cuenta con un código de conducta, el cual se encuentra vigente desde el año 2014. Sin embargo, el referido instrumento presenta una falencia en PDP, ya que no incluye ningún apartado en esta específica materia. Por ello, sería importante que las empresas que vayan a adoptar este instrumento, incorporen un apartado en materia de PDP, y en adición, que se establezca la obligación de llevar un monitoreo de cumplimiento de dicho código ético.

Tercero: El programa de cumplimiento normativo laboral debería de establecer un régimen disciplinario para refrenar conductas (Sánchez, 2017, p.1) contrarias a la PDP. Dicho régimen disciplinario podría estar establecido en el Reglamento Interno de la empresa, siendo importante que en éste se establezcan las faltas y las sanciones disciplinarias de cada una, tales como la amonestación verbal, amonestación escrita o la suspensión, las cuales serán impuestas siguiendo diferentes criterios, tal como la gravedad de la falta.

Cuarto: El programa de cumplimiento normativo laboral debería de brindar capacitación a sus empleados en materia de PDP. Sin duda, esto podría ser una forma para que las empresas clarifiquen a sus empleados sobre las consecuencias que podrían derivarse de algún incumplimiento con relación a la normativa en PDP.

Sobre este punto, podemos mencionar que Supermercados Peruanos S.A. hubiera evitado la comisión de las infracciones cometidas por los empleados del área de marketing si hubiesen recibido una adecuada capacitación en materia de PDP, específicamente, cumplir con: (i) tratar los DP de sus clientes con el previo consentimiento de los mismos y (ii) garantizar el derecho de los titulares de DP (clientes) de ser informados en forma detallada, sencilla y previamente a la recopilación de los

DP, sobre la finalidad para la cual su información será tratada; así como quienes son o serán sus posibles destinatarios.

Quinto: El programa de cumplimiento normativo laboral debería de incorporar medidas de seguridad, de cara al titular del banco de datos (en este caso, Supermercados Peruanos S.A.). Por ejemplo, de acuerdo a la Directiva de Seguridad del MINJUS, como medidas organizativas, la empresa podría optar por desarrollar un programa de creación de conciencia y entrenamiento en materia de PDP; así como, desarrollar y mantener un documento de compromiso de confidencialidad en el tratamiento de DP-aplicable a los empleados relacionados con el tratamiento de DP. En adición, como una medida específica, la empresa debería de cumplir con la seguridad en el flujo transfronterizo de DP.

Por otro lado, el caso español abordado en el capítulo precedente, lo constituye la empresa Cotronic S.A. vs. un ex trabajador, estando enmarcado dentro de la relación laboral empleador-empleado teniendo el primero responsabilidad en materia de PDP frente al segundo. En este caso es posible observar de forma clara la falta de cumplimiento con la Ley Orgánica de PDP 15/1999[16] de España (vigente en ese entonces), específicamente con el artículo 11.

Este caso se fundamentó en la conducta lesiva de la referida empresa a los derechos fundamentales de su ex trabajador (imagen y honor) mediante la cesión de sus DP a la empresa Telefónica S.A., incidiendo de forma negativa en su reputación, ya que al incluir al ex trabajador en un fichero de ‘’trabajadores conflictivos’’, le impidió ser contratado por otras empresas del rubro de telecomunicaciones.

La referida normativa española establece que los DP sólo podrán ser comunicados a un tercero con el previo consentimiento del interesado, y en adición, el numeral 2 del artículo 11 establece que dicho consentimiento no será preciso en seis situaciones. Por ende, podemos afirmar que al tratarse de ficheros de DP y no teniendo el consentimiento del ex trabajador, al caso en concreto no le es aplicable ninguna de las excepciones que dispone el numeral 2 del artículo 11 de la normativa española, considerándose dicha cesión de DP como ilícita, vulnerándose así con el derecho fundamental de PDP.

No obstante, podemos afirmar que en este caso en concreto existe un incumplimiento con el marco regulatorio de PDP español y con ciertos estándares establecidos en la misma norma, como es el caso del principio de consentimiento. Por ello, con el fin de

[16] Esta normativa fue derogada por la Ley Orgánica 3/2018 del 5 de diciembre, PDP y garantía de los derechos digitales.

evitar estas infracciones a la normativa de PDP y de fomentar las buenas prácticas empresariales, podemos establecer algunas propuestas que son relevantes para este caso en concreto, a saber:

Primero: El programa de cumplimiento normativo laboral que se incorpore debería de observar la normativa en materia de PDP y su reglamento. En este caso en concreto, la inclusión de los DEP en un fichero debe requerir el consentimiento del interesado. Por ello, circunscribiéndonos a la norma peruana en materia de PDP, se debe observar el artículo 13 numeral 5 el cual establece que los DP solo pueden ser objeto de tratamiento cuando exista consentimiento de su titular, salvo que exista alguna ley que autorice lo contrario. Por su parte, el artículo 14 de la LPDP establece seis límites al consentimiento para el tratamiento de DP, es decir que solo en esos casos no se requeriría el consentimiento del titular de DP. Un ejemplo de ello es lo establecido en el numeral 5, el cual dispone que no se requerirá dicho consentimiento cuando los DP sean necesarios para la ejecución de una relación laboral.

Segundo: El programa de cumplimiento normativo laboral debe observar que exista un contrato de cesión -entre el cedente y cesionario-, y que además, medie el consentimiento del interesado (en este caso del empleado) a quien se le debe de informar de manera clara y precisa qué datos se van a recopilar, los detalles de su tratamiento, así como de su transferencia. En adición, la empresa debería mantener un registro de dicho consentimiento. Por ello, el no contar con el consentimiento del interesado, dicha cesión se consideraría ilícita.

Tercero: El programa de cumplimiento normativo laboral debe tener en cuenta que el consentimiento del interesado se puede revocar. Por ello, resulta importante que las empresas cuenten con mecanismos simples y eficaces para realizar dicha revocación.

Con todo lo expuesto anteriormente, podemos afirmar que con el planteamiento de la casuística peruana y extranjera en materia de PDP dentro del marco las relaciones laborales, se ha podido observar la posible ausencia de un programa de cumplimiento normativo laboral; así como la existencia de malas prácticas al incumplirse con la normativa vigente y aplicable en materia de PDP de cada país.

En este tenor, debemos reiterar que el reto que tienen las empresas es evitar que existan malas prácticas con relación al tratamiento de los DP en el marco de las relaciones laborales, resultando relevante que éstas cuenten con herramientas idóneas capaces no sólo de verificar el cumplimiento normativo; sino también de mitigar los riesgos y de implantar un código ético que trate esta área de incidencia laboral de PDP.

Por ello, es importante que las empresas incorporen los sistemas de gestión de cumplimiento normativo laboral, en donde la PDP sea un componente relevante en dicho sistema, y por ende, en la cultura de cumplimiento empresarial. De esta manera, el *compliance* laboral sería considerado como un cambio en la filosofía de toda empresa, primando el compromiso por parte de estas de cumplir con sus obligaciones y promover una cultura de cumplimiento normativo en esta materia, en donde la ética y la responsabilidad social empresarial sean los principales ejes rectores.

CONCLUSIONES

- El verdadero reto que enfrentan las empresas hoy en día es la nueva era vinculada con la Protección de los Datos Personales (PDP), lo cual representa un gran desafío dentro del marco de las relaciones laborales.

- Es importante resaltar que la PDP, a pesar de que surgió a partir del derecho a la privacidad y la vida íntima, hoy en día se le considera como un derecho independiente, consustancial a la nueva era del avance de las nuevas tecnologías que hacen cada vez más endeble las informaciones de las personas.

- El tema de la PDP –dentro del marco laboral- ha cobrado mucha relevancia en el área de cumplimiento normativo laboral, existiendo una estrecha relación entre ambas, ya que una las áreas de actuación que debe abarcar el *compliance* laboral es precisamente el de la PDP, en donde sus sistemas de gestión de cumplimiento sirvan no solo para prevenir y gestionar incumplimientos laborales; sino también, afianzar las buenas prácticas en el ámbito laboral.

- Los sistemas de *compliance* laboral son considerados como una herramienta esencial para prevenir y gestionar los incumplimientos laborales, en donde el logro de sus políticas se basará en el cambio de criterio de interiorizar y hacer propia la responsabilidad social corporativa y la cultura de cumplimiento ético en el comportamiento de todos los integrantes de las empresas.

- La normativa jurídica de PDP en el Perú (Ley No. 29733 y su reglamento) se convierte en el principal instrumento jurídico que toda empresa debe observar, conocer y cumplir. De igual forma, a lo largo de nuestra investigación, se hizo mención a la normativa española en materia de PDP, ya que la ley peruana en PDP está inspirada en el ordenamiento jurídico español y presenta varias similitudes.

- La problemática de nuestra investigación se traducía en la posibilidad de las empresas de incurrir en malas prácticas en materia de PDP en el ámbito de las relaciones laborales, motivado no solo por el incumplimiento de la normativa aplicable con relación a sus obligaciones-tanto de los empleadores y/o empleados en esta materia- sino también por las empresas no asumir un

compromiso voluntario relacionado a la autorregulación, a la efectiva gestión de riesgos y al cumplimiento normativo en esta específica incidencia laboral.

- A pesar de que los riesgos pueden asumir muchas formas, en la presente investigación nos centramos en abordar específicamente el riesgo legal, siendo importante su gestión bajo dos modelos que han sido de utilidad (ISO 31000, 2009 y COSO, 2004), los cuales deben ser analizados de acuerdo a su aplicación para una u otra empresa.

- Para comprender nuestra referida problemática se dispuso que se utilizó la metodología del método comparado, la cual pretendió cotejar la normativa y la jurisprudencia nacional e internacional en materia de PDP, significando un notorio avance en esta materia dentro del marco de la prestación laboral. Asimismo, la metodología de riesgos legales, la cual pretendió identificar el impacto que podría tener el no cumplir con la normativa de PDP en el marco de las relaciones de trabajo o con el hecho de no haber implementado un correcto sistema de detección, gestión y prevención de riesgos a tiempo.

- Con relación a lo anterior, se realizó el análisis de tres casos -dos nacionales y uno extranjero- resultando relevantes por estar enmarcados dentro de la materia de PDP –nacional e internacional- en el marco de las prestaciones laborales y porque han permitido una notoria identificación de las obligaciones que deberían haber cumplido los diferentes agentes con relación al tratamiento de datos dentro del ámbito laboral.

- Mediante el análisis de los referidos casos se puso observar la posible ausencia de un programa de cumplimiento normativo laboral; así como la existencia de malas prácticas al incumplirse con la normativa vigente y aplicable en materia de PDP de cada país.

- En el capítulo de discusión, resultó posible establecer variadas propuestas alternativas con el fin de mitigar o prevenir los riesgos que podrían acarrear perjuicios legales, económicos y reputacionales de cara a las empresas; y de esta manera, fomentar no solo las buenas prácticas empresariales, sino además, motivar a éstas a que asuman un compromiso voluntario relacionado a la efectiva gestión de los riesgos, la autorregulación y el cumplimiento normativo en materia de PDP.

- Por último, es importante que las empresas incorporen los sistemas de gestión de cumplimiento normativo laboral, en donde la PDP sea un componente relevante en dicho sistema, y por ende, en la cultura de cumplimiento empresarial. De esta manera, el *compliance* laboral sería considerado como un cambio en la filosofía de toda empresa, primando el compromiso por parte de estas de cumplir con sus obligaciones y promover una cultura de cumplimiento normativo en esta materia, en donde la ética y la responsabilidad social empresarial sean los principales ejes rectores.

REFERENCIAS BIBLIOGRÁFICAS

Bacialupo, S. (2016). Cultura de cumplimiento e integridad: elemento clave de la prevención de riesgos penales. *Revista Internacional Transparencia e Integridad,* 2, 4.

Baltar, P. & Cuenca, J. (2018, 12 de marzo). La compatibilidad del Derecho Laboral con el compliance. *El Economista*. Recuperado de: CXZhttps://www.eleconomista.es/legislacion/noticias/8997931/03/18/La-compAAAAatibilidad-del-Derecho-Laboral-con-el-compliance.html

Banks, E. (Ed). (2012). *The simple rules of risk: revisiting the art of financial risk management.* Inglaterra: Reino Unido: John Wiley & Sons Ltd.

Bru, E. (2007*).* La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad. *Revista de los Estudios de Derecho y Ciencia Política de la UOC*, 1 (5), 78-92.

Cámara Guatemalteca de la Construcción. (2018). Importancia de los programas de compliance en los negocios. *Revista Contrucción.* Recuperado de: http://revistaconstruccion.gt/sitio/2018/09/14/importancia-de-los-programas-de-compliance-en-los-negocios/

Clavijo, C. (2014). Criminal compliance en el derecho penal peruano. *Revista de Derecho PUCP,* 73, 625-647.

Congreso de la República del Perú. (21 de junio de 2011). Ley de Protección de Datos Personales. [Ley 29733]. Recuperado de: http://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

Crespo, S. (2016). Programas de cumplimiento normativo y aspectos laborales. *Observatorio de Recursos Humanos y RR.LL.,* 36-40. Recuperado de: https://factorhuma.org/attachments/article/12686/c477_programas_de_cumplimiento_normativo.pdf

Dirección General de Protección de Datos Personales. (19 de agosto de 2016). Resolución Directoral No. 065-2016-JUS/DGPDP. Recuperado de: https://www.minjus.gob.pe/wp-content/uploads/2017/02/RD-65.pdf

Eguiguren, F. (2015). El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú. *Themis- Revista de Derecho 67*, 131-140.

Espinoza, R. (2017). El compliance como herramienta de prevención frente a la criminalidad empresarial. Una mirada desde la criminología moderna. *En Repositorio de la USMP.* Recuperado de: http://www.repositorioacademico.usmp.edu.pe/bitstream/usmp/2806/1/espinoza_bar2

Fortuny, M. (2014, 15 de octubre). ¿Qué sabemos del origen del compliance penal, el concepto de moda? *Diario Jurídico*. Recuperado de: https://www.diariojuridico.com/que-sabemos-del-origen-del-compliance-penal-el-concepto-de-moda/

Gamarra, S. (2015, 8 de mayo). El precio de los datos personales: la regulación de la Ley 29733. *Ius et Veritas.* Recuperado de:

http://ius360.com/publico/constitucional/el-precio-de-los-datos-personales-la-regulacion-de-la-ley-29733/

Londoño, L. & Núñez, M. (2010). Desarrollo de la administración de riesgos. *Revista Universidad EAFIT,* 46 (158). Recuperado de: http://www.redalyc.org/pdf/215/21520993004.pdf

Mahler, T. (2009). Una definición de riesgo legal. *Revista Foro de Derecho Mercantil*, 1 (22), 79-113. Recuperado de: http://legal.legis.com.co/document/Index?obra=rmercantil&document=rmercantil_7680752a8010404ce0430a010151404c

Martínez, R. (2007). El derecho fundamental a la protección de datos: perspectivas. *Revista de los Estudios de Derecho y Ciencia Política de la UOC*, 1 (5), 47-61.

Mejía, R. (2006). *Administración de Riesgos. Un enfoque empresarial.* Medellín, Colombia: Fondo Editorial Universidad EAFIT.

Miscenic, E. & Raccah, A. (Ed.). (2016). *Legal Risks in EU Law. Interdisciplinary Studies of Legal Risk Management and Better Regulation in Europe.* Suiza: Springer International Publishing.

Ministerio de Justicia y Derechos Humanos. (2013). *El Derecho Fundamental a la Protección de Datos Personales* (Informe No. 1). Lima: MINJUS. Recuperado de: https://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-Derecho-Fundamentalok.pdf

Ministerio de Justicia y Derechos Humanos (2013). *Directiva de Seguridad: Autoridad Nacional de Protección de Datos Personales APDP.* Lima: MINJUS. Recuperado de: https://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-de-Directiva-de-Seguridad.pdf

Montenegro, J. (2016) *Gestión del riesgo legal laboral en micro y pequeñas empresas: un estudio colectivo de casos de la UEI* (Tesis de Magíster). Recuperada de: http://bdigital.unal.edu.co/57071/1/1030571366.2016.pdf

Montezuma, O. (2010). *La Ley peruana de protección de datos personales.* Recuperado de: www2.congreso.gob.pe/sicr/cendocbib/con2_uibd.nsf/…/La_Ley_Peruana.pdf

Organización Internacional del Trabajo. (1997). *Repertorio de recomendaciones prácticas para la protección de los datos personales de los trabajadores,* Ginebra: OIT. Recuperado de: http://www.ilo.org/wcmsp5/groups/public/@ed_protect/@protrav/@safework/documents/normativeinstrument/wcms_112625.pdf

Pañella, J. (2018). El compliance laboral, una herramienta capaz de crear una nueva cultura empresarial. *En Corresponsables*. Recuperado de: http://corresponsables.com/actualidad/compliance-laboral-nueva-cultura-empresarial

Remolina, R. (2012). Aproximación constitucional de la protección de datos personales en Latinoamérica. *Revista Internacional de Protección de Datos Personales,* (1), 4-13.

Rodotá, S. (2003). Democracia y protección de datos. *Cuadernos de Derecho Público núms. 19-20,* 17.

Rojas, R. (2016). Compliance Laboral ¿Es posible un cumplimiento normativo laboral ético y responsable?. *LeFevbre El Derecho,* 2-4. Recuperado de: https://ecija.com/wp-content/uploads/2017/07/ebook-compliance-laboral.pdf

Rojas, R. (2017). El compliance laboral: una nueva herramienta *para* el cumplimiento ético y responsable de las obligaciones socio-laborales. *European Compliance & News*, 24-27. Recuperado de: http://www.aeaecompliance.com/images/documentos/Raul1.pdf

Rojas, R., Moraleja, E. & Gutiérrez, R. (Ed.). (2017). *Claves prácticas Compliance Laboral.* Madrid, España: Francis Lefebvre.

Sánchez, L. (2017, 12 de julio). Pautas para crear un sistema de cumplimiento laboral que mejore las relaciones en la empresa. *Confilegal.* Recuperado de: https://confilegal.com/20170712-pautas-para-crear-un-sistema-de-cumplimiento-laboral-que-mejore-las-relaciones-en-la-empresa/

Santos, E.; López, I. & Tejedor, V. (Ed.). (2005). *Protección de datos personales: Manual práctico para las empresas*, Madrid: FC Editorial.

Solís, J. (2007). Compliance o cumplimiento normativo*. Revista Partida Doble*, 191, 76-83.

Tarantino, A. (2008). *Governance, risk and compliance handbook: technology, finance, environmental and international guindance and best practices*. Canadá: Hoboken John Wiley & Sons Ltd, 1-972.

Thomann, L. (Ed.). (2011). *Steps to compliance with International Labour Standards. The International Labour Organization (ILO) and the Abolition of Forced Labour.* Bremen, Alemania: Dorothee Koch/ Anita Wilke

Toledo, M. (2010). La protección de datos personales y las relaciones laborales en España y Francia: Análisis de las recomendaciones de la Agencia Española de la Protección de Datos y La Commission Nationale de l'Informatique et des Libertés como ejercicio de derecho comparado previo a una traducción jurídica. *Revista Crítica de Historia de las Relaciones Laborales y de la Política Social*, 36-56.

Tribunal Constitucional del Perú. (22 de febrero de 2017) Expediente número 05532-2014-PA/TC. Caso Laura Denisse Vizquerra Houghton vs. Cencosud Perú S.A. Recuperado de: https://tc.gob.pe/jurisprudencia/2018/05532-2014-AA.pdf

Tribunal Europeo de Derechos Humanos, Gran Sala. (12 de enero de 2016) Expediente número 61496/2008. Caso Burbulescu vs. Rumanía. Recuperado de: https://www.uria.com/documentos/publicaciones/5096/documento/foro02.pdf?id=6757

Tribunal Supremo Español, Sala de lo Civil. (12 de noviembre de 2015). Expediente número 609/2015. Caso Humberto vs Cotronic S.A. Recuperado de: http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=7527471&links=proteccion%20de%20datos&optimize=20151120&publicinterface=true

Ulloa, D. (2012). Aspectos laborales en la ley de libertad religiosa y su reglamento. *Revista de la Facultad de Derecho*, 1 (68), 543-544.

Weinstein, S. & Wild, C. (Ed.). (2013). *Legal Risk Management, Governance and Compliance: A Guide to Best Practice from Leading Experts.* Reino Unido, Londres: Globe Law and Business.

Whalley, M. & Guzelian, C. (Ed.). (2017). *The legal risk management handbook: an international guide to protect your business for legal loss.* Londres, Gran Bretaña: British Library.

Zegarra, Diego. (2011, 4 de agosto). La Ley de Protección de Datos Personales, Ley 29733. *Enfoque Derecho.* Recuperado de: https://www.enfoquederecho.com/2011/08/04/la-ley-de-proteccion-de-datos-personales-ley-2973/

Zubiate, C. (2011). La protección de los datos personales de los trabajadores. *Info Capital Humano.* Recuperado de: http://www.infocapitalhumano.pe/recursos-humanos/alerta-legal/la-proteccion-de-los-datos-personales-de-los-trabajadores/

Zurita, M. (2015). *Riesgo Legal en las Relaciones de la Empresa* (Tesis de Maestría). Recuperado de: http://repositorio.usfq.edu.ec/bitstream/23000/5271/1/122911.pdf