PONTIFICIA UNIVERSIDAD
CATÓLICA DEL PERÚ

Escuela de Posgrado

El deber de diligencia digital de la administración de las sociedades, como parte de las normas de buen gobierno corporativo

Trabajo de Investigación para obtener el grado académico de Maestro en Derecho de la Empresa con mención en Gestión Empresarial
que presenta:

Gonzalo Gibaja Aucapuri

Asesor:
Edison Paul Tabra Ochoa

Lima, 2024

INFORME DE SIMILITUD

Yo, TABRA OCHOA, EDISON PAUL, docente de la Escuela de Posgrado de la Pontificia Universidad Católica del Perú, asesor(a) de la tesis/el trabajo de investigación titulado EL DEBER DE DILIGENCIA DIGITAL DE LA ADMINISTRACIÓN DE LAS SOCIEDADES, COMO PARTE DE LAS NORMAS DE BUEN GOBIERNO CORPORATIVO del/de la autor(a) GIBAJA AUCAPURI, GONZALO, dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 16%. Así lo consigna el reporte de similitud emitido por el software Turnitin el 28/06/2024.
- He revisado con detalle dicho reporte y la Tesis o Trabajo de Suficiencia Profesional, y no se advierte indicios de plagio.
- Las citas a otros autores y sus respectivas referencias cumplen con las pautas académicas.

Lugar y fecha:

Lima, 03 de julio de 2024

<table>
<tr><td colspan="2">Apellidos y nombres del asesor / de la asesora:
TABRA OCHOA, EDISON PAUL</td></tr>
<tr><td>DNI: 20112143</td><td rowspan="2">Firma:
  </td></tr>
<tr><td>ORCID: 0000-0002-6126-841X</td></tr>
</table>

RESUMEN

En la medida en que van surgiendo nuevas tecnologías que buscan soluciones eficientes para determinados procesos en las sociedades peruanas, surgen nuevos riesgos respecto de los cuales no se está prestando mucha atención: los riesgos digitales legales.

La prevención, mitigación y control de riesgos en una sociedad está a cargo de la administración de la misma. Los directorios y gerencias generales, según sea el caso, de las sociedades peruanas, en su rol de administradores, cuentan con un deber bastante relevante para la ejecución de sus funciones. Este deber se llama el deber de diligencia. El deber de diligencia de los administradores está relacionado a sus funciones de cuidado y supervisión de las actividades de una sociedad.

Sin embargo, tal como se encuentra regulado el deber de diligencia bajo las normas del gobierno corporativo, no atacaría directamente el problema planteado respecto de los riesgos digitales legales.

En ese sentido, el presente trabajo de investigación busca resolver dicho problema desde una perspectiva teórico y práctica: adecuar el deber de diligencia de los administradores de la sociedad a un deber de diligencia digital, como una submateria que considere, en particular, los riesgos digitales legales que surgen en la medida que van implementándose nuevas soluciones tecnológicas.

Una adecuada ejecución del deber de diligencia digital por parte de la administración de una empresa, implementado a través de una política interna de uso de nuevas tecnologías y un adecuado sistema de prevención de riesgos en una sociedad, que implemente controles eficientes para prevenir y mitigar riesgos digitales legales, servirá de herramienta eficiente para la ejecución de las laborales de dicha administración.

PALABRAS CLAVE: Derecho empresarial – Soluciones Digitales – Deber de Diligencia – Deber de Diligencia Digital - Buen Gobierno Corporativo.

ÍNDICE

INTRODUCCIÓN

Producto del mercado competitivo en el que se desarrollan las empresas, es que las mismas se encuentran en la necesidad constante buscar eficiencia empresarial. Esto hace que una empresa, para poder brindar productos o servicios competitivos, debe adecuarse a las innovaciones o tendencias propias del sector en el que opera. Si bien las innovaciones podrían ser de cualquier naturaleza, en estos últimos años, las innovaciones tecnológicas han cobrado bastante relevancia.

Sin duda alguna, el confinamiento generado por la pandemia que hemos vivido recientemente, ha generado la necesidad de digitalizar los procesos internos y externos de las empresas. No solo las empresas tuvieron que adoptar políticas de trabajo remoto, sino que tuvieron que adaptarse, en muchos casos, a relaciones digitales con sus propios clientes.

Así, las innovaciones digitales surgieron como solución ante el problema de la presencialidad. Muchos de las empresas optaron por softwares o productos digitales que le permitieron no solo adaptarse al contexto no presencial, sino que les permitían optimizar sus procesos internos.

En este contexto, en la medida en que dichas innovaciones tecnológicas brindaban soluciones eficientes a las empresas, se iban generando nuevos tipos de riesgos que no eran conocidos para las empresas: los riesgos digitales con repercusión legal (en adelante los "Riesgos Digitales Legales").

Estos Riesgos Digitales Legales nuevos para cualquier empresa, al igual que las innovaciones digitales, van cobrando relevancia en el mundo legal actual, ya que representan en muchos casos riesgos bastante elevados que incluso podrían significar que los accionistas decidan disolver una empresa.

Este nuevo tipo de riesgos, debe estar considerado como parte de los riegos inherentes de la actividad de una empresa, por lo que surge la duda de cómo es que se deberían afrontar. Sobre ello, consideramos que la propia empresa debería estar en la capacidad de identificarlos,

prevenirlos y/o mitigarlos, como un mecanismo de autorregulación, antes que salir a buscar respuestas de índole normativo.

En este orden de ideas, el concepto de deber de diligencia de los administradores de la sociedad, cobra mayor relevancia frente a dichos nuevos riesgos. Dicho deber de diligencia, como concepto propio de las normas de buen gobierno corporativo, son definidas, según señala Paz-Ares, como el "deber de cuidado", que les exige a los administradores de una sociedad que inviertan tiempo y dinero en la gestión o supervisión de la empresa a fin de maximizar la generación del valor (2003, p. 204).

Dicho esto, en base a este "deber de cuidado" de la administración de una empresa, es que los administradores deberán, sea de manera directa o a través de terceros especializados, tomar control sobre aquellos riesgos inherentes a la actividad de la empresa, más aún si la empresa está optando por adaptarse a un contexto cada día más tecnológico.

Abordado el problema que subyace a este trabajo de investigación, es que optamos por el siguiente tema de investigación: El deber de diligencia digital de la administración de las sociedades, como parte de las normas de buen gobierno corporativo. La principal pregunta que buscaremos responder en este trabajo de investigación es ¿Cómo adecuar el deber de diligencia de la administración de las sociedades al contexto digital actual?

Al respecto, tal como indicamos líneas arriba, consideramos que el sistema más adecuado como solución a la problemática planteada es el sistema de autogobierno de gobierno corporativo, y en particular respecto al deber de diligencia de la administración desarrollado en dicho sistema.

Cabe señalar que nos apoyaremos en preguntas específicas adicionales que nos ayudarán a abordar de mejor manera la pregunta principal. Las preguntas que hemos planteado como específicas son las siguientes: (i) ¿Cuáles son los riesgos asociados al uso de las nuevas tecnologías a los que están expuestas las sociedades y cuál debería ser el rol de la administración frente a ellos?, (ii) ¿Cuál es el fundamento, importancia y fuente normativa del deber de diligencia de la administración de las sociedades desde una perspectiva de gobierno corporativo?; y (iii) ¿Cuáles

son los beneficios de adecuar el deber de diligencia de la administración de una sociedad a los Riesgos Digitales Legales?.

Con el tema y problema planteando buscaremos sostener una hipótesis que brinde una solución no solo teórica sobre el problema, sino con un énfasis práctico relevante. El presente trabajo de investigación buscará desarrollar la siguiente hipótesis principal:

El deber de diligencia de la administración de las sociedades como concepto propio de las normas del gobierno corporativo, debe adecuarse al contexto digital actual y considerar los nuevos Riesgos Digitales Legales que surgen en la medida en que nuevas tecnologías se incluyen en la gobernabilidad y operatividad de los negocios de las sociedades. Para estos fines, éste deber debe contemplar los riesgos inherentes al uso de nuevas tecnologías, a fin de identificarlos, prevenirlos y/o mitigarlos.

Dicha hipótesis se apoyará en las siguientes sub – hipótesis:

(i) Los Riesgos Digitales Legales se dividen en riesgos operacionales, propios del giro de la empresa (externo), y de gobierno, inherentes a todas las empresas (interno). Los riesgos con mayor impacto/repercusión en las empresas son los siguientes: (i) operacionales: ciberataques y protección de datos personales de clientes que se encuentren en plataformas digitales; y (ii) de gobierno: suplantación de identidad en sesiones virtuales, y acceso al voto y participación digital restringido.

Ambos tipos de riesgos que hemos identificado repercuten de manera negativa, tanto para los intereses de los accionistas como para los de la empresa. El rol de la administración respecto a estos riesgos es de identificarlos, prevenirlos o buscar mitigarlos, en caso se hayan materializado.

(ii) El deber de diligencia como concepto de gobierno corporativo es sustancial para una adecuada prevención y mitigación de riesgos que buscan la protección de los intereses de la sociedad y terceros relacionados con la misma.

(iii) Adecuar el deber de diligencia a un deber de diligencia digital, no solo es beneficioso para los intereses de la sociedad, sino que es beneficioso para los intereses de los accionistas y terceros involucrados en las operaciones de la sociedad.

Como todo mecanismo de prevención, los beneficios de adecuar este deber a un deber digital están relacionados a la prevención de ocurrencia de dichos riesgos. Contar con un adecuado deber de diligencia digital podrá prevenir la ocurrencia de filtrado de información delicada de los clientes de una empresa, lo cual de ocurrir podría incurso significar el cierre de la empresa.

Una vez establecido claramente nuestro tema de investigación y la hipótesis central del mismo, conviene detallar los objetivos del presente trabajo de investigación. El principal objetivo de este trabajo será analizar cómo es que el deber de diligencia de la administración de las sociedades se debe adecuar al contexto digital actual.

Para poder cumplir a cabalidad con este objetivo principal necesitamos que se puedan conseguir objetivos específicos. Para estos efectos hemos delimitado los siguientes objetivos específicos:

(i) Identificar y desarrollar los riesgos asociados al uso de las nuevas tecnologías a los que están expuestas las sociedades y definir cuál debería ser el rol de la administración frente a estos.

(ii) Definir el fundamento, la importancia y fuente normativa del deber de diligencia de la administración de las sociedades desde una perspectiva de gobierno corporativo.

(iii) Identificar y desarrollar los beneficios de adecuar el deber de diligencia a los riesgos digitales en una sociedad.

Para sostener adecuadamente la hipótesis principal y abordar los objetivos antes planteados, es conveniente definir el enfoque metodológico principal que se utilizará en el presente trabajo de

investigación. Para estos efectos, y dada la naturaleza del trabajo de investigación proponemos utilizar un enfoque metodológico basado en la descripción de riesgos a través de casos, sean periodísticos o jurisprudenciales.

Este enfoque nos permitirá brindar mayor visibilidad sobre la problemática planteada, principalmente en relación con la magnitud de los Riesgos Digitales Legales a los que se enfrentan las sociedades en este contexto digital. Gran parte del trabajo busca identificar los riesgos a los que están expuestas las empresas en un contexto digital moderno, por lo que para lograr este fin debemos apoyarnos en casos ocurridos a nivel nacional como internacional.

Finalmente, es importante precisar que, de manera previa a la presentación de casuística para la identificación de los riesgos antes mencionados, se hará un estudio normativo previo para definir el contexto normativo actual del deber de diligencia de la administración como parte de las normas de buen gobierno corporativo.

CAPITULO 1

CONTEXTO DIGITAL MODERNO: NUEVAS SOLUCIONES TECNOLÓGICAS Y LOS RIESGOS LEGALES DIGITALES

Como ha sido antes mencionado, el problema del presente trabajo está vinculado al contexto digital en el que operan hoy en día las empresas, por lo que conviene que sentemos algunas ideas fuerza que nos permitirán entender de mejor manera el problema de la investigación.

En este capítulo desarrollaremos algunos conceptos clave que será utilizados a lo largo del presente trabajo. Entenderemos el contexto actual tecnológico empresarial y los riesgos legales asociados a dicho escenario.

1.1 Contexto digital empresarial.

La forma de hacer empresa hoy en día ha cambiado mucho debido a los avances tecnológicos que ofrece el mercado. Recordemos que la finalidad de toda empresa será la de generar valor. En este afán, las empresas buscan ser competitivas en el sector en el que operan; y en dicha búsqueda, cada una de ellas busca optimizar sus procesos internos y externos, ahora último a través de soluciones tecnológicas que ofrece el mercado.

En este contexto, es que se habla de una "transformación digital" como una nueva forma de administrar una empresa. Para entender mejor la figura, Vial se refiere a "Transformación Digital" (*Digital Transformation*) como un proceso que tiene por finalidad mejorar una sociedad (*entity*) a través de cambios significativos producto de la combinación de información, computación, comunicación y tecnologías de conectividad (2019, p. 118-119).

En la misma línea, Giraldo-Rios y otros señalan que "el mundo digital es un espacio en crecimiento que ofrece importantes oportunidades para la transformación de las organizaciones debido al alto potencial cibernético y la interconectividad existentes" (2021, p. 7).

Dicho esto, tenemos que, toda vez que las empresas están en la búsqueda de una transformación digital para mejorar sus procesos y hacerse competitivos en sus sectores económicos, buscarán tomar riesgos al implementar medidas o soluciones tecnológicas que los ayuden con este fin.

Si bien existen varias soluciones tecnológicas en el mercado, y existen varias específicas para cada sector empresarial, la gran mayoría de soluciones está relacionada con los siguientes conceptos:

(i) Aplicativos que permiten la firma electrónica certificada de documentos (ej. DocuSign[1], PandaDoc[2], entre otras).
(ii) Aplicativos que permiten la virtualidad de las sesiones de junta general de accionistas o directorio (ej. Espacios virtuales de las plataformas Zoom, Teams, Meet, o plataformas digitales propias como Enubes[3], entre otras),
(iii) Plataformas digitales que sirven de apoyo en la gestión masiva de clientes (*Customer Relationship Management)*,
(iv) Plataformas digitales que permiten y facilitan la gestión de contenido interno (*Enterprise Content Management*), sea de data interna (trabajadores) o externa (clientes, proveedores); y
(v) Sistemas digitales que permiten el análisis de datos de manera masiva (*Data Analytics*).

Asimismo, similares soluciones digitales encontramos en el sector legal. A continuación, describiremos algunas de las principales soluciones digitales que se utilizan en el ámbito legal:

(i) Aplicaciones de almacenamiento de documentos masivos (ej. Worldox[4], NetDocuments[5], entre otros)

[1] www.docusign.com
[2] www.pandadoc.com
[3] www.enubes.com
[4] https://www.worldox.com
[5] https://www.netdocuments.com/

(ii) Aplicativos que generan contratos de manera automática con algunos datos por completar (Webdox[6], Square[7], entre otros)

(iii) Programas que procesan contratos de manera masiva (Ebrevia[8], Kira[9], entre otros).

(iv) Espacios digitales que permiten el envío de documentos de manera masiva (Safedrop[10], OneDrive, WeTransfer[11], entre otros).

Ahora bien, es importante mencionar que, no todas las soluciones digitales antes descritas serán de uso y aplicación por parte de todas las empresas. Recordemos que para el uso de estas tecnologías, de deben asignar recursos y capacitaciones, por lo que nuestro espectro de estudio abarcaría a medianas y grandes empresas, o aquellas que, por el rubro en el que operan, puedan requerir de la inclusión de dichas soluciones digitales en sus operaciones (ej. Empresas de marketing digital, clínicas, mineras, bancos, entre otros).

Sin embargo, si bien existe una gran variedad de soluciones tecnológicas, éstas también traen consigo una gran variedad de riesgos; y muchos de esos riesgos al ser nuevos porque vienen con las novedades tecnológicas, no son visibles para la administración de una sociedad sino hasta cuando ocurren y generan una pérdida de valor para la misma.

1.2 Riesgos Digitales Legales.

Para entender el problema planteado, debemos aterrizar el concepto de "Riesgo Digital Legal" al que haremos referencia a lo largo del presente trabajo, y que viene asociado a lo indicado en la sección 1.1 anterior.

Para esto, debemos partir del concepto de "Riesgo", pero de un concepto alineado al contexto empresarial (económico-financiero). En esta línea, Soler y otros, refieren al "Riesgo" como la

[6] https://www.webdoxclm.com/
[7] https://squareup.com/
[8] https://ebrevia.com/
[9] https://kirasystems.com/
[10] https://safedrop.com/
[11] https://wetransfer.com/

posibilidad de sufrir un daño, pero un daño consistente en la pérdida de valor económico (1999, p. 4).

En un similar sentido, el literal ff) del artículo 2 del Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, aprobado por la Resolución SBS N° 272-2017 de fecha 18 de enero de 2017, define al "Riesgos" como "la posibilidad de ocurrencia de eventos que impacten negativamente en los objetivos de la empresa o su situación financiera".

De ambos conceptos, muy puntuales para la ilustración de nuestro punto de partida, podemos rescatar dos conclusiones: (i) el riesgo supone una probabilidad de ocurrencia de un determinado evento y (iii) que, producto de dicha ocurrencia o materialización, existe un impacto negativo o se genera una pérdida de valor en el objeto de estudio (la empresa).

Sobre el particular, debemos precisar que si bien existe este riesgo prácticamente en todas las operaciones que pueda realizar una empresa, como en la mayoría de casos, dichos riesgos son asumidos por parte de las empresas, ya que pueden dimensionar y mitigar el impacto de su ocurrencia.

Sin embargo, una empresa no podría tener la posibilidad de dimensionar, controlar o mitigar aquellos riesgos respecto de los cuales no tiene visibilidad, y una gran parte de esos riesgos son los riesgos digitales.

Este tipo de riesgos digitales, como su nombre indica, son aquellos inherentes a la actividad digital o a las soluciones tecnológicas aplicadas a una determinada entidad (empresa). Según Ganguly, "el riesgo digital es un aquel término que abarca todas las soluciones digitales que mejoran la eficacia y la eficiencia del riesgo, especialmente la automatización de procesos, la automatización de decisiones y el monitoreo digitalizado y la alerta temprana" (2017).

En esa línea, los riesgos digitales serán aquellos riesgos inherentes al uso de soluciones tecnológicas que buscan optimizar procesos internos y externos de una empresa. En tanto estas

soluciones buscan acelerar procesos dentro de una compañía (automatización de procesos o decisiones), pueden dejar de lado la salvaguarda de la información que manejan.

Los casos más ilustrativos sobre este tema son los vinculados a los *cibertaques*. A modo de ejemplo, recientemente ocurrió un ciberataque al hospital público "Clinic" en España. Un grupo denominado *RandomHouse* logró acceder al sistema del hospital público mencionado, y logró extraer datos personales de alrededor de 8,000 usuarios del hospital[12].

Este caso nos permite ejemplificar lo que significa en riesgo digital como tal. El hospital hizo uso de una solución tecnológica relacionada con el almacenamiento de datos masivos, y dicha solución tecnológica significó también para el hospital el riesgo de que terceros no autorizados puedan acceder a esa base de datos y la puedan filtrar de manera masiva en cualquier medio de comunicación (como lo es ahora el internet).

Ahora bien, como es inherente a todo tipo de riesgo empresarial, la consecuencia será siempre económica, en la medida en que dicha consecuencia significará una pérdida del valor económico para la empresa (Soler y otros, 1999, p. 4). Sin perjuicio de ello, si bien sea de manera directa o indirecta siempre el resultado de una materialización de un riesgo será económico, en muchos casos, la consecuencia directa de los mismos será legal.

Esto refleja lo que comúnmente denominamos como "Riesgo Legal", que de acuerdo con la definición planteada por el Estándar Internacional ISO 31022, son aquellos riesgos relacionados a aspectos legales (normativa), regulatorio y contractual, y a derechos y obligaciones no contractuales (2020, pp. 1).

En esa misma línea, Cedillo, Meneses y Raygada, señalan como "Riesgo Legal" a aquella posibilidad de pérdidas que se pueden generar en virtud de una resolución judicial, contratos defectuosos, procesos, tecnologías de la información y eventos externos sobre el sistema jurídico, entre otros (2010, p. 67). Complementando la idea de dichos autores, Quintás señala que dichos

[12] Disponible en. https://elpais.com/espana/catalunya/2023-03-30/los-ciberdelincuentes-filtran-de-madrugada-datos-robados-del-hospital-clinic.html

riesgos son tradicionalmente gestionados por los departamentos de asesoría jurídica de las empresas (2007, p. 7).

A nivel reglamentario en el Perú, el literal h) del artículo 2 del Reglamento para la Gestión del Riesgo Operacional, aprobado por Resolución SBS N° 2116-2009 de fecha 2 de abril de 2009, define como "Riesgo Legal" a la "posibilidad de ocurrencia de pérdidas financieras debido a la falla en la ejecución de contratos o acuerdos, al incumplimiento no intencional de las normas, así como a factores externos, tales como cambios regulatorios, procesos judiciales, entre otros".

Respecto de dichos conceptos, podemos concluir que el "Riesgo Legal" es un aquella probabilidad de ocurrencia de un evento cuyo impacto es negativo o perjudicial para una empresa, pero con la particularidad que su impacto tenga repercusión legal, lo cual podría verse materializado producto de un incumplimiento de normativa legal, contractual o por la ejecución de una sentencia desfavorable para la empresa.

En este orden de ideas, y teniendo en claro la definición de "Riesgo", "Riesgo Digital" y "Riesgo Legal", podemos llegar a la definición del "Riesgo Digital Legal" como aquella probabilidad de ocurrencia de un evento determinado que pueda producir efectos negativos o perjudiciales para una determinada persona o empresa ("Riesgo"), que está relacionado con el uso de soluciones tecnológicas ("Riesgo Digital"), y que cuya materialización tiene repercusión legal toda vez que podría llegar a generar un incumplimiento normativo o contractual ("Riesgo Legal").

Con la finalidad de ejemplificar nuestra definición antes descrita, en el caso del hospital antes mencionado (Clinic), podemos hablar de que estamos ante un Riesgo Digital Legal, toda vez que concurren todos los componentes de dicha definición: (i) evento que se materializó: la filtración de los datos personales de los usuarios del hospital, (ii) utilización de solución tecnológica: almacenar información sensible en un aplicativo de almacenamiento de información digital masiva, (iii) consecuencias económicas: pérdidas económicas que se generaron producto de las denuncias que recibió el hospital por la inadecuada seguridad sobre la información sensible de los usuarios que maneja el hospital; y (iv) repercusión legal: probablemente la resolución de las

denuncias o demandas presentadas frente el hospital, significarán no solo un incumplimiento en materia normativa, sino que también a nivel contractual con los pacientes.

1.3 Clasificación de Riesgos Digitales Legales.

Una vez definidos los Riesgos Digitales Legales, conviene clasificarlos a efectos de darles mayor visibilidad con respecto al problema planteando en el presente trabajo y poder luego referirnos a ellos cuando busquemos plantear una solución para los mismos.

Para efectos del presente trabajo, clasificaremos los Riesgos Digitales Legales en dos (2) tipos: (i) Riesgos Digitales Legales Internos y (ii) Riesgos Digitales Externos; ambos distinguidos respecto del usuario que pudiera verse afectado.

1.3.1 Riesgos Digitales Legales Internos (gobierno)

Esta clasificación de Riesgos Digitales Legales está relacionada con la posible afectación de intereses de internos de la empresa. Estamos hablando de los intereses de los accionistas y directores de la empresa, así como de los propios intereses de la empresa.

Dentro de los principales Riesgos Digitales Legales Internos (de gobierno) están los siguientes:

(i) <u>Suplantación de identidad en sesiones virtuales de accionistas y directores.</u>

Un primer Riesgo Digital Legal identificado es el que está relacionado con la virtualidad de las sesiones de junta de accionistas y/o directores de una empresa.

Si bien la virtualidad de las juntas de accionistas y/o directores buscaba darle una salida al contexto de confinamiento producido por la pandemia mundial, surgieron algunos problemas en su implementación.

En dicho contexto, Cebriá precisaba que los riesgos de la virtualidad de las sesiones de junta general de accionistas se encontraban directamente vinculados con (a) la asistencia, (b) participación y (c) voto (2022).

Efectivamente, uno de los riesgos más saltantes de esta virtualidad es la posibilidad de la ocurrencia de una suplantación de identidad de los accionistas o directores, que podría no solo afectar a datos sensibles propios de la empresa (información comercial sensible), sino que podría afectar a información personal propia de los accionistas o directores de la empresa.

(ii) Acceso restringido al voto y participación digital de accionistas y directores.

En la misma línea de Cebriá, otro riesgos identificado en relación con la virtualidad de las juntas, está relacionado al acceso restringido que puede significar la virtualidad de las juntas.

Si bien se presume que el acceso a internet globalmente, esto no significa que se pueda aprovechar de fallos de sistema para restringir el acceso al voto y participación de accionistas o directores de una empresa.

(iii) Vulneración de datos comerciales sensibles para la empresa.

Finalmente, existe un riesgo en la pérdida de datos comerciales sensibles para la empresa (secreto comercial), en la medida de que se utilicen plataformas digitales de gestión de contenido interno masivo (ej. Aplicaciones como SAP - *Systems, Applications, Products*[13]).

Usualmente toda la data interna de la empresa (información como precios, márgenes de venta, estrategias de venta, fórmulas, data sensible comercial en general), se encuentra almacenada en plataformas digitales de almacenamiento

[13] www.sap.com

masivo, las cuales se utilizan para la gestión y análisis de la información de una empresa.

Sin embargo, esta facilidad tecnológica trae consigo el riesgo de que terceros puedan romper la seguridad de dicha plataforma y acceder a la información ahí almacenada, generando un perjuicio económico abismal para la empresa.

Un ejemplo de la materialización de este riesgo, es el caso de la empresa Clorox[14]. En Agosto de 2023, la empresa Clorox, que se dedica a la fabricación y comercialización de productos de limpieza, se vio afectada por un ataque en sus sistemas de tecnología internos, que provocó una interrupción a gran escala de sus operaciones, obstaculizando su capacidad de fabricar sus principales productos (productos de limpieza), generándole millones de dólares en pérdidas.

1.3.2 Riesgos Digitales Legales Externos (Operacionales)

Esta clasificación de Riesgos Digitales Legales está relacionada con la afectación de intereses de terceros "ajenos" a la empresa, tales como clientes y/o proveedores de la misma, e incluso de los mismos trabajadores de la empresa.

Dentro de los principales Riesgos Digitales Legales Externos (operacionales) están los siguientes:

(i) Suplantación de identidad en la firma de contratos con clientes y/o proveedores.

Debido a la pandemia mundial, muchos países regularon la posibilidad de firmar contratos o documentos legales vinculantes de manera digital; servicio que es proporcionado por empresas que brindan plataformas digitales que certifican la firma de los participantes.

[14] Caso Clorox (2023). Disponible en: https://edition.cnn.com/2023/09/18/business/clorox-cyberattack-production-disruption/index.html

Sin embargo, existe el riesgo de que, ante un quiebre del sistema de dichas empresas, terceros puedan suplantar la identidad de representantes de una determinada empresa, y firmar contratos de mala fe con clientes o proveedores.

(ii) Vulneración de datos personales de clientes y/o proveedores y colaboradores de la empresa.

Al igual que el apartado 1.3.1 (iii), al almacenar todos los datos, en este caso de clientes, proveedores y/o trabajadores de la empresa, en una plataforma digital de almacenamiento masivo, o incluso en plataformas digitales que facilitan el envío de información a terceros, podría acarrear el riesgo de que dicha información sensible sea vulnerada.

Un claro ejemplo de la materialización de este riesgo es el caso del hospital Clinic en España que fue desarrollado anteriormente. Este riesgo podría implicar denuncias para la empresa que, según sea la magnitud de la vulneración, podría incluso quebrar a la empresa.

Otro ejemplo que ayuda a visualizar la importancia de dichos riesgos asociados a las nuevas tecnologías, es el caso de Meta[15] en 2023. En dicho año, Meta, empresa que opera la red social antes llamada como "Facebook", fue multada por la suma de 1.2 billones de euros, por transferir datos de sus usuarios desde la Unión Europea hacia Estados Unidos. En este caso, si bien la transferencia fue realizada por la misma empresa, los datos protegidos por norma europea fuero afectados, lo que generó efectos adversos no solo en la misma sociedad, sino en futuras reclamaciones que puedan hacer los usuarios.

(iii) Reclamos de clientes por canales no adecuados de atención al cliente.

[15] Caso Meta disponible en: https://www.nytimes.com/2023/05/22/business/meta-facebook-eu-privacy-fine.html

El uso de plataformas digitales que sirven de apoyo en la gestión masiva de clientes (*Customer Relationship Management*), si bien facilitan la gestión de atención al cliente en empresas con clientela masiva, no siempre significa que dicha plataforma sea adecuada en relación al tipo de servicio que brinda la empresa.

Ante este escenario, se pueden generar riesgos asociados a reclamos de clientes por una atención al cliente inadecuada, llevando reclamos ante autoridades que podrían sancionar económicamente a la empresa.

Tal es la posible materialización de este tipo de Riesgo Digital Legal que, en Octubre de 2022, se promulgó la Ley N° 31601 que modifica el Código de Protección y Defensa del Consumidor, a fin de garantizar que el usuario pueda tener atención personal por parte del proveedor en caso este utilice sistemas de atención automatizada.

Una vez definido el concepto de Riesgo Digital Legal y clasificado el mismo según los intereses que se puedan afectar con la ocurrencia del mismo, podemos entender la magnitud del problema materia de la presente investigación.

A manera de resumen, y a efectos de entender con claridad el problema objeto del presente trabajo, es importante mencionar los siguientes temas a los que hemos podido concluir:

(i) Nos encontramos ante un contexto de transformación digital empresarial, donde existen mayores oportunidades u opciones en el ámbito digital que permiten a las empresas adecuarse y volverse cada día más eficientes y competitivas en el mercado o sector donde operan.

(ii) Las diferentes soluciones digitales no solo traen consigo aspectos positivos para la empresa, sino que también representan nuevos riesgos para la misma, los que definimos como Riesgos Digitales Legales.

(iii) Cuando nos referimos a los Riesgos Digitales Legales, nos referimos la probabilidad de ocurrencia de un evento determinado que pueda producir efectos negativos o perjudiciales para una determinada persona o empresa, que está relacionado con el uso de soluciones tecnológicas, y que cuya materialización tiene repercusión legal toda vez que podría llegar a generar un incumplimiento normativo o contractual.

(iv) Para efectos del presente trabajo, hemos clasificado a los Riesgos Digitales Legales en Internos (de gobierno) y Externos (operacionales), lo cual dependerá de los intereses que se vean afectados con la materialización del Riesgo Digital Legal. Los principales riesgos que hemos podido identificar son los siguientes:

(a) Suplantación de identidad en sesiones virtuales de accionistas y directores (de gobierno).
(b) Acceso restringido al voto y participación digital de accionistas y directores (de gobierno).
(c) Vulneración de datos comerciales sensibles para la empresa (de gobierno).
(d) Suplantación de identidad en la firma de contratos con clientes y/o proveedores (operacional).
(e) Vulneración de datos personales de clientes y/o proveedores y colaboradores de la empresa (operacional).
(f) Reclamos de clientes por canales no adecuados de atención al cliente (operacional).

(v) Una vez definido el Riesgo Digital Legal y clasificado según los intereses que puedan verse afectados, podremos dimensionar dichos riesgos para poder implementar un plan adecuado de prevención y/o mitigación de dichos riesgos dentro de una empresa, como parte de la ejecución del deber de diligencia de los administradores de una sociedad.

CAPÍTULO 2

EL DEBER DE DILIGENCIA COMO PARTE DE LAS NORMAS DE GOBIERNO CORPORATIVO

Una vez explicado el contexto digital sobre el cual se desenvuelven las corporaciones y el concepto de Riesgo Digital Legal, resulta importante hacer una breve descripción de las normas de gobierno corporativo, incidir en su concepto y naturaleza, a fin de aterrizar en el concepto sobre el que planteamos conversar que es el concepto del deber de diligencia de los administradores en una sociedad mercantil.

Finalmente, haremos una precisión sobre la regulación de los planes de gestión de riesgos legales dentro de una corporación para poder hacer hincapié en cómo debería un sistema como tal, abordar los Riesgos Digitales Legales.

2.1 Las normas de gobierno corporativo.

Para entender mejor los conceptos que analizaremos en este capítulo, debemos revisar un concepto previo: conviene hacer una revisión de la definición, naturaleza e importancia de las normas de *soft law,* para luego revisar el concepto de gobierno corporativo, sus alcances y relevancia.

2.1.1 Un análisis previo: Las normas soft law

A diferencia de las normas de carácter obligatorio cuyo cumplimiento es exigido por el poder imperativo del Estado (*hard law*), las normas de *soft law* o conocidas también como *non-binding agreements*, surgen principalmente bajo una concepción doctrinal, como obligaciones de carácter opcional.

Según Cini, el concepto de *soft law* comenzó a desarrollarse en la literatura de derecho público por la década de 1970, y el concepto más aterrizado de dicha institución es el planteado por Snyder,

el cual lo define como aquellas reglas de conducta que, en principio, no tienen fuerza vinculante legal pero que sin perjuicio de ello, pueden tener efectos prácticos (2001, pp. 193-194).

En esa misma línea, la Organización para la Cooperación y el Desarrollo Económico (OECD) define a las *soft law* como la "cooperación basada en instrumentos que no son legalmente vinculantes, o cuya fuerza vinculante es algo más "débil" que la del derecho tradicional, tales como códigos de conducta, guías, hojas de ruta, revisiones de pares"[16].

Por su parte, Baldassare señala que el concepto de *soft law* nos remite a elementos normativos, sin valor de vinculación que, aunque no produzcan por sí algún derecho u obligación, pueden generar efectos jurídicos, e incluso transformarse en derecho inmediatamente preceptivo (2014, pp. 76).

En ese orden de ideas, las normas de *soft law*, entendidas como aquellas directrices, códigos de conducta, guías, estándares, entre otros, surgen como una alternativa distinta a las normas imperativas estatales como un mecanismo de autorregulación por decisión de distintos sectores del mercado. Sin embargo, dichas guías o directrices en muchos casos o adquieren la fuerza vinculante de las normas *hard law* o incluso son recogidas como normas *hard law*.

Tal es así la importancia de las normas de las normas de *soft law* que, como sucede con los principios Unidroit, muchos de ellos son aceptados en la rama o sector donde se desarrolla. En esa línea, Baldassare Pastore indica que dichos principios pueden considerarse como elementos esenciales que orientan la redacción de contratos comerciales, e incluso como estándares para la interpretación jurídica de dichas relaciones comerciales. En ese sentido, si bien dichos principios no están destinados a ser vinculantes, aún aceptados por los operadores, hace que se adapten a las condiciones variables del comercio internacional (2014, pp. 77).

[16] Traducción nuestra. Definición disponible en: https://www.oecd.org/gov/regulatory-policy/irc10.htm

2.1.2 Las normas de Gobierno Corporativo

Otro claro ejemplo de aceptación e integración de normas *soft law* son las normas de Gobierno Corporativo, las cuales vienen siendo implementadas e incorporadas en la regulación societaria nacional e internacional, en diferentes mercados.

Para entender la naturaleza y concepto de las normas de gobierno corporativo, debemos remontarnos al principal problema que tienen todas las sociedades: el problema de agencia. En líneas generales dicho problema de agencia explica su existencia ante el conflicto de interés que se genera por la colusión de los intereses de los accionistas (inversores) con los intereses de los administradores (gerencia general o directorio). En esa línea, Hundskopf señala que a fin de que los administradores (gerentes generales o directorio) obtengan buenos resultados, dichas personas se inclinan por maximizar la reinversión de las utilidades de una empresa, mientras que los accionistas desean ver dividendos al final de un determinado ejercicio (2001, p. 57).

Recordemos que este problema de agencia es un problema que siempre se encuentra presente en toda sociedad, toda vez que como bien señala Martínez, estas relaciones de agencia (Accionistas y Administradores) surgen en la medida que los accionistas no pueden realizar cierto tipo de actividades directamente y necesitan del apoyo de terceros para tal efecto, todo esto, en un contexto de alta incertidumbre y complejidad (2003, pp. 281).

Como hemos podido advertir, dicho problema de agencia crea una necesidad de regulación por parte de los ordenamientos jurídicos, a fin de evitar aprovechamientos o desprotecciones de intereses que cohabitan dentro de una empresa. Es por esto que, gran parte de la regulación societaria peruana, busca proteger intereses de los actores de una empresa (sean accionistas, administradores o terceros relacionados).

Sin embargo, esta regulación no necesariamente es completa o suficiente para cubrir tanto los intereses de los actores de una empresa, como de los intereses de la misma empresa. Es por esto que surgen lineamientos o recomendaciones como hemos visto antes (*soft law*) que buscan regular esta situación. Una de las salidas, son las conocidas como normas de gobierno corporativo.

Dichas normas buscan establecer algunos principios mínimos que toda empresa o sociedad debe seguir a fin de gestionar eficientemente este conflicto de intereses entre administración y accionistas. En palabras de la OECD, el gobierno corporativo son un conjunto de relaciones entre la dirección (función que podría cumplir el gerente general en el Perú), el consejo de administración (o directorio) y los accionistas y otros actores interesados (*stakeholders*); además de servir como una estructura mediante la cual se fijan los objetivos de una empresa y cómo será la forma de alcanzarlos (2016, p. 9) (añadido nuestro).

Sin embargo, hay que precisar que dichos lineamientos de gobierno corporativo no son estáticos. Al ser normas de *soft law*, dichos lineamientos van evolucionado durante el tiempo y se van acomodando a las necesidades puntuales de cada empresa. En esa línea, Elena Pérez, indica que el concepto de gobierno corporativo es un concepto evolutivo, donde la idea general que subyace es que dicho gobierno (o normas de gobierno) busquen regular cómo se distribuye el poder en su interior (2009, pp. 54).

La autora señala que si bien podrán existir diferentes normas de gobierno corporativo, donde en algunos casos se remitirán a cuestiones éticas, y en otros casos a cuestiones financieras o jurídicas, se debería elegir la centrada en la forma en la que se dirigen y organizan las empresas (Pérez, 2009, pp. 54).

En ese orden de ideas, podemos concluir, y a su vez construir un concepto de gobierno corporativo: (i) son normas soft law (guías, estándares, principios) cuya característica principal es que no son de obligatorio cumplimiento, salvo excepciones de normas específicas sectoriales, (ii) buscan dar solución al problema de agencia en las sociedades, al establecer cómo las empresas son dirigidas y controladas (asignación de responsabilidades), y (iii) no son de aplicación uniforme, en la medida que dichas normas podrían variar según el modelo económico del país, la estructura de propiedad y el sector en donde opera la sociedad en concreto.

2.1.3 Relevancia de la aplicación de las normas de Gobierno Corporativo y su impacto luego de la pandemia

Una vez definido del concepto de las normas de gobierno corporativo, conviene en detenernos en la relevancia de su correcta implementación y adecuación en las sociedades en donde no resulta obligatorio hacerlo.

Como indicamos líneas arriba, el problema de agencia significa una pugna de intereses entre accionistas y administradores que puede repercutir en altos costos para la empresa. Si bien estos intereses pueden conversar en la medida que tanto accionistas como administradores buscan que le vaya bien a la empresa, en muchas ocasiones estos intereses chocan. Estos intereses se enfrentan cuando estamos en situaciones de gobernabilidad y desarrollo de la sociedad.

La pugna entre los intereses de administradores frente a accionistas, significan en muchos casos costos elevados para la empresa. En este sentido, una buena estructura de gobierno entendida como normas, guías, directrices que regulen la gobernabilidad, no solo en su aspecto teórico sino práctico, conllevará en suma a seleccionar gerentes o administradores más hábiles y responsables frente a los inversionistas, los cuales serán debidamente incentivados para cumplir con tal fin (Tirole, 1999, pp. 10).

En este orden de ideas, un adecuado sistema de gobierno permitirá no solo reducir los costos de agencia, sino que permitirá tener mayor predictibilidad para la inversión que hicieron los accionistas de una empresa, en la medida que tendrán reglas claras que les permitirán delegar las facultades de gestión y administración en terceros especializados, sin tener la incertidumbre sobre el actuar de dichos terceros.

Finalmente hay que considerar que las normas de gobierno corporativo han sido bastante influidas por parte de la situación pandémica que se vivió recientemente. A entender de la OECD, la pandemia dio lugar a la implementación de varias medidas de digitalización que respondían más a una necesidad que a una estrategia, y por lo tanto sin la posibilidad de estar sujeto a rigurosas evaluaciones como sería en una situación normal (2022, p. 4).

En ese escenario, ante la necesaria adaptación del contexto pandémico en las empresas, lo que entendemos como una digitalización forzada, correspondería la necesaria adaptación de las normas de gobierno corporativo y el deber de los administradores frente a dicho cambio. Así, según lo discutido en la mesa redonda de la OECD – Asia sobre gobierno corporativo, los principales retos del gobierno corporativo post pandemia, están relacionados con (i) participación remota (digital) en sesiones de junta general de accionistas, y (ii) riesgos de seguridad digital y el papel de la administración de la empresa sobre ello (2022, p. 4).

Es por esto que, como hemos podido ir advirtiendo a lo largo del presente trabajo, no sola la labor de la administración de la empresa tiene la necesidad de adaptarse a los nuevos Riesgos Digitales Legales, sino que también las normas de gobierno corporativo, dada su constante evolución, deben ser adaptadas para que consigan su objetivo de una forma más eficiente y acertada.

2.2 El deber de diligencia de los administradores de la sociedad.

Una vez entendido el concepto de gobierno corporativo, la relevancia de una adecuada implementación de dicho sistema y los retos de dicho sistema en un contexto digital, conviene revisar el concepto de deber de diligencia como una norma que forma para de las normas de gobierno corporativo.

Antes de abordar este tema, debemos hacer la precisión que, para efectos del presente trabajo, cuando nos refiramos a la administración de una sociedad o empresa, estaremos haciendo la referencia al directorio o la gerencia general (en caso de directorio facultativo) de una determinada sociedad o empresa, en la medida que dichos órganos ostentan la administración de una sociedad, de conformidad con lo establecido en el artículo 152 de la Ley General de Sociedades peruana. Hacemos esta precisión ya que, las normas de gobierno corporativo al ser universales no precisan sobre qué órgano en específico hacen referencia cuando mencionan la administración de la sociedad. A manera de ejemplo, en el ordenamiento jurídico español, la administración de la sociedad recae sobre el Consejo de Administración.

2.2.1 Definición del deber de diligencia de los administradores

Como hemos venido sosteniendo, las normas de gobierno corporativo buscan asignar responsabilidades a los administradores de una sociedad, en la medida del rol que cumplen dentro de la misma. En este escenario, uno de los principales deberes que se les asigna es el deber de diligencia.

El deber de diligencia, según Paz-Ares, es el "deber de cuidado", el deber de diligencia de un "empresario ordenado", en virtud del cual se exige a los administradores una inversión de dinero, tiempo y esfuerzo, y desplieguen cierto nivel de pericia, en la gestión o supervisión de la empresa, a fin de maximizar la producción de valor (2003, pp. 204).

En esa misma línea, la guía sobre deberes y régimen de responsabilidades de los administradores elaborada por Uría, señala que el deber de diligencia se configura como pauta de conducta y como fuente de obligaciones en virtud de las cuales los administradores han de cumplir con deberes de diligencia impuestos por ley, estatutos o normas internas (Uría 2015, pp. 7).

En este sentido, el concepto del deber de diligencia puede ser resumido como: (i) un deber impuesto por normas de soft law (gobierno corporativo) a las personas que administran una sociedad (sean directores o gerentes), (ii) en virtud de este deber, se le exige a la administración de la sociedad un deber de cuidado, entendido como la inversión de dinero, tiempo y esfuerzo en su actuación de gestión y supervisión de las actividades de la empresa, y (iii) dicho deber, significa una responsabilidad de la administración frente a los accionistas de una sociedad.

2.2.2 Relevancia del deber de diligencia de los administradores

Para entender mejor esta figura, debemos detenernos en la relevancia de la misma. A estos efectos, recordemos que, gran parte del atractivo de una empresa como inversión es que les permite a sus inversionistas colocar capital en un vehículo donde no necesariamente tienen que involucrarse en la gestión para obtener los beneficios (Payet, 2003, pp. 86).

Sin embargo, como bien indicamos líneas arriba, esta posibilidad genera a su vez problemas de agencia en la medida que terceros especializados asumirían la administración de la empresa y los intereses no siempre conversarían.

En este contexto, las normas de gobierno corporativo, y en especial el deber de diligencia impuesto a los administradores de una sociedad (y claramente la imposición de responsabilidades de los mismos frente a este deber ante un incumplimiento), tal como señala Payet citando a Paz-Ares, actúa como mecanismo disuasivo de conductas que se aparten de los intereses de los accionistas, además de servir de correctivo para los costos de agencia (2003, pp. 86).

Dichos costos de agencia se verán reducidos en la medida que la implementación de un régimen de responsabilidad de los administradores, alineará los incentivos de los administradores con los intereses de los accionistas (Paz-Ares, 2002, pp. 3). Esto porque, en la medida que la amenaza de tener que indemnizar los daños que ocasionen los comportamientos incorrectos de los administradores, sirve de efecto disuasorio para que los administradores gestionen la empresa, en relación con los intereses de los accionistas (Paz-Ares, 2002, pp. 5).

En este sentido, el deber de diligencia de los administradores de una sociedad, toma bastante relevancia en la reducción de los costos de agencia, al ser un deber que busca incentivar la correcta actuación de los administradores de un sociedad, para que dicha actuación esté alineada con los intereses de los accionistas.

2.2.3 El deber de diligencia digital

Como mencionamos anteriormente, los retos a los que se enfrenta el gobierno corporativo que fueron discutidos en la mesa redonda de la OECD – Asia requieren de la adaptación de dichos lineamientos a las nuevas soluciones tecnológicas que son implementadas y explotadas por las empresas. Tanto la digitalización de las sesiones de junta general de accionistas, como los riesgos de seguridad digital, son frentes que hemos catalogado en el primer capítulo de nuestro trabajo como Riesgos Digitales Legales (de gobierno y operacionales, respectivamente).

En este escenario, y tomando en consideración lo debatido en la mesa redonda de la OECD-Asia y lo indicado anteriormente respecto de la constante evolución de las normas de gobierno corporativo, consideramos que el deber de diligencia "ordinario" como norma de gobierno corporativo, debe adaptarse a un deber de diligencia "digital".

Cuando nos referimos al deber de diligencia "digital", hacemos referencia a aquel deber de diligencia de la administración de una sociedad, con particular interés en los Riesgos Digitales Legales. Así, en la medida que el deber de diligencia abarque el deber de cuidado de la administración frente a posibles riesgos o amenazas, no solo ordinarios de la propia empresa, sino que a aquellos vinculados con las nuevas tecnologías; obligará a la administración a que implemente medidas de seguridad adecuadas.

Es importante precisar que, las medidas que surjan a fin de dar cumplimiento con este deber de diligencia digital pueden ser muchas y de diferente tipo dependiendo de cada empresa (sea por tipo o por sector en el que opera), pero que lo que debe quedar sentado es esta adaptación o precisión que se haga sobre el deber de diligencia en su aspecto digital.

2.3 Plan de gestión de riesgos.

Finalmente, en este capítulo conviene hacer referencia a una de las formas en que se materializa el deber de diligencia de los administradores: la gestión de riesgos legales.

Para entender mejor esta técnica, debemos entender a qué se refiere. Para esto nos referiremos a la definición que maneja la Superintendencia de Banca, Seguros y Administradoras de Fondos de Pensiones ("SBS"), en su Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, aprobado por Resolución SBS N° 272-2017.

Cabe señalar que usaremos este regulación en específica a manera de ejemplo, ya que se aplicación es obligatoria solo para determinadas sociedades que se encuentran reguladas por dicha

entidad; sin embargo, empresas que no estén sujetas a dicha regulación pueden, de manera voluntaria, adaptarse a los lineamientos previstos en dicho reglamento.

Continuando con el ejemplo, la SBS señala que la Gestión Integral de Riesgos es un proceso efectuado por la administración (directorio y/o gerencia) diseñado para identificar potenciales eventos que puedan perjudicar a la empresa, gestionarlos según el riesgo y proveer una seguridad razonable en el logro de sus objetivos; donde se incluye la totalidad de la empresa, sus líneas de negocio, procesos y unidades organizativas, incluyendo todos sus riesgos relevantes.

En ese sentido, la idea de una adecuada gestión integral de riesgos, está relacionada con la correcta identificación de los riesgos en una empresa, para darles visibilidad, asignar responsabilidades, y formas de control de los mismos. Este mecanismo sirve de práctica habitual de los administradores de la sociedad para poder cumplir con su deber de diligencia.

Finalmente, a fin de recapitular lo desarrollado en este capítulo conviene destacar algunos conceptos relevantes:

(i) Las normas de *soft law*, en comparación con las normas de *hard law*, son directrices, guías, códigos, entre otros que buscan resolver problemáticas o vacíos legales que no necesariamente son uniformes a nivel internacional.

Dichas normas se caracterizan por no tener fuerza vinculante, por lo que se les denomina como *non-binding agreements* o normas blandas.

Sin embargo, muchas de dichas normas se aplican indiscutiblemente en la práctica de cada sector. Tal es así que las normas de gobierno corporativo, son aplicadas incluso respecto de sectores regulados por entidades estatales.

(ii) Las normas de gobierno corporativo nacen como medida que busca cerrar la brecha creada por el problema de agencia, entre accionistas y administradores.

Las normas de gobierno corporativo entonces buscan regular la distribución de responsabilidades dentro de una empresa, que permitirá a un inversionistas tener la certeza de que podrá colocar capital en un vehículo donde no tiene que involucrarse en la gestión, sin que esto afecte a sus intereses naturales.

Las normas de gobierno corporativo buscan dar directrices o guías para una adecuada administración de la empresa, y sirve de incentivo tanto para los administradores como para los accionistas de una determinada sociedad.

(iii) Toda vez que las normas de gobierno corporativo no son estáticas en el tiempo, sino que deben ser adaptadas según necesidades o contextos, dichas normas deben encontrar su adaptación a las nuevas soluciones tecnológicas que surgieron en su mayoría producto de la situación pandémica que se vivió recientemente en el mundo. Como bien indicaron en su momento en la mesa redonda de la OECD-Asia, el reto que tiene el gobierno corporativo es poder adaptarse a la digitalización de las sesiones de junta general de accionistas y los riesgos de seguridad digital y el rol de la administración frente a ello.

(iv) Uno de los principales deberes que surgen en virtud de las normas de gobierno corporativo, es el deber de diligencia de los administradores.

En virtud de este deber de cuidado o diligencia, se le exige a la administración de la sociedad la inversión de dinero, tiempo y esfuerzo en su actuación de gestión y supervisión de las actividades de la empresa.

Al estar asignadas adecuadamente las responsabilidades y los incentivos para la administración de la sociedad, este deber sirve como mecanismo para reducir los costos de agencia: el incumplimiento de las obligaciones por parte de los administradores generaría responsabilidad frente a los accionistas.

(v) Una de las formas en donde se materializa el deber de diligencia de los administradores es en la implementación un adecuado plan de gestión de riesgos. En virtud de este plan,

los administradores de la empresa, tendrán que identificar los potenciales eventos que puedan perjudicar a la empresa (riesgos), gestionarlos según el riesgo y proveer una seguridad razonable en el logro de sus objetivos. Se deberá incluir la totalidad de las actividades de la empresa, sus líneas de negocio, procesos y unidades organizativas, incluyendo todos sus riesgos relevantes.

(vi) Dado la necesidad de adaptar las normas de gobierno corporativo al contexto digital actual, es que se debe adaptar el deber de diligencia "ordinario" de los administradores, hacia un deber de diligencia "digital" que busque no solo identificar, prevenir y mitigar riesgos asociados o amenazas propias del giro del negocio de la empresa, sino que tengan particular atención a los Riesgos Digitales Legales que surgen en base a las nuevas soluciones tecnológicas implementadas y explotadas por las empresas.

(vii) La implementación de un adecuado plan de gestión de riesgos, es un mecanismo ideal para cumplir adecuadamente con el deber de diligencia de los administradores de la empresa.

Con estos conceptos planteados y junto con los desarrollados en el capítulo 1 anterior, realizaremos el análisis de si el deber de diligencia, tal como está estructurado debe ser adecuado al contexto digital actual, a fin de que se incluya dentro de dicho deber, la identificación, mitigación y prevención de los Riesgos Digitales Legales.

CAPITULO 3

BENEFICIOS DE UN DEBER DE DILIGENCIA DIGITAL EN LA ADMINISTRACIÓN DE LAS SOCIEDADES

Como hemos ido viendo a lo largo del presente trabajo, el deber de diligencia digital no solo encuentra su justificación en la necesidad de adaptación a los nuevos retos de la administración de una sociedad y las normas de gobierno corporativo, sino que un adecuado ejercicio de dicho deber de diligencia digital permitirá que el órgano de administración de una empresa, pueda adaptar sus mecanismos de prevención de riesgos, a unos que incluyan la identificación, prevención y mitigación de los Riesgos Digitales Legales, cuyo impacto de materialización es altamente lesivo para los intereses de los socios o accionistas, administradores y terceros (*stakeholders*).

En el presente capítulo buscaremos validar nuestra hipótesis planteada al inicio de esta investigación: se requiere adecuar el deber de diligencia a un deber de diligencia digital en virtud del cual la administración de una sociedad deba identificar, prevenir y mitigar los Riesgos Digitales Legales. Para estos efectos, se propondrán dos medidas que podría adoptar la administración de una sociedad para implementar medidas prácticas que busque cumplir con un deber de diligencia digital.

Una primera medida estará relacionada con algunas recomendaciones para la administración de una sociedad, respecto a la digitalización de las sesiones de junta general de accionistas; y, otra medida relacionada con la consideración de los Riesgos Digitales Legales dentro de los modelos de prevención de riesgos, como parte de políticas internas de autorregulación implementadas desde la administración de una sociedad. Con estas medidas no solo se le podrá dar visibilidad a los Riesgos Digitales Legales, sino que servirá para poder prevenir y/o mitigar dichos riesgos y evitar o reducir el impacto negativo de la ocurrencia de los mismos dentro de la empresa.

3.1 Políticas internas para la celebración de juntas generales de accionistas virtuales

La primera medida que proponemos en el presente trabajo de investigación es establecer determinadas políticas internas que permitan una adecuada celebración de juntas generales de

accionistas de manera virtual. En esa misma línea, se propuso en la mesa redonda de la OECD – Asia, que, al igual que con otras novedades tecnológicas, era necesario garantizar que la implementación de juntas de accionistas y votaciones virtuales considere posibles inconvenientes y consecuencias no deseadas (2022, p. 10).

Dentro de las principales recomendaciones que se discutieron en dicha mesa redonda, fueron aquellas que se incluyeron dentro de "*The Principles and Best Practices for Virtual Annual Shareowner Meetings*" del 2018[17] (iniciativa de un sector empresarial privado). De acuerdo con esos principios, los cinco principios clave que la administración de una sociedad debería tomar en cuenta a la hora de celebrar sesiones virtuales de junta de accionistas son (i) se debe valorar y fomentar una amplia participación de los accionistas en las reuniones anuales, (ii) las asambleas deben promover un trato equitativo e igualitario de los accionistas participantes, (iii) se deben bridar oportunidades para un compromiso de los accionistas, (iv) se deberá detallar los beneficios de celebrar una junta virtual y (v) las reuniones virtuales deben utilizarse para proporcionar un espacio de dialogo abierto para los accionistas (OECD, 2022, p. 11).

Adicionalmente, dicho documento esboza algunas recomendaciones que recogemos como válidas y aplicables para contar con una adecuada política de sesiones virtuales de junta general de accionistas: (i) garantizar la igualdad de acceso, (ii) crear reglas de conducta, (iii) establecer pautas de tiempo razonables para intervenciones de accionistas, (iv) poner a disposición soporte técnico, y (v) archivar reuniones para revisión a futuro (OECD, 2022, p. 11).

En ese orden de ideas, podemos concluir que, a fin de contar con una adecuada política de celebración de juntas de accionistas virtuales se deben tomar en consideración los principios antes mencionados, e implementar las recomendaciones antes descritas. Esto permitirá crear un espacio digital que garantice a los accionistas, la posibilidad de asistir, participar y votar en sus sesiones de junta general de accionistas.

Como hemos podido advertir, la implementación de esta política permite dar visibilidad a los posibles riesgos o amenazas que trae consigo la digitalización de las sesiones de junta general de

[17] Documento disponible en: https://www.broadridge.com/_assets/pdf/broadridge-vasm-guide.pdf

accionistas; pudiendo lograr que la administración identifique, prevenga y mitigue la materialización de dichos riesgos.

3.2 Adecuación del sistema de prevención de riesgos de una sociedad.

La otra medida que pueden adoptar las administraciones de una sociedad es la adecuación o implementación de su sistema de prevención de riesgos interno (como una medida de autorregulación corporativa) para considerar a los Riesgos Digitales Legales dentro de ese esquema.

A estos efectos, consideraremos la herramienta estratégica que desarrolla Peter Kurer denominada "*Strategic Legal Risk Management*" o SLRM. Bajo dicha herramienta, Kurer precisa que para gestionar este tipo de riegos, se debe generar un circulo rotativo que involucre los siguientes pasos: (1) hacer visible el riesgo legal, (2) entender los impulsores de estos riesgos, (3) valorar dichos riesgos (darle una valoración económica a la materialización de los daños), (4) adoptar adecuadas decisiones sobre el mismo, (5) comunicar tales decisiones, (6) mitigar y gestionar estos riesgos, y (7) controlarlos (2015, pp. 57).

Bajo los lineamientos de la herramienta antes indicada, es que sugerimos la adaptación de los sistemas de *compliance* o prevención de riesgos de las empresas, hacia ese perfil: identificar, entender, valorar, decidir, mitigar y controlar los Riesgos Digitales Legales.

Ahora bien, incluir dentro de los sistemas de prevención de riesgos de una sociedad a estos Riesgos Digitales Legales no se puede hacer sin un análisis previo del tipo de actividad que desarrolla la empresa, sino el nivel de exposición a la que se enfrenta. A manera de ejemplo, el riesgo de protección de datos personales, no será el mismo en una empresa que se dedica a la importación y comercialización de materia prima en comparación con una empresa que administra una clínica que maneja información sensible de pacientes.

En ese sentido, la adecuación del sistema de prevención de riesgos que sea implementado a cargo de la administración de una sociedad, para cumplir con su deber de diligencia digital, debe, adecuadamente y según los niveles de exposición, incluir dichos Riesgos Digitales Legales.

A fines prácticos, el sistema de prevención de riesgos de una sociedad, cuando menos, debe incluir un mapa de riesgos en virtud del cual se establezcan los siguientes criterios:

(i) Encargado del proceso: donde se deberá precisar qué área de la empresa es responsable por el proceso donde se involucra el Riesgo Digital Legal (ej. Legal – Administración y Finanzas, CEO, CFO, COO, entre otros).

(ii) Riesgo Digital Legal: donde se le dará una denominación al Riesgo Digital Legal identificado (ej. Datos personales, Datos sensibles de la empresa, entre otros).

(iii) Descripción del Riesgo Digital Legal: donde se incluirá una descripción completa del Riesgo Digital Legal que se ha identificado (ej. Acceso por parte de terceros no identificados ajenos a la sociedad a los datos sensibles de la sociedad, datos comerciales, datos de trabajadores, datos de clientes, entre otros).

(iv) Ejemplo de materialización del Riesgo Digital Legal: donde se deberá incluir un ejemplo de materialización del Riesgo Digital Legal en el curso ordinario de la sociedad (ej. Hackeo de los sistemas internos de la sociedad por parte de terceros no identificados).

(v) Probabilidad de ocurrencia: donde se indicará cual es la probabilidad de ocurrencia o materialización del Riesgo Digital Legal identificado. Dependerá del criterio de la administración de la empresa para poder determinar el rango de ocurrencia (ej. Del 1 al 5, o por letras, A,B,C, pero lo importante es que quede claro cuál es el criterio que se le imputa a la ocurrencia de un determinado riesgo).

(vi) Impacto: donde, de la mano con el punto anterior, se califica el impacto de ocurrencia del Riesgo Digital Legal. En este punto, al igual que el anterior, se debe estimar criterios de impacto del Riesgo Digital Legal (ej. Del 1 al 10).

(vii) Riesgo inherente: donde se indicará el resultado de la probabilidad de ocurrencia por el impacto, dato que nos dará la severidad o riesgo inherente que tenemos frente al Riesgo Digital Legal que se ha identificado, considerando su ocurrencia o materialización y grado de impacto (ej. Del 1 al 20, dependiendo de los valores asignados en los puntos (v) y (vi) anteriores).

(viii) Control: donde se indicará cual es el mecanismo de control que se ha previsto para prevenir la ocurrencia del Riesgo Digital Legal identificado (ej. Política de seguridad de la información, sistema de protección de datos personales, Circuito cerrado de comunicaciones, entre otros).

(ix) Tipo de control: donde se indicará de qué tipo de control se trata (ej. Preventivo, de detección, de mitigación, entre otros).

(x) Grado de efectividad: donde se indicará el grado de efectividad que tiene el mecanismo de control antes indicado. En este apartado el encargado del sistema de prevención deberá evaluar y estimar qué tan efectivo el es mecanismo de control que ha planteado para la prevención o mitigación del Riesgo Digital Legal identificado (ej. 30%, 40%, 80% de efectividad).

(xi) Riesgo Residual: donde se calculará cual es el riesgo residual que resultaría de multiplicar el monto del riesgo inherente por el grado de efectividad del mecanismo de control. Dicho valor servirá para determinar el grado de severidad o el riesgo inherente que queda luego de haber aplicado los controles previstos. Este riesgo residual permitirá saber a la administración de la empresa si necesita implementar más mecanismos de prevención o si con los controles previstos es suficiente (ej. Del 1 al 10).

Como hemos podido ver en este apartado, un deber de diligencia digital como el que proponemos no solo encuentra su solución en un tema de visibilidad del problema, sino que recién podríamos dar por cubierto dicho deber, con una adecuada incorporación de los Riesgos Digitales Legales de una determinada sociedad, considerando no solo la descripción del mismo, sino también considerando el grado de ocurrencia, el mecanismo de control y el riesgo residual del mismo. Recién con esta valoración adecuada del Riesgo Digital Legal, la administración de la empresa tendrá las herramientas que le permitirá tener control sobre dicho riesgo.

Una vez descritas nuestras sugerencias que permitirán materializar adecuadamente el deber de diligencia digital de los administradores a nivel práctico, corresponde que nos pronunciemos sobre los beneficios de contar con ese tipo de medidas, tanto para los accionistas, administradores y terceros interesados (*stakeholders*).

3.3 Beneficios para los socios o accionistas.

Como vimos en el capítulo primero, existen Riegos Digitales Legales Internos (gobierno) cuya materialización impactaría directamente a los intereses de los socios o accionistas de una determinada sociedad. Dentro de los principales Riesgos Digitales Legales identificados, rescatamos aquellos cuyo impacto podría generar una desprotección de los datos personales de los socios o accionistas.

En ese sentido, en la medida que la administración establezca una política adecuada y garantice un espacio seguro para las sesiones de junta de accionistas virtuales, y cuente con un adecuado sistema de prevención de riesgos que identifique, prevenga y mitigue este tipo de Riesgos Digitales Legales, no solo evitará o mitigará los efectos de dichos riesgos, sino que creará un ambiente seguro para la toma de decisiones de los socios o accionistas de una sociedad.

Con la creación de un ambiente seguro para la discusión de temas propios de la sociedad, no solo se protegen datos de los socios o accionistas, sino que también se protegen datos propios de la empresa. Es así que con la prevención o mitigación de dichos riesgos, se protegen los intereses de los socios o accionistas respecto de su inversión en la misma sociedad.

3.6 Beneficios para los administradores de la sociedad

Ahora bien, la adecuación del sistema de prevención de riesgos a los Riesgos Digitales Legales será una herramienta fundamental para el adecuado desarrollo de las actividades ordinarias de la sociedad.

Como hemos podido notar en la sección 3.2 anterior, un mapa de riesgos con una valorización adecuada de los Riesgos Digitales Legales, permitirá a la administración de la sociedad, contar con las herramientas adecuadas para prevenir los Riesgos Digitales Legales o en caso de ocurrencia, mitigar el impacto de los mismos, siendo también una herramienta adecuada para deslindar de alguna responsabilidad que les pudiera aplicar.

Recordemos que uno de los principales intereses de los administradores de la sociedad es mantener viva la sociedad, por lo que protegiendo los intereses de la misma sociedad, evitando la ocurrencia de riesgos que le afecten económicamente, indirectamente están protegiendo sus intereses.

A manera de ejemplo, podemos mencionar dos casos en los que, por no contar con medidas adecuadas que permitan identificar, prevenir y mitigar Riesgos Digitales Legales, significaron un costo económico bastante elevado para la empresa.

Un primer caso es el de la empresa Equifax en 2017, que debido a producto de una vulneración de sus sistema de almacenamiento de datos de sus clientes, se perdió información financiera y confidencial de los mismos. Dos años después, la empresa tuvo que pagar alrededor de 575 millones de dólares a la Oficina de Protección Financiera del Consumidor de Estados Unidos[18].

Otro caso reciente es el caso de la empresa *Capital One* en 2021, empresa que tuvo que llegar a un acuerdo en una demanda colectiva por el monto de 190 millones de dólares por la violación

[18] Información disponible en: https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach

de datos personales e información financiera de sus clientes, además de pagar una multa ascendente a la suma de 80 millones de dólares[19].

De lo expuesto, podemos concluir que si dichas empresas hubiesen tomado en particular consideración los Riesgos Digitales Legales inherentes a su giro de negocio, pudieron haber de alguna manera prevenido o mitigado el impacto del Riesgo Digital Legal, y así haber evitado la afectación económica de los mismos.

3.7 Beneficios para terceros o *stakeholders*.

Por último, conviene resaltar el beneficio de nuestra propuesta respecto de terceros relacionados con la sociedad: los llamados *stakeholders*.

Como idea previa, debemos entender a qué nos referimos cuando hablamos de *stakeholders*. Al respecto, Freeman (2002) hace referencia a los *stakeholders* como aquel grupo de personas como clientes, empleados, proveedores, comunidades, financistas, entre otros, que tiene una relación directa con los intereses de la sociedad. Asimismo, Mayer (2020) sostiene que, al apoyar los intereses de estos *stakeholders*, las sociedades establecen relaciones más fidelizadas con sus clientes, empleados más comprometidos, proveedores confiables y ambientes sostenibles, teniendo un impacto directo en los ingresos de una sociedad, reduciendo costos, y por lo tanto, generando mejores utilidades y beneficios para los accionistas de una sociedad.

En ese orden de ideas, no podemos no pronunciarnos sobre el impacto de nuestra medida de solución frente a los Riesgos Digitales Legales respecto de los *stakeholders* de una sociedad. Al respecto, debemos precisar que, como vimos en el capítulo primero, existen también Riesgos Digitales Legales que impactan en trabajadores, clientes y proveedores de una empresa, básicamente respecto a la protección de sus datos personales.

En ese sentido, nuevamente, un sistema de prevención de riesgos adecuado a los Riesgos Digitales Legales, permitirá que, dichos riesgos que impactan sobre los datos personales de

[19] Información disponible en: https://www.nytimes.com/2021/12/23/business/capital-one-hacking-settlement.html

stakeholders de una sociedad, estén controlados, permitiéndoles mecanismos de prevención y mitigación eficientes, dependiendo de las actividades propias de la sociedad.

Finalmente, como hemos podido apreciar en este capítulo, concluimos que con la visibilidad de estos Riesgos Digitales Legales que van surgiendo en la medida que se emplean nuevas soluciones legales en la industria, y su inclusión, de manera adecuada y eficiente, en los sistemas de prevención de riesgos en las sociedades, permitirán que la administración de una sociedad pueda estar en la capacidad de contar con las herramientas necesarias para prevenir y mitigar este tipo de riesgos; y así, tener un impacto positivo respecto de los socios o accionistas, administradores y *stakeholders* de una determinada sociedad.

CONCLUSIONES

A modo de conclusión, resaltaremos las principales ideas recogidas a lo largo del presente trabajo de investigación, que fortalecen y sustenta nuestra hipótesis principal planteada en la introducción del presente trabajo:

(i) Nos encontramos ante un contexto de transformación digital empresarial, que exige a las sociedades en el Perú a adaptarse a los nuevos cambios y oportunidades que surgen a nivel tecnológico. Estos cambios permiten a las empresas adecuarse y volverse cada día más eficientes y competitivas en el mercado o sector donde operan.

Si bien estas innovaciones tecnológicas traen consigo muchos beneficios para las empresas, también debemos considerar que dichas nuevas soluciones tecnológicas, traen nuevos riesgos para la misma, los que definimos en el presente trabajo de investigación como "Riesgos Digitales Legales".

Para entender a lo que nos referimos como "Riesgos Digitales Legales", los hemos definido como aquellos riesgos inherentes al uso de nuevas tecnologías, cuya materialización tienen repercusión no solamente económica sino legal, desde un punto de vista normativo, regulatorio o contractual.

Los Riesgos Digitales Legales los hemos clasificados en 2 tipos: (i) Los Riesgos Digitales Legales de Gobierno (aquellos riegos vinculados con la gobernanza de la sociedad) y (ii) Los Riesgos Digitales Legales operacionales (aquellos riesgos vinculados con las operaciones empresariales de la sociedad).

(ii) Las normas de gobierno corporativo surgieron como normas *soft law* en diferentes ordenamientos jurídicos. Las normas de *soft law*, en comparación con las normas de *hard law*, son directrices, guías, códigos, entre otros que buscan resolver problemáticas o vacíos legales que no necesariamente son uniformes a nivel internacional. Dichas normas se caracterizan por no tener fuerza vinculante, por lo que se les denomina como *non-binding*

agreements o normas blandas. Sin embargo, muchas de dichas normas se aplican indiscutiblemente en la práctica de cada sector. Tal es así que las normas de gobierno corporativo, son aplicadas incluso respecto de sectores regulados por entidades estatales.

Las normas de gobierno corporativo buscan resolver el problema de agencia, entre accionistas y administradores estableciendo responsabilidades dentro de una empresa para brindar confianza a los inversionistas. Además, ofrecen directrices para la gestión empresarial y actúan como incentivos tanto para los administradores como para los accionistas.

Uno de los principales deberes que emanan de estas normas es el deber de diligencia de los administradores, que implica dedicar recursos y esfuerzos a la gestión y supervisión de la empresa. Al asignar adecuadamente responsabilidades e incentivos, este deber ayuda a reducir los conflictos de intereses: el incumplimiento de los administradores conlleva responsabilidad frente a los accionistas.

Una manera en que se manifiesta esta diligencia es a través de la implementación de un plan de gestión de riesgos. Esto implica identificar y manejar eventos que puedan perjudicar a la empresa y proporcionar seguridad en la consecución de sus metas, abarcando todas las actividades, procesos y riesgos relevantes de la empresa. Este plan es un medio efectivo para cumplir con el deber de diligencia de los administradores.

(iii) La respuesta que proponemos frente a una realidad no atendida en el mundo empresarial como lo son los Riesgos Digitales Legales, es la adecuación del deber de diligencia a un deber de diligencia digital. En ese sentido, el deber de diligencia deberá, además del deber de cuidado general, adaptarse y prestarle mayor atención a los Riesgos Digitales Legales.

Dicho deber de diligencia digital puede materializarse de diferentes formas, siempre que se cumpla con el objetivo antes mencionado. Sin perjuicio de ello, en el presente trabajo se propusieron dos medidas prácticas: (i) el planteamiento de una política interna para la celebración de sesiones virtuales de accionistas o directores, y (ii) la adecuación del sistema

de *compliance* o los mecanismos de prevención de riesgos de una empresa, a fin de que puedan considerar dentro de dichos sistemas los Riesgos Digitales Legales de cada empresa.

Con estas medidas no solo se le podrá dar visibilidad a los Riesgos Digitales Legales, sino que servirá para poder prevenir y/o mitigar dichos riesgos y evitar o reducir el impacto negativo de la ocurrencia de los mismos dentro de la empresa.

(iv) Como se ha podido apreciar, tener un sistema de *compliance* o mecanismos de prevención de riesgos adecuado a los Riesgos Digitales Legales no solo beneficia a los accionistas o inversionistas de una sociedad, sino que también vela por los intereses de los administradores de la sociedad.

Dichas sugerencias sirven de herramientas para los administradores de una sociedad, puedan estar en la capacidad de cumplir a cabalidad con su deber de diligencia y así prevenir y mitigar este tipo de nuevos riesgos.

Este beneficio para los administradores de la sociedad está relacionado no solo con su labor como tales en una determinada empresa (deber de diligencia), sino que va relacionado también con la permanencia de la sociedad; lo cual también influye en los intereses de los diferentes *stakeholders* de la misma.

(v) Con lo antes expuesto, concluimos que el deber de diligencia de la administración de las sociedades (como concepto propio de las normas del gobierno corporativo), debe (y puede) adecuarse al contexto digital actual y considerar los nuevos Riesgos Digitales Legales que surgen en la medida en que nuevas tecnologías se incluyen en la gobernabilidad y operatividad de los negocios de las sociedades. Para estos fines, éste deber debe contemplar los riesgos inherentes al uso de nuevas tecnologías, a fin de identificarlos, prevenirlos y/o mitigarlos.

BIBLIOGRAFÍA

Baldassare, Pastore (2014). Soft Law y la teoría de las fuentes del derecho. Universita degli Studi de Ferrara., 75-89.

Cebriá, L. (2022). La Digitalización en el Derecho de Sociedades: "Cuestiones sobre el derecho de asistencia y participación del socio en las juntas generales por medios telemáticos". Pontificia Universidad Católica del Perú. Disponible en: https://www.youtube.com/watch?v=0NKLF0AOW_M

Cedillo, F., Meneses, H., y Raygada, M. (2010). Gestión del Riesgo Legal. *Cengage Learning*.

Cin, Michelle (2001). The soft law approach: Commission rule-making in the EU's state aid regime en Journal of European Public Policy, 192-207.

FREEMAN, R. E., Phillips, R. (2002), "Stakeholder theory: A libertarian defense", Business Ethics Quarterly, 331–350.

Ganguly, Saptarshi (2017) Digital Risk: Transforming risk management for the 2020s. McKinsey&Company. En: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/digital-risk-transforming-risk-management-for-the-2020s

Giraldo-Ríos, L, Duque Oliva, E, y Sanchez-Torres, J. (2021). ¿Cómo se relacionan la Transformación digital, la ciberseguridad y el modelo de negocio? XIX Congreso ALTEC, 27 a 29 de octubre – 2021, Lima, Perú.

Hundskopf, Oswaldo. Facultades de la junta general de accionistas, en Diálogo con la jurisprudencia, Tomo 38, Gaceta Jurídica, Lima, noviembre, 2001.

Kurer, Peter. Legal and Compliance Risk: A Strategic Response to a Rising Threat for Global Business. Oxford University Press, Incorporated, 2015. Pp. 57.

Martínez, Juan José (2003). Apuntes sobre el rol del derecho frente al problema de agencia en las organizaciones. En Themis N° 46. Pp. 279-286.

Mayer, Colin (2020). Shareholderism versus Stakeholderism – A Misconceived Contradiction. A Comment on "The Illusory Promise of Stakeholder Governance" by Lucian Bebchuk and Roberto Tallarita. Pp. 1-2.

Payet, J. A. (2003). "Empresa, gobierno corporativo y derecho de sociedades: Reflexiones sobre la Protección de las Minorías". Themis, (46), Pp.77-103.

Paz-Ares, Cándido. "La responsabilidad de los administradores como instrumento de gobierno corporativo". En: Ius et Veritas. Número 27. Lima, 2003, Pp. 202-246.

Paz-Ares, Cándido, Deberes Fiduciarios y Responsabilidad de los Administradores, conferencia presentada en The Third Meeting of the Latin American Corporate Governance Roundtable, 8 – 1 O de abril de 2002, en Ciudad de México. Pp. 1-50.

Pérez Carrillo, E. (2009). "Gobierno corporativo comparado" en Gobierno corporativo y responsabilidad social de las empresas. Marcial Pons, Madrid, pp. 49-77.

Quintás, J. (2007). La gestión del riesgo normativo en el sistema financiero. Revista Galega de Economía, Pp. 1-17.

Soler Ramos, J. A., Staking, K. B., Ayuso Calle, A., Beato, P., Botin O'Shea, E., Escrig Melia, M., & Falero Carrasco, B. (1999). Gestión de riesgos financieros: un enfoque práctico para países latinoamericanos. Washington DC: Banco Interamericano de Desarrollo.

Tirole, Jean (1999). "El Gobierno Corporativo". En Academic Journal N° 44. Pp. 9-60.

Uría Menéndez (2015). "Guía práctica sobre deberes y régimen de responsabilidad de los administradores en el ámbito mercantil". Madrid.

Vial, G. (2019). Underestanding digital transformation: A review and research agenda. Journal of Strategic Information Systems, 118-144.

Caso Hospital Clinic (2023). Disponible en: https://elpais.com/espana/catalunya/2023-03-30/los-ciberdelincuentes-filtran-de-madrugada-datos-robados-del-hospital-clinic.html.

Caso Meta (2023). Disponible en: https://www.nytimes.com/2023/05/22/business/meta-facebook-eu-privacy-fine.html

Caso Clorox (2023). Disponible en: https://edition.cnn.com/2023/09/18/business/clorox-cyberattack-production-disruption/index.html

ISO 31022 (2020). Risk Management – Guidelines for the management of legal risk. First Edition.

OCDE. https://www.oecd.org/gov/regulatory-policy/irc10.htm.

OCDE (2016). Principios de Gobierno Corporativo de la OCDE y del G20, Éditions OCDE, Paris. http://dx.doi.org/10.1787/9789264259171-es

OECD (2022), *Digitalisation and Corporate Governance: Background note for the OECD-Asia Roundtable on Corporate Governance (October 2022)*, disponible en https://www.oecd.org/corporate/background-noteAsia-roundtable-digitalisation-and-corporate-governance.pdf

Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, aprobado por la Resolución SBS N° 272-2017 de fecha 18 de enero de 2017.

Reglamento para la Gestión del Riesgo Operacional, aprobado por Resolución SBS N° 2116-2009 de fecha 2 de abril de 2009.