El deber de diligencia digital en el gobierno de las sociedades comerciales como práctica de buen gobierno corporativo

The digital duty of care in the corporate governance in companies as corporate governance practice

Gonzalo Gibaja Aucapuri[1]

ORCID Id: https://orcid.org/0009-0001-2424-8727

Jefe Legal Corporativo del Grupo Anders, Perú.

Edison Paul Tabra Ochoa[2]

ORCID Id: https://orcid.org/0000-0002-6126-841X

Docente. Pontificia Universidad Católica del Perú (PUPC) Perú

Fecha de recepción: 20 de enero de 2025 **Fecha de aceptación:** 2 de mayo de 2025

Received: January 20, 2025 **Accepted:** May 2, 2025

DOI: https://doi.org/10.18601/16923960.v24n2.09

1 Abogado por la Pontificia Universidad Católica del Perú. Magister en Derecho de la Empresa con Mención en Gestión Empresarial por la Pontificia Universidad Católica del Perú. Jefe Legal Corporativo del Grupo Anders. Experiencia de más de 8 años experiencia. Correo-e: ggibaja@pucp.pe

2 Doctor Internacional y Máster en Gobierno y Cultura de las Organizaciones por la Universidad de Navarra (España); Magíster en Derecho de la Empresa por la Pontificia Universidad Católica del Perú (PUCP); Abogado y Árbitro. Es profesor universitario, árbitro y consultor en materias relacionadas con empresa y al Derecho Comercial y corporativo. Tiene publicaciones en Inglaterra, España, Suiza, Perú y Ecuador. Dentro de ellas destacan sus libros *Solidaridad y Gobierno Corporativo: una mirada a los organismos internacionales* (JM Bosch, 2015), *Ética y Solidaridad: Perspectivas históricas y normativas* (*Globethics*, 2017) y *Responsabilidad social y gobierno corporativo en la empresa solidaria* (USIL, 2017). Past presidente de la Comisión Regional de INDECOPI-Junín, encargada de resolver controversias sobre Eliminación de Barreras Burocráticas, Competencia Desleal en materia publicitaria y Protección de los Derechos del Consumidor. Fue integrante del Grupo Revisor de la Ley General de Sociedades de 1998. Ha ejercido labor investigadora y docente en prestigiosos centros académicos, como el Instituto Empresa y Humanismo (España), el *National University of Singapore* (NUS), el *Institute Catholique* de Rennes (Francia), la Universidad de Valencia (España), la Pontificia Universidad Católica del Ecuador (PUCE), la Universidad Da Vinci (Guatemala), la Universidad de Piura (Perú), la Universidad San Ignacio de Loyola (Perú) y la Universidad Continental (Perú). En la actualidad es profesor de la Facultad de Derecho y en el Programa de Maestría en Derecho de la Empresa en la Pontificia Universidad Católica del Perú (PUCP). Correo-e: etabra@pucp.edu.pe

RESUMEN

En la medida en que van surgiendo nuevas tecnologías que buscan soluciones eficientes para determinados procesos en las sociedades peruanas, se presentan nuevos riesgos respecto de los cuales no se está prestando mucha atención: los riesgos digitales legales. Estos riesgos requieren ser prevenidos, mitigados y controlados por su administración. De acuerdo con la legislación societaria peruana, la gestión de riesgos es de competencia de los directorios y gerencias generales para el caso de las sociedades anónimas. Para ello, los administradores gestionan dichos riesgos de la compañía según los parámetros que les permite el deber de diligencia. Este deber está relacionado con sus funciones de cuidado y supervisión de las actividades de una sociedad. Sin embargo, el desarrollo de esta obligación no comprende, o no ha contemplado por el momento, gestionar aquellos riesgos provenientes del uso de la tecnología. En ese sentido, el presente trabajo de investigación busca resolver dicho problema desde una perspectiva teórico-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. Así, hablamos del "deber de diligencia digital" que todo órgano de gobierno debe implementar por medio de una política interna de uso de nuevas tecnologías y un adecuado sistema de prevención de riesgos en una sociedad comercial.

Palabras clave: Derecho empresarial, Soluciones Digitales, Deber de Diligencia, Deber de Diligencia Digital, Buen Gobierno Corporativo.

ABSTRACT

As new technologies emerge in pursuit efficient solutions for specific technical processes in Peruvian companies, new risks are also emerging: legal digital risks. These risks must be prevented, mitigated, and controlled by the management. According to Peruvian corporate law, the risk management is the responsibility of the board of directors and general management in case of corporations. To this end, administrators manage the company's risks according to the parameters established by their duty of care. This duty of care relates to their roles of oversight and supervision of the company's activities. However, the execution of this duty does not include, nor has it currently considered, the management of risks derived from the use of technology. In this context, this research aims to fill this gap from theoretical and practical legal perspectives: by adapting the traditional duty of care of directors and CEOs to a newly defined digital duty of care vision – a

subcategory that considers the legal digital risks as part of new technological solutions. For this reason, we introduce the concept of the "digital duty of care", which board of directors and management should adopt through an internal corporate policy on the use of technology and an appropriate risk prevention framework.
Keywords: Corporate Law, Digital Solutions, Duty of Care, Digital Duty of Care, Corporate Governance.

INTRODUCCIÓN

Producto del mercado competitivo en el que se desarrollan las empresas, estas se encuentran en la necesidad constante de 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 generó o aceleró la necesidad de digitalizar los procesos internos y externos de las empresas. No solo las empresas debieron adoptar políticas de trabajo remoto, sino que tuvieron que adaptarse, en muchos casos, a establecer relaciones digitales con sus propios clientes. Así, las innovaciones digitales surgieron como solución ante el problema de la presencialidad. Muchas de las empresas optaron por utilizar *software* o productos digitales que les permitieron no solo adaptarse al contexto virtual, sino que les permitió 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 de naturaleza corporativa: los de tipo digital con repercusión legal. Estos denominados *Riesgos Digitales Legales* son nuevos para cualquier empresa y, al igual que las innovaciones digitales, van cobrando relevancia en el mundo legal actual, ya que representan en muchos casos contingencias bastante elevadas que incluso podrían significar que los accionistas acuerden disolver su empresa.

No cabe duda de que este nuevo tipo de riesgos debe estar considerado como parte de los riegos inherentes de la actividad de una sociedad; sin embargo, surge la duda de cómo 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 normativa. 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. Para Paz-Ares, el concepto de *deber de cuidado* 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[3].

Dicho esto, con base en este deber de cuidado de la administración de una empresa, sus 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 esta investigación, optamos por desarrollar el deber de diligencia digital de la administración de las sociedades, como parte de las normas de buen gobierno corporativo. En esa dirección, nos enfocaremos a responder la pregunta ¿Cómo adecuar el deber de diligencia de la administración de las sociedades al contexto digital actual?

Al respecto, consideramos que el sistema más adecuado como solución a la problemática planteada es el sistema de gobierno corporativo de forma autorregulada, y, en particular, respecto al ejercicio del deber de diligencia de la administración de acuerdo con los intereses propios de la empresa y de sus inversionistas. Cabe señalar que nos apoyaremos en responder preguntas específicas adicionales que nos ayudarán a resolver 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?

Una vez que hemos planteado el tema y el problema, buscaremos argumentar como hipótesis que el deber de diligencia del gobierno de una sociedad, 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, este deber debe contemplar los riesgos inherentes al uso de nuevas tecnologías, para identificarlos, prevenirlos y/o mitigarlos.

Para sostener nuestra hipótesis desarrollaremos (i) el concepto de Riesgo Digital Legal y sus clasificaciones, (ii) el deber de diligencia como concepto propio de las normas de gobierno corporativo, y, finalmente (iii) el cómo es que el deber de diligencia de la administración de las sociedades debe

3 Cándido Paz-Ares, "La responsabilidad de los administradores como instrumento de gobierno corporativo". *Ius et Veritas. Número* 27. 2003, p. 204.

adaptarse al contexto digital actual[4]; así como los beneficios que esto trae tanto para los accionistas, administradores y *stakeholders*.

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

En este apartado desarrollaremos algunos conceptos clave que serán 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 en la actualidad

En la actualidad, la tecnología se ha convertido en una herramienta vital en la empresa, ya que afecta positivamente a la eficiencia en su funcionamiento. Sin embargo, el uso de dicho recurso se ha convertido en una preocupación para su administración[5]. La forma de hacer empresa hoy en día ha cambiado mucho debido a los avances tecnológicos que ofrece el mercado. Recordemos que su finalidad es la de generar valor. En este afán, las compañías buscan ser competitivas en el sector en el que operan; y en dicho proceso, 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[6].

En la misma línea, Giraldo-Ríos 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 a la interconectividad existentes" (2021, p. 7). Dicho esto, tenemos que, toda vez que las empresas están en la búsqueda de una transformación digital para

4 Para efectos del presente trabajo, conforme con lo establecido en el artículo 152º de la Ley General de Sociedades de Perú, toda mención a la administración de una sociedad, empresa o compañía se referirá al directorio o la gerencia general de una determinada sociedad o empresa, en la medida que dichos órganos ostentan la administración de una sociedad. Para el caso de las sociedades comerciales de tipo cerrada consideraremos únicamente al gerente dado que el directorio es facultativo.

5 John Armour, "Corporate Governance and Technological Risks" (2017). Disponible en: https://blogs.law.ox.ac.uk/business-law-blog/blog/2017/02/corporate-governance-and-technological-risks

6 Gregory Vial, "Understanding digital transformation: A review and research agenda", *Journal of Strategic Information Systems*, 2019, pp. 118-119.

mejorar sus procesos y hacerse competitivos en sus sectores económicos, buscarán tomar riesgos al implementar medidas o soluciones tecnológicas que los ayuden a lograr dicho 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[7], PandaDoc[8], 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[9], 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).
v) Sistemas digitales que permiten el análisis de datos de manera masiva (*Data Analytics*).

Asimismo, similares soluciones digitales encontramos en el sector legal. Así, mencionamos a algunas que se utilizan en el ámbito legal:

i) Aplicaciones de almacenamiento de documentos masivos (ej. Worldox[10], NetDocuments[11], entre otros).
ii) Aplicativos que generan contratos de manera automática con algunos datos por completar (Webdox[12], Square[13], entre otros).
iii) Programas que procesan contratos de manera masiva (Ebrevia[14], Kira[15], entre otros).
iv) Espacios digitales que permiten el envío de documentos de manera masiva (Safedrop[16], OneDrive, WeTransfer[17], entre otros).

7 www.docusign.com
8 www.pandadoc.com
9 www.enubes.com
10 https://www.worldox.com
11 https://www.netdocuments.com/ ,
12 https://www.webdoxclm.com/
13 https://squareup.com/
14 https://ebrevia.com/
15 https://kirasystems.com/
16 https://safedrop.com/
17 https://wetransfer.com/

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 su uso requiere de la asignación de recursos y contar con capacitaciones, por lo que nuestro marco 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, estas también traen consigo una gran variedad de riesgos; y muchos de estos, al ser nuevos, no son visibles para la administración de una sociedad sino hasta cuando se materializan y generan, por tanto, una pérdida de valor para la misma. Por ejemplo, Armour menciona los riesgos reputacionales que podrían provenir por el mal uso de la información que posee la compañía[18].

1.2. Riesgos digitales legales

Debemos partir que el concepto de *Riesgo* tiene un significado propio del contexto empresarial (económico-financiero). En esta línea, Soler y otros lo refieren como la posibilidad de sufrir un daño, pero un daño consistente en la pérdida de valor económico[19]. En un similar sentido, el literal ff) del artículo 2º del Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, aprobado por la Resolución de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones N° 272-2017 de fecha 18 de enero de 2017, define al *Riesgo* 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 destacar dos ideas: (i) el riesgo es la probabilidad de ocurrencia de un determinado evento y (ii) la existencia de un impacto negativo o la generación de una pérdida de valor en el objeto de estudio como resultado de la materialización del riesgo en 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 los casos, dichos riesgos son asumidos por 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 carece de visibilidad, y una gran parte de esos riesgos son los riesgos digitales. Este tipo de riesgos son aquellos

18 John Armour, "Corporate Governance and Technological Risks", 2017. Disponible en: https://blogs.law.ox.ac.uk/business-law-blog/blog/2017/02/corporate-governance-and-technological-risks

19 José Soler *et alia*, "Gestión de riesgos financieros: un enfoque práctico para países latinoamericanos". Banco Interamericano de Desarrollo (Washington DC: Banco Interamericano de Desarrollo, 1999, p. 4.

inherentes a la actividad digital o a las soluciones tecnológicas aplicadas a una determinada entidad (empresa). Según Ganguly, "el riesgo digital es 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"[20].

En esa línea, los riesgos digitales serán aquellos riesgos inherentes al uso de soluciones tecnológicas que buscan optimizar procesos internos y externos de una compañía. 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 *ciberataques*. A modo de ejemplo, en 2023, ocurrió un ciberataque al Hospital Público Clinic (España). Un grupo denominado *RandomHouse* logró acceder al sistema informático del hospital y logró extraer datos personales de alrededor de 8.000 usuarios del hospital[21].

Este caso nos permite ejemplificar el significado del riesgo digital como tal. El hospital hizo uso de una solución tecnológica relacionada con el almacenamiento de datos masivos, y dicha solución tecnológica le significó también la probabilidad de que terceros no autorizados accedan su base de datos y puedan filtrar la información 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 ya que generará una pérdida del valor económico para la empresa[22] . Sin embargo, los perjuicios también serán de tipo jurídico, lo cual podría incidir en la sostenibilidad de la compañía.

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[23]. 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[24]. A su turno, Quintás

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

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

22 José Soler *et alia*, "Gestión de riesgos financieros: un enfoque práctico para países latinoamericanos". Banco Interamericano de Desarrollo. Washington DC: Banco Interamericano de Desarrollo, 1999, p. 4.

23 ISO 31022. Risk Management – Guidelines for the management of legal risk. First Edition. 2020, 1.

24 Francisco Cedillo, Humberto Meneses y Miguel Ángel Raygada, M. (2010), "Gestión del Riesgo Legal". *Cengage Learning*. 2010, p. 67.

señala que dichos riesgos son tradicionalmente gestionados por los departamentos de asesoría jurídica de las empresas[25].

A nivel reglamentario en el Perú, el literal h) del artículo 2 del Reglamento para la Gestión del Riesgo Operacional, aprobado por Resolución de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones 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". De esta manera, podemos concluir que la definición de Riesgo Legal está relacionada como la probabilidad de ocurrencia de un evento que, de ser negativo, será perjudicial para la empresa y, consiguientemente, tendrá repercusión legal. Esta repercusión podría materializarse en un incumplimiento de tipo normativo, contractual, o por la ejecución de una sentencia o laudo arbitral desfavorable para la empresa.

En este orden de ideas, y teniendo en claro la definición de Riesgo, Riesgo Digital y Riesgo Legal, podemos conceptuar el de 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 asociado al 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 Clinic de Barcelona antes mencionado, podemos afirmar de que estamos ante un Riesgo Digital Legal, porque 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 también a nivel contractual con los pacientes.

Este tipo de riesgos requerirá que la administración de toda compañía se cerciore de que la organización refuerce sus sistemas de supervisión y toma de decisiones para mitigar su comisión. Asimismo, el uso de la tecnología

25 Juan Quintás, "La gestión del riesgo normativo en el sistema financiero". *Revista Gallega de Economía*. 2007, p. 7.

en este proceso podría degenerar en el uso de sistemas informáticos en el cual los administradores tengan una menor injerencia o control[26]. Como, por ejemplo, el uso de inteligencia artificial en la búsqueda y la recopilación de la información puede generar información inexacta o errónea, lo cual influirá en el trabajo tanto de los directorios como de las gerencias y, eventualmente, un perjuicio a los intereses de los inversionistas o accionistas.

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 luego referirnos a ellos cuando busquemos plantear una solución para los mismos. Para esta investigación, clasificaremos los Riesgos Digitales Legales en dos (2) tipos: (i) Riesgos Digitales Legales Internos y (ii) Riesgos Digitales Legales 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 compañía. Estamos hablando de los intereses de sus accionistas y directores, así como de sus propios como organización. Dentro de los principales Riesgos Digitales Legales Internos (de gobierno) están los siguientes:

i) Suplantación de identidad en sesiones virtuales de accionistas y directores

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 precisa 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[27].

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 de una sociedad anónima, lo que podría no solo afectar

26 John Armour, "Corporate Governance and Technological Risks" (2017). Disponible en: https://blogs.law.ox.ac.uk/business-law-blog/blog/2017/02/corporate-governance-and-technological-risks

27 Luis Cebriá, "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. 2022. https://www.youtube.com/watch?v=0NKLF0AOW_M

los datos sensibles propios de la empresa (información comercial sensible), sino que podría afectar la información personal propia de los accionistas o directores de la empresa.

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

Para Cebriá[27], otro riesgo está identificado con la virtualidad de las juntas de accionistas y se refiere al acceso restringido que puede significar la virtualidad de sus sesiones. Por ejemplo, los fallos del sistema informático de la compañía que podrían, eventualmente, limitar el ejercicio del voto, la participación del socio o accionista y el trabajo del directorio.

iii) Vulneración de datos comerciales sensibles para la empresa

Finalmente, existe un riesgo de 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*[29]). 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 masivo, las cuales se utilizan para la gestión y análisis de la información de una empresa.

Sin embargo, esta facilidad tecnológica genera 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[30]. En agosto de 2023, la empresa Clorox se vio afectada por un ataque en sus sistemas de tecnología internos lo 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

28 *Ídem.*

29 www.sap.com

30 Empresa dedicada a la fabricación y comercialización de productos de limpieza. Caso Clorox, 2023. Disponible en: https://edition.cnn.com/2023/09/18/business/clorox-cyberattack-production-disruption/index.html

proveedores de esta, e incluso de los mismos trabajadores de la empresa. Dentro de los principales Riesgos Digitales Legales Externos (operacionales) están los siguientes:

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

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. Sin embargo, existe el riesgo de que, ante un desperfecto del sistema informático 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 de Barcelona (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[31] 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 fueron afectados, lo que generó efectos adversos no solo en la misma compañía, sino en futuras reclamaciones que puedan hacer los usuarios.

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

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

El uso de plataformas digitales que sirven de apoyo en la gestión masiva de clientes (*Customer Relationship Management*), si bien facilita la gestión de atención al usuario en empresas con clientela masiva, no siempre significa que dicha plataforma sea adecuada en relación con el tipo de servicio que brinda la empresa. Ante este escenario, se pueden generar riesgos asociados a reclamos de parte de los consumidores por una atención inadecuada, lo cual podría generar reclamos ante autoridades que, eventualmente, generarían sanciones económicas 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 para garantizar que el usuario pueda tener atención personal por parte del proveedor en caso este utilice sistemas de atención automatizada.

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, haremos una descripción de las normas de gobierno corporativo e incidiremos en su concepto y naturaleza. Posteriormente, elaboraremos un concepto que nos permita discutir en relación con el deber de diligencia de los administradores en una sociedad mercantil. Por último, 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 esta parte de la investigación, 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 usado 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[32].

En esa misma línea, la Organización para la Cooperación y el Desarrollo Económico (OECD) define al *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"[33]. Por su parte, Baldassare señala que el *soft law* 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[34].

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[35].

2.1.2. Las normas de gobierno corporativo

Según Armour, la práctica del gobierno corporativo está relacionada con los mecanismos empleados para asegurar o garantizar que la administración de

32 Michelle Cin, "The soft law approach: Commission rulemaking in the EU's state aid regime" *Journal of European Public Policy*, 2001, pp.193-194.

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

34 Pastore Baldassare. "Soft Law y la teoría de las fuentes del derecho" *Universita degli Studi de Ferrara*, 2014, p. 76.

35 Pastore Baldassare, "Soft Law y la teoría de las fuentes del derecho", p. 77.

la empresa toma en cuenta los intereses de sus inversionistas o accionistas[36]. Sus normas son un ejemplo de aceptación e integración de normas *soft law* y vienen siendo implementadas e incorporadas en la regulación societaria nacional e internacional, en diferentes mercados. Para entender su naturaleza y concepto, 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).

Al respecto, Hundskopf[37] 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. Como señala Martínez, el problema de agencia es un problema que siempre se encuentra presente en toda sociedad, toda vez que 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[38].

Dicho problema de agencia crea una necesidad de regulación por parte de los ordenamientos jurídicos que prevengan 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 por lo 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 compañía debe seguir y que le permita gestionar este conflicto de intereses entre administración y accionistas de forma eficiente. 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

36 John Armour, "Corporate Governance and Technological Risks", 2017. Disponible en: https://blogs.law.ox.ac.uk/business-law-blog/blog/2017/02/corporate-governance-and-technological-risks

37 Oswaldo Hundskopf, "Facultades de la junta general de accionistas" *Diálogo con la jurisprudencia Gaceta Jurídica*, Tomo 38, 2001, p. 57.

38 Juan José Martínez, "Apuntes sobre el rol del derecho frente al problema de agencia en las organizaciones" *Themis N° 46*. 2003, p. 281.

(*stakeholders*)[39]. También permite la creación de una estructura mediante la cual se fijan los objetivos de una empresa y cómo será la forma de alcanzarlos.

Sin embargo, hay que precisar que dichos lineamientos de gobierno corporativo no son de ninguna forma estáticos. Como normas de *soft law*, dichos lineamientos evolucionan durante el tiempo y se acomodan a las necesidades puntuales de cada empresa. 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[40]. 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[41].

Por su parte, Tabra sustenta que el gobierno corporativo requiere de normas de naturaleza "facilitadora" y "preventiva" de la actividad económica de la empresa en el mercado (2019, p. 69). A su turno, Payet asume el concepto elaborado por Cadbury[42] y define al gobierno corporativo como un conjunto reglas e instituciones que determinan la forma de conducción, dirección y administración de las empresas (2003, p. 78). Asimismo, constituye el objeto del derecho societario ya que tiene relación con la organización y el funcionamiento de las sociedades, las relaciones entre sus socios, las relaciones socios-administradores, los vínculos entre la sociedad y sus acreedores y otros terceros (2003, p. 78).

En ese orden de ideas, podemos definir al gobierno corporativo como: (i) normas de *soft law* (guías, estándares, principios) no obligatorias de cumplimiento, salvo excepciones de normas específicas sectoriales; (ii) medio de 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 en 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[43].

39 OCDE, "Principios de Gobierno Corporativo de la OCDE y del G20", *Éditions OCDE*, 2016, 9. http://dx.doi.org/10.1787/9789264259171-es

40 Elena Pérez Carrillo, "Gobierno corporativo comparado" *Gobierno corporativo y responsabilidad social de las empresas*. Marcial Pons, 2009, p. 54.

41 *Ídem*.

42 Para Lord Cadbury, el gobierno corporativo es el sistema por la cual las compañías son administradas y controladas, (Hopt, 2011, p. 7).

43 De acuerdo con Hopt, el gobierno corporativo se manifiesta de varias formas. Por ejemplo, en empresas que listan en bolsa, las empresas familiares, empresas de propiedad estatal, personas jurídicas sin fines lucrativos (asociaciones) y las fundaciones. Debido a la crisis financiera, las empresas bancarias y compañías intermediarias han empezado a tener atención (2011, p. 10).

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, evaluaremos su relevancia de su implementación y adecuación en las sociedades comerciales en donde no resulta obligatorio hacerlo. 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 coincidir en la medida que tanto accionistas como administradores buscan la rentabilidad de la compañía en muchas ocasiones estos intereses no coinciden y se enfrentan a situaciones de gobernabilidad y funcionamiento.

La pugna entre los intereses de administradores frente a accionistas significa, 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 seleccionar gerentes o administradores más hábiles y responsables frente a los inversionistas, los cuales serán debidamente incentivados para cumplir con tal fin[44]. Así, un adecuado sistema de gobierno permitirá no solo reducir los costos de agencia, sino que se contará con normas claras que permitirán delegar las facultades de gestión y administración en terceros especializados. Como consecuencia de ello, una compañía incrementará sus posibilidades de resguardar los intereses de sus accionistas o inversores.

Por último, hay que considerar que las normas de gobierno corporativo han sido bastante influidas por parte de la situación pandémica que se vivió recientemente. Según 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 sujeta a rigurosas evaluaciones como sería en una situación normal[45]. En ese escenario de contar con una digitalización forzada, correspondía la necesaria adaptación de las normas de gobierno corporativo y el deber de los administradores. De esta manera emergieron los principales retos del gobierno corporativo postpandemia, como: (i) la participación remota (digital) en sesiones de junta general de accionistas, y (ii) los riesgos de seguridad digital y el papel de la administración de la empresa sobre ello[46].

Por ello, consideramos que no solo la administración de la empresa tiene la necesidad de adaptarse a los nuevos Riesgos Digitales Legales, sino también, las normas de gobierno corporativo que, dada su constante evolución,

44 Jean Tirole, "El Gobierno Corporativo". *Academic Journal N° 44*. 1999, p. 10.

45 OECD. "Digitalization and Corporate Governance: Background note for the OECD-Asia Roundtable on Corporate Governance" 2022, p. 4. https://www.oecd.org/corporate/background-noteAsia-roundtable-digitalisation-and-corporate-governance.pdf

46 *Ibídem*.

se deben adaptar para que cumplan con su objetivo de 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 en la administración y funcionamiento en la empresa y sus retos en un contexto digital, conviene revisar el concepto de deber de diligencia como una norma que forma parte de las normas de gobierno corporativo.

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 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 que desplieguen cierto nivel de pericia, en la gestión o supervisión de la empresa, a fin de maximizar la producción de valor[47].

Por su parte, 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[48]. Para Hernando Cebría, el deber de diligencia es un modelo general y objetivo de conducta que posee relación con la expectativa de actuación de todo "ordenado comerciante"[49]. Dicha conducta se debe ejercer de acuerdo con criterios de "racionalidad" y "prudencia", con "conocimiento informado", de modo "honesto", con "orientación al interés social" y con respecto al "interés general" y la "legalidad"[50].

Por ende, el concepto del deber de diligencia puede estar definido como: (i) un deber impuesto por normas de *hard law* (legislación societaria) y

47 Cándido Paz-Ares, "La responsabilidad de los administradores como instrumento de gobierno corporativo". *Ius et Veritas. Número* 27. 2003, p. 204.

48 Uría Menéndez, "Guía práctica sobre deberes y régimen de responsabilidad de los administradores en el ámbito mercantil". Madrid. 2015, p. 7. https://www.uria.com/documentos/publicaciones/4558/documento/guia_UM.pdf?id=5679

49 Luis Hernando Cebriá, El deber de diligente administración en el marco de los deberes de los administradores sociales. Marcial Pons. 2009, p. 50.

50 Ídem.

complementado con 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; (iii) dicho deber significa una norma de conducta exigible a los administradores respecto a los accionistas y a la sociedad en general, y (iv) conforme a los criterios exigidos a todo "ordenado comerciante".

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[51]. Sin embargo, esta posibilidad genera a su vez problemas de agencia en la medida que la administración puede recaer en terceros no socios o accionistas que, a su vez, podrían priorizar sus propios intereses en perjuicio de la sociedad. Esto se debe a que nos encontramos ante la necesidad de requerir el ejercicio de deberes decisorio-empresariales. A diferencia de las obligaciones legales y estatutarias que demandan a los administradores a cumplir con la ley o el estatuto, los deberes decisorio-empresariales se basan en el desarrollo de la diligencia, fidelidad y, en menor grado, de la lealtad y secreto a través de códigos de conducta[52] o, lo que es lo mismo, a través de instrumentos autorregulatorios.

En este contexto, consideramos que la importancia del deber de diligencia descansa en su configuración legal como una pauta o regla de conducta y como una fuente de obligaciones[53]. En el primer caso, según Hernando Cebría, la diligencia se configura como "el modo según el cual el administrador habrá de ejecutar una determinada actividad, y para su verificación se ha atender a los medios que se sirva para tomar conocimiento y adquirir un juicio fundado respecto de las decisiones a adoptar"[54]. Según esta afirmación, el comportamiento de todo gestor no se evalúa de acuerdo con el

51 José Antonio Payet, "Empresa, gobierno corporativo y derecho de sociedades: Reflexiones sobre la Protección de las Minorías". *Themis N° 46*. 2003, p. 86.

52 Luis Hernando Cebriá, El deber de diligente administración en el marco de los deberes de los administradores sociales. Marcial Pons. 2009, p. 60.

53 Uría Menéndez, "Guía práctica sobre deberes y régimen de responsabilidad de los administradores en el ámbito mercantil". Madrid. 2015, p. 7.

54 Luis Hernando Cebriá, 2009, p. 53.

resultado obtenido durante su gestión sino por la calidad del proceso que se realizó para adoptar la decisión[55].

Por otra parte, la diligencia como conjunto de deberes significa que el cargo de administrador implica cumplir con deberes afines, como son el ejercicio efectivo del cargo (compromiso con el cumplimiento de funciones), la vigilancia o supervisión (control de la actividad de la sociedad) y la información (utilidad para el ejercicio del cargo)[56]. De esta forma, el ejercicio de la diligencia contribuirá con la reducción de los costos de agencia, ya que desincentivará cualquier incorrecta actuación de los administradores de la sociedad y la alineará con los intereses de los accionistas y de la empresa en general.

2.2.3. El deber de diligencia digital

Como ya mencionamos, los retos actuales a los que se enfrenta el gobierno corporativo requieren de la adaptación de dichos lineamientos a las nuevas soluciones tecnológicas para que sean implementadas y utilizadas por las empresas. Tanto la digitalización de las sesiones de junta general de accionistas como los riesgos de seguridad digital son Riesgos Digitales Legales tanto de gobierno como operativos respectivamente. En este escenario, tomando en cuenta los estudios elaborados por la OECD y considerando 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".

Así, cuando nos referimos al deber de diligencia "digital" hacemos referencia a aquel deber de diligencia de la administración de una sociedad que posee particular interés en los Riesgos Digitales Legales. De esta manera, a medida que el deber de diligencia abarque el compromiso de cuidado de la administración frente a posibles riesgos o amenazas, tanto ordinarios como a aquellos vinculados con las nuevas tecnologías, obligará a sus órganos de gobierno a implementar medidas de seguridad que aseguren tanto el bienestar de la compañía como el de sus grupos de interés. Por ejemplo, el deber de lealtad aplicado a medios tecnológicos, como la inteligencia artificial, deberá de garantizar de que su uso no beneficie a algunos inversores o administradores de la empresa sino a toda la sociedad en sí.

Las medidas que surjan para dar cumplimiento con este deber de diligencia digital pueden ser muchas y de diferente clase dependiendo el tipo de empresa (modelo, sector o tamaño). Sin embargo, consideramos importante

55 Para el caso peruano, el artículo 171º de la Ley General de Sociedades establece que el ejercicio del cargo de directorio se hace de acuerdo con la "diligencia de un ordenado comerciante".

56 Uría Menéndez, "Guía práctica sobre deberes y régimen de responsabilidad de los administradores en el ámbito mercantil". Madrid. 2015, p. 7.

precisar que el deber de diligencia digital debe priorizar la gestión de los riesgos tecnológicos por parte de su administración. Por ende, sus estatutos o políticas de gobierno deben incorporar este deber que les permita contratar al personal idóneo para ejercer dicho deber[57]. De igual forma, ante los casos de incumplimiento al deber de diligencia digital se debe determinar al responsable[58].

2.3. Plan de gestión de riesgos

En el ámbito corporativo, cualquier riesgo, sea legal o de otro tipo, debe ser objeto de prevención. De esta manera se logrará disminuir las posibilidades de su materialización y, por ende, perjudicar los intereses de la compañía. En el ámbito financiero peruano, la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (SBS) señala la necesidad de que su administración implemente un proceso 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[59].

En ese sentido, la idea de una adecuada administración integral de contingencias que se aplique a la prevención de riesgos digitales debe contemplar la implementación de un proceso de gobierno. Este proceso debe contar con las herramientas tecnológicas que permitan a toda compañía contar con la identificación de los riesgos digitales, la asignación de responsabilidades, y el establecimiento de formas de control de estos. Con la implementación y uso de este proceso, los administradores de la sociedad podrán contar con una sólida herramienta que les permitirá acreditar el cumplimiento de su deber de debida diligencia. Esto sin perjuicio de las sesiones de directorio y/o plana gerencial en la que los administradores deberán acreditar el ejercicio de su deber.

57 Por extensión, esta propuesta debe aplicarse a los órganos de apoyo del gobierno de una sociedad. Destacamos los casos del secretario corporativo y al gerente legal o *general counsel*. En el caso del secretario, resulta importante porque le permitirá aconsejar a los integrantes del directorio de forma idónea durante las sesiones. Por su parte, el gerente legal estará en mejor posición de asesorar al área de nuevas tecnologías e innovación.

58 Para el caso peruano, el artículo 177° de la Ley General de Sociedades establece la responsabilidad subjetiva en el caso de los administradores (director y gerente). Su responsabilidad ante la sociedad, los accionistas y los terceros es ilimitada y solidaria por los daños y perjuicio que causen sus acuerdos o actos contrarios a la ley, al estatuto o por los realizados con dolo, abuso de facultades o negligencia grave.

59 Superintendencia de Banca y Seguros y Administradoras Privadas de Fondos de Pensión – SBS, Gestión Integral de Riesgos. Resolución S.B.S. N° 272 -2017.

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

Podemos partir de la idea de que 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 su ejercicio 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 apartado buscaremos sustentar nuestra hipótesis que fue planteada al inicio de esta investigación: la adecuación del deber de diligencia a un deber de diligencia digital. Esta adecuación le permitirá a la administración de una sociedad identificar, prevenir y mitigar sus riesgos de tipo jurídico y digital. Para estos efectos, se propondrán dos medidas para que toda administración de una sociedad implemente medidas prácticas que le permitan cumplir con el deber de diligencia digital.

La primera medida estará relacionada con proponer algunas recomendaciones para la administración de una sociedad, respecto a la digitalización de las sesiones de la junta general de accionistas y del directorio; y, la 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 se visibilizará la probabilidad de ocurrencia de los Riesgos Digitales Legales y, además, permitirá la prevención y/o mitigación de dichos riesgos lo cual permitirá 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 y las sesiones de directorio

La primera medida propuesta es establecer determinadas políticas internas que permitan una adecuada celebración de juntas generales de accionistas y directorio de manera virtual. En esa misma línea, la OECD propuso 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[60]. Estas propuestas

60 OECD, "Digitalization and Corporate Governance: Background note for the OECD-Asia Roundtable on Corporate Governance" 2022, p. 10. https://www.oecd.org/corporate/backgroundnoteAsia-roundtable-digitalisation-and-corporate-governance.pdf

incluyeron las sugerencias elaboradas en el *The Principles and Best Practices for Virtual Annual Shareowner Meetings* del 2018[61].

De acuerdo con este documento, los cinco principios clave que la administración de una sociedad debería tomar en cuenta a la hora de convocar y celebrar sesiones virtuales de junta de accionistas son (i) valoración y fomento a una mayor participación de los accionistas o socios en las reuniones anuales; (ii) promoción de un trato equitativo e igualitario a los socios o accionistas participantes; (iii) facilitación de un mayor compromiso entre los accionistas y los directores de la compañía; (iv) difusión detallada de los beneficios de celebrar una sesión de junta virtual, y (v) uso de las reuniones virtuales como un medio para proporcionar un espacio de diálogo abierto para los accionistas[62].

Adicionalmente, dicho documento propone algunas recomendaciones que recogemos como válidas y aplicables para contar con una adecuada política de sesiones virtuales de junta general de accionistas: (i) garantía de igualdad de acceso; (ii) creación de reglas de conducta; (iii) creación de pautas de tiempo razonables para regular las intervenciones de accionistas; (iv) implementación del servicio de soporte técnico en línea, y (v) creación de un servicio de archivo de reuniones virtuales en caso se requiera revisar alguna información[63].

En ese orden de ideas, podemos concluir que, a fin de contar con una adecuada política de celebración de juntas de accionistas virtuales, se debe considerar 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. De esta manera el ejercicio de sus derechos en el ámbito digital estará garantizado.

Por ejemplo, el Grupo Credicorp Ltd., uno de los principales grupos económicos del Perú dedicado al sector financiero, realiza sesiones de junta general de accionistas no presenciales (virtuales) desde 2020[64] hasta la actualidad[65]. En los avisos de notificación se establece que los accionistas del grupo podrán asistir y votar en la sesión de junta de forma no presencial. Para participar en la asamblea podrían utilizar un dispositivo inteligente (computadora, teléfono inteligente o *tablet*). También el voto por poder (Proxy) podrán hacerlo usando el servicio de voto en línea[66]. El uso de este

61 Documento disponible en: https://www.broadridge.com/_assets/pdf/broadridge-vasm-guide.pdf

62 OECD, "Digitalization and Corporate Governance: Background note for the OECD-Asia Roundtable on Corporate Governance" 2022, p. 11.

63 *Ídem*.

64 https://credicorp.gcs-web.com/static-files/b85727ac-bdf9-4911-9889-ef448ca3167a

65 https://credicorp.gcs-web.com/static-files/bde29926-4a43-4bd8-891a-db599b7d9e2e

66 También Intercorp Financial Services utiliza el sistema de participación no presencial: https://ifs.com.pe/documents/d/ifs/ifs-guia-para-junta-general-accionistas-2023-pdf.

mecanismo tiene relación con la política de seguridad en la información que tienen todas las subsidiarias del grupo. Dicha política establece que los clientes y usuarios deben seguir una serie de recomendaciones para prevenir que su información se usada para robos, fraudes y otros delitos[67].

Por otro lado, Alicorp S.A.A., una empresa líder en el sector de consumo masivo en Perú, también realiza sus sesiones de junta general de accionistas de manera virtual (a través de la plataforma *Microsoft Teams*). A estos efectos, la administración de Alicorp S.A.A. emite documentos informativos mediante los cuales reglamenta el proceso para llevar a cabo las sesiones no presenciales[68]. Cabe anotar que dicho documento no solo regula la estructura que tendrá la junta no presencial (registro de accionistas, participación, voto, entre otros), sino que regula un mecanismo propio de verificación de la identidad de sus participantes, lo que hace más robusto su sistema de prevención de Riesgos Digitales Legales relacionados con ese aspecto.

Por último, cabe destacar también la adaptación a este tipo de regulación digital por parte de Corporación Aceros Arequipa S.A., empresa peruana dedicada a la producción y comercialización de acero. Al igual que Credicorp Capital y Alicorp, Aceros Arequipa cuenta con un documento informativo que regula sus sesiones de junta general de accionistas no presenciales (a través de la plataforma "*iQuorum*")[69]. Dicho documento reglamenta no solo el mecanismo de acreditación de los accionistas, sino también la forma de participación en la sesión, la toma de decisiones, e incluso brinda pautas particulares sobre el uso y acceso a la plataforma digital mencionada.

Como hemos podido advertir, la utilización de este tipo de políticas permite minimizar la posibilidad de materialización de Riesgos Digitales Legales que mencionamos en nuestro primer capítulo (Riesgos Digitales Legales de Gobierno). A manera de ejemplo, contar con un adecuado mecanismo de identificación de accionistas (validación de identidad con video y documentación que lo respalde), previene casos de suplantación de identidad que podrían sufrir los participantes de la sesión virtual. Asimismo, tener claridad sobre el funcionamiento de la plataforma digital (formas de acceso y reglas de observancia para la participación en la plataforma), previene el riesgo de una vulneración del derecho de los accionistas a la participación y voto en junta general de accionistas.

Ahora bien, por el lado de los directorios, consideramos que el deber de diligencia digital debe de estipular también la responsabilidad por el uso de la tecnología para el proceso de toma de decisiones. Por ejemplo, cuando

67 https://www.credicorpcapital.com/Paginas/SDI.aspx

68 https://www.alicorp.com.pe/media/calls/documento_informtaivo_junta_general_de_accionistas.pdf

69 https://investors.acerosarequipa.com/storage/items-de-bloques/March2025/Kkq57L3zdu3a-nUcbwD6O.pdf

discutimos la aplicación de la inteligencia artificial[70], las responsabilidades de un directorio se evaluarán según cada caso concreto y de acuerdo con los tipos de inteligencia artificial que se utilizaron para el ejercicio de sus competencias. Por ejemplo, la valoración de los procesos de adopción de decisiones deberá de considerar si la información proporcionada por la IA era razonablemente suficiente o no. Según Chamorro, su uso eliminaría la "diferenciación" y la "competitividad" de una sociedad que surge por el equipo gestor que posee[71].

En el caso de temas de alta complejidad que requieran el pronunciamiento de la administración, se deberá evaluar si el aplicativo de inteligencia artificial cuenta con la capacidad suficiente de generar información cierta y precisa. Asimismo, su uso podría generar una dependencia de las evaluaciones o predicciones que hagan sobre determinada decisión. Otros potenciales riesgos serían que las aplicaciones no están adecuadas a los marcos legales, éticos y económicos; o que no se cuente con la formación suficiente para usar la herramienta de forma correcta[72].

De superarse estos cuestionamientos, consideramos que el uso de sistemas IA fortalecería el grado de diligencia digital que se requiere de toda administración. Aun así, creemos que los órganos de gobierno de toda sociedad asumirán la responsabilidad por su uso, ya que el deber de diligencia digital les exigirá conocer los riesgos de aplicar la tecnología y dejar su uso en manos de las máquinas. Por ello, iniciativas como la creación de comités de tecnología y digitalización o la inclusión de expertos en el uso de tecnología contribuirían a un buen uso de la IA y, por ende, a facilitar el correcto deber de diligencia digital por parte de los directorios y gerencias.

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) que incluya a los Riesgos Digitales Legales dentro de ese esquema. Para lograr esta medida,

70 Para más Desarrollo, revisar el trabajo de Florian Möslein, Möslein, Florian, "Robots in the Boardroom: Artificial Intelligence and Corporate Law" (September 15, 2017). in: Woodrow Barfield and Ugo Pagallo (eds.), Research Handbook on the Law of Artificial Intelligence, Edward Elgar, (2017/18, Forthcoming), Available at SSRN: https://ssrn.com/abstract=3037403 or http://dx.doi.org/10.2139/ssrn.3037403

71 María Chamorro, "La aplicación de sistemas de inteligencia artificial en el seno del órgano de administración de las sociedades de capital". *Revista de Derecho de Sociedades* No 59. 2020. Adicionalmente, para la autora, la toma de acuerdos en el ámbito societario requiere de la experiencia, el instinto, la destreza y la perspicacia que es propio de los gestores humanos.

72 *Ídem*.

consideraremos el uso de la herramienta estratégica desarrollada por Peter Kurer denominada *Strategic Legal Risk Management* o SLRM.

Gracias a su uso, Kurer precisa que la gestión de este tipo de riegos debe generar un círculo rotativo que involucre los siguientes pasos: (1) hacer visible el riesgo legal; (2) comprender las causas o motivos de estos riesgos; (3) valorar dichos riesgos y, en especial, dar una valoración económica a la materialización de los daños; (4) adoptar adecuadas decisiones sobre la forma ideal de mitigar o gestionar el riesgo; (5) comunicar de tales decisiones a los grupos de interés relevantes de la empresa; (6) hacer cumplir los acuerdos dirigidos a mitigar y gestionar estos riesgos, y (7) lograr el control o mitigación de los riesgos[73].

Bajo los lineamientos de la herramienta antes indicada, sugerimos la adaptación de los sistemas de *compliance* o prevención de riesgos de las empresas a uno donde se incluyan los riesgos tecnológicos. En otras palabras, que permita identificar, entender, valorar, decidir, mitigar y controlar los Riesgos Digitales Legales. Ahora bien, la inclusión de los Riesgos Digitales Legales en los sistemas de prevención de riesgos de una sociedad requerirá que se realice un análisis previo del tipo de actividad que desarrolla la empresa. Esto permitirá conocer el grado de nivel de exposición a la que se enfrenta. Por 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 digitales en concordancia con el deber de diligencia digital debe, adecuadamente y según los niveles de exposición, incluir un mapa de riesgos en virtud del cual se establezcan los siguientes criterios:

i. Nombramiento de un encargado del proceso: 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. Definición de la noción de Riesgo Digital Legal: se le dará una denominación al Riesgo Digital Legal identificado (ej. Datos personales, Datos sensibles de la empresa, entre otros).
iii. Descripción del contenido conceptual del Riesgo Digital Legal: se incluirá una descripción completa del Riesgo Digital Legal que se ha identificado (ej. Acceso por parte de terceros no identificados ajenos

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

a la sociedad a los datos sensibles de la sociedad, datos comerciales, datos de trabajadores, datos de clientes, entre otros).

iv. Creación de modelo que materialice el Riesgo Digital Legal: 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. Mención de la probabilidad de ocurrencia: se indicará cuál 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. Calificación de la noción de Impacto: de la mano con el punto anterior, se evalúa 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. Definición del riesgo inherente: 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. Establecimiento del mecanismo de control: se indicará cuál 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. Indicación del tipo de control: se indicará de qué tipo de control se trata (ej. Preventivo, de detección, de mitigación, entre otros).

x. Mención del grado de efectividad: se indicará el nivel 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 es el mecanismo de control que ha planteado para la prevención o mitigación del Riesgo Digital Legal identificado (ej. 30%, 40%, 80% de efectividad).

xi. Determinación del riesgo Residual: se calculará cuál 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).

De esta manera, un deber de diligencia digital como el que proponemos no solo encuentra su solución en un tema de visibilidad del problema, sino que 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 permitirán 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 hemos desarrollado antes, existen Riegos Digitales Legales Internos cuya materialización puede impactar directamente a los intereses de los socios o accionistas de una determinada sociedad comercial. Dentro de los principales riesgos identificados, rescatamos aquellos cuyo impacto podría causar una desprotección de los datos personales de los socios o accionistas. 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, no solo evitará o mitigará sus efectos, sino que creará un ambiente seguro para la toma de decisiones de los socios o accionistas.

De igual forma, el uso de la tecnología para facilitar las sesiones de junta de accionistas facilitará el ejercicio de sus derechos tanto políticos como económicos. Así, el uso correcto del *blockchain* asegurará podría constituirse en ese instrumento de protección de derechos, ya que garantizará la identificación de los accionistas, así como cautelará que puedan participar y votar en las sesiones. Por último, resaltamos la importancia de cuidar la sostenibilidad del negocio de la empresa, así como su permanencia en el mercado.

3.4. Beneficios para los administradores de la sociedad

La adecuación e implementación del sistema de prevención de riesgos a uno que incluya a los Riesgos Digitales Legales permitirá a la administración de la sociedad comercial contar con las herramientas adecuadas para prevenir dichos riesgos, o, en caso de ocurrencia, mitigar el impacto de estos, siendo también una herramienta adecuada para deslindar de alguna responsabilidad

que se pueda imputar a la administración. Recordemos que uno de los principales intereses de los administradores de la sociedad es mantener viva la sociedad, por lo que, protegiendo sus propios intereses, estarán evitando la ocurrencia de riesgos que le afecten de forma económica.

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 una vulneración de sus sistemas 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 Comisión Federal de Comercio (FTC) de Estados Unidos[74]. Otro caso reciente es el de *Capital One,* en 2021, que llegó a un acuerdo extrajudicial por 190 millones de dólares por la violación de datos personales e información financiera de sus clientes y pagó ,una multa de 80 millones de dólares[75] al supervisor federal.

De lo expuesto, podemos afirmar que, si aquellas compañías hubieran incorporado la noción de los Riesgos Digitales Legales inherentes a su giro de negocio, habrían contado con un sólido plan de gestión de contingencias de riesgo digital de tipo jurídico. Y este plan habría cumplido con su rol preventivo o mitigador del Riesgo Digital Legal con lo cual se pudo haber evitado incurrir en una infracción y, posterior, multa administrativa que afecte su patrimonio. Asimismo, esta noción puede facilitar el ejercicio de las funciones de los directores, en especial de los independientes, así como la creación de comités de tecnología.

3.5. Beneficios para terceros o *stakeholders* o grupos de interés de la empresa

Por último, conviene resaltar el beneficio de nuestra propuesta respecto de terceros relacionados con la sociedad: los llamados *stakeholders*. Aunque lo hemos hecho, consideramos que merecen un tratamiento propio. Al respecto, Freeman hace referencia a los *stakeholders* como aquel grupo de personas como clientes, empleados, proveedores, comunidades, financistas, entre otros, que tienen una relación directa con los intereses de la sociedad[76]. Asimismo, Mayer sostiene que cuando las sociedades comerciales tienden a conside-

74 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

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

76 Edward Freeman, Robert Phillips, "Stakeholder theory: A libertarian defense", *Business Ethics Quarterly*, 2002, p- 333.

rar o cautelar los intereses de sus *stakeholders*, el resultado es que mejorará las relaciones comerciales con sus clientes, empleados más comprometidos, proveedores confiables y ambientes sostenibles[77].

La implementación de la noción de los Riesgos Digitales Legales permitirá identificar los potenciales riesgos digitales que podrán perjudicar a cada uno de los *stakeholders* y trazará un plan de prevención. Gracias a ello, costos como los reputacionales o económicos se reducirán y, por ende, generarán mayores beneficios económicos tanto para la compañía, los inversionistas como para el resto de sus grupos de interés.

CONCLUSIONES

La noción de Riesgo Digital Legal se desarrolla en un contexto de constante transformación digital empresarial que obliga a las compañías a desarrollar procesos que les permita adecuarse a dichos cambios para mantenerse competitivas en el mercado o sector donde operan. Así, este tipo de riesgos se refieren a la probabilidad de ocurrencia de un evento determinado por el uso de tecnologías y que puede producir efectos negativos o perjudiciales para una empresa. Su materialización tiene repercusión legal bajo la forma de incumplimiento de una norma, contrato, sentencia judicial o laudo arbitral.

La clasificación de los Riesgos Digitales Legales se divide en Internos (de gobierno) y externos (operacionales), lo cual dependerá de los intereses que se vean afectados. 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).

Las normas de *soft law* son directrices, guías, códigos, entre otros, que buscan resolver problemáticas o vacíos legales que no necesariamente son uniformes

77 Colin Mayer, "Shareholderism versus Stakeholderism – A Misconceived Contradiction". *The Illusory Promise of Stakeholder Governance* 2020, pp. 1-2.

a nivel internacional. Se caracterizan por no tener fuerza vinculante, por lo que también se les denomina como *non-binding agreements* o normas blandas. También pueden aplicarse de forma vinculante en algunos sectores, como el bancario o financiero. La implementación de normas que gestionen o prevengan los riesgos asociados al uso de las tecnologías se hará a través de las normas de gobierno corporativo y tanto su implementación como su cumplimiento se harán de forma voluntaria. De esta manera, la compañía exigirá responsabilidades a sus órganos de administración sobre la gestión de riesgos digitales, lo cual generará la discusión sobre el concepto de Riesgos Digitales Legales.

Mediante el ejercicio del deber de diligencia, los administradores de la empresa tienen la responsabilidad de 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. Su adaptación al contexto digital implica la exigencia de un deber de diligencia "digital" que busca 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. La implementación de un adecuado plan de gestión de riesgos es un mecanismo ideal adecuado para cumplir con el deber de diligencia de los administradores de la empresa.

El ejercicio del deber de diligencia digital puede darse a través de 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.

Las empresas deben implementar un sistema de prevención de riesgos que contemple los Riesgos Digitales Legales, lo que permitirá ejercer control por medio de mecanismos de prevención y mitigación eficientes, dependiendo de las actividades propias de la sociedad. La visibilidad de estos riesgos surgirá 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.

BIBLIOGRAFÍA

Armour, John. Corporate Governance and Technological Risks, 2017. En: https://blogs.law.ox.ac.uk/business-law-blog/blog/2017/02/corporate-governance-and-technological-risks

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

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

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

Cebriá, Luis Hernando. El deber de diligente administración en el marco de los deberes de los administradores sociales. Marcial Pons, 2009.

Cebriá, Luis Hernando. 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, 2022. Disponible en: https://www.youtube.com/watch?v=0NKLF0AOW_M

Cedillo, Francisco, Meneses, Humberto y Raygada, Miguel Ángel. Gestión del Riesgo Legal. Cengage Learning, 2010.

Chamorro, Maria de la Concepción. "La aplicación de sistemas de inteligencia artificial en el seno del órgano de administración de las sociedades de capital", *Revista de Derecho de Sociedades* No 59 (mayo-agosto 2020).

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

Freeman R. E., Phillips, R. "Stakeholder theory: A libertarian defense", *Business Ethics Quarterly*, 2002, pp. 331-350.

Ganguly, Saptarshi. *Digital Risk: Transforming risk management for the* 2020s. McKinsey&Company, 2017. 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. ¿Cómo se relacionan la Transformación digital, la ciberseguridad y el modelo de negocio? XIX Congreso ALTEC, 27 a 29 de octubre – 2021, Lima, Perú.

Hopt, Klaus. Comparative Corporate Governance: The State of the Art and International Regulation. The American Journal of Comparative Law, 20101, pp. 1-74.

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

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

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. "Apuntes sobre el rol del derecho frente al problema de agencia en las organizaciones", *Themis* N° 46, 2003, pp. 279-286.

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

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

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

OECD. *Digitalization 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

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

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.

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

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

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

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.

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

Tabra, Edison. "El rol de la autorregulación en el gobierno corporativo: aspectos jurídicos societario y constitucionales en el marco legal peruanao". En Revista de Actualidad Mercantil No 6, 2019, pp. 64-87.

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

Uría Menéndez. *Guía práctica sobre deberes y régimen de responsabilidad de los administradores en el ámbito mercantil*. Madrid, 2015. https://www.uria.com/documentos/publicaciones/4558/documento/guia_UM.pdf?id=5679

Vial, G. "Understanding digital transformation: A review and research agenda". *Journal of Strategic Information Systems*, 2019, pp. 118-144.