



UNIVERSIDAD  
PRIVADA  
DEL NORTE

# FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

Carrera de Derecho y Ciencias Políticas

**“EL ESPIONAJE CORPORATIVO Y SU INCIDENCIA EN  
EL FUNCIONAMIENTO INTERNO DE LAS EMPRESAS  
PRIVADAS DEL PERIODO 2007 - 2013”**

Tesis para optar el título profesional de:

Abogado

**Autor:**

Cotrina Roldan, Roy Eduardo

**Asesor:**

Dr. Carlos Uriarte Medina

Trujillo - Perú

2020

## **DEDICATORIA**

A Dios y a nuestro Señor Jesucristo, por ser  
nuestros guías en todo momento

A nuestros nuestros padres, por siempre creer en  
nosotros y su apoyo incondicional

A nuestros docentes por siempre orientarnos y  
apoyarnos durante el desarrollo de la investigación

## **AGRADECIMIENTO**

A nuestros docentes, que fueron vitales e importantes para mi desarrollo y crecimiento como profesional del Derecho.

## **ÍNDICE:**

1. Introducción: .....	p.9
1.1. Realidad problemática: .....	p.9
1.2. Justificación: .....	p.11
1.3. Formulación del Problema: .....	p.13
1.4. Objetivos: .....	p.13
1.4.1. Objetivo General: .....	p.13
1.4.2. Objetivos Específicos: .....	p.13
1.5. Hipótesis: .....	p.14
1.5.1. Hipótesis General: .....	p.14
1.5.2. Hipótesis Específicas: .....	p.14
II. Marco Teórico: .....	p.15
2.1. Antecedentes: .....	p.15
2.2. Bases Teóricas: .....	p.26
2.2.1. Estudio Preliminar .....	p.26
2.2.2. Posición Normativa .....	p.28
2.2.3. El Espionaje Empresarial a Nivel Internacional .....	p. 29
2.2.3.1. Información o Conocimiento relativo a la Empresa .....	p. 33
2.2.3.2. El Espionaje corporativo y violación del Secreto Comercial .....	p. 33
2.2.3.3. El Ciberespionaje Empresarial .....	p. 35
2.2.3.4. La inteligencia Competitiva .....	p. 38
2.2.3.5. Los MetaDatos y la Información secreta de Empresa .....	p. 39

2.2.4. CAPÍTULO I: Las Personas Jurídicas .....	p.40
2.2.4.1. Subcapítulo I: El Know How y los Tipos de Información Secreta de Empresa .	p.40
2.2.4.1.1. Características del Know How (Secreto Empresarial) .....	p.42
2.2.4.1.2 Mecanismos de Protección del Secreto Empresarial .....	p.42
2.2.4.2. Subcapítulo II: El Know How y el Secreto Comercial .....	p.44
2.2.4.2.1. El Know How .....	p.44
2.2.4.2.2. Categorías del Know How: .....	p.45
2.2.4.2.3. El Secreto Comercial: .....	p.46
2.2.4.2.4. Normativa Aplicable: .....	p.47
2.2.4.2.5. El bien Jurídico en los Delitos Económicos: .....	p.49.
2.2.4.2.6. Perspectivas del Secreto Empresarial: .....	p.50.
2.2.4.2.7. El Secreto Comercial y el Derecho Relativo a los Secretos Comerciales: ....	p.51.
2.2.4.2.8. Tipos de Información Confidencial: .....	p.53.
2.2.4.2.9. ¿Cuándo estamos frente a un secreto empresarial? .....	p.55.
2.2.4.2.10. Deber de Reserva: .....	p.56.
2.2.4.2.11. Requisitos para la Existencia de un Secreto Empresarial: .....	p.58.
2.2.4.2.12. El Secreto de las Comunicaciones: .....	p.59.
2.2.4.2.13. Libre competencia. ....	p.62.
2.2.4.2.14. Libre formación de precios: .....	p.62.
2.2.4.2.15. El tipo subjetivo de la violación de secretos de empresa .....	p.64.
2.2.4.3. Subcapítulo III: Criminal Compliance en las Personas Jurídicas .....	p. 68.
2.2.5. CAPÍTULO II: El Espionaje Corporativo .....	p.87
2.2.5.1. Subcapítulo I: Concepto y Características del Espionaje Corporativo .....	p.88

2.2.5.1.1. La Competencia como Bien Jurídico Tutelado: .....	p.94
2.2.5.1.2. La Protección Penal de la Competencia Leal: .....	p.95
2.2.5.1.3. Proceso de Ingresos y Egresos del Estado: .....	p.96.
2.2.5.1.4. Cargo de Confianza: .....	p.97.
2.2.5.2. Subcapítulo II: El Contrato de Franquicia .....	p.98.
2.2.5.2.1. Concepto del Contrato de Franquicia: .....	p.98.
2.2.5.2.2. Características del Contrato de Franquicia: .....	p.98.
2.2.5.2.3. El Secreto Comercial en el Contrato de Franquicia: .....	p.99.
2.2.5.2.4. Principales Pagos: .....	p.103.
a) Honorario Inicial (Franchising Fee) .....	p.103.
b) Regalías (Royalties) .....	p.103.
c) Fondos de Publicidad .....	p.104.
2.2.5.2.5. Tipos de Contratos de Franquicia: .....	p.104.
2.2.5.3. Subcapítulo III: Personas Jurídicas - Riesgos Empresariales del Espionaje Corporativo .....	p.105.
2.2.5.3.1. Los retos de la protección .....	p.107.
2.2.5.3.2. La protección de los secretos empresariales: .....	p.108.
2.2.5.3.3. Riesgos Empresariales: .....	p. 108.
2.2.5.3.4. Riesgos Directos en relación con las Personas que tienen Acceso a Información Confidencial .....	p. 110.
2.2.5.3.5. Pequeñas Empresas: .....	p. 111.
2.2.5.3.6. Tipo de Daños .....	p. 111.
a) Daños al patrimonio inmovilizado: .....	p.111.
b) Daños a los Valores Monetarios: .....	p.112.

c)	Daños a los archivos, informes y documentación: .....	p.112.
d)	Daños a la propiedad industrial: .....	p.112.
e)	Manipulación maliciosa de los productos: .....	p.113.
f)	Fraude o estafa .....	p.113.
	2.2.5.3.7. Actos contra los Hombres Clave de la Empresa .....	p.113.
	2.2.5.4. Subcapítulo IV: Los Secretos Empresariales como Derechos de Propiedad intelectual .....	p.114
	2.2.5.4.1. Patentes de Invención .....	p. 116
	2.2.5.4.2. Información Tecnológica y las Patentes .....	p.103
	2.2.5.5. Subcapítulo V: La violación de Secreto empresarial y el Espionaje .....	p. 120
	2.2.5.5.1. Los supuestos de ignorancia deliberada respecto del origen ilícito de la obtención del secreto empresarial .....	p.120
	2.2.5.6. Subcapítulo VI: El Espionaje Empresarial en materia penal - Criterios Doctrinales .....	.p.123.
	2.2.5.6.1. Sujeto pasivo y elemento subjetivo del Espionaje Empresarial .....	p.123.
	2.2.5.6.2. Consumación del Espionaje Corporativo: .....	p.123.
	2.2.5.6.3. Tipo de peligro concreto .....	p.124.
	2.2.5.6.4. Participación Necesaria: .....	p.125.
	2.2.5.6.5. Deber de Guardar Reserva: .....	p.125.
	2.3 Matriz de Operacionalización de Variables: .....	p.126.
III.	METODOLOGÍA .....	p.140.
3.1.	Tipo de investigación .....	p.140
3.2.	Población y muestra (Materiales, instrumentos y métodos) .....	p.140
3.2.1.	Unidad de Estudio .....	p.140

3.2.2. Población .....	p.143
3.2.3. Muestra .....	p.143
3.3. Técnicas y Materiales .....	p.174
3.4. Procedimiento .....	p.191
3.5. Aspectos Éticos .....	p.191
IV. Resultados .....	p.192
V. Discusión de Resultados .....	p.201
VI. Conclusiones .....	p.214
VII. Referencias: .....	p.217
7.1. Referencias Teóricas: .....	p.217
7.2. Antecedentes Jurídicos: .....	p.226
7.3. Referencias Legales: .....	p.227
VIII. Anexos .....	p.229

## I. CAPÍTULO I. INTRODUCCIÓN

### 1.1. Realidad problemática

Según el foro económico mundial (WEF), gran parte de las pérdidas económicas pasan sin ser detectadas en el Perú, especialmente por el espionaje industrial. Temas como información sobre infraestructura nacional y recursos naturales, propiedad intelectual, fuga de información confidencial estratégica, fraudes siguen sin estar completamente monitoreados. (Gestión, 2017)

La encuesta de EY (Ernst & Young) señala que la falta de mejora en los niveles globales de corrupción empresarial en los últimos seis años muestra que las empresas se mantienen vulnerables a impactos financieros y reputacionales significativos y la reducción del comportamiento antiético en los negocios sigue siendo un gran desafío, pese al incremento de la persecución de estas conductas de mala fe a nivel global. El criminal compliance o los programas de cumplimiento adoptados por los empleadores para contrarrestar los actos de sabotaje empresarial, deben mantener el ritmo de los rápidos avances tecnológicos y del entorno de riesgo cada vez más complejo en las operaciones de los negocios. (Gestión, 2018)

Estadísticas indican que en el 80% de los casos, quien toma la información secreta de empresa por medio de actos de espionaje son los mismos trabajadores de las entidades, quienes se prestan a este tipo de cosas por diferentes razones: quieren cambiar de empleo o adquirir mayor valor para la competencia, se ven incentivados por terceras personas de mala fe, etc. Este es un problema que implica muchos valores como son: la confianza, la responsabilidad, la moral, la seguridad, de los cuales, si no existen pruebas, resulta difícil de asignar responsabilidad. (Velandó, 2012)

La pandemia del COVID-19 ha puesto en riesgo la capacidad de las empresas para llevar a cabo una vigilancia efectiva que vele por el cumplimiento, supervisión

y control de actividades dentro de las organizaciones, creando una apertura para los delitos económicos y comportamientos anti-éticos. Los agentes desleales pueden buscar el uso de información confidencial de las empresas a través del espionaje corporativo como *modus operandi*, donde los empleados o trabajadores de confianza se apropian indebidamente y sin autorización, de la información confidencial y los secretos empresariales susceptibles de explotación económica, para su posterior divulgación a terceras personas, y lograr sacar un provecho económico indebido. (Gordon, 2020)

Desde un análisis penal – económico, el espionaje corporativo en el Perú y su falta de regulación jurídica - penal, incentiva a que el agente delictivo obre de mala fe y busque un provecho económico, mediante el uso sin autorización de la información secreta de empresa, poniendo en riesgo el funcionamiento interno de las empresas privadas, lo cual conlleva a perturbar la capacidad competitiva y financiera de las empresas privadas - peruanas, las ganancias de las franquicias, los intereses de los consumidores, los trabajadores y los empleadores.

La normativa penal no contempla expresamente los supuestos de espionaje corporativo, como *modus operandi* para tomar conocimiento ilegítimo de las operaciones comerciales y administrativas realizadas cotidianamente en el interior de las compañías comerciales y el contenido reservado y confidencial de los secretos empresariales, para su posterior divulgación y explotación económica sin autorización del titular, generando perjuicios a la capacidad competitiva y financiera de las entidades privadas, la imagen y status empresarial de las marcas comerciales, en virtud al espionaje realizado por parte de los trabajadores espías y terceras personas por medios ilícitos o contrarios a los usos comerciales honestos y la buena fe empresarial. (Rodríguez, 2014)

Los empleadores, franquiciantes e inventores se encuentran en una situación de indefensión ante la existencia de vacíos de punibilidad frente a las conductas delictivas y antiéticas de espionaje por parte de los trabajadores espías y terceras personas, orientadas a la obtención indebida de conocimientos mercantiles

respecto a las actividades comerciales y administrativas realizadas al interior de las empresas y la obtención ilegítima de secretos empresariales de carácter estratégico, comercial y susceptibles de explotación económica.

Los ataques cibernéticos contra las empresas se han vuelto más frecuentes, donde los ciberdelincuentes no solo buscan paralizar los negocios de los empresarios, sino también generar perjuicios económicos a través de la obtención indebida del know-how, los secretos empresariales patentados y planes estratégicos que ayudan a un mejor posicionamiento empresarial en el libre mercado. (Domingo, 2020)

El titular de un determinado secreto empresarial, puede verse perjudicado por comportamientos de terceras personas (Espías); por lo que, es necesario, no sólo por el interés del titular sino por determinados bienes jurídicos que pueden verse afectados, que el Derecho Penal intervenga. La conducta delictiva del sujeto activo por espionaje corporativo, incide en un secreto de empresa, por su alto valor económico y susceptible de contratación. (Gómez, 1974)

Respecto a los cuatro expedientes de Indecopi en materia de competencia desleal, en el periodo 2007 – 2013 se cometieron actos internos de espionaje corporativo en las empresas privadas de la ciudad de Lima, por parte de los agentes económicos y trabajadores de confianza, como actos atípicos de sabotaje empresarial en perjuicio de la ventaja competitiva, las utilidades y el patrimonio de las personas jurídicas privadas. Debido a la falta de fiscalización o persecución penal de este tipo de supuestos, los agentes económicos y trabajadores desleales no fueron sancionados y fueron absueltos por la Comisión de Indecopi, de los cargos que se le imputaron, como la violación del secreto empresarial, en cuatro resoluciones administrativas bastante controvertidas, donde primó la libre competencia por encima de los derechos afectados de los empleadores.

Por lo expuesto, en esta investigación abordaré la problemática del espionaje corporativo y los conflictos de intereses de relevancia penal – económica que se

presentan dentro de las entidades del sector privado, con el fin esencial de determinar el modo de repercusión del espionaje corporativo, en el funcionamiento interno de las empresas privadas de la ciudad de Lima, del periodo 2007- 2013.

## **1.2. Justificación:**

El presente trabajo de investigación es importante porque busca enriquecer la tratativa legislativa poco abordada en los supuestos de espionaje corporativo que debe afrontar el juez, al momento de emitir una decisión judicial, siendo fundamental para trabajos posteriores de mayor amplitud. La presente investigación aporta información relevante referida al espionaje empresarial, los tipos de información secreta, y los requisitos para que esta sea considerada como secreto empresarial.

El titular de secretos empresariales como el empleador o franquiciante se encuentra en una situación de indefensión ante la existencia de vacíos de punibilidad frente a comportamientos maliciosos de terceras personas y agentes económicos desleales en los supuestos atípicos de espionaje corporativo, ya sea para la obtención de beneficios lucrativos y ventajas estratégicas competitivas en el libre mercado.

Por ello, es pertinente no sólo por el interés del empleador o titular de la información secreta de empresa, sino también por determinados bienes jurídicos involucrados como la capacidad competitiva y financiera de las entidades privadas, los intereses de los consumidores, trabajadores, y la generación de empleo en nuestro país, que el derecho penal intervenga, ante las conductas delictivas de trabajadores espías y terceras personas por medio de espionaje corporativo, para la obtención ilegítima de información confidencial concerniente a las operaciones administrativas y comerciales de las entidades privadas y los secretos empresariales susceptibles de explotación económica, por su valor comercial.

Asimismo, la presente investigación aporta criterios doctrinales en el ámbito penal que son aplicables en los supuestos de espionaje corporativo, los secretos industriales y comerciales, los tipos de daños y riesgos derivados del espionaje corporativo en el ámbito organizacional de las Personas Jurídicas. Es pertinente realizar la presente investigación ante la problemática de los vacíos legislativos

existentes en los supuestos de espionaje corporativo de los secretos empresariales, en una economía social de Mercado donde los participantes o agentes económicos compiten deslealmente, basándose en cuestiones distintas a su propia eficiencia o esfuerzo.

Por ello, realizo la presente investigación, porque busco fomentar una administración de justicia adecuada, en base a los principios generales del derecho, la justicia y la equidad, a fin de que los empleadores, inventores, franquiciantes y franquiciados reciban protección legal adecuada frente a los supuestos de espionaje corporativo en materia penal.

### **1.3. Formulación del problema**

- ¿De qué manera el vacío de tipo penal del espionaje corporativo, incide en el funcionamiento interno de las empresas privadas fiscalizadas por la Comisión de Indecopi de Lima en el periodo 2007 – 2013?

#### **1.3.1. Problemas Específicos:**

- ¿Qué efectos tiene el espionaje corporativo en la esfera jurídica patrimonial de las empresas fiscalizadas por la Comisión de Indecopi de Lima en el periodo 2007-2013?
- ¿Qué efectos generan los vacíos legales existentes del espionaje corporativo, en las obligaciones contractuales pactadas entre el trabajador y el empleador?
- ¿De que manera el vacío del tipo penal de espionaje corporativo, exime de responsabilidad penal al trabajador espía en su condición de sujeto activo?
- ¿Qué efectos tiene el espionaje corporativo, en los secretos empresariales de las empresas privadas fiscalizadas por la Comisión de Indecopi de Lima en el periodo 2007 – 2013?

## **1.4. Objetivos**

### **1.4.1. Objetivo general**

- Determinar de qué manera incide el vacío del tipo penal de espionaje corporativo, en el funcionamiento interno de las empresas privadas fiscalizadas por la Comisión de Indecopi de Lima en el periodo 2007 – 2013.

### **1.4.2. Objetivos específicos**

- Especificar los efectos del espionaje corporativo, en la esfera jurídica patrimonial de las empresas privadas fiscalizadas por la Comisión de Indecopi de Lima en el periodo 2007 – 2013.
- Determinar las consecuencias de los vacíos legales existentes del espionaje corporativo, en las obligaciones contractuales pactadas entre el trabajador y el empleador.
- Determinar de qué manera el vacío del tipo penal de espionaje corporativo, exime de responsabilidad penal al trabajador espía en su condición de sujeto activo.
- Especificar los efectos del espionaje corporativo, en los secretos empresariales de las empresas privadas fiscalizadas por la Comisión de Indecopi de Lima en el periodo 2007 – 2013.

## **1.5. Hipótesis**

### **1.5.1. Hipótesis general**

- ❖ El vacío del tipo penal de espionaje corporativo afecta negativamente el funcionamiento interno de las empresas privadas fiscalizadas por la Comisión de Indecopi de Lima en el periodo 2007 – 2013.

### 1.5.2. Hipótesis específicas

- La falta de fiscalización del espionaje corporativo en materia penal, incide negativamente en la esfera jurídica patrimonial de las empresas privadas fiscalizadas por la Comisión de Indecopi de Lima en el periodo 2007 – 2013.
- Los vacíos del tipo penal de espionaje corporativo, inciden negativamente en las obligaciones contractuales de los trabajadores de las empresas privadas fiscalizadas por la Comisión de Indecopi de Lima en el periodo 2007 – 2013.
- Los vacíos del tipo penal de espionaje corporativo, eximen de responsabilidad penal al trabajador espía en su condición de sujeto activo.
- Los vacíos del tipo penal de espionaje corporativo, inciden negativamente en los secretos empresariales de las empresas privadas fiscalizadas por la Comisión de Indecopi de Lima en el periodo 2007 – 2013.

## II. Marco Teórico:

### 2.1. Antecedentes:

2.1.1. Cornejo, L. (2015) realizó la investigación titulada “*Reglas Claras o Presunciones: el Derecho de Reserva a Razón de la Franquicia*”, en la Pontificia Universidad Católica del Perú, con el propósito de estudiar el contrato de franquicia, así como la información confidencial de carácter pecuniario que se maneja, en especial la reservada, y de esa manera inquirir si existe algún tipo de protección legal a esta (información reservada). En el marco teórico, se identificó conceptos generales referidos a la franquicia tales como sus características, tipos, elementos, las obligaciones que derivan de las partes, así como su tratamiento legal. Asimismo, propuso un proyecto de ley que involucre el reconocimiento del know how como información reservada, así como su debida manipulación, enfocándose en el derecho a guardar reserva y no divulgación a terceros.

#### 2.1.1.1. Contribución:

Este estudio es pertinente con la investigación aquí planteada, porque demostró la pertinencia de que la información valiosa de empresa que forma parte del patrimonio empresarial, en este caso del contrato de franquicia, reciba protección legal adecuada, por ser de carácter pecuniario. Asimismo, demostró la importancia de cumplir con los deberes éticos de guardar reserva y actuar conforme a la buena fe empresarial, a fin de que los empleadores, titulares de esta información, no se vean perjudicados por actos de sabotaje empresarial, y reciban protección legal adecuada frente a este tipo de casos.

La investigación llegó a las siguientes principales conclusiones:

- i. El hecho de que dentro de estas sociedades (S.A.C. y S.R.L., u otras) se maneje información de carácter confidencial, hace que esta información requiera ser reconocida como tal y este protegido dentro de nuestro ordenamiento jurídico.
- ii. En toda sociedad el rol de la información juega un papel determinante, más aún en el caso de que esta sea considerada como “secreta” o reservada”, siendo este último carácter una excepción a la regla del derecho de información.

2.1.2. Valdivia, P. (2012) realizó la investigación titulada “*Los delitos contra los Derechos de Autor en el Perú*”, en la Universidad Nacional Mayor de San Marcos, en Perú, con el propósito de determinar los niveles de eficacia de las normas penales en la protección de los Derechos de Autor y conexos, así como los factores que inciden en la eficacia o ineficacia de las mismas. Al respecto, propuso ideas que procuran una eficaz protección de los secretos societarios frente a su revelación y aprovechamiento indebidos por parte de los órganos sociales.

### 2.1.2.1. Contribución:

Este trabajo es pertinente con la investigación aquí planteada, porque demostró la relevancia que tiene la eficacia de las normas penales en la protección de los derechos de autor, y resaltó la importancia de brindar una protección legal adecuada a la información secreta de empresa, para no perjudicar las utilidades o las rentas percibidas, frente a los actos de sabotaje empresarial por parte de terceras personas.

La investigación llegó a las siguientes principales conclusiones:

- i. Los procesados por delitos contra derechos de autor y conexos, tienen conocimiento de los ilícitos en los cuales están incurso, sin embargo, al percibir que existe impunidad y escaso control en materia penal por parte del Estado, justifican su actitud y comportamiento, y hacen de su actividad ilícita algo permanente y habitual.
- ii. Las formas de infracción más frecuentes son la piratería y la reprografía, y ambos constituyen infracción al derecho patrimonial que tiene el autor de ser el único quien decide cómo reproducir y distribuir su obra o material inédito.

2.1.3. Fernández, C. (2018) realizó la investigación titulada: “La Amenaza de las Nuevas Tecnologías en los Negocios: el Ciberespionaje Empresarial”, en la Revista de Derecho UNED, con el propósito de encontrar las posibles carencias del ciberespionaje en materia penal y la necesidad de encontrar soluciones jurídicas a las mismas, acudiendo a la legislación, la jurisprudencia y la doctrina española e internacional. En el mencionado artículo, se estudio la regulación penal del ciberespionaje corporativo en España, aludiendo al sujeto activo del delito, y al objeto de la conducta atípica. En segundo lugar, se analizan las modalidades comisivas más frecuentes de ciberespionaje cuya peculiaridad es un acceso ilícito telemático. Asimismo, planteó la necesidad de

ofrecer una mejor protección sobre la propiedad inmaterial corporativa susceptible de explotación económica, ante los supuestos de obtención ilegítima del secreto empresarial o información confidencial, sin autorización del titular.

#### **2.1.3.1. Contribución:**

Este trabajo es pertinente con la investigación aquí planteada, porque demostró la relevancia jurídica que tiene los supuestos de ciberespionaje corporativo y el apoderamiento u obtención indebida del secreto empresarial como propiedad inmaterial corporativa por medios telemáticos, tecnológicos y resaltó la importancia de brindar una protección legal adecuada al empresario o titular de los secretos empresariales o información confidencial de empresa, ante la situación de indefensión en la que se encuentra frente a los avances tecnológicos y medios telemáticos que utiliza el agente infractor o espía corporativo para el apoderamiento ilegítimo de los secretos comerciales en perjuicio del empleador o dueño de empresa.

La investigación llegó a las siguientes principales conclusiones:

- i. El supuesto de ciberespionaje se configura cuando el espía infractor realiza actos de espionaje por medios técnicos telemáticos, correos corporativos y técnicas de inteligencia competitiva (recolección de datos) ante el descuido de la víctima o titular del secreto empresarial, para el apoderamiento de su información digitalizada de carácter reservado y secretos empresariales susceptibles de explotación económica. Además, tienen que existir medidas de protección del titular sobre sus secretos de empresa, destinados a preservar su reserva y confidencialidad para la imputación del espionaje empresarial.
- ii. Asimismo, existe lagunas de punibilidad en el supuesto de espionaje corporativo, cuando se configura el apoderamiento y obtención indebida de

la información secreta de empresa, para su explotación económica, siendo necesario una sanción punitiva de esta conducta maliciosa y fraudulenta de lege ferenda.

2.1.4. Rivadeneira, M. (2010) realizó la investigación titulada: “Los Conocimientos Técnicos Secretos y la Problemática de su Protección dentro del Régimen Jurídico Ecuatoriano”, en la Universidad Internacional SEK, con el propósito de estudiar los Conocimientos Técnicos Secretos y su protección en Ecuador. En el marco teórico, desarrolló los conceptos de Know How, los conocimientos técnicos secretos, patentados, la obligación de no divulgar el conocimiento técnico secreto a terceras personas, las autoridades competentes, el titular de la información secreta y los actos desleales de divulgación de los secretos empresariales. Asimismo, planteo la necesidad de ofrecer una mejor protección legal a los conocimientos técnicos de carácter confidencial, con el fin esencial de preservar el valor económico o comercial a favor del titular del secreto empresarial.

#### **2.1.4.1. Contribución:**

Este trabajo es pertinente con la investigación aquí planteada, porque demostró la relevancia jurídica de resguardar el valor económico, comercial de los conocimientos técnicos de carácter reservado, secretos empresariales, know hows, con el fin esencial de brindar una mejor protección a los empleadores, agentes económicos del libre mercado que se encuentran en situación de indefensión ante los actos espionaje corporativo y divulgación indebida del secreto empresarial.

La investigación llegó a las siguientes principales conclusiones:

- i. Los conocimientos técnicos secretos son susceptibles de valorización económica significativa, lo cual dependerá de diversos factores como su demanda en el libre mercado, su carácter oculto, la voluntad e interés del

titular del know-how de mantenerlo en reserva, para resguardar su valor comercial.

- ii. Los Conocimientos técnicos secretos comprenden los secretos industriales o de fábrica, como las fórmulas químicas - industriales, los procesos de elaboración y fabricación de productos del sector industrial; mientras que los secretos comerciales engloban las listas de clientes, proveedores, estrategias de mercadotecnia, cálculos de precios, técnicas de marketing, sondeos de opinión, entrenamiento de empleados, y los secretos organizacionales o administrativos consisten en aspectos de la organización interna y relaciones de la empresa, cuyo conocimiento sería valioso para la obtención de una ventaja estratégica competitiva. (situación financiera, relaciones laborales y contratos de la corporación)

2.1.5. Mallo, P. (2014) realizó la investigación titulada: “Descubrimiento y Revelación de Secretos”, en la Universidad de Sevilla, con el propósito de estudiar la problemática de la violación de la intimidad y revelación de secretos documentales, empresariales o información de carácter confidencial en los sistemas informáticos. En el marco teórico, desarrolló el derecho a la intimidad, el secreto documental, la manipulación de datos reservados registrados en ficheros o soportes informáticos y la revelación o cesión de datos confidenciales. Asimismo, propuso realizar una tipificación de las posibles conductas que, con el auxilio de las nuevas tecnologías, invaden fácilmente la esfera íntima de todos los individuos ante la falta de un adecuado monitoreo en el manejo de datos reservados, secretos empresariales y revelación de información secreta de empresa, por parte de los trabajadores, que cuentan con acceso a correos corporativos e información confidencial.

#### **2.1.5.1. Contribución:**

Este trabajo es pertinente con la investigación aquí planteada, porque demostró la importancia de preservar por la intimidad del individuo o víctima frente a la

divulgación ilegítima e indebida de sus secretos empresariales, información privada de carácter económico ante los medios tecnológicos existentes que facilitan que el espía infractor o agente desleal, desarrolle el espionaje por autoría mediata o inmediata en perjuicio del empleador o titular del secreto comercial.

La investigación llegó a las siguientes principales conclusiones:

- i. El surgimiento de nuevos medios tecnológicos, herramientas informáticas posibilita que terceras personas, espías infractores con conductas maliciosas e intención fraudulenta, invadan la esfera íntima y privada del empleador o titular del secreto empresarial, a través de la realización de actos de apoderamiento indebido de datos confidenciales, secretos de empresa e información confidencial de la víctima.
- ii. La revelación de información secreta, datos confidenciales a terceras personas es cada vez más frecuente ante los avances tecnológicos y las lagunas de punibilidad existentes para reprimir este tipo de conductas atípicas de espionaje y divulgación indebida de secretos empresariales y datos confidenciales de la víctima agraviada, titular de la información confidencial, siendo fundamental la intervención del derecho penal empresarial para sancionar punitivamente este tipo de supuestos.

2.1.6. Jiménez, S. (2014) realizó la investigación titulada: “La Necesidad de Protección del Secreto Empresarial en el Mercado Interior”, en la Universidad de Salamanca, con el propósito de determinar la ilicitud del agente infractor en los supuestos de obtención, utilización y divulgación de secretos. En el marco teórico, desarrolló el secreto empresarial, la protección del saber hacer e información corporativa no divulgados, la revelación indebida de secretos comerciales y el know-how. Asimismo, planteo la necesidad de una mayor protección por parte de los Estados legislativos en el ámbito internacional privado en los supuestos de espionaje corporativo ante el desarrollo constante

de las nuevas tecnologías y las comunicaciones, que han posibilitado el desarrollo de herramientas más eficaces para la realización de actividades de inteligencia, robo de información confidencial y secretos empresariales.

#### **2.1.6.1. Contribución:**

Este trabajo es pertinente con la investigación aquí planteada, porque demostró la relevancia jurídica de combatir la divulgación indebida de secretos empresariales, sancionar punitivamente aquellas conductas maliciosas o fraudulentas de los trabajadores y terceras personas orientadas al espionaje y revelación ilegítima de la información confidencial, con el fin esencial de brindar una mejor protección legal al titular del secreto comercial, preservar el carácter reservado y valor económico de la información secreta de empresa, lista de clientes, balance patrimonial, fórmulas industriales susceptibles de explotación económica y planes estratégicos de posicionamiento en el libre mercado.

La investigación llegó a las siguientes principales conclusiones:

- i. La protección de secretos empresariales o información reservada de empresa es vital para el resguardo de su valor comercial, la preservación de su carácter de confidencialidad y exclusividad para su explotación económica y el registro de futuros derechos de patentes.
- ii. El avance de las nuevas tecnologías y comunicaciones ha facilitado el espionaje y robo de información confidencial de empresa, siendo el modus operandi del espía infractor, la sustracción de información reservada del empleador de manera ilegítima a través de medios telemáticos, con el uso de herramientas informáticas (ciberespionaje), por medios físicos y de comunicación.

2.1.7. Fernández, C. (2017) realizó la investigación titulada: “La Violación de Secretos Empresariales por Persona Ajena a la Empresa”, en la Universidad

de Málaga, con el propósito de identificar el bien jurídico protegido en el delito de espionaje empresarial en la legislación española y el alcance del secreto empresarial como elemento central del hecho imputable, los tipos básico y agravado que el precepto recoge, tanto por lo que respecta a su conducta típica y otros elementos del tipo objetivo, como del subjetivo. En el marco teórico, desarrolló el espionaje corporativo, el apoderamiento del secreto empresarial, los supuestos de espionaje a través de medios técnicos, el secreto de empresa como bien inmaterial, la capacidad competitiva de la empresa como objeto de tutela penal y el interés económico del empresario de mantener la reserva como interés tutelado. Asimismo, propuso solucionar los problemas concursales que el espionaje empresarial presente frente a otros delitos, especialmente por lo que respecta al delito de daños.

#### **2.1.7.1. Contribución:**

Este trabajo es pertinente con la investigación aquí planteada, porque demostró la importancia de proteger los intereses económicos del empleador o titular de información secreta de empresa frente a los supuestos de apoderamiento y revelación del secreto empresarial a terceras personas, en los supuestos de espionaje corporativo, y sancionar punitivamente determinadas conductas maliciosas, fraudulentas y con animus lucrandi del espía corporativo o agente desleal, que buscan sacar un provecho económico indebido y generar perjuicios económicos en el empleador.

La investigación llegó a las siguientes principales conclusiones:

- i. En los supuestos de espionaje corporativo y violación del secreto empresarial, tenemos como objeto de tutela, la intimidad, la propiedad inmaterial o secretos de empresa, la capacidad competitiva organizacional de las corporaciones y los intereses privados y económicos del empleador en preservar la confidencialidad de la información de empresa.

- ii. Los supuestos de espionaje corporativo tienen como objeto la obtención ilegítima y sin autorización del empleador o titular de secretos industriales, comerciales e información confidencial de empresa, cuya distintividad y carácter de exclusividad es por su valorización económica y por representar una ventaja estratégica competitiva para un mejor posicionamiento en el libre mercado, siendo vital el resguardo y protección de los derecho de uso o explotación en exclusiva de estos bienes inmateriales frente a los supuestos atípicos de espionaje empresarial.

2.1.8. Pacheco, E. (2015) realizó la investigación titulada “El Derecho de la Competencia en Guatemala tras la Ratificación del Acuerdo de Asociación suscrito entre la Unión Europea y Centro américa”, en la Universidad Rafael Landívar, en Guatemala, con el propósito de analizar el Acuerdo de Asociación entre la Unión Europea y Centroamérica, respecto de las disposiciones relacionadas al derecho de la competencia para así determinar las acciones que debe tomar Guatemala a raíz de la ratificación de dicho instrumento internacional. En el marco teórico, se identificó conceptos generales que comprenden el derecho de la competencia, aspectos laterales que afectan a las actividades de las empresas y la relación del Derecho de la Competencia con otras ramas del Derecho. Asimismo, planteo la necesidad de que el Estado de Guatemala cuente con una Ley que regule el derecho competencia cumpliendo con el Acuerdo de Asociación entre la Unión Europea y Centroamérica.

#### **2.1.8.1. Contribución:**

Este trabajo es pertinente con la investigación aquí planteada, porque demostró la relevancia jurídica de combatir la competencia desleal en una economía social de mercado, y regular las conductas de mala fe de los agentes económicos (empleadores), trabajadores y terceras personas, con el fin esencial de brindar una mejor protección a los competidores de buena fe

(empleadores) y resarcir el daño concurrencial negativo producido por los actos de sabotaje empresarial del agente infractor, en perjuicio de la imagen, buena reputación y posicionamiento estratégico de los competidores leales.

La investigación llegó a las siguientes principales conclusiones:

- i. La Constitución Política de la República de Guatemala fundamenta la base para la creación de leyes ordinarias en materia de competencia, inclusive, contiene un precepto constitucional el cual previene y prohíbe la creación de monopolios los cuales son perjudiciales para la economía nacional y para los consumidores y demás empresas que interactúan dentro del mercado.
- ii. Asimismo, existen leyes que protegen al consumidor y al usuario frente a los proveedores de abusos y que contiene sanciones, pero no es una ley de competencia que pueda regular el desenvolvimiento del mercado.

2.1.9. Soto, J. (2012) realizó la investigación titulada “Vías de Aplicación del Derecho de la Competencia”, en la Universidad Autónoma de Madrid, en España, con el propósito estudiar la Comisión Europea y la Tradicional Vía de Aplicación de la Normativa Antitrust, los aspectos estructurales y funcionales de la Autoridad de Competencia Europea. En el marco teórico, se identificó conceptos generales en lo que comprende a la protección de los competidores, las conductas contrarias a las normas de libre competencia, el secreto profesional y la descentralización del poder económico. Asimismo, planteo que las particularidades del arbitraje deben actuar como incentivo en la búsqueda de adecuar los mecanismos comunes de cooperación, a esta forma alternativa de solución de controversias.

### 2.1.9.1. Contribución:

Este trabajo es pertinente con la investigación aquí planteada, porque demostró la importancia de disuadir las conductas contrarias a las normas antitrust y a la buena fe empresarial, y velar por el adecuado proceso competitivo de las empresas, con la finalidad de tutelar los derechos involucrados de los agentes económicos, y evitar daños concurrenciales que generen externalidades negativas en las utilidades y el posicionamiento estratégico de las empresas.

La investigación llegó a las siguientes principales conclusiones:

- i. La Defensa de la Competencia se enriquece gracias a la coexistencia de dos sistemas de aplicación de la normativa que le respalda, toda vez que la protección de los mercados y los agentes participantes en ellos, se encuentra mejor sustentada por medio de la participación de las Autoridades administrativas y de los Tribunales Nacionales, ya que se alcanza un nivel mayor y contundente de disuasión que afecta a aquellos con expectativas de contravenir las normas antitrust y se erigen mecanismos idóneos para tutelar los derechos involucrados.

## 2.2. Bases Teóricas:

### 2.2.1. Estudio Preliminar

Los agentes racionales deciden si cometen o no una infracción comparando el valor esperado de cometer el ilícito versus el valor esperado de cumplir con las normas. De esta forma, si el valor esperado de cometer el ilícito, que depende de la probabilidad de detección y de las posibles sanciones que se enfrenten, es mayor que el valor esperado de no infringir la ley, entonces el agente racional cometerá una infracción. **(Bullard, 2012)**

**Según Becker** citado por **Bullard (2012)**, “las personas se convierten en criminales no debido a que sus motivaciones básicas difieran, sino debido a que sus beneficios y costos difieren”. Así, se tiene que el número de infracciones que una persona cometerá es una función de:

- a. Las probabilidades de detección ( $p$ )
- b. El castigo si es detectado ( $f$ )
- c. Otras variables tales como ingreso disponible en actividades legales e ilegales, etc. ( $u$ ).

El Espionaje Corporativo actualmente no se encuentra regulado en materia penal, lo cual, pone en riesgo diversos bienes jurídicos de relevancia como la información secreta de las empresas (Secretos Empresariales), la situación patrimonial de las personas jurídicas del Perú, y la competencia leal, debido a la ausencia de persecución penal de las conductas atípicas de mala fe, del competidor desleal, quien se verá incentivado a sacar una ventaja estratégica indebida, a través del aprovechamiento económico y sin autorización del Know How (Secreto Empresarial). (Bullard, 2012)

El espionaje corporativo es una situación de vacío en la ley que ha sufrido la patología jurídica de omitir en el Código Penal Peruano la regulación concreta de una determinada situación en materia de competencia desleal, y que no encuentra respuesta legal específica. El espía corporativo; frente a los vacíos legales existentes, realiza actos contra la competencia leal, a través de la violación del secreto empresarial del titular. (Basterra, 2003)

Desde un análisis económico del derecho, los vacíos legales existentes del espionaje corporativo en materia penal, disminuirán la probabilidad de detección del agente delictivo, al no existir persecución penal, lo cual aumentará la utilidad

esperada del potencial infractor y, por ende, tenderá a aumentar el número de conductas atípicas del espía corporativo. (Bullard, 2012)

La aplicación de sanciones en el **Derecho penal** tiene, en general, **dos etapas**:

- a) En la primera etapa, el Juez debe determinar la pena básica. Esto es, verificar el mínimo y el máximo de pena conminada aplicable al delito. Por ejemplo, para el delito A serán 15 y 35 años, respectivamente.
  
  - b) En la segunda etapa, el Juzgador debe individualizar la pena concreta, entre el mínimo y el máximo de la pena básica, evaluando, para ello, diferentes circunstancias agravantes y atenuantes. Se denomina circunstancias a aquellos factores objetivos o subjetivos que influyen en la medición de la intensidad del delito (antijuridicidad o culpabilidad), haciéndolo más o menos grave. Su función principal es coadyuvar a la graduación o determinación del quantum de pena aplicable al hecho punible cometido. (Bullard, 2012)
- ❖ Actualmente, debido a la carente tratativa legislativa en materia penal del espionaje corporativo, que constituye un modus operandi atípico que atenta contra la situación patrimonial y la competencia leal de las empresas peruanas (personas jurídicas), las soluciones jurisprudenciales de las Comisiones y Oficinas del INDECOPI son aceptadas, pese a que algunas de ellas son muy discutibles o controversiales y carecen de base legal sólida. (Abanto, 1997)

Es por ello, que surge el Derecho Penal Económico peruano, como una rama jurídica indispensable para desarrollar un auténtico Derecho Contravencional peruano, situado entre el Derecho meramente administrativo y el Derecho estrictamente penal, donde se podrá contribuir realmente a crear mayor seguridad en el destinatario de la norma, y a reforzar con ello la legitimidad de las autoridades administrativas y judiciales que actúan en el difícil y versátil campo de las interrelaciones económicas y sociales de los agentes del mercado. (Abanto, 1997, p. 154)

### 2.2.2. Posición Normativa

Existe una protección penal adicional a la administrativa en algunos casos de ataques graves contra los bienes jurídicos como la libre competencia, la competencia leal (y, secundariamente, la protección al consumidor). Aunque la ley no prevé criterios expresos y claros para delimitar el ilícito administrativo del ilícito penal, la jurisprudencia de las Comisiones de **INDECOPI** tiende a aplicar dos criterios fundamentales que constituirían el carácter penal de las infracciones:

- a) **El dolo especial** (malicia, intención fraudulenta)
  
- b) **El grave perjuicio** (perjuicio también contra los consumidores, pluralidad de afecciones, entidad económica de los daños, etc.). (Abanto, 1997, p. 153)

En el marco de la legislación y del desarrollo jurisprudencia de las **Comisiones de INDECOPI** se está llegando a cimentar una serie de principios del Derecho Administrativo sancionatorio (contravencional) similares a los existentes en la legislación y jurisprudencia comparadas:

- a. Se reconoce la responsabilidad objetiva para determinar la existencia de una infracción y ordenar el cese de la práctica. No obstante, para imponer sanciones, rige el principio de culpabilidad (dolo o imprudencia).
  
- b. En todos los casos de competencia de las Comisiones y Oficinas del INDECOPI se tiene que agotar la vía administrativa antes de acudir a la vía judicial (artículo 16 del Decreto Ley N° 25868), salvo que exista una regulación distinta y expresa sobre la materia que establezca otra cosa.

- c. Sólo la mayor gravedad de la infracción configura la necesidad de una persecución penal. Ella está dada mayormente por un **dolus malus** (malicia). (Abanto, 1997, p. 154)

### 2.2.3. El Espionaje Empresarial a Nivel Internacional

- El espionaje corporativo comprende el acceso ilícito en la esfera privada de la empresa donde se encuentra la información, para lo cual es necesaria la superación ilícita de las barreras impuestas por su titular para protegerla. Asimismo, el espía infractor ve facilitada su labor al emplear medios telemáticos, el uso de correo corporativo con ayuda de trabajadores de confianza, para la transferencia ilegítima de información valiosa, de carácter comercial como los secretos industriales (fórmulas químicas para elaboración de productos rentables), así como también la información secreta para la obtención de ventaja estratégica competitiva como la lista de clientes, proveedores, balance patrimonial, el plan de marketing y mercadotecnia. (Fernandez, 2018, p. 40)
- Actualmente, las empresas se están adaptando a nivel internacional a un nuevo modelo de "business as usual" para minimizar los riesgos de salud asociados con los empleados y clientes que están en estrecho contacto físico. Esta adaptación ha empujado a millones de personas a estructuras de trabajo remotas o a interacciones en línea entre clientes y empresas. Con este cambio de comportamiento vienen riesgos adicionales de seguridad de la información para la confidencialidad, integridad y disponibilidad de los sistemas de información clave. (Lovejoy, 2020, p. 2)
- La comisión del espionaje corporativo tenía lugar predominantemente mediante el robo de documentación en formato papel, se torna en nuestros días en una actividad sin fronteras, de contornos indefinidos, que abarca además del llamado secreto industrial, información reservada de naturaleza comercial y constituyendo la vía de ataque por antonomasia mecanismos que emplean de

una u otra forma artificios técnicos y medios telemáticos, dando lugar al nacimiento de una nueva forma de conducta, el llamado ciberespionaje. (Fernandez, 2018, p. 20)

- Los agentes espías que llevan a cabo el robo de datos con fines de extorsión, ataques de rescate disruptivos o destructivos, y/o que tratan de dañar la marca de una empresa, se han dirigido a organizaciones que se consideran bajo una tensión relacionada con la pandemia actual. Además, las acciones o declaraciones de una empresa que se consideren inapropiadas podrían desencadenar amenazas de "hacktivistas" y de personas con información privilegiada que den lugar a interrupciones en los diversos negocios, o a robos y divulgación de información confidencial de empresas. (Lovejoy, 2020, p. 4)

#### **i. Información Empresarial no Divulgada**

- Por lo que respecta al objeto del espionaje corporativo, este viene constituido por los secretos de empresa, que engloban toda información de índole industrial y comercial (en especial, las listas de clientes), se define a partir de lo establecido en el artículo 39.2 del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio o el 2.1 de la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo de 8 de junio de 2016 relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas. (Fernandez, 2018, p. 24)
- Según Fernández (2018) y acorde a la normativa mencionada anteriormente, la información debe cumplir tres requisitos:
  - 1) Esta ha de tener carácter reservado, entendiendo por tal que no sea generalmente conocida ni fácilmente accesible por las personas que pertenecen al círculo donde normalmente aquella se utiliza.

- 2) El titular de la información debe manifestar su voluntad de mantenerla en secreto, adoptando para ello medidas razonables en el caso concreto
  - 3) La información tiene que tener un valor empresarial, lo cual dependerá de cada empresa, por lo que incluso las cosas más triviales en apariencia pueden ser calificadas como secreto empresarial, si para su titular tienen valor. (Fernandez, 2018, p. 24)
- Actualmente toda empresa tiene presencia en internet y la mayoría de sus datos digitalizados, lo cual aumenta exponencialmente los riesgos de ataque. Las actuales tendencias como la migración de los datos a la nube y la salida de la red interna de la empresa hacia los aparatos móviles hacen que la tarea de proteger la propiedad intelectual de una empresa sea mucho más difícil, lo cual se agrava en el caso de las pequeñas y medianas empresas, que como se ha dicho, predominan en España, normalmente vinculadas a una actividad concreta y menos tendentes a prestar atención al desarrollo de un efectivo programa de ciberseguridad. (Fernandez, 2018, p. 31)

## ii. El Deber de Guardar Reserva

- Para Vergara (2014), el sujeto destinatario de la información de valor competitiva no debe de ser imputado como partícipe o a no ser que haya cooperado activamente en la realización del mismo. Habría que diferenciar por tanto dos supuestos:
  - 1) Que este tercer sujeto se haya limitado a recibir la información, en cuyo caso quedará impune;
  - 2) Que el mismo haya participado de manera activa en la difusión, revelación o cesión del secreto, en cuyo caso será condenado como coautor o partícipe, dependiendo del caso basta con que el sujeto actúe con el conocimiento de que está poniendo en riesgo la capacidad competitiva de la empresa. (Vergara, 2014)

- Baucells, citado por Vergara (2014) señala que la obligación de guardar reserva aparecerá sólo cuando al sujeto le han sido confiados los secretos de empresa, bien porque estos constituyen el objeto del contrato (el investigador, el licenciatario del know-how), o bien porque son la materia que le corresponde analizar para desarrollar las tareas propias de su trabajo, añadiendo que de este modo quedaría fuera de la relevancia penal de este precepto la revelación de secretos realizada por otros sujetos, a pesar de que mantuviesen una relación laboral con el titular del secreto.” (Vergara, 2014)
- El sector doctrinal español ha venido afirmando que mientras la relación jurídica entre el sujeto y el titular del secreto (contrato de trabajo, prestación de servicios, etc.) permanezca vigente, el sujeto que, en contra de los deberes básicos de buena fe y diligencia profesional divulgue o emplee en provecho propio información relevante de la empresa, será condenado por la comisión del delito contemplado en el artículo 279 del código penal español. (Vergara, 2014)

#### **2.2.3.1. Información o Conocimiento relativo a la Empresa**

- La naturaleza de la información o conocimiento que puede protegerse como secreto empresarial se caracteriza, ya en su misma denominación (“secreto empresarial”) y requisitos de protección (“valor empresarial”), por versar sobre cualquier aspecto de la actividad empresarial; en este sentido, incluye informaciones y conocimientos que pertenecen a la esfera industrial, científica, tecnológica, organizativa, comercial y financiera u otra de la actividad empresarial, esto es, de la actividad de producción y mediación de bienes y servicios, cualquiera que sea el ámbito o fase de esa actividad a la que se refieran (desde la concepción de la idea hasta la implementación de su desarrollo, ejecución y comercialización o utilización). (Massaguer, 2019, p. 52)

#### **2.2.3.2. El Espionaje corporativo y violación del Secreto Comercial: Legislación Extranjera**

- Dentro de la protección de Derecho identificamos dos elementos fundamentales, el primero consiste en el reconocimiento y protección legal del derecho a poseer y proteger un secreto comercial tanto a nivel supranacional como a nivel de los ordenamientos jurídicos nacionales y el segundo es la defensa de este derecho en sede jurisprudencial.
- En el ámbito supranacional la protección del secreto comercial se constata en el artículo 39 de los Acuerdos de la Organización Mundial del Comercio sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), el cual reconoce el derecho a la protección a la información no divulgada y establece que, como parte de una protección eficaz contra la competencia desleal, los Miembros tienen la obligación de proteger la información no divulgada y de carácter confidencial. (ADPIC, 1994, art. 39)
- El segundo párrafo de la norma señala que las personas físicas y jurídicas tendrán la posibilidad de impedir que la información que esté legítimamente bajo su control se divulgue a terceros o sea adquirida o utilizada por terceros sin su consentimiento de manera contraria a los usos comerciales honestos, en la medida que dicha información cumpla los requisitos de: no ser conocida en el ámbito de la actividad, tener un valor comercial por ser secreta y que sea objeto de medidas razonables para mantenerla secreta. (ADPIC, 1994, art. 39)
- En el caso de México, la Ley sobre Propiedad Industrial tipifica como delitos conductas como la revelación de secretos comerciales a personas no autorizadas, apoderarse por cualquier medio y el uso de información considerada como secreta en beneficio propio. (Ley Federal de Propiedad Industrial, 2020, art. 401)
- En el caso de España encontramos que en la Ley de Competencia Desleal se sancionan como actos desleales la divulgación o explotación del secreto

sin autorización del titular, de secretos industriales o de cualquier otra especie de secretos empresariales a los que se haya tenido acceso legítimamente, pero con deber de reserva, o ilegítimamente, con ánimo de obtener provecho, propio o de un tercero. (Ley 3/1991, 1991, art. 13)

- También se sanciona el perjuicio ocasionado al titular del secreto y que la divulgación o explotación tenga lugar como consecuencia de la inducción a trabajadores, proveedores, clientes y demás obligados, a infringir los deberes contractuales básicos que han contraído con los competidores. (Ley 3/1991, 1991, art. 14)
- Además, se sanciona la inducción a la terminación regular de un contrato o el aprovechamiento en beneficio propio o de un tercero de una infracción contractual ajena sólo se reputará desleal cuando, siendo conocida, tenga por objeto la difusión o explotación de un secreto industrial o empresarial o vaya acompañada de circunstancias tales como el engaño, la intención de eliminar a un competidor del mercado u otras análogas. (Ley 3/1991, 1991, art. 14)

### **2.2.3.3. El Ciberespionaje Empresarial**

- El ciberespionaje se reprime en el Código penal español en el artículo 278.1, el cual establece la aplicación de una pena de dos a cuatro años de prisión o de doce a veinticuatro meses de multa a “El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197”. Este último precepto, alude también al apoderamiento de ciertos soportes, la interceptación de las telecomunicaciones y la utilización de artificios técnicos de escucha, transmisión, grabación, reproducción del sonido, de la imagen, o de cualquier otra señal de comunicación. (Fernandez, 2018, p. 23)

- La doctrina ha puesto de manifiesto que a pesar de que las empresas a menudo realizan importantes inversiones para generar ideas y productos, es frecuente que no lo hagan significativamente en la protección de su valioso capital intelectual. El ciberespionaje en España encuentra castigo en la referencia a la interceptación de las telecomunicaciones, la cual, junto a la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, procede del mismo antecedente legislativo, esto es, la regulación de las llamadas escuchas ilegales. (Fernández, 2018, p. 24)

#### **2.2.3.3.1. La Utilización de la información obtenida mediante ciberespionaje**

- La utilización de la información obtenida mediante ciberespionaje definido ya el ámbito típico de la revelación como toda puesta bajo el dominio o control de un tercero de información empresarial reservada que no debería conocer, queda claro que el desvalor de acción de este comportamiento difiere del de la conducta de utilización de secretos de empresa. Esta última debe ser entendida como sinónimo de explotación o de aprovechamiento. Según una interpretación teleológica de la conducta de utilización referida a secretos de empresa, por tal debe entenderse toda actuación guiada por el contenido de dicha información, independientemente de que esta llegue o no al conocimiento de terceros. (Fernández, 2018, p. 44)
- Dicha concepción del término abarcaría cualquier explotación del secreto de empresa derivada de su ejecución o puesta en práctica en un ámbito de negocio (supuestos de aprovechamiento activo) o bien del aprovechamiento de su conocimiento para conseguir una ventaja omitiendo una actuación en un determinado sentido, si se trata de una información negativa que permite dar a conocer vías de actuación fallidas (supuestos de aprovechamiento omisivo). (Fernández, 2018, p. 45)

- La aceptación de estos últimos casos puede plantear mayores dificultades, si pretende entenderse la utilización como una conducta exclusivamente activa. Sin embargo, su admisión es perfectamente posible, pudiendo apreciarse que se da un comportamiento activo u omisivo de aprovechamiento del secreto empresarial, cuando existe un nexo intelectual entre el conocimiento del contenido de este y la conducta del sujeto activo. (Fernández, 2018, p. 45)

#### **2.2.3.3.2. La revelación de la información obtenida mediante ciberespionaje**

- El ciberespionaje constituye una de las modalidades comisivas del tipo de espionaje empresarial del artículo 278.1 del Código Penal Español. Sin embargo, el mismo precepto en su apartado segundo recoge una agravación de las consecuencias punitivas del espionaje, castigando al sujeto activo de este delito con la misma pena de multa, de doce a veinticuatro meses, y con prisión de tres a cinco años «si se difundieren, revelaren o cedieren a terceros los secretos descubiertos». (Fernández, 2018, p. 42)
- La previsión por el legislador penal de los verbos típicos de difundir, revelar y ceder, derivada del traslado acríptico que este hizo de los delitos relativos a la intimidad (artículo 197.1 Código Penal Español) para la tipificación del espionaje empresarial, responde a la voluntad de intentar abarcar todo tipo de comunicación de la información, desde la que se da a un solo sujeto (revelación y cesión) hasta aquella otra en la que esta se convierte en pública y notoria (difusión). De este modo, cabría concluir que en realidad la difusión no es más que una revelación o cesión realizada a un gran número de destinatarios. (Fernández, 2018, p. 42)

#### **2.2.3.3.3. El acceso ilícito como presupuesto típico del ciberespionaje**

- El acceso ilícito constituye el presupuesto típico del espionaje empresarial, debiendo producirse de forma remota o telemática en el caso del ciberespionaje, esto es, en el escenario virtual y sin acción física o directa sobre el equipo atacado. Sin embargo, no es suficiente con que este concurra para entender que se ha consumado el delito, siendo necesario algo más, esto es, que el sujeto efectivamente tenga el dominio sobre la información reservada. (Fernández, 2018, p. 24)

#### **2.2.3.4. La inteligencia Competitiva**

- La inteligencia, basada en el concepto de estrategia, consiste en encontrar y analizar información para actuar de forma estratégica, cualquiera que sea su ámbito y constituye el reverso de las distintas conductas de espionaje, surgiendo también para combatirlo ante las dificultades que su lucha presenta. Dichas dificultades se acrecientan ante la realidad actual en la que dos elementos marcan el rumbo de la actividad económica: la globalización de los mercados y el constante auge de las nuevas tecnologías. A los efectos que aquí interesan, aludiremos a tres tipos de inteligencia: la económica, la jurídica y la competitiva o empresarial. (Fernandez, 2018, p. 35)
- En primer lugar, el concepto de inteligencia económica puede entenderse como el conjunto de acciones coordinadas de investigación, tratamiento y distribución de la información para tomar decisiones en el orden económico. En esta actividad, en el ámbito español, el actor principal sería el Estado, con el fin de defender sus intereses económicos en el marco internacional. El reverso de este tipo de actividad lícita sería el espionaje económico que tiene lugar entre Estados, del que serían buen ejemplo los casos de Rusia o China. La alusión a este tipo de inteligencia resulta necesaria para no confundirla con la que aquí interesa, que es la empresarial o competitiva, y que podría englobarse dentro de la económica, cuando el actor de esta fuera el Estado. (Fernandez, 2018, p. 36)

- En segundo lugar, la llamada inteligencia jurídica puede definirse como el conjunto de técnicas y medios que permiten a un actor privado o público conocer el entorno jurídico en el que participa, para identificar y anticipar los riesgos y las oportunidades potenciales de actuación, así como disponer de las informaciones y derechos necesarios para poder poner en práctica los instrumentos jurídicos aptos para realizar sus objetivos estratégicos. El conocimiento de este tipo de información permite a las empresas, como actores privados, garantizar la protección jurídica de sus bienes inmateriales, como son los secretos de empresa, desarrollando estrategias preventivas para ello. (Fernandez, 2018, p. 36)
- Un requisito fundamental de la inteligencia competitiva es la licitud de sus medios de búsqueda en fuentes de acceso público, por lo que toda indagación de información empresarial de un competidor cuya obtención suponga vulnerar las barreras de lo legítimo, quedaría extramuros del concepto de inteligencia y pasaría a formar parte del espionaje empresarial. Así, existen ciertas vías lícitas de hacerse con información empresarial ajena, sin el consentimiento de su titular, siempre que sobre ella no recaiga un derecho absoluto de propiedad industrial. Entre ellas se encuentran la ingeniería inversa, las investigaciones independientes y los descubrimientos por azar y todos ellos serían medios posibles en el contexto de la inteligencia competitiva. (Fernandez, 2018, p. 37)

#### **2.2.3.5. Los MetaDatos y la Información secreta de Empresa**

- Los metadatos son definidos como como descripciones de la información contenida en un documento físico o electrónico. Estos datos sobre el documento, pueden aportar valiosa información sobre el contenido de aquel, aun cuando no se acceda a este. Como ejemplo tenemos el título que damos a un documento electrónico cualquiera, ya sea privado o en el contexto de una empresa, el cual sería un dato del texto, a la vez que un metadato, pues

estaría entre la información que describe el documento. Los metadatos se desprenden de una simple llamada telefónica o de un correo electrónico, pues si accedemos al registro de llamadas o a la bandeja de entrada podemos ver información como la hora, la fecha, el emisor o incluso la localización de una llamada o mensaje, y en este último caso también su asunto puede tener un importante valor. (Fernandez, 2018, p. 38)

- Los metadatos puedan ser considerados secreto de empresa, y como ocurre con cualquier tipo de información, es necesario que su titular haya adoptado las medidas pertinentes para su protección, lo cual en el caso de este tipo de información es habitual que se descuide. En el supuesto de una cuenta de correo electrónico corporativo o de un teléfono, en la medida en que se establecen contraseñas de acceso y medidas de seguridad para proteger la información contenida en ellos, los metadatos reciben también dicha protección. Sin embargo, hay otros supuestos en los que se descuida por parte del titular la protección de esta información, como por ejemplo, cuando se publican ciertos documentos para su descarga en la web de la empresa, sin que se suprima previamente la información añadida sobre dicho documento. (Fernandez, 2018, p. 39)

## **2.2.4. CAPÍTULO I: Las Personas Jurídicas**

### **2.2.4.1. Subcapítulo I: El Know How y los Tipos de Información Secreta de Empresa**

Stumpf, citado por Alfaro (2013), se refiere al know how como un contrato que trata sobre un saber (técnico, comercial, económico) no protegido por derechos de tutela industriales, usualmente mantenido como secreto, y cuya explotación le permite al beneficiario no sólo la producción y la venta de objetos sino también otras actividades empresariales.

Narvéez García, citado por Alfaro (2013) señala que el contrato de know how: "versa sobre prestación de conocimientos relativos a objetos (piezas de

prueba, modelos no registrados, máquinas, aparatos, herramientas, instalaciones de mecanización, inventos no patentados, etc.) datos y antecedentes técnicos que incluyen cálculos, fórmulas, planos, especificaciones, dibujos o diseños, etc.; e instrucciones para fabricar, producir o explotar un producto; o sobre procedimientos de fabricación; o comunicación de experiencias de explotación, o consejos prácticos y explicaciones sobre una patente determinada; o indicaciones para planificar la producción, distribución o venta directa y demás que se estimen complementarias. (Alfaro, 2013)

Según definición de la Cámara de Comercio Internacional know how significa, conocimientos aplicados métodos y datos que son necesarios para la utilización efectiva y puesta en práctica de técnicas industriales. Asimismo, según esta Cámara, el know how consiste en la totalidad de los conocimientos del saber especializado y de la experiencia, volcados en el procedimiento y en la realización técnica de la fabricación de un producto. (Alfaro, 2013)

Es el conjunto de conocimientos técnicos relativamente originales y secretos, o por lo menos escasos, que permiten a quien los detenta una posición privilegiada en el mercado". El contrato de know how, en consecuencia, sería aquel en que "una parte mediante el pago de cierta suma, provee a otra, informaciones tecnológicas escasas, de forma que posibilite a ésta una posición privilegiada en el mercado". En suma, lo que se trasfiere, en realidad, no es la tecnología, sino la oportunidad comercial que de ella resulta. (Alfaro, 2013)

**El Know How** es el saber o conocimiento técnico aplicable a nivel empresarial, de carácter secreto por su **alto valor económico** y susceptible de contratación. Este concepto limita lo entendido por conocimiento a lo estrictamente técnico, es decir, propio de un determinado ámbito tecnológico, industrial, comercial, entre otros; asimismo, depende de su eficacia (traducida en utilidad económica) para una persona natural o jurídica, y, por

su carácter reservado excluye el conocimiento que se enseña o los adquiridos para una actividad diaria o corriente, máxime si lo complementamos con lo susceptible de contratación. Igualmente, al indicar conocimiento o saber, en el mismo, ya se está agrupando a los procedimientos, métodos, fórmulas, experiencia, habilidad u otra forma que indique la resultante de un procedimiento de abstracción de algo. (Benavente, 2012)

#### **2.2.4.1.1. Características del Know How (Secreto Empresarial)**

La información empresarial se encuentra conformada por el conjunto de datos que permite a una empresa acceder al mercado o generar el conocimiento necesario para permanecer en el mismo. Muchas veces, con la experiencia que obtienen de la propia competencia y/o gracias a la inversión en investigación y desarrollo que realizan, por mencionar algunas formas, las empresas obtienen información que les otorga una ventaja competitiva, la cual, en la mayoría de casos, no desean que sea conocida por sus competidores. (Sosa, 2016, p. 248)

#### **2.2.4.1.2. Mecanismos de Protección del Secreto Empresarial**

Según Sosa (2016), los titulares del secreto empresarial, suelen usar mecanismos para protegerla:

- i. El primero de ellos es proteger dicha información como patente, en la medida que ésta cumpla con los requisitos u obra, con lo cual obtiene un derecho de exclusiva sobre el uso de la misma, impidiendo, de este modo, la utilización de dicho bien por terceros, pero únicamente por un determinado periodo de tiempo (veinte años, en el caso de la patente; y la vida del autor más setenta años en el caso de obra protegida por los Derechos de Autor). (p.247)

- a. Asimismo, el uso del sistema de patentes implica que sus competidores tengan acceso a ella, lo cual muchas veces no es deseado por el agente económico titular de la información que considera secreta pues entiende que, de conocer dicha información, sus competidores pueden ahorrarse costos en investigación e incluso desarrollar un producto mejor que les genere en un futuro una ventaja competitiva. (Sosa, 2016, p.247)
- b. El mecanismo alternativo de protección es privado y, de hecho, más eficiente pues, si se maneja bien, puede quizás no solo generarle en la práctica un uso exclusivo a su titular, sino además impedir efectivamente el acceso a la información a sus competidores durante el periodo de tiempo que desee. (Sosa, 2016, p.247)
- c. Dicho mecanismo es la protección interna que puede implementar la misma empresa para que dicha información no sea divulgada, adquirida o explotada por otros agentes económicos; es decir, el “titular” asume los costos de protección de su secreto empresarial a través de mecanismos de seguridad y, en caso de apropiación o sustracción de dicha información sin su consentimiento, podrá recurrir al Estado que, a través del Decreto Legislativo 1044 –Ley de Represión de la Competencia Desleal (LRCD)–, sanciona estos actos. (Sosa, 2016, p.247)
- d. En efecto, la protección que le brinda la Ley de Represión de la Competencia Desleal al poseedor del secreto no se trata de una tutela al secreto en sí, sino contra los actos contrarios al principio de competencia por eficiencia que se deriven de la sustracción de dicho secreto; en este caso en particular, la divulgación, apropiación y explotación indebida del secreto por terceros sin autorización de su titular. (Sosa, 2016, p.247)

“Los Países Miembros otorgarán patentes para las invenciones, sean de producto o de procedimiento, en todos los campos de la tecnología, siempre que sean nuevas, tengan nivel inventivo y sean susceptibles de aplicación industrial”. (Decisión N° 486, 2000, Art. 14)

- ii. La protección de la empresa por parte del Estado frente a la sustracción ilícita de sus secretos comerciales tiene fundamento económico, a pesar de que se trata de un costo privado que podría generar beneficios a la sociedad, toda vez que se revelaría información que puede ser utilizada de modo productivo generando con ello mayor competencia en el mercado (a diferencia de un robo de propiedad material). Sin embargo, dicho beneficio social será inferior a la suma de los costos sociales generados por la sustracción de información por robo o espionaje, medidos por los recursos destinados a conseguir y a evitar una transferencia de riqueza involuntaria, así como la reducción de incentivos a la actividad inventiva. (Sosa, 2016, p. 250)

De este modo, la posición de Sosa (2016) es que se justifica la sanción a la obtención de un secreto empresarial por la fuerza o por fraude ya que, de no ser así, se incurriría en elevados costos en concepto de autorremedios y, además, los incentivos para la actividad inventiva se verían dañados.

#### **2.2.4.2. Subcapítulo II: El Know How y el Secreto Comercial**

##### **2.2.4.2.1. El Know How**

Se ha entendido que el know how es el saber especializado o habilidad técnica o conocimiento práctico que permite lograr un objetivo específico. Dicho saber se mantiene en secreto, por lo tanto, no son patentables en la medida que las patentes son de carácter público y su protección es limitada en el tiempo. (Mercado, 2009, p. 398)

Según Aníbal Sierralta, citado por Mercado (2009) el Know How es un conocimiento técnico, comercial científico o industrial de naturaleza secreta. Hay quienes, como la Organización Mundial de la Propiedad Intelectual,

consideran al Know How ligado a las patentes de invención, los que opinan que no deben limitarse sólo a aspectos industriales e incluso los que opinan que no tienen que ser secretos. (p. 399)

Gómez, citado por Alfaro (2013) señala, al referirse al aspecto oculto del secreto, que "el carácter reservado y el desconocimiento por los terceros es un presupuesto esencial para la existencia del secreto industrial. Más aún, se puede decir que la falta de divulgación del secreto constituye el elemento fundamental y decisivo para la existencia del secreto empresarial. La condición de know how de ese conocimiento técnico transmitido con restricción de difusión, se encuentra determinada por la situación de que su posesión represente una ventaja en el giro de negocio de quien la recibe. (Alfaro, 2013, p. 239)

En lo que concierne propiamente al "know how" o secreto empresarial, abarca tanto los secretos industriales como empresariales. Asimismo, se concibe en doctrina que su esencia consiste en un secreto sobre un conjunto de conocimientos de carácter industrial (de productos o procedimientos), comercial o para la prestación de un servicio, que proporciona una ventaja competitiva a quien lo posee, y que se esfuerza por no divulgarlos. (Alfaro, 2013, p. 240)

#### **2.2.4.2.2. Categorías del Know How:**

- a)** La primera categoría alude al secreto industrial, que engloba conocimientos relativos a la fabricación de un determinado producto, a la aplicación de un determinado procedimiento, a la producción y prestación de un determinado servicio y, en fin, cualquier información relacionada con el ámbito técnico-productivo de la actividad económica. En este sentido, el término producción abarca no sólo el sector de la fabricación, sino también el de la reparación, montaje, etc. (Morón, 2002)

- b) El secreto comercial, definido residualmente respecto al industrial, incluye información atinente a la organización interna de la empresa (administración) o a las relaciones entre empresa y clientela (distribución) o proveedores (suministro), esto es, todo lo que afecta a la organización o estructura comercial de la empresa; así, comprende listas de proveedores y clientes, estrategias financieras, planes publicitarios, técnicas de venta, programas de marketing, estudios de mercado, etc. (Morón, 2002)

#### **2.2.4.2.3. El Secreto Comercial:**

Se entiende por secreto comercial como el conjunto de las informaciones escasas, de carácter financiero, económico, comercial o tecnológico, que permiten a la empresa que las posee una posición privilegiada. La información confidencial, que igualmente puede ser de carácter financiero, comercial, e inclusive tecnológico, es parte de un secreto comercial transmitido bajo reserva de difusión, a cambio de alguna ventaja para el trasmisor. (Alfaro, 2013)

Según Vivian Chateloin Lorenzo citado por Mercado (2009), dependiendo del sistema jurídico, la protección de los secretos comerciales forma parte del concepto general de protección contra la competencia desleal, o de base en disposiciones específicas o jurisprudenciales sobre la protección de información confidencial. Por lo tanto, el Know How y los secretos comerciales incluidos en una iniciativa, para gozar de protección tienen que ser perfectamente identificados o identificables y deben ser declarados expresamente en la petición como información confidencial y reservada aún en el supuesto que la iniciativa se haga pública. La forma de protección se determinará en cada caso. (p. 400)

#### **i. Contenido del Secreto Comercial:**

Aracama, citado por Fonseca (2017) lo ha dividido en dos clases atendiendo al tipo de información que se protege, a saber, en secretos

comerciales técnicos y secretos comerciales de gestión. **Los primeros** encierran información relacionada con fórmulas, procedimientos, recetas, técnicas de producción o de clasificación, prototipos, compilaciones de datos, un programa, un dispositivo, entre otras informaciones de similar naturaleza. **Los segundos**, contienen información sobre sistemas de comercialización o gestión del negocio, métodos y estrategias de ventas y publicidad, perfiles de empleados y consumidores, selección de personal, organización empresarial entre otros.

#### **2.2.4.2.4. Normativa Aplicable:**

En los casos en los que se alegue una infracción a una patente cuyo objeto sea un procedimiento para obtener un producto, corresponderá al demandado en cuestión probar que el procedimiento que ha empleado para obtener el producto es diferente del procedimiento protegido por la patente cuya infracción se alegue. A estos efectos se presume, salvo prueba en contrario, que todo producto idéntico producido sin el consentimiento del titular de la patente, ha sido obtenido mediante el procedimiento patentado, si:

- a) El producto obtenido con el procedimiento patentado es nuevo.
- b) Existe una posibilidad sustancial de que el producto idéntico haya sido fabricado mediante el procedimiento y el titular de la patente de este no puede establecer mediante esfuerzos razonables cuál ha sido el procedimiento efectivamente utilizado. En la presentación de pruebas en contrario, se tendrán en cuenta los intereses legítimos del demandado o denunciado en cuanto a la protección de sus secretos empresariales. (Decisión N° 486, 2000, art. 240)

Al referirnos a los secretos empresariales, aludimos a una forma de propiedad intelectual con las peculiaridades que ello puede implicar. La calificación de la propiedad intelectual como “propiedad” no ha estado ni está exenta de debate. La propiedad intelectual, en general, implica el reconocimiento u otorgamiento de un derecho de exclusiva a favor del titular con relación al objeto protegido (un signo con aptitud distintiva o una invención patentable, por ejemplo). (Rodríguez, 2014, p. 52)

Ese derecho de exclusiva se proyecta, de ordinario, de forma negativa. Decimos de forma negativa porque estos derechos suelen consistir en facultades para impedir la realización de ciertos actos no autorizados con relación a las titularidades existentes. La concesión de una patente farmacéutica no autoriza al titular a comercializar el producto en el mercado de la misma forma que el registro de la marca no implica una autorización para usar el signo. (Rodríguez, 2014, p. 52)

Asimismo, la propiedad intelectual, suele ser concebida con dos limitaciones importantes:

- (i) Limitaciones de orden temporal referidas al plazo de vigencia del derecho.
- (ii) Limitaciones de orden estructural que incluyen las denominadas excepciones al derecho que, en realidad, no hacen a la configuración del mismo, sino que aluden a los campos no cubiertos por éste. (Rodríguez, 2014, p. 52)

A nivel nacional, es el Decreto Legislativo N° 1044 “Ley de Represión de la Competencia Desleal” la fuente normativa que ha desarrollado los denominados actos de competencia desleal en la modalidad de violación de secretos empresariales. Los actos de violación de secretos

empresariales consisten en la realización de actos que tengan como efecto, real o potencial, lo siguiente:

- a) Divulgar o explotar, sin autorización de su titular, secretos empresariales ajenos a los que se haya tenido acceso legítimamente con deber de reserva o ilegítimamente.
- b) Adquirir secretos empresariales ajenos por medio de espionaje, inducción al incumplimiento de deber de reserva o procedimiento análogo. (Decreto Legislativo N° 1044, 2008, art. 13)

En ese orden de ideas, podría discutirse si es la vía de la competencia desleal el mecanismo de tutela para los secretos comerciales, en cuyo caso el reproche no versará sobre el empleo no autorizado del secreto, sino sobre las formas o medios empleados para hacerse de éste. (Rodríguez, 2014, p. 52)

La disciplina de la represión de la competencia desleal lo que se sanciona es el empleo de **medios indebidos**. Esto tiene sentido si se considera que lo que el derecho pretende evitar es que los participantes del mercado compitan basándose en cuestiones distintas a su propia eficiencia o esfuerzo (mérito de las propias prestaciones): cuando uno gana al cliente del competidor porque mejora su producto de forma que lo hace más atractivo, compite sobre la base de su propio esfuerzo o su propia eficiencia. (Rodríguez, 2014, p. 52)

#### **2.2.4.2.5. El bien Jurídico en los Delitos Económicos:**

El bien jurídico susceptible de tutela penal se identifica con los intereses que, conforme a la convicción general de la sociedad, son especialmente valiosos y particularmente necesitados de protección. El bien jurídico es presupuesto para satisfacer una necesidad humana, proveyendo así, a la

autorrealización del individuo. De estas características se desprende que el bien jurídico se encuentra ligado indisolublemente a la estructura de la sociedad y la evolución de la misma. (Bramont, 1992, p. 87)

El "orden económico del Estado", se identifica por el campo de acción regulado expresamente por el Estado en materia económica, vale decir, los aspectos económicos que le interesan al Estado regular a efectos de lograr un sistema económico que brinde los mayores servicios a la colectividad. De esta forma, se excluyen todos los aspectos en los cuales el Estado no interfiera en la economía. (Bramont, 1992, p. 88)

El orden económico del Estado es la regulación jurídica del intervencionismo estatal en la economía. En consecuencia, sólo interviene el Derecho Penal (defendiendo un bien jurídico "orden económico") cuando se afecta el plan económico previsto, elaborado y ejecutado por el Estado. Cualquier conducta que dañe el bien jurídico no constituirá delito, sino sólo aquella que se realice mediante una acción disvaliosa, es decir aquella conducta que manifieste un desprecio por el bien jurídico, mediante una grave agresión al mismo, por parte del sujeto activo. (Bramont, 1992, p. 88)

#### **2.2.4.2.6. Perspectivas del Secreto Empresarial:**

Existen dos perspectivas en referencia a los secretos comerciales que ha formulado la doctrina y que resultan absolutamente aplicables al género de los secretos empresariales.

- (i) Una visión que propugna o admite la propietarización de los secretos.
- (ii) La perspectiva que concibe al derecho sobre los secretos empresariales como uno de carácter conductual (atiende a los

medios indebidos y no al bien en sí mismo). (Rodríguez, 2014, p. 53)

Desde la primera perspectiva (el secreto como forma de propiedad intelectual), Epstein citado por Rodríguez (2014) sostiene que es precisamente porque existe un derecho de los individuos a mantener el secreto que existe la facultad para permitir la revelación de esa información a terceros bajo condición de confidencialidad. Así, se consideraría extraño pretender la ejecución de un contrato de información confidencial si el poseedor original no tuviera derecho de propiedad alguno sobre el secreto. (p.53)

Desde la perspectiva conductual, se sostiene que un secreto comercial no constituye propiedad en el sentido usual, ni en el sentido de la propiedad real, ni en el sentido de la propiedad intelectual; ya que no es algo sobre lo cual el poseedor tenga un derecho de exclusiva de uso y disfrute. (Rodríguez, 2014, p. 53)

#### **2.2.4.2.7. El Secreto Comercial y el Derecho Relativo a los Secretos Comerciales:**

Sobre la base de esta última postura, Goldstein citado por Rodríguez (2014) distingue entre el secreto comercial y el derecho relativo a los secretos comerciales de la siguiente manera:

- a) El Secreto Comercial encarna la información apropiada por una empresa y resguardada a través de distintas medidas de seguridad y prácticas del personal.
- b) El derecho sobre los secretos comerciales comienza cuando el secreto termina protegiendo a la compañía que, a pesar de las

medidas y esfuerzos adoptados, no pudo preservar el secreto a pesar de la razonabilidad de las previsiones adoptadas para su manutención. (p. 53)

**Confidencialidad:** La Protección del secreto consiste en no difundir la tecnología o invención y mantenerla en reserva. Para que se haga efectiva la protección, se celebran acuerdos de confidencialidad y también se incluyen cláusulas de confidencialidad dentro de todos los contratos de investigación y colaboración. Esta protección permite preservar el secreto de la información frente a todo intento de revelación indebida y utilización por terceros sin autorización. (Saavedra, 2016)

El propósito del derecho es proteger la información empresarial de la caza furtiva de empleados poco leales o de los intrusos indeseados; de esta forma, el derecho sobre los secretos comerciales sería una red de seguridad (safety net) que adolecería de cierta debilidad dado que confiere una protección circunstancial y variable. (Rodríguez, 2014, p. 53)

🚦 Respecto a limitación en el campo de protección que confiere el derecho sobre los secretos, Friedman, Landes y Posner, citados por Rodríguez (2014) refieren que existen dos consideraciones:

- (i) El factor reciprocidad, que se basa en el hecho de que todo productor de información es también consumidor de información, debiéndose considerar el dato económico que revela y que, cuando los costos sociales de proteger un secreto a través del sistema legal son altos, es probable que los beneficios de la información compartida excedan los beneficios de una protección legal demasiado sólida.

- (ii) Debe considerarse los costos y beneficios diferenciales con respecto a las diversas maneras de apropiarse de los secretos y de evitar tales apropiaciones. En cierta forma, el derecho debería dar una respuesta ad hoc que tienda a otorgar únicamente la protección eficiente en cada caso. (p. 53)

Lemley, citado por Rodríguez (2014) argumenta que, aceptándose que el derecho de exclusiva no es absoluto, este derecho genera incentivos para inventar en el sentido que confiere al desarrollador de información valiosa y nueva el derecho de impedir que otros la usen, maximizando la posibilidad de aprovechamiento económico que se derivan de la información. (p. 53)

El derecho sobre los secretos comerciales genera incentivos para la revelación de información en dos formas distintas:

- (i) En tanto que actúa como sustituto de las inversiones en medidas físicas de preservación de secretos (ocultar una planta de nueva y alta tecnología podría ser físicamente costoso por lo que el derecho substituye esa necesidad)
- (ii) Que la existencia del derecho permite a su titular revelarla para negociar con relación a la misma. Para vender una idea de forma eficiente es esperable que se necesite revelarla, pero esa revelación haría perder la condición de secreto que, precisamente, le da el valor especial. Así, sin protección legal a esta titularidad, el valor del secreto se pierde; en cambio, con la protección, se puede impedir que terceros usen la idea en contravención a la confidencialidad de la relación existente. (Rodríguez, 2014, p. 54)

#### **2.2.4.2.8. Tipos de Información Confidencial:**

No toda la información que maneja una empresa tiene carácter de secreto comercial. Según Sosa (2016), la información que posee una empresa se puede dividir en tres categorías:

- a) **La información de dominio público**, que por su propia naturaleza puede ser tomada o utilizada por cualquier agente económico. Sobre esta información no protección jurídica alguna, debido a que su uso es permitido por cualquiera al tratarse de información que es de acceso público. Por ejemplo, los clientes de una empresa o sus planes de expansión si son publicados en su página web, las próximas promociones de una empresa de telefonía móvil si las revela a través de sus catálogos publicitarios, etc.
  
- b) **La información protegida por derechos de propiedad intelectual**, tales como una patente de invención, una patente de modelo de utilidad o una obra protegida por los derechos de autor. En esta categoría solo existen dos opciones lícitas para que la información que se protege pueda ser conocida por una empresa distinta a la titular:
  - (i) Que el titular permita su uso mediante licencias.
  
  - (ii) Que la vigencia de la protección haya vencido y la información protegida se haya trasladado al dominio público.
  
- c) La información que la empresa considera secreta y asume sus costos de protección con el fin de utilizarla en su beneficio exclusivo. En esta categoría, sólo existen tres posibilidades jurídicamente lícitas para que un agente económico distinto a su titular pueda tomar o utilizar dicha información:
  - (i) Que la empresa titular permita su uso o conocimiento restringido a determinados agentes mediante contrato con deber de reserva.

- (ii) Que la empresa titular libere dicha información, de modo voluntario o involuntario y que, en consecuencia, se pierda su reserva y se haya convertido en información de dominio público.
- (iii) El uso de ingeniería inversa. (Sosa, 2016, p. 249)

#### 2.2.4.2.9. ¿Cuándo estamos frente a un secreto empresarial?

- De acuerdo con el artículo 40 inciso 2 de la Ley de Represión de la Competencia Desleal - Decreto Legislativo N° 1044, la información empresarial, para considerarse como secreta, debe reunir las siguientes características:
  - a) Debe tratarse de un conocimiento que tenga carácter de reservado o privado sobre un objeto determinado.

Respecto del primer requisito, se dice que la información necesariamente debe versar sobre un objeto determinado, en el sentido de que debe referir algún dato específico e identificable. Una vez individualizada la información y determinada su existencia, se podrá apreciar si ésta es de naturaleza reservada, lo cual supone analizar si se encuentra o no a disposición de terceros no autorizados. (Sosa, 2016, p. 250)

Es importante precisar que el hecho de que determinada cantidad de personas disponga de la información no implica que ésta deje de ser secreta. Este es el caso de los trabajadores de una empresa que tengan acceso a dicha información, autoridades públicas a las que se les haya revelado el secreto o la información secreta que se haya revelado a otra empresa en una negociación, todos ellos sujetos a un deber de confidencialidad contractual o legal. (Sosa, 2016, p. 250)

- b) Que quienes tengan acceso a dicho conocimiento posean voluntad e interés consciente de mantenerlo reservado, adoptando las medidas necesarias para mantener dicha información como tal.

Ahora bien, conforme al segundo requisito, es indispensable para el titular demostrar una inequívoca voluntad de mantener el carácter secreto de la información, o al menos que haya adoptado precauciones significativas para su protección pues, de lo contrario, ninguna persona que pueda tener acceso a dicha información tendrá conocimiento de su carácter secreto y podría considerar que se trata de información de dominio público. (Sosa, 2016, p. 250)

- c) Que la información tenga un valor comercial, efectivo o potencial.

En relación con el tercer requisito, en reiterados pronunciamientos el INDECOPI ha señalado que podremos hablar de valor comercial efectivo o potencial de un secreto comercial cuando su uso reporte un provecho patrimonial para el empresario que lo posee y, consecuentemente, ello genere una ventaja frente a los competidores que lo desconocen. Este es justamente el principal motivo por el cual el empresario que posee dicha información tiene interés en mantenerla reservada y confidencial. Sobre este último requisito, es importante precisar que el término “valor comercial” debe ser entendido como “valor competitivo”, ya que no solo se limita a la información que pueda servir al agente económico en el intercambio de bienes o servicios. (Sosa, 2016, p. 250)

#### **2.2.4.2.10. Deber de Reserva:**

En el caso de la información que se comparte con deber de reserva a los empleados, ésta no pierde su carácter de secreto ya que, sin la colaboración o ayuda de éstos, el empresario no podría aplicar sus conocimientos secretos. Lo mismo podemos decir respecto de la información secreta que se comparte con **deber de reserva** en una negociación con otro agente económico, pues dicho traslado de

información muchas veces es relevante para poder llegar a un acuerdo, por ejemplo, en el caso de una fusión empresarial. (Sosa, 2016, p. 251)

Sobre la información que se le revele a una autoridad pública, ésta no pierde su carácter secreto pues dicha entidad estatal tiene una obligación legal de reserva, aparte de la responsabilidad que recae sobre la parte de solicitar la reserva de la información que envía, lo cual solo demuestra su intención de mantenerla en reserva. La información secreta puede incluso no trascender el ámbito interno de la organización productiva o consistir en información sobre procedimientos, técnicas, datos operativos o fórmulas que, luego del estudio de su utilidad o funcionalidad, se haya concluido que no son aplicables o que resultan irrelevantes. (Sosa, 2016, p. 251)

En efecto, por ejemplo, en el caso de la información de “valor negativo”, dicha información generará igual una ventaja competitiva al agente toda vez que, gracias a esos resultados negativos, conocerá qué camino no debe recorrer para cumplir su objetivo. Esto, de hecho, significa un ahorro importante en costos de investigación que podría tener un tercero en caso de apropiarse de dicha información. Por ello decimos, dentro de este requisito de evaluación, que la información que no trascienda del ámbito interno calificará como secreta cuando permita al agente una participación más eficiente en el mercado. (Sosa, 2016, p. 251)

**Sosa (2016)** menciona los siguientes ejemplos para determinar si se cumplen los requisitos para constituir secreto empresarial:

- a) **Lista de clientes.** Si se trata de una simple lista de clientes que contiene el nombre del agente y su información de contacto, evidentemente no va a configurar secreto empresarial al no cumplir con el primer requisito, ya que dicha información por lo general es de dominio público (bastaría con revisar la página web de los clientes para conocer la información de

contacto). Para que una lista de clientes sea considerada un secreto empresarial debe contener información complementaria sobre, por ejemplo, las negociaciones o los descuentos por volumen aplicados, volúmenes de comercialización, entre otros, establecidos de manera particular y que reporten una ventaja competitiva al poseedor.

- b) **Contratos de Know How.** La naturaleza de este contrato, a diferencia del secreto comercial, tiene como objeto trasladar información, aunque sea de forma limitada. Parte de dicha información, por lo general, cumple con los requisitos antes mencionados, pues se trata de información sensible que de ser conocida por el resto de competidores puede generarles una ventaja competitiva. (p. 252)
- De hecho, si bien existe información que puede calificarse como secreta en el know how, también es cierto que parte de la información que se traslada es sumamente trivial y de libre acceso al público. Un claro ejemplo lo encontramos en la fórmula de atención al cliente o el trade dress que imponen muchas franquicias. En ese sentido, podemos concluir que no todo know how implica un secreto comercial, pero sí en aquello que cumpla con los requisitos para obtener el carácter confidencial. (Sosa, 2016)

#### **2.2.4.2.11. Requisitos para la Existencia de un Secreto Empresarial:**

Para ser considerada como secreto comercial y poder ser susceptible de protección y defensa por parte de su poseedor, debe reunir los siguientes requisitos:

- a) El primer requisito es que se trate de una información específica que tenga una utilidad práctica para la actividad comercial en la que se utiliza.

- b) Segundo, no debe ser una información conocida en el ámbito de esa actividad ni ser fácilmente colegible por la competencia.
- c) Tercero, que represente para su poseedor un valor económico, por el mismo hecho de que no es conocida por la competencia y poder explotarla exclusivamente
- d) Como cuarto requisito el hecho de que el poseedor del secreto comercial haya tomado las medidas razonablemente efectivas para su protección. (Fonseca, 2017)

#### **2.2.4.2.12. El Secreto de las Comunicaciones:**

##### **i. Regulación Jurídica:**

En el Perú, el **artículo 2 inciso 10 de la Constitución** reconoce la libertad de las comunicaciones y dispone que el secreto solo puede ser levantado por mandamiento motivado del juez. Es decir, acoge la tesis del monopolio judicial de las intervenciones o, en palabras del Tribunal Constitucional, la «garantía de judicialidad. **(STC 1058-2004-AA/TC, FJ 22).**

##### **ii. Alcances del derecho al Secreto de las Comunicaciones**

**El artículo 2 inciso 10) de la Constitución** reconoce este derecho en los términos siguientes:

- a) Toda persona tiene derecho al secreto y a la inviolabilidad de sus comunicaciones y documentos privados. Las comunicaciones, telecomunicaciones o sus instrumentos sólo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez, con las garantías previstas en la ley. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen.

- b) Los documentos privados obtenidos con violación de este precepto no tienen efecto legal.
- c) Los libros, comprobantes y documentos contables y administrativos están sujetos a inspección o fiscalización de la autoridad competente, de conformidad con la ley. Las acciones que al respecto se tomen no pueden incluir su sustracción o incautación, salvo por orden judicial.  
**(Constitución Política del Perú, 1993, art. 2)**

### iii. **Características del Derecho al Secreto de las Comunicaciones: Jurisprudencia Nacional y Comparada**

El Tribunal Constitucional español en la STC 114/1984, de 29 de noviembre, lo ha reconocido como El bien constitucionalmente protegido es así la libertad de las comunicaciones y lo admite la doctrina:

- a) “El bien constitucionalmente protegido es, pues, el derecho de los titulares a mantener el carácter reservado de una información privada o, lo que es lo mismo, a que ningún tercero pueda intervenir en el proceso de comunicación y conocer de la idea, pensamiento o noticia transmitida.”
- b) El Tribunal Constitucional ha sostenido en la STC 2863-2002-AA/TC, que el derecho a la inviolabilidad de las comunicaciones y documentos privados tiene eficacia **erga omnes**, es decir, garantiza su no penetración y conocimiento por terceros, sean estos órganos públicos o particulares, ajenos al proceso de comunicación.
- c) Los titulares de este derecho son las personas que se comunican, es decir, aquellos que intervienen en el proceso de comunicación, ya sean personas naturales o jurídicas. Aunque, en este último caso, en un sentido figurado pues obviamente quienes se comunican son personas físicas. En consecuencia, este derecho se

opone a los terceros, que pueden ser particulares, empresas privadas que realizan interceptaciones ilegales o entidades públicas, y servicios de inteligencia, mas no a quienes intervienen en el proceso mismo de la comunicación. (Abad, 2012, p. 16)

#### **iv. La dignidad de la persona**

Para Jované (2014), una de las limitaciones a las que se ve enfrentado el poder de dirección del empleador es precisamente cuando se ve afectada la dignidad del trabajador como persona humana. Estrechamente ligada a la dignidad se encuentra también la intimidad del trabajador, por lo cual, en la medida en que el colaborador de una empresa vea su decoro, integridad y pudor restringido o afectado, entonces hasta allí llega el límite al ejercicio del poder de dirección. En este sentido, Palomeque y Álvarez, citados por Jované (2014) nos comentan que:

El ejercicio de los derechos del empresario, su posición dominante, se ve limitada por el respeto debido a la dignidad y a los derechos fundamentales y libertades públicas del trabajador. En el contrato de trabajo se implica personalmente el trabajador en el desempeño de la prestación y, de ahí, que se concrete como límites al poder de dirección: el debido respeto a derechos constitucionales como la intimidad, la libertad religiosa o la ideológica; el derecho a la igualdad de trato y a no ser discriminado. (Jované, 2014)

#### **v. El contrato de trabajo como límite:**

El documento o pacto de la prestación de la fuerza de trabajo o mejor conocido como contrato de trabajo suscrito entre el empleador y el trabajador, será el instrumento que definirá los márgenes de actuación del propietario o los directivos de la empresa. En este sentido, el empresario no puede controlar la vida personal de trabajador más allá de la mera relación laboral. De tal manera, que el dueño de los medios de producción (empresario), no puede inmiscuirse dentro de la esfera o el ámbito de la intimidad privada del

trabajador; por lo que el poder de dirección se encuentra condicionado o limitado. (Jované, 2014)

#### **2.2.4.2.13. Libre competencia.**

Estimando que la libertad es la base del programa, y además constituye uno de los niveles de libertad de todas las personas, se sanciona a la persona que evite la libre competencia a través de acciones o acuerdos ilícitos encaminados a excluir la participación de otros agentes económicos dentro del mercado. En estos tipos delictivos se hace expresa referencia a los monopolios u oligopolios, por cuanto tales entidades justamente impiden la participación de cualquier otro competidor en el mercado (desvalor del resultado); sin embargo, no basta sólo esto, sino que además los monopolios u oligopolios hayan realizado actos destinados a interferir en la libre competencia (desvalor de la acción). (Bramont, 1992, p.89)

La posibilidad de intervenir dentro del mercado sin que existan restricciones foráneas al mismo, es la base de una economía que respete la libre competencia. Si esta competencia es impedida por determinados agentes económicos, normalmente monopolios u oligopolios, éstos se constituyen como los determinantes del valor de los bienes y servicios, impidiendo que otros agentes económicos, al ofertarlos en el mercado, puedan equilibrar el valor de dichos bienes y servicios, beneficiando a los consumidores. (Bramont, 1992, p. 89)

#### **2.2.4.2.14. Libre formación de precios:**

Dentro de una economía mixta, los precios deben formarse en el mercado, por lo menos en su generalidad; esto supone que los agentes económicos que pueden libremente intervenir en el mercado, originan el valor de los bienes y servicios teniendo en consideración sus costos, pero también de acuerdo a los precios que señalen sus competidores. (Bramont, 1992, p. 89)

La consecuencia de la libertad de empresa determina que el mercado, de acuerdo a sus necesidades, fije el precio de sus bienes y servicios; ningún ente particular ni estatal debe intervenir en la formación de los precios, los cuales se originan de la oferta y la demanda que exista en el mercado. A mayor oferta, el precio se reduce y ante mayor demanda el precio aumenta. (Bramont, 1992, p. 89)

El Derecho busca asegurar esta formación de precio y por tanto sanciona a quienes alteran la formación de precios a través de prácticas ilícitas, nuevamente estarían fuera de tal supuesto las empresas que, en base a su tecnología y condiciones de trabajo, imponen precios que el mercado debe respetar por surgir de la libre competencia y, naturalmente, por beneficiar a los consumidores. Según Bramont (1992), las conductas delictivas estarían dadas por:

- a) **La Sustracción o retiro del mercado** de cierta cantidad de un producto, lo cual implica que la oferta de tal producto se reduce, y siendo la oferta menor a la demanda, el precio de tal producto se incrementa, pero no por efecto del mercado sino del agente económico que altera el funcionamiento del sistema económico en la formación de precios.
- b) **La Adulteración o cambio en la esencia de un producto**, es decir se reduce el valor de costo del producto a través de la disminución de su calidad; siendo así, se está en condiciones de rebajar el valor de venta de tal bien. La rebaja del precio implica que el precio del bien no se ha formado en el mercado, sino que depende de prácticas ilícitas de un agente económico destinadas a disminuir los costos de producción, a través de la disminución de la calidad de los productos. (Bramont, 1992, p.90)

#### **2.2.4.2.15. El tipo subjetivo de la violación de secretos de empresa**

El aspecto subjetivo está formado por la **presencia de dolo o culpa** en el agente que realizó el comportamiento atípico. Por dolo se entiende el conocimiento y la voluntad del sujeto activo en realizar los elementos del tipo o aspecto objetivo; asimismo, la culpa es la negligencia, la infracción del deber de cuidado de parte del agente. (Jakobs, 1997)

##### **A) La Culpa**

###### **i. La Culpa Objetiva**

Es la Culpa por la violación de las leyes, donde el ordenamiento determina el parámetro de comportamiento y si el agente no lo cumple, este es responsable. También se le llama culpa in abstracto, la cual, se opone a la culpa in concreto o subjetiva. Según la Doctrina tradicional francesa, apreciar la culpa in concreto es examinar el estado espiritual del agente, averiguar si su conciencia le reprocha algo. Apreciar la culpa in abstracto es preguntarse, lo que habría hecho otra persona en las mismas circunstancias, proceder por comparación con la conducta de un tipo abstracto. (Espinoza, 2013)

###### **ii. La Culpa Subjetiva**

Es aquella que se basa en las características personales del agente. Este tipo de culpa engloba la imprudencia (el sujeto hace más de lo debido) y a la negligencia (el sujeto hace menos de lo que debe). En la negligencia hay de parte del sujeto una omisión de cierta actividad que habría evitado el resultado dañoso. En la imprudencia, en cambio, el sujeto obra precipitadamente o sin prever íntegramente las consecuencias en las que podía desembocar su acción, de por sí irreflexiva. (Alterini, 1987, p. 95)

### **iii. La Culpa Omisiva**

Dentro de nuestro sistema jurídico, el comportamiento del buen samaritano es exigible frente a personas que se encuentran en peligro y, sin riesgo para el agente o un tercero. Por consiguiente, de su incumplimiento se deriva tanto una responsabilidad penal, como civil. (Espinoza, 2013)

### **iv. Culpa grave**

Es el no uso de la diligencia, que es propia de la absoluta mayoría de los hombres, es decir, quien ha tenido una conducta tal que no ha hecho lo que todos los hombres hacen comúnmente. El artículo 1319 del código civil peruano define como culpa inexcusable (que coincide con el concepto de culpa grave) a la negligencia grave. (Espinoza, 2013)

### **v. Culpa Leve**

Es el no uso de la diligencia propia de las personas de capacidad media. El artículo 1320 del código civil peruano la define como la omisión de aquella diligencia ordinaria exigida por la naturaleza de la obligación y que corresponda a las circunstancias de las personas, del tiempo y del lugar. (Espinoza, 2013)

### **vi. Culpa Profesional**

- En relación con la materia de responsabilidad civil de profesionales, el artículo 1762 del código civil peruano.; referente al contrato de prestación de servicios, establece que:

“Si la prestación de servicios implica la solución de asuntos profesionales o de problemas técnicos de especial dificultad, el prestador de servicios no responde por los daños y perjuicios, sino en caso de dolo o culpa inexcusable. (Espinoza, 2013)

Según Gutiérrez (2000), la interpretación que ha de hacerse del art. 1762 es aquella que sólo admita las especiales dificultades técnicas de la prestación que hacen que el profesional sólo responda por dolo o culpa grave; es decir, si la prestación profesional es aquella de las que pueden calificarse de normales en el ejercicio de la actividad profesional, inevitablemente el profesional se halla sometido a las reglas generales. (Gutiérrez, 2000, p. 67)

## **B) El Dolo**

Según Espinoza (2013); en materia penal, se diferencia en:

### **i. Dolo Directo:**

El Sujeto actúa para provocar el daño. Según Salvi, citado por Espinoza (2013) se observa que es opinión generalmente compartida que el dolo, se identifica con la noción penal del dolo genérico, que prescinde de elementos específicos de intencionalidad o fraude, resolviéndose en la voluntad de ocasionar el daño.

### **ii. Dolo Eventual:**

El Sujeto obra, aunque se represente la posibilidad de un resultado dañoso, que no descarta; como cuando para ganar una carrera automovilística continúa su marcha a pesar de hallar en su camino a una persona que puede herir con su vehículo, y afronta el riesgo de así hacerlo. En este supuesto, no hay dolo directo, toda vez que el sujeto en la alternativa que le plantea continuar su acción con la eventualidad de producir el daño, y desistir de ella para descartarlo, continúa su acto. (Espinoza, 2013)

Respecto de la graduación de la responsabilidad por los factores de atribución subjetivos, basta reflexionar que, también en la hipótesis de actos y hechos dolosos y culposos, la medida del resarcimiento se mide de acuerdo a la cantidad del daño jurídicamente relevante. En efecto, si el daño se debió a dolo o culpa, ello no influye de manera alguna en la obligación resarcitoria. (Espinoza, 2013)

### **C) El Nexo Causal:**

Según Trazegnies (2001), la relación de responsabilidad descansa, en una relación de causalidad. Por consiguiente, para que exista responsabilidad civil se requiere que exista un nexo causal entre la víctima y el autor del hecho dañino.

- i. **Causalidad natural y causalidad jurídica.** En algunos casos, este esquema se hace algo más complejo en razón de que la víctima puede exigir el pago también a una tercera persona (empleador, representante legal de la persona incapacitada, Compañía de Seguros, etc.). (Trazegnies, 2001)

- ii. **Causalidad y autoría.** *La causa jurídica* tiene, en la mayor parte de los casos, una característica más personal que la causa natural: es una dimensión existencial del ser humano. *La causalidad natural*, de carácter mecánico, apunta únicamente al "enlace material entre un hecho antecedente y un hecho consecuente", mientras que la autoría se refiere a la posibilidad de imputar un obrar a una persona determinada. (Trazegnies, 2001)
- iii. **Causalidad y culpabilidad:** Según Goldenberg, citado por Trazegnies (2001), para saber si una persona es culpable debe demostrarse primero que es autor del hecho; recién después de que esto quede demostrado podrá indagarse si es culpable o no. "Se trata de un planteamiento, en el cual se juzga la actuación del sujeto en sí misma, sin abrir opinión acerca de su contenido espiritual".

La relación causal pertenece al plano factual y se establece mediante un juicio de ser que describe la conducta, mientras que la culpabilidad pertenece al plano del deber ser y se establece con un juicio de valor que aprecia la conducta. (Trazegnies, 2001)

### **2.2.4.3. Subcapítulo III: Criminal Compliance en las Personas Jurídicas**

#### **2.2.4.3.1. Concepto y Características**

- A) Los programas de cumplimiento normativo en materia penal denominados Criminal Compliance Programs, aluden a la adopción por parte de las empresas de medidas de autorregulación. Dicho en términos positivos, Criminal Compliance significa “autovigilancia” y fomento de una mentalidad corporativa de fidelidad al Derecho, lo que visto a la inversa se traduce en la adopción de medidas destinadas a neutralizar factores culturales o dinámicas de grupo favorecedoras de

comportamientos de connotación delictiva en el seno de la actividad empresarial. (Reaño, 2015, p. 142)

- B) La finalidad específica de los programas de Criminal Compliance es la de evitar o mitigar la responsabilidad penal de la propia empresa, lo que ciertamente implica la adopción de medidas destinadas a:
- (i) Evitar que sus accionistas, directores, ejecutivos y trabajadores incurran en la comisión de delitos con ocasión de su actividad en la empresa; o, en caso ello no sea posible,
  - (ii) Evitar que la imputación de responsabilidad penal pueda dirigirse contra la empresa en cuyo seno se cometió el comportamiento tipificado como delito. (Reaño, 2015, p. 142)
- C) Un buen programa de Criminal Compliance será aquel que confiera bases jurídico penales seguros, para desvincular a la propia persona jurídica de los hechos delictivos que pudieran cometer sus integrantes en el desempeño de sus cargos. Expresado en palabras de uno de los mayores especialistas en Criminal Compliance, “un concepto de Compliance dirigido a una completa evitación de la responsabilidad penal debe por lo tanto tomar en consideración la empresa en su conjunto, en su caso a todos los trabajadores de la empresa y no solo a la cúpula directiva”. (Reaño, 2015, p. 142)

La preocupación de las empresas por contar con programas de Criminal Compliance nace con la modificación del concepto de riesgo de negocio, tradicionalmente concebido como riesgo puramente económico y, como tal, fundamentalmente referido a las posibilidades de competir exitosamente en el mercado y a la propia capacidad de

endeudamiento en función a la estimación de ganancias futuras.  
(Reaño, 2015, p. 143)

A la noción económica de riesgo del negocio se añadió el concepto de riesgo de responsabilidades jurídicas o dicho con mayor precisión riesgo de responsabilidades por incumplimientos normativos, destacando por la gravedad de sus consecuencias, los asociados a la inobservancia de normas de naturaleza penal. (Reaño, 2015, p. 143)

#### **2.2.4.3.2. El Criminal Compliance en Perú**

- A) Es frecuente que las empresas con operaciones en Perú, que se encuentran dentro del ámbito de aplicación transfronteriza de las normas anteriormente reseñadas, cuenten con programas de Criminal Compliance orientados a:
- (i) Prevenir la comisión de aquellos comportamientos que desencadenen la instauración de procedimientos en jurisdicción británica, norteamericana o canadiense, cuya sola formalización es susceptible de generar cuantiosos daños económicos en términos de riesgo de negocio y de reputación comercial; y, en caso de instauración de un procedimiento.
  - (ii) Evitar la imposición de sanciones o mitigar la responsabilidad penal por las infracciones cometidas, lo cual muchas veces se concretiza a través de la suscripción de acuerdos de no persecución. (Reaño, 2015, p. 144)
- B) Entre las medidas de prevención adoptadas por las empresas con operaciones en Perú sujetas a la aplicación de normas transfronterizas, se encuentra:

- (i) La adopción de Códigos de Conducta, en los que se recogen principios programáticos de actuación, como aquellos vinculados al establecimiento de estándares o parámetros de conducta enfocados a evitar actos de corrupción o delitos vinculados a la criminalidad empresarial.
  - (ii) La implementación de programas de Criminal Compliance, que incluyen canales y procedimientos de denuncia interna (whistleblowing policy), protocolos de investigaciones internas (internal investigation procedures) o el nombramiento de un funcionario de la compañía como supervisor de la efectiva implementación y seguimiento del adecuado funcionamiento del Programa de Criminal Compliance. (Reaño, 2015, p. 144)
- C) Los programas de cumplimiento se muestran atractivos para que las empresas mitiguen el riesgo legal y mejoren su imagen corporativa. En ese sentido, la implementación de los programas de cumplimiento puede ser rentables para las empresas si se les considera como una inversión a largo plazo. Algunos estudios económicos señalan una relación directa entre, por un lado, el alto valor económico de las acciones de una empresa y, por otro, la buena reputación corporativa de la que gozan en el mercado. (Astudillo, 2015, p. 242)

Un sistema de gestión de cumplimiento que busque insertar una política empresarial basada en el cumplimiento de la legalidad, estaría en plenas condiciones de influir en el valor de la empresa por permitir mejorar su posición en el mercado. (Astudillo, 2015, p. 242)

Según Astudillo (2015), el cumplimiento de la legalidad se ha convertido tanto en un valor ético como en un activo fundamental de toda empresa. Así también, constituye el resultado de una organización

que cumple sus obligaciones, haciéndose sostenible mediante su integración en la cultura empresarial de la organización y en la actitud de las personas que trabajan en ella, mediante una permanente capacitación y difusión de los valores empresariales. Un programa de cumplimiento eficiente en la empresa le permitirá demostrar su compromiso con el cumplimiento de las leyes, la ética, las normas internas de la organización y de buen gobierno corporativo, lo cual redundará en la obtención o incremento del importe activo relativo a la buena reputación empresarial. (Astudillo, 2015, p. 243)

Estos programas constan de un conjunto de elementos: un responsable encargado de la administración del riesgo, un sistema de documentación y análisis de riesgos, un código ético, protocolos de investigaciones internas, canales de denuncias, controles generales y específicos y un catálogo de medidas dirigidas a evitar el incumplimiento de las normas por parte de los miembros de la organización. (Astudillo, 2015, p. 243)

#### **2.2.4.3.3. El Cumplimiento Normativo**

Silva Sánchez, citada por Astudillo (2015) sostiene que los programas de cumplimiento no se circunscriben solo a la adopción de medidas de vigilancia (controles, determinación de flujos de información), pues también se integran con medidas positivas de formación dirigidas no solo a neutralizar factores culturales o dinámicas de grupo favorecedoras de hechos ilícitos, sino también a incentivar culturas de grupo de fidelidad al derecho. (Astudillo, 2015, p. 245)

Bock, citado por Astudillo (2015) considera que, si la empresa ha asumido el riesgo penal en relación con la fidelidad al derecho de sus empleados, es explicable que el concepto de compliance se concentre en el deber de supervisión de la dirección empresarial. En ese sentido, el criminal compliance se ocuparía de la cuestión de la responsabilidad empresarial; esto es, de las medidas que la dirección empresarial en el

marco de su deber de supervisión debe haber adoptado para evitar infracciones de deberes jurídico-penales por parte de sus empleados. (Astudillo, 2015, p. 245)

Atendiendo a la finalidad de lo que buscaría el cumplimiento, un sector de nuestra doctrina considera que no se trata simplemente de impedir infracciones legales imputables a algún miembro de la empresa, sino también de aquellas que se explican de una defectuosa ordenación de la actividad global de la corporación. (Astudillo, 2015, p. 245)

De allí que los programas de cumplimiento pongan especial énfasis en la capacitación y formación de todos los miembros de la organización en cuestiones de valores éticos, ya que la concientización de las personas constituye la vía idónea para incentivar a los miembros de la empresa a comportarse de acuerdo a derecho. (Astudillo, 2015, p. 245)

Según Astudillo (2015), el nuevo sistema de compliance de Siemens (Compañía transnacional) se basa en una metodología clara que debe integrar todas las actuaciones de compliance del grupo. Tiene tres etapas:

- a) **Prevenir:** La etapa de prevención es probablemente la más importante, pues tiene que ver con la formación y supervisión de los empleados y socios de la empresa, socios del negocio y proveedores de la empresa. Para todos ellos, existe un código ético común y de obligado cumplimiento, así como especificaciones y normas propias en cada caso. La formación de los empleados se efectúa en un 80% de manera presencial y personalizada, estableciéndose un sistema interno y absolutamente confidencial de atención a los empleados y directivos para evacuar consultas y resolver dudas en torno a cualquier aspecto sobre el que sea necesario arrojar luz.

- b) Detectar:** La etapa de detección cuenta también con un sistema de canales de información internos y externos, como la contratación de un defensor del empleado que permiten denunciar cualquier tipo de conducta que se suponga irregular y que alguien presuma que se está llevando a cabo en el seno de la empresa.
- c) Responder:** La última etapa es la respuesta que da la compañía cuando se detecta una infracción a las normas éticas de la empresa. Se ha establecido un catálogo de sanciones internas para aquellos que cometan algún tipo de irregularidad según el grado de incumplimiento en relación a la corrupción y la falta de ética en la actuación. (Astudillo, 2015, p. 248)

Como señala Bacigalupo, citado por Astudillo (2015), una cultura empresarial basada en valores es un factor del éxito empresarial y, al parecer, la cultura del cumplimiento de la legalidad tiene que ver con una nueva visión de hacer negocios por parte de las empresas y que, de lograrse, tendrá una directa incidencia económica en la manera como se valoriza una compañía. Por un lado, porque no contar con un programa de cumplimiento puede incrementar o disminuir la sanción pecuniaria, a la que se encuentra expuesta la empresa en el caso de que se detecte una infracción legal; y, por otro, porque el programa de cumplimiento estaría en condiciones de agregar valor a la empresa gracias a la reputación corporativa ganada. (Astudillo, 2015, p. 248)

En la experiencia comparada se han establecido estándares de cumplimiento cuya fuente de referencia se encuentra en la US Federal Sentencing Guidelines for Corporations, con relación a la implementación de un programa de cumplimiento empresarial. Se destacan, como elementos esenciales de dicho programa, los siguientes:

- a) El nombramiento de un compliance officer y la delegación de funciones en el ejercicio de responsabilidades operativas.
- b) Establecimiento de estándares y procedimientos para prevenir y detectar la conducta criminal.
- c) Ejercicio por parte del consejo de administración de una autoridad supervisora sobre la implementación y mejora del programa de compliance.
- d) Reporte periódico a los miembros del consejo de administración y altos directivos.
- e) Impartición de formación continuada en materia de compliance, monitorización y auditoría constante de la eficacia del programa.
- f) La exclusión de empleados incumplidores de los puestos de responsabilidad. (Astudillo, 2015, p. 250)

De manera similar, Gómez-Jara, citado por Astudillo (2015), considera que un programa de cumplimiento común debería contener los siguientes elementos:

- a) Código de conducta escrito.
- b) Supervisión de esfuerzos de cumplimiento por personal cualificado.
- c) Reforzamiento mediante sistemas efectivos de control y auditoría.
- d) Reforzamiento mediante procedimientos disciplinarios.
- e) Adopción de medidas cautelares tras detección de una infracción.

- f) Seguimiento de una formación continuada a directivos y empleados.
- g) Comunicación efectiva de los estándares y procedimientos de los códigos de conducta. (Astudillo, 2015, p. 251)

Magro Servet, citado por Astudillo (2015) considera que el programa de cumplimiento empresarial debe contener los siguientes elementos:

- a) **Un sistema de evaluación de riesgos o risk assessment.** En este sentido, la empresa debe estar en condiciones de evaluar de forma periódica el sistema de riesgos de caer en responsabilidad por la actuación de directivos y/o empleados. Además, debe adecuarlo a cada esfera de negocio de su empresa. Dentro de esta área, se focaliza también el programa de continuous improvement o autoevaluación del rendimiento empresarial para asegurarse de que el sistema implantado es el adecuado en cada momento para sus operaciones.
- b) **Puntos de control o control points.** Dentro del programa de cumplimiento normativo, se establece puntos de control para individualizar cuáles son los riesgos que pueden existir, por lo que se refuerza el establecimiento del control del comportamiento de la empresa en diferentes áreas, a fin de individualizar el control según cada área de la empresa, para no fallar estableciendo un programa general que se olvide de las particularidades de áreas concretas de la empresa.
- c) **Documentación adecuada del programa de cumplimiento normativo.** Es fundamental que se elabore por la empresa un soporte documental acerca del programa de cumplimiento normativo, lo que conlleva que este deba estar escrito y que la documentación esté en poder de directivos y empleados. (Astudillo, 2015, p. 252)

Con el compliance se garantiza a los inversionistas o a cualquier otra persona que quiera vincular sus intereses económicos a la gestión exitosa

de una empresa, que los riesgos de ver a la empresa inmersa en una disputa o conflicto judicial se encuentran de alguna manera controlados por un programa de cumplimiento normativo. Si bien las empresas no están obligadas legalmente a adoptar un compliance, la actuación ética frente a los terceros interesados se lo exige como un aspecto esencial del buen gobierno corporativo. (García, 2016, p. 227)

Es oportuno destacar aquí que los incentivos adicionales para que las empresas adopten un programa de cumplimiento normativo no se han quedado en la obligación de informar de ello a los inversores como un elemento de juicio que influye decisivamente en el valor de cotización de sus acciones o títulos. El que la empresa haya implementado un sistema de cumplimiento normativo ha comenzado a ser tenido en cuenta también en la imposición misma de sanciones jurídicas. (García, 2016, p. 227)

#### **2.2.4.3.4. Funciones del Compliance:**

La función del Compliance es por un lado preventiva, pues su contenido está inspirado en evitar que la empresa incurra en infracciones normativas y por ende en responsabilidad penal; como señala el profesor García Caveró, citado por Espinoza (2016), lo que se busca es impedir las infracciones legales que pueda cometer individualmente un trabajador de la empresa y, además, aquellas infracciones que se derivan de la organización defectuosa de la actividad a la que se dedica la empresa. (Espinoza, 2016, p. 6)

Por otro lado, tiene una función de confirmación del derecho. Esta función consiste en establecer mecanismos para detectar las irregularidades que se cometan dentro de la empresa, así como para reparar las infracciones que se generen e, incluso, ponerlas en conocimiento de la autoridad correspondiente (Espinoza, 2016, p. 6)

#### **2.2.4.3.5. Factor Económico del Compliance:**

Además de este beneficio importante, no hay que obviar que contar con un Programa de Cumplimiento dentro de una organización reduce las infracciones normativas cometidas por una empresa lo cual genera ganancias, pues la empresa ha dejado de perder como consecuencia de ya no incurrir en tales infracciones. Además, esta la buena imagen que pueda tener en el mercado frente a accionistas y clientes, una mayor valorización de las acciones debido a que existen reglas internas de la empresa destinadas a la prevención de infracciones, una mejora en la transparencia de la información, entre otros. (Espinoza, 2016, p. 7)

#### **2.2.4.3.6. Contenido de un Programa de Cumplimiento eficiente y eficaz**

Adoptar e implementar un Programa de Cumplimiento o Modelo de Prevención, denominativo que utiliza la Ley N° 30424 – Ley que regula la responsabilidad administrativa de las personas jurídicas por el delito de Cohecho activo transnacional, es una labor compleja, debido a que depende de diversos factores como la actividad empresarial, complejidad de la organización, y los riesgos de incurrir en infracciones normativas. (Espinoza, 2016, p. 9)

Respecto a la adopción o elaboración del Programa de Cumplimiento se realiza de la siguiente manera:

- a) **En primer lugar**, se debe formular el programa de cumplimiento normativo. Esto quiere decir, recoger los procedimientos empresariales internos para la gestión de prevención de riesgos de infracción legal. Para ello, será necesario identificar los riesgos, definir las medidas de prevención, detección y comunicación, para, de esa manera, determinar la estructura del programa de Compliance.
- b) **En segundo lugar**, se debe implementar el programa en la empresa, para ello será necesario informar al personal a todo nivel a fin de que

conozcan los alcances del programa y adecuen su comportamiento al mismo.

- c) **En tercer lugar**, se debe buscar consolidar el programa y su mejoramiento. En esta etapa se deberá determinar aquellos puntos en los cuales el programa no ha sido eficaz y entender por qué no ha logrado cumplir su finalidad. Asimismo, deberá detectarse a los infractores dentro de la empresa y, dado el caso, imponer una sanción correspondiente. (Espinoza, 2016, p. 9)

El Proyecto de Código Penal establece en su artículo 141° numeral 2, los elementos mínimos que debe contener todo Modelo de Prevención de una persona jurídica. El referido artículo establece que:

- a) El máximo órgano de la administración de la persona jurídica debe designar una persona u órgano que ejerza la función de auditoría interna de prevención, debiendo contar con el personal, medios y facultades necesarias para cumplir su función adecuadamente; debiéndose garantizar su autonomía funcional respecto del órgano de administración, propietarios, accionistas o socios de la persona jurídica.
- b) Deben de existir medidas preventivas referidas a:
- ✓ La identificación de las actividades o procesos de la persona jurídica que generen o incrementen riesgos de comisión de delitos.
  - ✓ El establecimiento de procesos específicos que permitan a las personas que intervengan en éstos, programar y ejecutar sus tareas o labores de una manera que prevengan la comisión de delitos.

- ✓ La identificación de los procesos de administración y auditoria de los recursos financieros que permitan a la entidad prevenir su utilización en la comisión de conductas delictivas.
- ✓ La existencia de sistemas de denuncia, protección del denunciante, persecución e imposición de sanciones internas en contra de los trabajadores o directivos que incumplan el Modelo de Prevención.
- ✓ Un mecanismo de supervisión interna del conocimiento del modelo de prevención, el cual debe ser aprobado por un reglamento emitido por la persona jurídica. (Espinoza, 2016, p. 10)

#### **2.2.4.4. Subcapítulo IV: Poder Empresarial y el secreto de las comunicaciones**

##### **2.2.4.4.1. Control y Vigilancia del Empleador:**

La vigilancia es el esfuerzo sistemático y organizado por la empresa de observación, captación, análisis, difusión precisa y recuperación de información sobre los hechos del entorno económico, tecnológico, social o comercial, relevantes para la misma por poder implicar una oportunidad u amenaza para ésta. Requiere una actitud de atención o alerta individual. De la suma organizada de estas actitudes resulta la función de vigilancia en la empresa. En definitiva, la vigilancia filtra, interpreta y valoriza la información para permitir a sus usuarios decidir y actuar más eficazmente. (Palop y Vicente, 1999, p. 22)

La vigilancia posibilita el desarrollo y ejercicio de la función de inteligencia al velar por la adecuada y precisa difusión y comunicación de la información dentro de la empresa. La utilización de información y conocimiento para la toma de decisiones, es el ámbito propio de la inteligencia empresarial o competitiva. (Palop y Vicente, 1999, p. 22)

Las empresas suelen justificar esas conductas alegando su finalidad de garantizar el cumplimiento de las obligaciones contractuales a las que obliga al trabajador el propio contrato, así como evitar problemas de seguridad, virus y fuga de datos; unos fines que, si bien son legítimos, pueden acarrear problemas legales. (Barría, 2009, p.36)

Las empresas, al verse afectadas por el uso abusivo que hacen o pueden llegar a hacer sus trabajadores de los medios tecnológicos puestos a su disposición, han comenzado a utilizar diversos mecanismos para evitar los riesgos que dicho uso conlleva o puede acarrear a la organización. Ninguna de ellas está exenta del riesgo de llegar a vulnerar algún derecho del trabajador, ninguna es absolutamente efectiva en cuanto a prevenir los riesgos del uso de la Internet o, específicamente, del correo electrónico, pero a medida que se vayan masificando y estudiando jurídicamente, pueden ser perfeccionadas tanto en sus aspectos técnicos, como en las repercusiones que pueden llegar a tener respecto de los derechos de los trabajadores afectados por las mismas. (Barría, 2009, p.37)

**Fraudes:** Los fraudes que involucran sistemas de información pueden ser categorizados como manipulación de los registros de entrada, de los registros de procesamiento, o los registros de salida. La manipulación de los datos de entrada consiste en el ingreso de datos falsos o fraudulentos en los sistemas de información, mientras que la manipulación de los registros de salida es robar datos como listas de clientes, planes de fusión, y secretos comerciales. La manipulación de los datos en el procesamiento incluye la alteración de los programas de computación o sus códigos. Muchos controles no físicos en los sistemas de información son claves para prevenir fraudes que puedan brotar de aquellos tipos de actividades. (Pacini y Brody, 2005, p. 5)

#### 2.2.4.4.2. Principios del Poder Empresarial:

- a) **Principio de transparencia.** Debe asegurarse que hay una información previa y específica al trabajador sobre la posibilidad de que el empresario adopte medidas de vigilancia de su correspondencia y de sus otras comunicaciones, así como de la puesta en práctica de tales medidas. El carácter previo supone que la información ha de ser anterior al inicio de la vigilancia.
- b) **Principio de causalidad real y seria.** El empresario ha de proporcionar motivos concretos que justifiquen la vigilancia de las comunicaciones del trabajador.
- c) **Principio de proporcionalidad.** Ha de valorarse el alcance de la vigilancia realizada (grado de intrusión en la vida privada del empleado), por lo que admite que sea variable, siempre y cuando resulte necesario y adecuado. Asimismo, deben ponderarse debidamente las consecuencias concretas en la vida privada del trabajador, de modo que la máxima sanción debiera reservarse para máximos incumplimientos, atendiendo igualmente a la prevalencia que han de tener los derechos fundamentales de los trabajadores como personas, porque tales derechos exigen interpretación expansiva, no restrictiva.
- d) **Principio de efectividad de la tutela.** En todo caso, el trabajador debe haber recibido las debidas garantías, en particular cuando las medidas de vigilancia del empresario tenían un carácter intrusivo. (Molina, 2017, p. 293)

#### 2.2.4.4.3. Medidas Adoptadas por el Empleador:

Según Barría (2009), entre medidas adoptadas por las empresas, ya sea para controlar, restringir, vigilar o intervenir el uso que del Internet o del correo electrónico hacen los trabajadores, tenemos los siguientes:

- a) **Portales.** Consisten en una página web que contiene aquellos vínculos a los que pueden acceder los trabajadores, siendo sólo éstos a los que se permite el acceso. De esta manera, el empleador predetermina los sitios en la red que considera “deseables”, y puede asegurarse, dentro de cierto rango, que los trabajadores sólo visiten sitios relacionados con su actividad laboral.
- b) **Bloqueo de Páginas Web.** El empleador establece cuáles páginas o sitios considera “indeseables”, y bloquea el acceso de los trabajadores a éstas. Esto puede obtenerse de dos maneras: bloqueando los sitios específicos a los cuales no se desea que los trabajadores accedan; y estableciendo palabras clave, las cuales, al estar incluidas en ciertas páginas, son detectadas por el computador, bloqueando el acceso.
- c) **Software de vigilancia.** Consiste en un tipo de programas computacionales o informáticos que permite poner en manos del empleador –o de quien éste designe-, el control del acceso a Internet de los empleados. Estos programas permiten monitorear el tráfico de Internet, supervisar la utilización del ancho de banda, monitorear la utilización de las aplicaciones de la red, bloquear sitios improductivos, clasificar sitios visitados según productividad, avisar al administrador sobre actividades inusuales, etc. Estos programas constituyen verdaderos espías instalados dentro del computador del usuario, el que registra e informa todas las actividades realizadas en el servidor por el usuario.
- d) **Archivos que almacenan información sobre sitios visitados.** Un cookie es “un fragmento de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a

petición del servidor de la página. Esta información puede ser luego recuperada por el servidor en posteriores visitas. (Barría, 2009, p.38)

- Según Hernández y Herrera, citados por Barría (2009), apoyado en estas medidas tecnológicas el empresario puede comprobar si el trabajador cumple o no con sus deberes laborales básicos y realiza el trabajo convenido. Además, le permiten controlar la productividad y utilización de los recursos, supervisando de forma rutinaria la actividad de los trabajadores.

#### **2.2.4.4. Inteligencia Competitiva en la Empresa:**

##### **A. Concepto:**

La inteligencia competitiva es un proceso dinámico, sistemático y recursivo que transforma, empleando técnicas analíticas específicas, la información relevante y legalmente obtenida sobre el entorno competitivo del pasado, presente y futuro, con el propósito de facilitar la toma de decisiones en beneficio de la empresa. (Gógova, 2015, p. 4)

La Inteligencia Corporativa debe ir acompañada, dentro de la organización empresarial, de las adecuadas medidas de prevención, códigos de ética y gestión diligente del proceso de obtención y elaboración informativa. (De Espona, 2017, p. 43)

##### **B. Características:**

- ✓ La inteligencia competitiva es un proceso dinámico, sistemático, recursivo.

- ✓ La inteligencia competitiva se basa en información y datos relevantes sobre el entorno competitivo (macro y micro).
- ✓ La inteligencia competitiva maneja datos e información del pasado, del presente y previsiones, tendencias, prospectivas del futuro.
- ✓ La inteligencia competitiva se alinea con las necesidades concretas de la empresa. Implica un conocimiento profundo de nuestra propia empresa.
- ✓ Los procedimientos de obtención de información en inteligencia competitiva son legales, éticos.
- ✓ La fase analítica de la inteligencia competitiva se fundamenta en técnicas específicas.
- ✓ El propósito de la inteligencia competitiva es facilitar la toma de decisiones con menor grado de riesgo e incertidumbre, en beneficio de la empresa. (Gógova, 2015, p. 4)

### **C. La Contra Inteligencia:**

La contra-inteligencia es una función de los servicios de inteligencia complementario y de apoyo a la misión fundamental de recolección, análisis de información para la producción de inteligencia y comunicación o difusión de la misma. El fin de la contrainteligencia es proteger y preservar la seguridad de todo el proceso sistemático de inteligencia competitiva y, al igual que la inteligencia competitiva, los procedimientos de contra-inteligencia se llevan a cabo de manera ética y legal. (Valdés, 2013, p. 22)

El objetivo de la contra-inteligencia es blindar a la empresa ante la competencia desleal y otros grupos de espionaje, pudiéndose definir

como el conjunto de actividades destinadas a anular las acciones de inteligencia hostiles de la competencia y a proteger la información y el material clasificado propios, por medio de acciones legales y éticas. (Valdés, 2013, p. 22)

Según Navarro, citado por Vilas (2017) para preservar la seguridad física de las instalaciones y sus documentos, con la finalidad de evitar el acceso de aquellas personas sin autorización, se establecen medidas tales como defensas estáticas, vallas, alarmas, sistemas de videovigilancia, guardias de seguridad, camuflaje de instalaciones y vehículos, identificación y control de visitantes, restricciones de acceso, uso de contraseñas, inspecciones oculares, identificación de personas, escaneo y apertura de equipajes, controles de seguridad periódicos, etc. (Vilas, 2017, p. 134)

#### **2.2.4.4.5. Responsabilidad Social Corporativa:**

La responsabilidad social corporativa es una política de acción empresarial que tiene como base la asunción de responsabilidad por los efectos que su funcionamiento causa en sus miembros y la sociedad en general. El concepto de responsabilidad social corporativa se ha desarrollado a partir del interés de los empresarios en mantener una relación armoniosa con la comunidad, lo cual, si bien tiene bases éticas, también responde a una estrategia de permanencia y legitimidad de la empresa en el mediano y largo plazo. (Salmón, 2012, p. 37)

En materia de responsabilidad social las áreas de acción más comunes son:

La protección del medio ambiente, educación, deporte y cultura, estas decisiones de acción social se orientan a considerar como primeros beneficiarios a los trabajadores de la empresa, ya que estos como principales partes interesadas o públicos de la organización, se destacan por su relevancia en la estrategia empresarial; seguidos de accionistas,

clientes, comunidades, entre otros grupos de interés que la empresa defina, basada en su relación e impacto mutuo. (Chirinos, Fernández y Sánchez, 2012, p. 3)

- Según Porter y Kramer (2006) la responsabilidad social corporativa se basa en los siguientes fundamentos:
  - a) **El argumento moral:** Las empresas tienen el deber de ser buenas ciudadanas y de “hacer lo correcto” y pide a sus miembros “lograr el éxito comercial en formas que honren los valores éticos y respeten a las personas, las comunidades y el ambiente natural”.
  - b) **La sustentabilidad:** Enfatiza la tutoría medioambiental y comunitaria. Busca satisfacer las necesidades del presente sin comprometer la capacidad de las futuras generaciones para cubrir sus propias necesidades.
  - c) **La noción de licencia para operar:** Se deriva del hecho de que toda empresa necesita permiso tácito o explícito de los gobiernos, comunidades y muchos otros stakeholders para hacer negocios.
  - d) **La Reputación:** Finalmente, la reputación es utilizada por muchas empresas para justificar iniciativas de responsabilidad social corporativa bajo el argumento de que mejorarán la imagen de una empresa, fortalecerán su marca, elevarán la moral e incluso incrementarán el valor de sus acciones. (Porter y Kramer, 2006, p. 5)

## 2.2.5. CAPÍTULO II: El Espionaje Corporativo

Según Foguel, citado por Benavente (2012), el espionaje ha nacido de la necesidad de saber. El comerciante y el industrial que no supieran nada de los mercados que le interesan, nada de la clientela que compra sus

productos, nada de sus competidores, de lo que éstos fabrican, de sus procedimientos, de sus planes, de sus nuevas presentaciones, nada de la competencia nacional o extranjera y de nuevos mercados posibles, se vería abocado a corto plazo a la quiebra. El espionaje comienza cuando estos informes tienen que ver con la competencia, y cuando ésta no desee que sean revelados. La frontera entre la búsqueda de informes y el espionaje es movediza e incierta. (Benavente, 2012, p. 78).

#### 2.2.5.1. Subcapítulo I: Concepto y Características del Espionaje Corporativo

**Concepto:** El espionaje corporativo tiene distintos nombres: espionaje industrial, espionaje empresarial, inteligencia competitiva, entre otros, pero todos se refieren a lo mismo, obtener e interpretar información de valor estratégico de la industria o de los competidores. Es la obtención ilícita de información relativa a la investigación, desarrollo y fabricación de prototipos, mediante las cuales las empresas pretenden adelantarse a sus competidores en la puesta en el mercado de un producto novedoso. (Jarabo, 2015)

Son todas aquellas acciones que, para descubrir un secreto de empresa, se apoderan por cualquier medio, de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo. (Jiménez, Bonilla y Gil, 1997)

El **espionaje industrial** es una herramienta política económica comunista, ejecutados exclusivamente por los órganos del estado con sus inagotables posibilidades financieras, técnicas y de política de poder (situación que se da en países con este régimen o en países pseudo socialistas como Venezuela que privatizan empresas opositoras); mientras que en el occidente es el espionaje en las empresas de la competencia, en la medida que realmente se ejercen, sirven a la consecución de ventajas en la economía de mercado. (Fernández, 1996)

El espionaje masivo inhibe el desarrollo del ser humano y también pone en riesgo a la democracia, en tanto sentirse vigilado provoca la autocensura. Desde un análisis económico del Derecho, los individuos ven limitados el ejercicio de sus derechos dentro de la sociedad, porque se sentirán monitoreados o vigilados, mientras realizan sus actividades diarias al no existir protección legal frente a los supuestos de espionaje, viéndose de esta manera en peligro su privacidad e intimidad. (Zaffaroni y Croxatto, 2015)

Mucho del espionaje a nivel empresarial se realiza en el sector minero, banca y telecomunicaciones. También hay seguimiento e interceptación de comunicaciones a empresas que buscan ser proveedoras o vender algún producto al consumidor. (Mora, 2015)

El espionaje macroeconómico, se refiere al uso de agencias secretas en nombre del gobierno de un Estado con el fin de obtener inteligencia relacionada con los desarrollos y actividades del mundo económico legal, con el propósito futuro de avanzar en sus intereses estratégicos. De tal manera, el espionaje macroeconómico ha sido, es y será un componente estructural del sistema internacional de los estados-nación y, una herramienta principal de los gobiernos que cargan con el peso decisonal para el buen curso de la política económica interna y externa. (Venegas, 2016, p. 12)

La principal incidencia del espionaje (especialmente el económico) se sitúa en la pérdida de conocimiento estratégico, competitividad y capacidad de desarrollo y avances como consecuencia del robo de conocimiento. Como consecuencia de las crisis energéticas y económicas globales, el espionaje económico e industrial ha alcanzado un protagonismo determinante entre el conjunto de variadas y particulares acciones de los espías y ladrones de secretos de aplicación económica. (Navarro, 2013, p. 26)

i. **Formas de Espionaje Corporativo:**

Según Jarabo (2015), hay dos formas principales:

**a. Infiltración de personal.**

**b. Ciberataques.**

El espionaje corporativo, también conocido como espionaje industrial, ha evolucionado a través del tiempo para convertirse en un flagelo que en algunos casos utiliza las técnicas más avanzadas de espionaje conocidas. Entre las que figura la **instalación de cámaras** y micrófonos de forma imperceptible para el ojo inexperto en áreas sensitivas de una empresa, como pueden ser oficinas de altos mandos o salas de reuniones. Sin embargo, algunas técnicas siguen siendo simples, como rastrear información en la basura, para citar un ejemplo, uno de los métodos más sencillos de espionaje corporativo. (Jarabo, 2015)

Otra manera muy común de espionaje es que el trabajador de confianza tome papeles de encima del escritorio o fax, o entrar al computador personal, siendo la solución el mantener los cajones con llaves y un protector de pantalla o simplemente cerrar la sesión cuando uno no se encuentra en su lugar de trabajo. (Pinto, 2007, p. 1)

Asimismo, el espía infractor utiliza softwares un poco más sofisticados, que logran capturar toda la actividad de los usuarios que utilizan en una computadora, y capturan imágenes de la pantalla cada cierta cantidad de tiempo, almacenan en archivos de imagen y hasta de video, robando, por ejemplo, información confidencial, password tipeados, fórmulas secretas, precios, sueldos, espiar conversaciones, revisar las páginas web visitadas, etc, etc. sin que el usuario ni siquiera lo imagine. (Pinto, 2007, p. 1)

Es importante reconocer que gran porcentaje del valor de una compañía se basa en la información que esta posee. El robo de esta información no solo representa pérdidas económicas potenciales para las empresas, sino que también tiene repercusiones significativas en cuanto a su imagen ante sus clientes y el público en general, debido a que estos pueden percibir que su información privada podría ser vulnerada. (Jarabo, 2015)

Han existido casos, en que el robo de información ha hecho perder a industrias millones de dólares como por ejemplo sacar al mercado días antes, productos con el mismo nombre, o simplemente falsificar un invento a menor costo, copiando la fórmula de preparación, estrategias de fabricación, negociaciones millonarias, robo de patentes o contratos, etc. (Pinto, 2007, p. 1)

## ii. **Conducta Desleal:**

Conforme a la doctrina, tendrá así mismo la consideración de desleal, la adquisición de secretos empresariales (Know How) por medio de actividades de espionaje corporativo. Así pues, incurrirá en actos de competencia desleal el tercero que tenga acceso ilegítimo a un secreto empresarial y lo divulgue o explote, o el tercero que habiendo tenido acceso legítimo a un secreto empresarial lo divulgue o explote sin autorización de su titular, violando su deber de reserva. En este último caso sobresale el de los empleados que tienen acceso legítimo a la información secreta de la empresa, puesto que estos tienen obligaciones en virtud del contrato laboral, dentro de las cuales se encuentran la obediencia y fidelidad para con el empleador. (Sanín, 2013)

Está claro que la fórmula de un producto comercializado cuando se oculta por la empresa propietaria, es secreto de empresa, sin embargo, el listado de clientes, productos, precios y de proveedores, si bien es cierto son información de carácter confidencial, no tendrán el mismo valor económico que una fórmula única y distintiva. En estos casos el empresario minorista, ávido de conocer los precios de sus competidores, tiende a ofrecer a un trabajador de la competencia, que tenga una cláusula de confidencialidad, que le facilite el citado listado de precios. En la doctrina española, se considera también como violación del secreto empresarial y se sanciona severamente con dos años de pena privativa de libertad, presentándose un problema de ponderación. (López, 2009)

### **2.2.5.1.1. La Delincuencia Informática:**

La delincuencia informática es percibida por las empresas como uno de los riesgos emergentes más preocupantes y con mayor impacto que el crimen convencional. La pérdida de beneficios, las horas del personal perdidas en la gestión de los ataques de seguridad en las tecnologías de la información y los daños de reputación e imagen están considerados como problemas más importantes que los ocasionados por el crimen convencional. (Villén, 2010, p. 2)

Los impactos en el negocio incluyen además de las pérdidas económicas directas, las derivadas del lucro cesante por cierres temporales de las operaciones para limitar los efectos de un ataque y el intangible derivado del impacto en la reputación e imagen por el incremento de la publicidad negativa en los medios. (Villén, 2010, p. 2)

Para la sociedad los ataques contra las infraestructuras críticas tanto energéticas, sanitarias, transportes, telecomunicaciones son objetivos estratégicos capaces de afectar a un porcentaje altísimo de la población e impedir el suministro de los servicios esenciales. (Villén, 2010, p. 2)

El cibercrimen comprende toda actividad delictiva cometida por medio de herramientas informáticas o contra los sistemas informáticos. La característica principal de este tipo de actos es que para ser perpetrados es necesario acceder a redes de información o medios informáticos. (González, 2014, p. 2)

Los recursos que se deben considerar frente a las amenazas a la seguridad de la información, son los siguientes:

1. **Hardware:** Procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadores personales, impresoras, unidades de disco externas, líneas de comunicación, servidores terminales, routers.
2. **Software:** Programas fuente, programas objeto, programas de diagnóstico, sistemas operativos, programas de comunicación.
3. **Datos:** Durante la ejecución, almacenados en línea, archivados fuera de línea, respaldos, registros de auditoría, bases de datos.
4. **Personas:** Usuarios, personas necesarias para operar dichos sistemas.
5. **Documentación:** Sobre programas, hardware, sistemas, procedimientos administrativos.
6. **Suministros:** Papel, formularios, cintas, medios magnéticos.  
(González, 2014, p. 10)

La Confidencialidad se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático, basándose en este principio, las herramientas de seguridad informática deben proteger el sistema de invasores y accesos por parte de personas o programas no autorizados. Este principio es particularmente importante en sistemas distribuidos, es decir, aquellos en los que los usuarios, computadores y datos residen en localidades diferentes, pero están físicamente y lógicamente interconectados. (González, 2014, p. 11)

#### **2.2.5.1.2. La Competencia como Bien Jurídico Tutelado:**

**Según Abanto (1997)**, la competencia es en sí un bien, cuya protección legal es necesaria para el buen funcionamiento del sistema económico de economía de mercado. Pero esa competencia tiene dos aspectos:

- a) El referido a la libertad de los agentes económicos durante su actuación en el mercado.
- b) La (debida) lealtad entre los agentes económicos al momento de competir.

En el primer caso, trata del Derecho de la Libre Competencia o de sus sinónimos Derecho Antitrust o Derecho contra las prácticas restrictivas de la competencia. En el segundo caso se trata del Derecho contra la competencia desleal. (Abanto, 1997, p. 144)

Ahora bien, la libertad de competencia como valor, dentro de una economía social de mercado, ha sido unánimemente reconocida como bien jurídico. Su importancia radica en la operatividad que otorga al sistema de economía de mercado; la libre competencia es el instrumento que hace real la consecución, no solamente de fines económicos (aumento de bienestar), sino también de fines políticos: el permitir el máximo desarrollo posible de libertad individual (No puede haber economía (social) de mercado sin libertad de competencia. (Abanto, 1997, p. 144)

Tampoco puede existir libertad de competencia, si ésta no tiene una mínima protección legal, pues se sabe por experiencia que un sistema, que en sus inicios puede ser competitivo, tiende a ser destruido por los propios agentes económicos mediante prácticas restrictivas, si éstas no son controladas administrativa y/ o penalmente. Queda entonces claro que la protección de la competencia no interesa únicamente a los agentes del

mercado y participantes directos en el proceso económico, sino a toda la colectividad. (Abanto, 1997, p. 144)

### **2.2.5.1.3. La Protección Penal de la Competencia Leal:**

Junto con el derecho de competir, existe un deber relacionado con la forma cómo debe realizarse la competencia. Existen entonces métodos prohibidos por constituir competencia desleal en contra de los demás competidores y de los consumidores. El objeto de protección o bien jurídico protegido en este ámbito no es pasible de una distinción específica y exclusiva; aquí confluyen varios intereses protegidos. (Abanto, 1997, p. 148)

Como dice **Rittner citado por Abanto (1997)**, refiriéndose al fin de protección de la ley alemana contra la competencia desleal, no se necesita una construcción dogmática especial, ya que la ley sólo pretende impedir acciones desleales de competencia, pues ellas entran en conflicto con intereses de los competidores, pero también con los de la generalidad y de los consumidores. (Abanto, 1997, p. 148)

El legislador peruano ha reconocido a la “libre competencia” (económica) como instrumento básico de la economía de mercado y como bien necesitado de una adicional protección legal. En una economía de mercado, tal como ha demostrado la experiencia, no se puede dejar todo al libre juego de la oferta y la demanda si, previamente, no se dispone de reglas básicas que deben ser respetadas por todos los agentes económicos. Se debe garantizar, por ello, la “libertad” de competir a todos los agentes económicos en aquellos sectores del mercado, donde tal “libre competencia” sea posible y deseable. (Abanto, 2006)

La competencia está basada en la libertad de decisión de los que participan en el mercado, en un contexto en el que las reglas de juego son claras para todos y se cumplen. La libre competencia se basa fundamentalmente en la libertad de elección tanto para el consumidor, como para el productor.

Tanto la libertad de elección del consumidor como la del productor son inseparables, de ellas depende en gran medida que se logre una asignación eficiente de recursos en la economía. A través de estos principios, cuando se cumplen ciertas condiciones básicas, es a través del mecanismo del mercado asegurando que los recursos productivos se dirijan a aquellos usos más productivos, entendiendo por ello aquellos bienes y servicios que los consumidores prefieren en mayor medida. (Berenguer, 2009)

#### **2.2.5.1.4. Proceso de Ingresos y Egresos del Estado:**

La sociedad actual, debido al modelo de producción que tiene, ocasiona la desigualdad en la distribución de la riqueza; existe un sector que recibe el monto mayor del producto nacional y otro que recibe un mínimo de tal producto. Es por esto que, el Estado, interviniendo en la economía, trata de disminuir tal brecha, para lo cual recauda un porcentaje de las ganancias del grupo que recibe el mayor monto de ingresos y lo reparte entre los grupos con menos ingresos. El medio utilizado para recaudar tales ingresos es el tributo, el mismo que se dirige a gravar las expresiones de riqueza de las personas: patrimonio, renta, consumo. (Bramont, 1992, p. 90)

El reparto de lo recaudado mediante los tributos es a través de servicios a la colectividad dirigidos mayoritariamente a los sectores de menos ingresos y traducidos en salud pública, educación, energía eléctrica, agua, etc. Además, la redistribución no sólo se orienta a compensar a los estratos sociales más bajos, sino que constituye un verdadero instrumento de política económica, por cuanto posibilita que el Estado a través del otorgamiento de ciertos caminos encamine la inversión del sector privado, al facilitarles la realización de sus actividades; por otro lado, posibilita el capital que requiere el Estado, en tanto interviene en determinados

sectores económicos como un agente económico más. (Bramont, 1992, p. 90)

Según Bramont (1992) el dañar el proceso de ingresos y egresos que realiza el Estado (desvalor del resultado) no es suficiente para la existencia de la sanción penal; ésta requiere además el engaño, fraude o artificio en el sujeto activo con la finalidad de no pagar el tributo o pagar una suma reducida por tal concepto (desvalor de la acción). (Bramont, 1992, p. 90)

#### **2.2.5.1.5. Cargo de Confianza:**

##### **A. Definición y Base Legal**

Trabajadores de confianza son aquellos que laboran en contacto personal y directo con el empleador o con el personal de dirección, teniendo acceso a secretos industriales, comerciales o profesionales y, en general, a información de carácter reservado. Asimismo, aquellos cuyas opiniones o informes son presentados directamente al personal de dirección, contribuyendo a la formación de las decisiones empresariales. (Ley de Productividad y Competitividad Laboral, 1997, art. 43°)

El personal de confianza, a diferencia de un trabajador de dirección quien tiene facultades para representar a la empresa ante otros trabajadores y terceros, es aquel que tiene acceso a información administrativa, comercial, industrial y en general de carácter confidencial como lo señala la norma pertinente expuesta. (Valdivia, 2012, p.16)

#### **2.2.5.2. Subcapítulo II: El Contrato de Franquicia**

##### **2.2.5.2.1. Concepto del Contrato de Franquicia:**

El contrato de franquicia es aquel contrato por el cual el titular de una marca o nombre comercial llamado franquiciante, otorga licencia a una empresa distinta e independiente llamada franquiciado permitiéndole que produzca exactamente su sistema de explotación del negocio, que puede ser la venta de bienes o la prestación de servicios de reconocido prestigio y eficiencia, poniendo a su disposición a cambio de una contraprestación económica, su marca, su saber hacer (know-how) y sus métodos comerciales y empresariales. Es un contrato atípico, que en el Perú no se encuentra regulado legalmente. (Espinoza, 2006, p. 3)

La Legislación Española define al contrato de franquicia como aquel por el cual una empresa, el franquiciador, cede a otra, el franquiciado, a cambio de una contraprestación financiera, el derecho a la explotación de una franquicia sobre un negocio o actividad mercantil para comercializar determinados tipos de productos o u otros derechos de propiedad intelectual o industrial y una presentación uniforme de los locales o medios de transporte; la comunicación por el franquiciador al franquiciado de unos conocimientos técnicos o un “saber hacer”, que deberá ser propio, sustancial y singular; y la prestación continúa por el franquiciador al franquiciado de una asistencia comercial o técnica. (Real Decreto 201/2010, 2010, art. 2 inc. 1)

#### **2.2.5.2.2. Características del Contrato de Franquicia:**

La figura de la franquicia ha permitido poner al alcance de los inversionistas el poder invertir en un negocio exitoso, ya estructurado y con todos los manuales y "recetas" puestas a disposición para poder asimilar ese know how, a cambio de un pago. Esto le permite al inversionista poder tener utilidades casi garantizadas, pues el formato de negocio ha probado que puede generar beneficios económicos. Al respecto es oportuno establecer de manera clara la diferencia que existe entre know y franquicia. (Alfaro, 2013)

Según el Dr. Víctor Pérez, citado por Alfaro (2013): "La franquicia comercial es, entre otras cosas, un contrato de transferencia de tecnología, de transferencia de know how. Sin embargo, el know how es sólo uno de los componentes de la franquicia comercial. Franchising puede implicar transferencia de know how, su función va más allá."

La transmisión del know how que tiene lugar en la franquicia es uno de sus elementos principales, donde el franquiciado es destinatario y beneficiario de la recepción de este y el franquiciador deberá tomar las providencias necesarias para evitar la divulgación de esta información y su explotación por personas distintas a las autorizadas por él o que habiendo sido autorizadas en un momento determinado, intenten utilizar este conocimiento fuera del marco de lo contratado para obtener beneficios económicos ilícitos. (Fonseca, 2017)

En la Guía de Franquicias de UNIDROIT se señala que el término know-how se refiere generalmente al conjunto de conocimientos profesionales que es adquirido por las personas dedicadas a una actividad específica y que es distintivo de esa actividad. Este conocimiento es usualmente una combinación de información fáctica acerca de la actividad y de la experiencia obtenida en su ejercicio. (Alfaro, 2013)

#### **2.2.5.2.3. El Secreto Comercial en el Contrato de Franquicia:**

**Concepto:** El secreto Comercial es el conjunto de conocimientos que el franquiciador utiliza en la práctica como resultado de su experiencia en el desarrollo de una actividad comercial determinada, que le aportan una ventaja competitiva en el mercado y por tal motivo mantiene esta información en secreto. (Fonseca, 2017)

La protección del secreto comercial en el contrato de franquicia se puede deslindar en **dos vertientes**, la vía **formal** que se materializa en la concertación de acuerdos de confidencialidad, cláusula de exclusividad y otras de similar naturaleza, así como el control que debe ejercer el franquiciador sobre el negocio del franquiciado a fin de prevenir la creación de redes paralelas de distribución que utilicen el know how del que es titular. La vía **no formal**, consiste en la colaboración y compromiso que se establece entre ambas partes, lo que se evidencia desde la selección del franquiciado en base al carácter *intuitu personae* del contrato de franquicia y en la relación que establezcan las partes mediante la capacitación y asistencia técnica y comercial continua que provee el franquiciado al franquiciador. (Fonseca, 2017)

#### **i. Legislación Comparada:**

La legislación mexicana en materia de propiedad industrial señala que existirá franquicia, cuando con la licencia de uso de una marca, otorgada por escrito, se transmitan conocimientos técnicos o se proporcione asistencia técnica, para que la persona a quien se le concede pueda producir o vender bienes o prestar servicios de manera uniforme y con los métodos operativos, comerciales y administrativos establecidos por el titular de la marca, tendientes a mantener la calidad, prestigio e imagen de los productos o servicios a los que ésta distingue. (Ley de Propiedad Industrial, 1991, art. 142)

Asimismo, la legislación brasileña en materia de franquicias, señala que el negocio de franquicia es el sistema por el cual un franquiciador concede al franquiciado el derecho al uso de la marca o patente, junto con el derecho exclusivo de distribución de productos o servicios o semi-exclusivos y posiblemente también el uso de tecnología adecuada el despliegue y la gestión de los negocios o el sistema operativo desarrollado por el

franquiciador o en poder de la remuneración directa o indirecta. (Ley N°. 8.955, 1994, art. 2)

## ii. Las Partes del Contrato:

- En el contrato de franquicia participan dos sujetos:
  - a) **El franquiciante.** Es el dueño de una marca y un negocio, titular de la licencia quien la otorga a una empresa independiente para que venda bienes o preste servicios.
  - b) **El franquiciado.** Es aquella empresa independiente que vende los bienes o presta los servicios de los que es titular el franquiciante. (Espinoza, 2006, p. 4)
- **El franquiciador** es la persona jurídica que cede la utilización del modelo de empresa a franquiciar y el **franquiciado** que es el tomador de dicho modelo. Aunque los sujetos deben ser independientes, al ser un contrato que genera un alto grado de colaboración duradera, entre ambas partes se produce una integración tal que las identifica a ambas frente a terceros. (Fonseca, 2017)

### a) Obligaciones contraídas:

#### i. El Franquiciante:

- Según lo pactado en cada contrato, las obligaciones del franquiciante pueden ser:
  - a) Proporcionar al franquiciado los productos, marcas, nombres y el know-how (conocimientos), tales como recetas, procedimientos y manuales para la elaboración de los productos o servicios que ofrecen, lineamientos de control de calidad, forma de comercializarlos, etc.

- b) Contactar al franquiciado con los proveedores considerando precios bajos y con entregas puntuales.
- c) Brindar educación continua, entregando manuales de operación detallando temas importantes para manejar correctamente el negocio.
- d) Hacer investigaciones y desarrollar continuamente los productos o servicios a fin de mantener la calidad de sus productos o servicios, independientemente de cuál sea al país donde se encuentre la franquicia. (Espinoza, 2006, p. 4)

Entre los elementos objetivos podemos referir la cesión del uso de derechos de propiedad industrial entre los que se pueden encontrar las marcas y las patentes; la capacitación y asistencia técnica continua que deberá prestar el franquiciador durante la vigencia del contrato; el control ejercido por este sobre la gestión del negocio y su comportamiento en el mercado; el pago del canon de entrada y de las regalías o royalties por los beneficios obtenidos de la explotación de la franquicia y la transferencia del know how, materializado en la entrega de manuales operativos del sistema de franquicia. (Fonseca, 2017)

## **ii. El Franquiciado:**

Según lo pactado en cada contrato, las obligaciones del franquiciado pueden ser:

- b)** Cumplir con el pago inicial para obtener la franquicia y de las regalías, éstas últimas pactadas generalmente como un porcentaje sobre las ventas mensuales.
- c)** Cumplir con la calidad del producto y someterse a las diferentes evaluaciones que el franquiciante realice en la empresa.

- d) Respetar los lineamientos establecidos en los contratos, las medidas y decoraciones de los locales destinados a ofrecer el servicio, apearse a los patrones de producción y métodos de servicio establecidos.
- e) No hacer uso indebido de la marca, respetar los precios fijados, guardar la debida reserva de la información suministrada por el franquiciante durante el desarrollo del negocio. (Espinoza, 2006, p. 4)

#### **2.2.5.2.4. Principales Pagos:**

La justificación de la contraprestación económica que debe pagar el franquiciado al franquiciador en forma de canon de entrada y regalías es la explotación del know how y de la marca, complementado por las mejoras continuas del sistema que realiza el franquiciado con el fin de mantener su competitividad en el mercado. (Fonseca, 2017)

- Según Espinoza (2006), los principales pagos son los siguientes:

##### **a) Honorario Inicial (Franchising Fee)**

Es el importe que el franquiciado, cancela al franquiciante por utilizar una marca debidamente registrada. Este monto no incluye ni el costo del local ni de los equipos o mobiliario de trabajo.

##### **b) Regalías (Royalties)**

Es el importe que debe pagar periódicamente el franquiciado por el uso de la marca que le fue otorgada. Generalmente, este importe se calcula en función a los ingresos que obtiene el franquiciado.

##### **c) Fondos de Publicidad**

Es el importe mensual que cobran algunas franquicias para destinarlo a un fondo único de mercadeo y promoción de la marca y sus productos. (Espinoza, 2006, p. 5)

#### **2.2.5.2.5. Tipos de Contratos de Franquicia:**

- Según Espinoza (2006) los tipos de contratos de franquicia, son los siguientes:

##### **a. Franquicia de distribución**

En este tipo de franquicia, el franquiciante vende o fija al franquiciado los productos que tiene que vender, completando el trabajo con la aportación de una marca y varios servicios de organización y venta.

##### **b. Franquicia de servicio**

El franquiciado suministra un servicio organizado a través de una técnica o normativa determinada, cuya fórmula original es propiedad del franquiciante bajo una misma marca.

##### **c. Franquicia industrial**

En este caso, el franquiciante se asocia a otras industrias para que fabriquen sus productos bajo licencia, beneficiándose estas industrias de su tecnología, marca y ayuda técnica.

##### **d. Franquicia maestra**

Se trata de la relación contractual en la que el franquiciante es extranjero, quien cede al franquiciado el derecho a implantar y operar unidades en determinado territorio, usualmente un país, actuando este último como franquiciado y al mismo tiempo como franquiciante de

determinados puntos de venta que se inauguran, siendo directamente responsable del desarrollo y representación del franquiciante extranjero de forma exclusiva en el territorio (país o países). (p. 5)

#### **e. El Know How en el Contrato de Franquicia:**

La transmisión del know how es el elemento sine qua non del contrato de franquicia, ya que en este radica la esencia del funcionamiento del modelo de empresa creado por el franquiciador, deviniendo el resto de los elementos señalados en complementos de la transmisión del know how. En el caso de las marcas y signos distintivos, estos cumplen la función de diferenciar el negocio en el mercado y atraer a clientes y consumidores, pero es el know how utilizado el que los fideliza y marca la preferencia por el negocio. Sin la existencia de un know how y la necesidad de su transmisión al franquiciado no sería necesaria la capacitación inicial y asistencia técnica que debe prestar el franquiciador, así como tampoco sería necesario el control que este debe ejercer a fin de evitar actuaciones ilícitas por parte del franquiciado en relación con las ventas o la utilización inadecuada del modelo. (Fonseca, 2017)

#### **2.2.5.3. Subcapítulo III: Personas Jurídicas - Riesgos Empresariales del Espionaje Corporativo**

Persona jurídica (o persona moral) es un sujeto de derechos y obligaciones que existe, pero no como individuo, sino como institución y que es creada por una o más personas físicas para cumplir un objetivo social que puede ser con o sin ánimo de lucro. (Ferrara, 1929)

En el ámbito organizacional de la empresa, la competencia desleal bajo la modalidad de espionaje comprende aquella actividad del trabajador que utiliza las herramientas, contactos y conocimientos adquiridos en una

empresa para aplicarlos en otra actividad bien sea por cuenta ajena o por cuenta propia sin el consentimiento del empresario, siempre y cuando le cause a dicho empresario un perjuicio real o potencial. Por lo tanto, la competencia desleal se produce cuando el trabajador abusa de la buena fe contractual y utiliza en su provecho y sin consentimiento unos medios formativos que le han sido ofrecidos por una empresa. (Gonzales, 2011)

El empresario puede limitar, a través de un pacto de no competencia, que el trabajador preste servicios en una empresa de la competencia con el fin de que la formación que ha recibido no sea explotada por una empresa del mismo sector durante un periodo determinado. El pacto de no competencia se puede realizar entre empresa y trabajador al inicio de la relación laboral, durante la vigencia del mismo o a la extinción del contrato de trabajo. (Gonzales, 2011)

Según Stucchi (2016) una empresa podrá poseer:

- A. **Secretos industriales**, tales como fórmulas, recetas, composiciones de productos, investigaciones sobre nuevos productos, planos, técnicas de producción industrial, diseños de plantas o de maquinaria, etc.
- B. **Secretos comerciales**, tales como listas de clientes, listas de proveedores, estructura de costos, metodologías propias de fijación de precios, estudios propios de preferencias de los clientes, perfiles de consumidores, etc.
- C. **Secretos internos**, tales como aquellos sobre la organización interna de la empresa, las estrategias corporativas, las estrategias de financiamiento e inversión, los estados financieros (salvo que la empresa se encuentre obligada a su divulgación por participar en el mercado de valores), etc. (Stucchi, 2016)

### **2.2.5.3.1. Los retos de la protección**

Los secretos empresariales son información que las empresas utilizan para su actividad. Ello implica el reto de darles uso mientras, a la vez, se deben mantener reservados. Situación difícil. Este reto reviste mayores exigencias debido a la permanente evolución tecnológica dirigida a la captación, registro, transmisión y reproducción de información. (Stucchi, 2016)

En este contexto, la empresa tendrá que evaluar si vale la pena asumir los costos de evitar que un colaborador suyo, una contraparte contractual o un espía industrial, tome y/o comparta indebidamente sus secretos. Ello dependerá del valor que generan tales secretos y si este supera los costos indicados. Evaluado lo anterior, la empresa podrá tomar una decisión eficiente. (Stucchi, 2016)

Cualquier perjudicado por actos de competencia desleal declarados por la Comisión o, en su caso, por el Tribunal, podrá demandar ante el Poder Judicial la pretensión civil de indemnización por daños y perjuicios contra los responsables identificados por el INDECOPI. (Decreto Legislativo N° 1044, 2008, art. 58)

#### **2.2.5.3.1.1. Importancia de la Información para las Organizaciones**

Considerando que toda organización, está compuesta por un conjunto de procesos sinérgicos que se comunican entre sí a través del intercambio de información transformada por cada uno de ellos y que de la completitud, disponibilidad, integridad y calidad de la misma depende el éxito de la operación corporativa al igual que la toma de decisiones necesarias para dirigir el rumbo de toda compañía, puede afirmarse que la información es el activo más importante de toda empresa y que esta debe hacer todo lo necesario para salvaguardarlo. (Santiago y Sánchez, 2017, p. 5)

Puede afirmarse que la seguridad de la información depende de que se garanticen sus principios conocidos como: la confidencialidad, integridad y disponibilidad al igual que se garantice el no repudio, autenticidad y la trazabilidad de la misma en los procesos en los que se haga uso de ella. Podría decirse que las medidas de riesgo de la seguridad de la información, los controles que deben usarse para protegerla y la efectividad de los mismos se miden en relación a los principios antes mencionados. (Santiago y Sánchez, 2017, p. 5)

#### **2.2.5.3.2. La protección de los secretos empresariales:**

Si la decisión es proteger sus secretos empresariales, la única opción efectiva para ello es que la propia empresa implemente medidas eficaces en su organización y en sus relaciones contractuales. Primero, la empresa debe lograr que aquellos que accedan a sus secretos con autorización asuman la obligación de hacerlo con reserva y de no utilizarlos para otros fines; y, que en efecto ello sea cumplido. (Stucchi, 2016)

#### **2.2.5.3.3. Riesgos Empresariales:**

El riesgo es la probabilidad que una eventualidad se aproveche de las vulnerabilidades de un sistema e imposibilite el cumplimiento de su objetivo o ponga en peligro a los bienes de la organización, ocasionándole pérdidas o daños. (Domínguez, 2015, p. 13)

La actual incursión de las tecnologías de la información ha causado que se empeore la situación, debido a que las empresas guardan mucha de su información más importante en medios digitales a los cuales se puede acceder por la red. Pero también existen otros métodos: uno de los principales inconvenientes son los mismos empleados de la empresa, en la medida en que el mismo recurso humano puede ser una de las mayores

filtraciones de información en una empresa, lo cual apoya las teorías que buscan mejores ambientes laborales. (Stave, 2013, p. 66)

#### **2.2.5.3.3.1. Clasificación de Riesgos**

- A) **Riesgo Estratégico:** tipo de riesgo delicado de tratar, se produce a niveles altos de la empresa ya que se asocia con la forma en que se administra.
  - B) **Riesgos Operativos:** Comprenden los riesgos relacionados con deficiencias en los sistemas de información o controles internos, cubre dos aspectos claves: la integridad de los procesos de negocios y la habilidad de mantener la entrega de productos en forma consistente y oportuna.
  - C) **Riesgos Financieros:** Se relacionan con los recursos de la empresa.
  - D) **Riesgos de Cumplimiento:** Se asocian con la capacidad de la empresa para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
  - E) **Riesgos de Tecnología:** Dicho riesgo se relaciona con la capacidad tecnológica disponible por la empresa para satisfacer sus necesidades actuales, futuras y de soporte al cumplimiento de su misión. (Domínguez, 2015, p. 13)
- **Sector Agrícola:** Buainain y Loyola (2015) afirman que la dinámica productiva basada en el uso intensivo de tecnología implica un riesgo tecnológico, que ha sido poco advertido, pero que siempre amenaza el segmento, que depende de la

“continuidad del proceso de innovación, sea para responder a los problemas creados por la propia tecnología, desde la resistencia a las plagas hasta la reducción de la producción, sea para asegurar nuevas ganancias de productividad y rentabilidad”, más aún, para adaptar la producción agropecuaria a las crecientes exigencias socioambientales y de seguridad de los alimentos. (Buainain y Loyola, 2015, p. 60)

#### **2.2.5.3.4. Riesgos Directos en relación con las Personas que tienen Acceso a Información Confidencial**

En relación con las personas con accesos especiales, existen tres tipos principales de peligros que pueden facilitar el espionaje corporativo:

- a) **Soborno:** Es posible que los empleados reciban ofertas directas de agentes de inteligencia de otras corporaciones, que ofrecen dinero en metálico a cambio de información confidencial o protegida.
- b) **Ingeniería Social:** La manipulación de un administrador de redes o de otras personas del departamento de sistemas (ya sea por parte de personas de la propia corporación o por parte de terceros) para que divulguen información, como datos de inicio de sesión u otros datos de autenticación, que pueden usarse a continuación para obtener el acceso a la información delicada.
- c) **Complicidad en Grupos:** Cuando varios empleados se alían para usar sus conocimientos y privilegios colectivos para obtener el acceso a la información. (Guillermo y Edwin, 2003)

#### **2.2.5.3.5. Pequeñas Empresas:**

Las empresas competidoras pequeñas se ven perjudicadas, en virtud al establecimiento de territorios de comercio exclusivo a través de las siguientes formas:

- a) Bajando los precios artificialmente en el país donde existan empresas de menor envergadura, y conservando los precios normales en otros países.
- b) Ejerciendo presión sobre distribuidores o manejando directamente la comercialización de la producción, de manera que se cierran mercados vitales para las empresas nacionales.
- c) Mediante el espionaje industrial.
- d) Aumentando los costos de producción en la zona local, mientras se distribuyen los costos adicionales en otras zonas, de manera que aquel aumento no las perjudique verdaderamente.
- e) Prácticas laborales injustas, mediante interferencias en la elaboración de contratos colectivos, soborno a líderes sindicales, espionaje interno. (Ramos, 2015, p. 136)

#### **2.2.5.3.6. Tipo de Daños**

##### **a) Daños al patrimonio inmovilizado:**

La creciente competitividad en los mercados, la crisis económico social y los fenómenos terroristas han sido las causas principales del nacimiento de los denominados actos vandálicos o malintencionados contra el patrimonio empresarial, también llamados actos de sabotaje en terminología jurídica. (Gonzales, 1987, p. 36)

Atendiendo a las causas mencionadas, se podría distinguir entre el sabotaje laboral que tiene su origen en la problemática socio-laboral dentro de la propia empresa y viene originado por actos de los empleados en conflicto, el sabotaje penal causado por terceros ajenos a la empresa, que pretenden infringir un daño por malquerencia u otras

razones y, finalmente, el sabotaje político social que proviene de los actos terroristas, los cuales pretenden atentar contra la seguridad ciudadana como medio de infundir el terror colectivo. (Gonzales, 1987, p. 36)

**b) Daños a los Valores Monetarios:**

Los valores monetarios de la empresa (dinero, cheques, letras de cambio, etc, se ven amenazados por el riesgo de robo, atracos, falsificaciones, infidelidad de los empleados (apropiación indebida, malversaciones de fondos, etc). Durante los últimos años, estos riesgos han sido los que más agravación presentan, pasando a ser una de las más importantes fuentes de pérdida para las empresas. (Gonzales, 1987, p. 36)

**c) Daños a los archivos, informes y documentación:**

A medida que la empresa ha ido aumentando su desarrollo, la dependencia de sus archivos resulta vital. Con la mecanización paulatina de las empresas, al existir una gran concentración de toda ella, resultan más vulnerables frente a cualquier acto de saboteadores, empleados deshonestos, manipulación de soportes magnéticos, etc. (Gonzales, 1987, p. 37)

**d) Daños a la propiedad industrial:**

Otro de los riesgos que ha adquirido más auge es el comúnmente conocido espionaje industrial, que se produce mediante el robo de información de nuevos productos, planos, patentes, listas de clientes, precios, etc. Tiene su causa, en la agresiva y dura competencia de mercados, junto a los rápidos avances tecnológicos. (Gonzales, 1987, p. 38)

**e) Manipulación maliciosa de los productos:**

Fundamentalmente consiste en actos de sabotajes en los productos de la empresa, a fin de ocasionar una pérdida de imagen y subsiguiente pérdida de mercado (caso Tilenol en los EE UU, la emisión de falsos rumores sobre la nocividad de determinados productos, etc.). (Gonzales, 1987, p. 38)

**f) Fraude o estafa**

La crisis socio-económica ha originado una inestabilidad empresarial con numerosas desapariciones de empresas, surgimiento de otras nuevas. etc. Que ha sido aprovechada por delincuentes profesionales para, fingiendo una actividad empresarial lícita, hacer pedidos o comprometerse a realizar suministros, que a la postre han resultado ser estafas o fraudes, habiendo recibido previamente las mercancías o las cantidades correspondientes a estos pedidos. (Gonzales, 1987, p.38)

**2.2.5.3.7. Actos contra los Hombres Clave de la Empresa**

Además de los daños patrimoniales referidos, en la actualidad, el atentado contra los hombres clave de la empresa constituye un factor de riesgo importante que puede provocar pérdidas tan altas o aún mayores que las causadas por los fenómenos previamente citados. La desaparición de los hombres clave de la empresa ya sea por secuestro o fallecimiento por un acto criminal, pueden conducir a una importante pérdida para la empresa, tanto por su incidencia en la cadena productiva como por la dificultad de encontrar un sustituto. (Gonzales, 1987, p. 38)

En la búsqueda de los riesgos que afectan a los hombres clave de la empresa, hay que pensar que son estas personas el objetivo potencial de

los actos criminales, bien por finalidades políticas, por deseos de venganza, chantajes, etc. (Gonzales, 1987, p. 39)

#### 2.2.5.4. Subcapítulo IV: Los Secretos Empresariales como Derechos de Propiedad intelectual

Las iniciativas privadas muchas veces contienen secretos o información reservada que se presentan con la petición, y que gozaría o podría gozar de protección de la legislación de Propiedad Industrial u otra, en la medida que esos secretos sean partes de patentes de invención, secretos industriales, el llamado Know How o métodos de negocio u otros elementos protegidos o protegibles por la legislación especializada en Propiedad Intelectual. (Mercado, 2009, p. 402)

Según Alfaro (2013), de acuerdo a lo que han señalado los doctrinarios y el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (Acuerdo sobre los ADPIC), para que la información no comunicada pueda ser sujeta a protección es necesario que se den las siguientes condiciones:

- a) **Que sea secreta**, en el sentido de que no sea, en la configuración y reunión precisas de sus componentes, conocida en general ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza el tipo de información en cuestión. Cabanellas de las Cuevas manifiesta al respecto, que "la condición de confidencialidad de la tecnología es un requisito fundamental para su protección jurídica".
- b) Que tenga **un valor comercial** por ser secreta. El valor comercial de esta información tiene una relación directa con la condición de ser secreta, pues si se convirtiera en información de dominio público perdería ese valor.

- c) Que haya sido objeto de **medidas razonables**, en las circunstancias, para mantenerla secreta, tomadas por la persona que legítimamente la controla". Al respecto, la jurisprudencia de Costa Rica ha señalado en una resolución ya mencionada anteriormente: "Este último aspecto de ausencia de divulgación se materializa en el hecho de que el titular de los derechos ejecuta acciones tendentes a impedir que terceros conozcan el secreto empresarial, de donde se deduce que si el poseedor del secreto que le otorga ventajas competitivas no toma las medidas de ocultamiento correspondientes no podrá hablarse de secreto empresarial, ni el ordenamiento jurídico otorgará protección al poseedor del secreto. (Alfaro, 2013)
- En el **Título III de la Decisión N.º 486** respecto a las Patentes de Invención, en el artículo 15º se establecen qué no se consideran patentes. En ese sentido se enumeran las siguientes:
    - (1) Los descubrimientos, las teorías científicas y los métodos matemáticos.
    - (2) El todo o parte de seres vivos tal como se encuentran en la naturaleza, los procesos biológicos naturales, el material biológico existente en la naturaleza o aquel que pueda ser aislado, inclusive genoma o germoplasma de cualquier ser vivo natural.
    - (3) Las obras literarias y artísticas o cualquier otra protegida por el derecho de autor.
    - (4) Los planes, reglas y métodos para el ejercicio de actividades intelectuales, juegos o actividades económico-comerciales.
    - (5) Los programas de ordenadores o el soporte lógico, como tales.
    - (6) Las formas de presentar información. (Decisión N° 486, 2000, art. 15)

Los Países Miembros otorgarán patentes para las invenciones, sean de producto o de procedimiento, en todos los campos de la tecnología, siempre que sean nuevas, tengan nivel inventivo y sean susceptibles de aplicación industrial. (Decisión N° 486, 2000, art. 14)

#### **2.2.5.4.1. Patentes de Invención**

##### **a) Definición:**

Es un privilegio de explotación monopolística que la ley concede al inventor en retribución o como compensación a su aporte tecnológico. “La patente industrial se individualiza por la idea de invención, que consiste, en definitiva, en el empleo original de una combinación de fenómenos físicos para la solución de un problema de técnica industrial. (Callaghan, 2001)

Fernández Rodríguez, citado por Aguila y Gallardo (2011) afirma que la patente es un título concesional que otorga determinados derechos subjetivos al inventor respecto de la Administración y de todos los miembros de la comunidad.

Las ideas se materializan por medio de la invención efectuada. El Estado es quien reconoce el derecho de exclusividad del inventor por medio de una certificación específica denominada patente de invención, que corresponde, como derecho, a la clasificación de los derechos inmateriales. La patente convierte al creador en el dueño de su invención protegiéndolo de las posibles copias de otras personas y, evitando que otras personas la exploten sin obtener éste ningún beneficio. (Aguila y Gallardo, 2011)

La patente confiere los derechos de: uso exclusivo, producción exclusiva (monopolio legal), comercialización exclusiva y la posibilidad de ceder y otorgar licencia de sus derechos. (Aguila y Gallardo, 2011)

## b) CARACTERÍSTICAS:

Según Aguila y Gallardo (2011), tenemos las siguientes características:

- **Constitutivo:** La concesión es diferente de la autorización porque concede al inventor o al grupo de inventores la posibilidad de un reconocimiento a partir de un registro.
- **Excluyente:** Reconoce al inventor que asuma un conjunto de medidas en defensa de su derecho y le proporciona el uso económico privativo durante un periodo determinado en el tiempo.
- **Discrecionalidad:** Todo invento es susceptible de solicitud de registro, sin embargo, la Administración, a partir de la dirección competente determina si la solicitud guarda los elementos esenciales para que proceda la patentabilidad, es decir, la solicitud no necesariamente conlleva la obtención de la misma, sino que se dan las etapas de evaluación que, solo de ser satisfechas convenientemente, acarrearán un registro satisfactorio.
- **Estabilidad:** Aprobada la solicitud, y durante la vigencia de ella, el derecho del inventor es irrestricto y se encuentra normado para garantizar la explotación económica rentable, pues conceden los plazos lo suficientemente amplios. Asimismo, la extinción del derecho y la facultad del uso exclusivo están minuciosamente legisladas de tal forma que garanticen la concesión obtenida. (Aguila y Gallardo, 2011)

### c) REQUISITOS:

Según Aguila y Gallardo (2011), los requisitos son los siguientes:

- ❖ **La Novedad:** Se produce cuando el invento no se encuentra comprendido en el denominado “estado de la técnica” expresión que alude a que el invento sujeto de patente no hubiera estado en conocimiento del público en cualquier forma antes de la fecha de presentación de la solicitud.
- ❖ **La Actividad inventiva:** Implica que el invento no provenga en forma directa del estado de la técnica, bajo ningún aspecto (aplicación, método, combinación de métodos, resultado industrial logrado, etc). Además, hay que tener en consideración que en la actualidad es frecuente que los inventos también puedan ser perfeccionamiento de una invención ya patentada o también que se produzcan inventos que toman como base a otras invenciones ya patentadas, lo que constituiría una patente dependiente.
- ❖ **Susceptible de aplicación industrial en cualquier área tecnológica:** Este requisito se refiere al hecho de ser posible el empleo del invento de manera inmediata no solamente en cuanto se trata de un objeto sino además de su propio desarrollo.
- ❖ El criterio de industriabilidad que se plantea, consiste en la capacidad de repetir el proceso de fabricación indefinidamente con resultados constantes. **(Aguila y Gallardo, 2011)**

#### 2.2.5.4.2. Información Tecnológica y las Patentes

Según Alfaro (2013), cuando se patentiza la información tecnológica los Estados conceden una exclusividad legal de uso del conocimiento o

tecnología que se ha registrado y le concede el monopolio sobre éste. Esto trae como resultado que el Estado que concede la patente libera la divulgación y favorece la libre circulación de las informaciones tecnológicas. Es por ello que la OIUPP (Oficinas internacionales unidas para la protección de la propiedad industrial, literaria y artística), en su modelo de ley para países en desarrollo, en relación con las invenciones se refiere al know how como la antítesis de un derecho de patente y al respecto sostiene:

"La esencia del know how se funda en el hecho de que el inventor prefiere mantener en secreto los elementos desconocidos de su invento, en vez de revelarlos totalmente mediante la solicitud de patente. O bien la solicita, pero eludiendo la obligación de dar determinadas indicaciones esenciales acerca del aprovechamiento del invento". (Alfaro, 2013)

### **(1) Transferencia de Tecnología**

Sinani y Meyer, citados por Alfaro (2013), hacen una sistematización específica de la transferencia de tecnología, cuando señalan que los derramamientos de transferencia de tecnología pueden materializarse mediante tres canales:

#### **a) Demostración-Imitación**

Es propiciado por la existencia de un producto determinado en el mercado que es estudiado e investigado por quien quiere aprender de él, de sus características, o por quien quiere imitar el producto (o copiarlo).

#### **b) La información tecnológica libre:**

Esta información está presente en el mercado y se puede acceder a ella de muy diversas maneras, ya sea a través de material escrito, en libros o revistas, o en internet.

#### **c) La participación de profesionales:**

Las compañías extranjeras o denominadas también transnacionales contratan profesionales del país donde instalan

sus filiales y cuando estos empleados dejan de laborar con esas compañías inevitablemente se llevan consigo una porción de ese conocimiento que necesariamente se puede trasladar a empresas locales o a las que éstos podrían iniciar. (Alfaro, 2013)

- Kelso citado por Alfaro (2013), hace un planteamiento muy interesante acerca del tema del spillover o conocimiento derramado, que tiene por intención caracterizar a este fenómeno como un tipo de transferencia de tecnología que difiere del concepto de know how fundamentalmente por no contar con el carácter secreto del conocimiento, pero que no obstante posee un valor comercial. El conocimiento transmitido mediante el derrame o spillover es un conocimiento aparte, un conocimiento no enmarcado dentro de las consideraciones del contrato de know how por no ser necesariamente secreto y porque no se transmite, por definición, necesariamente con un contrato.

#### **2.2.5.5. Subcapítulo V: La violación de Secreto empresarial y el Espionaje**

##### **2.2.5.5.1. Los supuestos de ignorancia deliberada respecto del origen ilícito de la obtención del secreto empresarial**

El deber se considera infringido con la realización de una conducta que, a pesar de ser evitable para el autor, lesiona o pone en peligro, de modo penalmente típico, un bien jurídico-penal. La realización de la conducta se considera evitable cuando se lleva a cabo con conocimiento de su carácter peligroso para el bien jurídico-penal, o cuando se ejecuta con desconocimiento imputable al autor. El desconocimiento se considera imputable cuando se debe a un error vencible, o cuando ha sido provocado por el mismo autor. En este último caso se habla de ignorancia deliberada. (Estrada, 2015)

En la doctrina, el conocimiento de la lesión o puesta en peligro típica del bien jurídico-penal constituye el denominador común del concepto de dolo. El error vencible sobre la creación de un peligro o lesión típica de un bien jurídico-penal integra el concepto de imprudencia. En los supuestos de ignorancia deliberada falta el conocimiento de la creación de un riesgo concreto. Por ello, con un concepto de dolo basado, en el conocimiento, la ignorancia deliberada debe castigarse, en todo caso, como una forma de imprudencia, con las correspondientes consecuencias penológicas que esto conlleva. (Estrada, 2015)

Sin embargo, si se atiende al fundamento del distinto tratamiento punitivo del dolo y la imprudencia, se puede advertir que algunos supuestos de ignorancia deliberada manifiestan un grado de indiferencia hacia el bien jurídico-penal capaz de generar un daño ideal y psicológico-social de entidad, si no equivalente, muy próxima a la del daño ideal y/o psicológico-social producido con la comisión de la conducta con conocimiento del riesgo concreto. (Estrada, 2015)

#### **2.2.5.5.2. Derechos y Deberes de las Partes: Secreto Industrial**

Existen puntos ineludibles para el caso de que se otorgue solamente su uso:

- A. Obligación de quien lo adquiera de guardar la confidencialidad sobre el secreto industrial.
- B. Hacer uso del mismo dentro de los parámetros en que fue otorgado. No sub licenciarlo.
- C. Prohibición del uso post-contractual. Respecto a este punto, hay países que limitan temporalmente su protección a una cantidad de años. En México, el plazo máximo no supera los 10 años. En

Argentina, respecto al contrato de Know-how, el plazo no supera los 5 años, por ser el plazo en que la tecnología se vuelve obsoleta.

D. Indemnizar en caso de que haga un uso contrario a las prácticas comerciales honestas.

E. Pagar la regalía. (Praxedis, 2003, p. 40)

#### **2.2.5.5.3. Legislación Comparada:**

A. El autor infringe un deber negativo cuando introduce dolosamente el secreto empresarial en su ámbito de organización y, con ello, pone en peligro o lesiona el bien jurídico protegido. Pero el merecimiento de pena es, sin duda, menor que el de quien espía o dispone deslealmente de un secreto empresarial. (Estrada, 2015)

B. Desde una perspectiva de análisis de Derecho comparado, el rigor punitivo del régimen penal español en materia de violaciones de secretos empresariales contrasta, de nuevo, con el alemán, cuando se comparan las penas asignadas a los respectivos tipos de extensión de la violación de secreto empresarial. Mientras que la conducta típica prevista en el art. 280 del Código Penal Español, puede llegar a ser castigada con penas de prisión de 1 a 3 años y multa de 12 a 24 meses, el tipo de extensión en Alemania se castiga, o bien con la pena de privación de libertad de hasta tres años, o bien con una pena de multa, alternativa. (Estrada, 2015)

#### **2.2.5.6. Subcapítulo VI: El Espionaje Empresarial en materia penal - Criterios Doctrinales**

##### **2.2.5.6.1. Sujeto pasivo y elemento subjetivo del Espionaje Empresarial**

El sujeto pasivo directo del delito es el titular del secreto de empresa y es este último quien sufre directamente el ataque al bien jurídico protegido. Sobre él recae el peligro causado por la conducta del sujeto activo. Por tratarse de un delito de naturaleza económica, es posible que se identifique como sujeto pasivo a una persona jurídica. (Vergara, 2014)

Por otra parte, tal y como han defendido autores como Morón Lerma y Morales Prats, citados por Vergara (2014), un segundo sujeto pasivo es el mercado, entendido como el conjunto de miembros y entidades que lo integran. Por medio de este delito se está poniendo en peligro el normal funcionamiento y la libre competencia en el mercado.

Asimismo, el espionaje corporativo se trata de un *modus operandi* atípico, en el que el *animus* o intención del sujeto activo, es el atacar la capacidad competitiva de la empresa titular, lograr una ventaja estratégica en el libre mercado y sacar provecho económico indebido. Este sector doctrinal entiende que el actor obra impulsado por el ánimo de realizar alguna de estas tres conductas (que también pueden acumularse) en un momento posterior (también se entiende, a pesar de la laguna legal respecto al tipo cualificado, que el sujeto puede obrar con ánimo de emplearlo en provecho propio). (Vergara, 2014)

#### **2.2.5.6.2. Consumación del Espionaje Corporativo:**

El sujeto activo es el que lleve a cabo actos encaminados a descubrir el secreto de empresa con el ánimo de, en un momento posterior, difundirlo, revelarlo o cederlo a terceras personas. Conforme a la doctrina española, para la consumación del delito no se exige la lesión efectiva del bien jurídico tutelado (la capacidad competitiva de la empresa) sino que basta con que el sujeto lo ponga en peligro. Según Morón para la consumación del delito basta con que el sujeto activo difunda, revele o ceda a terceros el secreto empresarial descubierto. (Vergara, 2014)

No obstante, sí se exige que los actos llevados a cabo por el sujeto sean susceptibles por sí mismos de poner en peligro la capacidad productiva de la empresa, así como el normal funcionamiento del mercado. Según dijo Caronell Mateu, citado por Vergara (2014), “la acción debe de ser apta para la producción de un perjuicio económico a la empresa y se esté amenazando con ello el libre mercado, debiendo bastar con que el sujeto actúe con finalidad económica”.

### **2.2.5.6.3. Tipo de peligro concreto**

Los actos de espionaje corporativo suponen una amenaza real para la capacidad competitiva de la empresa. Lo que realmente importa aquí es resaltar que el peligro de lesión del bien jurídico aumenta en estos casos en los que el sujeto que conoce el secreto empresarial (por haber accedido ilícitamente al mismo), lo difunde, revela o cede a terceras personas, en un momento posterior. (Vergara, 2014)

La razón del incremento del peligro de lesión del bien jurídico protegido es la siguiente. El descubrimiento del secreto por parte del sujeto activo supone un peligro para la capacidad competitiva de la empresa ya que aquél puede en cualquier momento decidir revelarlo a terceras personas, o emplearlo en provecho propio. No obstante, esto último no constituye más que una intención del sujeto activo. El sujeto activo ha logrado finalmente materializar esta intención que le impulsó a cometer el tipo básico (espionaje empresarial), y consecuentemente, terceras personas han podido acceder a la información relevante. (Vergara, 2014)

Esta segunda circunstancia incrementa el riesgo de que la capacidad competitiva de la empresa se vea efectivamente lesionada. Esto es así por una razón muy sencilla: al haber aumentado el número de sujetos conocedores del secreto, las posibilidades de que finalmente este sea

empleado (en provecho propio y perjuicio de la empresa titular del mismo) aumentan. (Vergara, 2014)

#### **2.2.5.6.4. Participación Necesaria:**

La acción típica se agota en el empleo de cualquiera de los medios prescritos para descubrir el secreto de empresa, conducta para cuya realización el sujeto activo no requiere en principio de la colaboración de ningún otro sujeto. Por el contrario, para la ejecución del tipo cualificado, el sujeto activo requiere necesariamente de la participación de otro sujeto, que va a ser la persona que reciba la información. (Vergara, 2014)

#### **2.2.5.6.5. Deber de Guardar Reserva:**

Consiste en el cumplimiento de la obligación de preservar la confidencialidad el empleador le ha confiado al trabajador de confianza, a socios comerciales y a terceras personas involucradas. El deber de guardar reserva puede surgir de la Ley o de un contrato. Su incumplimiento constituye un quebrantamiento de deberes específicos por parte del sujeto obligado. (Vergara, 2014)

Este sector doctrinal entiende que los deberes genéricos de buena fe contractual, entendidos como deberes básicos exigibles a todos los trabajadores (y recogidos en el estatuto de los Trabajadores), no son suficientes para fundamentar la responsabilidad penal del sujeto, siendo exigible por tanto la existencia un deber específico que conste en una concreta cláusula contractual o un precepto legal. (Vergara, 2014)

No obstante, una vez extinguida la relación jurídica que unía a ambos sujetos, para la consumación del delito será exigible la infracción de un deber de reserva específico, esto es, incorporado de expresamente en un precepto legal o una cláusula contractual (en estos casos este

deber específico no es perpetuo- en la mayoría de los supuestos.  
(Vergara, 2014)

Los trabajadores tienen como deberes básicos:

- a) Cumplir con las obligaciones concretas de su puesto de trabajo, de conformidad a las reglas de la buena fe y diligencia
- b) no concurrir con la actividad de la empresa (Vergara, 2014)

La doctrina alemana admite la “eximente de consentimiento”. Se trata de aquellos supuestos en los que el sujeto que tiene deber de guardar reserva del secreto empresarial, lo ha difundido, revelado o cedido a terceros a causa del consentimiento de su titular. El titular del secreto, en cuanto que tal, tiene la libre disposición sobre este, y por tanto el consentimiento que en su caso otorgue a un sujeto para que difunda, revele o ceda a otro su información confidencial es perfectamente válido.  
(Vergara, 2014)

### 2.3. Matriz de Operacionalización de Variables

VARIABLE	DEFINICIÓN CONCEPTUAL	DIMENSIONES	DEFINICIÓN DE TÉRMINOS BÁSICOS	INDICADORES
		<b>Aspecto subjetivo</b>	El aspecto subjetivo está formado por la presencia de dolo o culpa en el agente que	¿Por qué se da frecuentemente el espionaje corporativo como modalidad de competencia desleal? ¿Son garantía

			<p>realizó el comportamiento atípico. Por lo tanto se entiende el conocimiento y la voluntad del sujeto activo en realizar los elementos del tipo o aspecto objetivo; asimismo, la culpa es la negligencia, la infracción del deber de cuidado de parte del agente. (Jakobs, 1997)</p>	<p>suficiente los acuerdos de confidencialidad, en un libre mercado y ante los avances tecnológicos y la competencia vigorosa?  ¿Como podría afectar el espionaje corporativo a la imagen y buena reputación de las empresas?</p>
<p>V1 (Supuesto de Espionaje Corporativo)</p>	<p>Son todas aquellas acciones que, para descubrir un secreto de empresa, se apoderan por cualquier medio, de datos, documentos</p>	<p><b>Secreto Industrial”</b></p>	<p>Abarca tanto los descubrimientos científicos como las invenciones patentables no patentadas, las aplicaciones industriales, las ejecuciones de detalle y los ensayos y</p>	<ul style="list-style-type: none"> <li>❖ Las aplicaciones industriales</li> <li>❖ Beneficiario</li> </ul>

	<p>escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo. (Jiménez, Bonilla y Gil, 1997)</p>		<p>pruebas que son realizados hasta alcanzar tales resultados. (Jiménez, Bonilla y Gil, 1997)</p>	
		<p><b>“Secreto Comercial”</b></p>	<p>Abarca todos los datos reservados de la empresa, que afectan a la vida y manejo de la misma: Situación financiera, lista de clientes y proveedores, campañas publicitarias, proyectos de reestructuración internos o externos, contratación de personal especializado, fusiones, etc. (Jiménez,</p>	<ul style="list-style-type: none"> <li>▪ Informe (Balance) Financiero</li> <li>▪ Datos reservados de la empresa</li> <li>▪ Personal de Dirección</li> <li>▪ Trabajadores de Confianza</li> </ul> <p>¿Cuáles son los efectos generados por mala fe de los trabajadores de confianza, al tener acceso a información secreta de la empresa?</p>

			Bonilla y Gil, 1997)	
		<b>Vacíos Legales</b>	<p>Es una situación de vacío en la ley que ha sufrido la patología jurídica de omitir en su texto la regulación concreta de una determinada situación, parte, o negocio, que no encuentra respuesta legal específica. (Basterra, 2003)</p> <p>El espía corporativo; frente a los vacíos legales existentes, realiza actos</p>	<ul style="list-style-type: none"> <li>• Conducta atípica del espía corporativo</li> <li>• <b>Las probabilidades de detección (p)</b></li> <li>• <b>El castigo si es detectado (f)</b></li> <li>• Ausencia de Persecución Penal</li> <li>• Legitimidad de las autoridades judiciales</li> <li>• ¿Qué probabilidades hay de que un trabajador de confianza,</li> </ul>

			<p>contra la competencia desleal, a través de la violación del secreto empresarial (Que Engloba tanto el secreto industrial como el comercial).</p>	<p>cumpla con el deber de confidencialidad y de guardar reserva, ante la falta de una sanción punitiva, en materia penal?</p>
		<p><b>Know How (Secreto Empresarial)</b></p>	<p><b>El Know How</b> es el saber o conocimiento técnico aplicable a nivel empresarial, de carácter secreto por su <b>alto valor económico</b> y susceptible de contratación. Este concepto limita lo entendido por conocimiento a lo estrictamente técnico, es decir, propio de un determinado ámbito</p>	<ul style="list-style-type: none"> <li>❖ Utilidad pecuniaria</li> <li>❖ Valor económico</li> <li>❖ Contrato de Know How</li> <li>❖ ¿Son garantía suficiente los acuerdos de confidencialidad, en un libre mercado y ante los avances tecnológicos y la competencia vigorosa?</li> </ul>

			tecnológico, industrial, comercial, entre otros. (Benavente, 2012)	
		<b>Agente de inteligencia</b>	Es una persona o espía capacitado y entrenado técnicamente, que ocultando su identidad explota adecuadamente determinadas fuentes de información, para un órgano de inteligencia del cual depende. (Fernández, 1996)	<ul style="list-style-type: none"> <li>❖ El Dolo Especial</li> <li>❖ El Grave Perjuicio</li> <li>❖ El principio de culpabilidad (dolo o imprudencia).</li> <li>❖ Dolus Malus (malicia).</li> </ul>

VARIABLE	DEFINICIÓN CONCEPTUAL	DIMENSIONES	CONCEPTO TEÓRICO	INDICADORES
V2 (Funcionamiento interno de las Empresas Privadas)	<p>El funcionamiento de la persona jurídica está compuesto por miembros que lo integran, además de las obligaciones y derechos que ésta pueda tener, son absolutamente independientes de los de sus miembros. (Ferrara, 1929)</p> <p>La persona jurídica tiene su propio patrimonio y estará obligada a satisfacer sus propias deudas, mientras que sus miembros no tendrán obligación de pagarlas.</p>	<p><b>La Competencia Leal</b></p>	<p>La Competencia leal contiene el derecho de competir, junto a un deber relacionado con la forma cómo debe realizarse la competencia, basados en la lealtad y la buena fe en los negocios. Existen entonces métodos maliciosos que constituyen competencia desleal en contra de los demás competidores y de los consumidores. (Abanto,</p>	<ul style="list-style-type: none"> <li>• Lealtad entre los agentes económicos</li> <li>• Buena Fe Empresarial</li> <li>• Secretos Empresariales</li> </ul>

			1997)  El objeto de protección o bien jurídico protegido en este ámbito no es pasible de una distinción específica y exclusiva; aquí confluyen varios intereses protegidos.	
		<b>Secreto Empresarial</b>	Se considerará como secreto empresarial cualquier información no divulgada que una persona natural o jurídica legítimament	<ul style="list-style-type: none"> <li>▪ Libertad de los agentes económicos</li> <li>▪ Aumento de Bienestar</li> <li>▪ Actos de engaño</li> </ul>

			<p>e posea, que pueda usarse en alguna actividad productiva, industrial o comercial, y que sea susceptible de transmitirse a un tercero. (Decisión N° 486, 2000, art. 260)</p>	<ul style="list-style-type: none"> <li>▪ Violación de secretos</li> </ul>
		<p><b>Personas Jurídicas</b></p>	<p>Persona jurídica (o persona moral) es un sujeto de derechos y obligaciones que existe, pero no como individuo, sino como institución y</p>	<ul style="list-style-type: none"> <li>• Esfera Jurídica Patrimonial</li> <li>• Funcionamiento y Administración</li> </ul>

			<p>que es creada por una o más personas físicas para cumplir un objetivo social que puede ser con o sin ánimo de lucro. (Ferrara, 1929)</p> <p>En otras palabras, una persona jurídica es todo ente con capacidad para adquirir derechos y contraer obligaciones y que no sea una persona física.</p>	<ul style="list-style-type: none"> <li>• Asamblea de Socios</li> <li>• Animus Lucrandi</li> </ul>
		<b>Poder Económico del Empleador</b>	<p>Solamente las personas que tengan</p>	<ul style="list-style-type: none"> <li>▪ Status Socioeconómico</li> </ul>

			<p>una posición preponderante dentro del mercado serán capaces de influir en el orden económico. De esta manera, el sujeto activo en los delitos económicos será normalmente una persona de status socioeconómico alto y con excelente calificación profesional. (Bramont, 1992)</p> <p>De esta constatación surgen problemas en cuanto a la sanción penal</p>	<ul style="list-style-type: none"> <li>▪ Poder adquisitivo</li> <li>▪ Fraude en la administración de personas jurídicas</li> </ul>
--	--	--	--	--

			para dichas personas, no sólo por su influencia económica y normalmente política, sino también por razones criminológicas que ocasionan la dificultad de ver a estas personas como delincuentes.	
		<b>Trabajadores de confianza</b>	El personal de confianza, es aquel que tiene acceso a información administrativa, comercial, industrial y en general de carácter confidencial.	<ul style="list-style-type: none"> <li>• Obligaciones Contractuales</li> <li>• Empleador</li> <li>• Responsabilidad Penal</li> </ul>

			(Valdivia, 2012)	<ul style="list-style-type: none"> <li>• Intereses privados</li> </ul>
--	--	--	---------------------	--

### III. METODOLOGÍA:

#### 3.1. Tipo de Investigación

- Cualitativa

##### 3.1.1.1. Según el Propósito:

- ✓ Descriptivo

##### 3.1.1.2. Según Diseño de Investigación:

- ✓ No experimental

#### 3.2. Población y muestra (Instrumentos, Materiales y Métodos)

##### 3.2.1. Unidad de Estudio

- ✓ Para la realización de la investigación se ha utilizado como unidades de estudio los siguientes precedentes vinculantes:
  - EXP N° 063-2007/CCD-INDECOPI
  - EXP N° 297-2013/CCD-INDECOPI
  - EXP N° 009-2011/CCD-INDECOPI
  - EXP N° 035-2012/CCD-INDECOPI

<b>CRITERIOS DE SELECCIÓN DE PRECEDENTES ADMINISTRATIVOS - INDECOPI</b>	
<b>EXP N° 063- 2007/CCD-INDECOPI</b>	<ul style="list-style-type: none"> <li>✓ Principio de Legalidad</li> <li>✓ Violación de Secretos</li> <li>✓ Dolus Malus (Malicia)</li> <li>✓ Animus Lucrandi (Ánimo de Lucro)</li> <li>✓ Distintividad</li> <li>✓ Acuerdo de Confidencialidad</li> <li>✓ Competencia Desleal</li> <li>✓ Arbitrariedad</li> <li>✓ Ventaja Estratégica – competitiva</li> <li>✓ Proceso Competitivo</li> </ul>
<b>EXP N° 297- 2013/CCD-INDECOPI</b>	<ul style="list-style-type: none"> <li>✓ Principio de Legalidad</li> <li>✓ Dolus Malus (Malicia)</li> <li>✓ Deber de Guardar Reserva</li> <li>✓ Secretos Industriales</li> <li>✓ Divulgación del Secreto Empresarial</li> <li>✓ Animus Lucrandi (Ánimo de Lucro)</li> <li>✓ Competencia Desleal</li> <li>✓ Arbitrariedad</li> <li>✓ Ventaja Estratégica – competitiva</li> <li>✓ Autoría Mediata e inmediata del espionaje corporativo</li> <li>✓ Proceso Competitivo</li> </ul>
<b>EXP N° 009- 2011/CCD-INDECOPI</b>	<ul style="list-style-type: none"> <li>✓ Principio de Legalidad</li> <li>✓ Violación de Secretos Empresariales</li> <li>✓ Inducción a la Infracción Contractual</li> <li>✓ Dolus Malus (Malicia)</li> </ul>

	<ul style="list-style-type: none"> <li>✓ Animus Lucrandi (Ánimo de Lucro)</li> <li>✓ Distintividad</li> <li>✓ Deber de Guardar Reserva</li> <li>✓ Trabajador de Confianza</li> <li>✓ Confidencialidad</li> <li>✓ Arbitrariedad</li> <li>✓ Sabotaje Empresarial</li> <li>✓ Competencia Desleal</li> <li>✓ Difusión del Secreto Industrial</li> <li>✓ Difusión de información confidencial de empresa</li> <li>✓ Ventaja Estratégica – competitiva</li> <li>✓ Daños concurrenciales negativos: Captación indebida de cartera de clientes</li> <li>✓ Autoría Mediata e inmediata del espionaje corporativo</li> <li>✓ Proceso Competitivo</li> </ul>
<p><b>EXP N° 035- 2012/CCD-INDECOPI</b></p>	<ul style="list-style-type: none"> <li>✓ Principio de Legalidad</li> <li>✓ Dolus Malus (Malicia)</li> <li>✓ Animus Lucrandi</li> <li>✓ Competencia Desleal</li> <li>✓ Mala fe del trabajador</li> <li>✓ Deber de Guardar Reserva</li> <li>✓ Difusión del secreto industrial</li> <li>✓ Autoría inmediata del espionaje corporativo</li> <li>✓ Proceso Competitivo</li> </ul>

### 3.2.2. Población

- ✓ La población en base a los 47 expedientes de Indecopi, son 92 personas representativas, donde se cometieron actos de sabotaje empresarial, violación del secreto empresarial, vulneración de la buena fe empresarial en las entidades e inducción a la infracción contractual por parte de agentes económicos desleales en perjuicio de las empresas privadas fiscalizadas por la Comisión de Indecopi de Lima, en materia de competencia desleal.

### 3.2.3. Muestra: No Probabilístico

#### 3.2.3.1. Muestreo Aleatorio Simple

##### A. Número de Expedientes de Indecopi: Cuatro

- ✓ La elección de los casos se realizó en base a la consulta a cuatro abogados especialistas:
  - a) Ricardo Luperdi Gamboa
  - b) Sixto Chávez Ávalos
  - c) Claudia Cotrina Roldán
  - d) Santos Urtecho Navarro

<b>CRITERIOS DE SELECCIÓN DE ESPECIALISTAS</b>		
Ricardo Gamboa	Luperdi	<b>1) Educación</b> <ul style="list-style-type: none"> <li>➤ Universidad Privada del Norte de Trujillo (2007)</li> <li>➤ Estudios de Maestría con mención en Ciencias Penales en la Universidad Nacional Mayor de San Marcos.</li> </ul>

	<p><b>2) Experiencia laboral previa</b></p> <ul style="list-style-type: none"> <li>➤ Abogado interno del Grupo Oviedo, encargándose de temas penales de las empresas Agroindustrial Pomalca S.A.A., Empresa Agroindustrial Tumán y del Club Deportivo Juan Aurich (2010-2011)</li> <li>➤ Muñiz, Ramírez, Pérez-Taíman &amp; Luna-Victoria Abogados, Trujillo (2008-2010)</li> </ul> <p><b>3) Actividad académica</b></p> <ul style="list-style-type: none"> <li>➤ Docente auxiliar del curso de Derecho Procesal Penal en la Universidad Privada del Norte (2007)</li> </ul> <p><b>4) Idiomas</b></p> <ul style="list-style-type: none"> <li>➤ Español, inglés e italiano</li> </ul> <p><b>5) Áreas de especialización</b></p> <ul style="list-style-type: none"> <li>➤ Derecho Penal</li> <li>➤ Derecho Procesal Penal y Penitenciario</li> </ul>
<p>Sixto Chávez Ávalos</p>	<p><b>1) Experiencia laboral previa</b></p> <ul style="list-style-type: none"> <li>➤ Abogado interno del Banco Financiero</li> </ul>

	<p><b>2) Actividad académica</b></p> <ul style="list-style-type: none"> <li>➤ Docente del curso de Derecho de Competencia y Regulación de Servicios Públicos en la Universidad Privada del Norte.</li> <li>➤ Docente del curso de Derecho Financiero en la Universidad Privada del Norte.</li> <li>➤ Docente del curso de Derecho Bancario y Mercado de Valores en la Universidad Privada del Norte.</li> </ul> <p><b>3) Idiomas</b></p> <ul style="list-style-type: none"> <li>➤ Español</li> <li>➤ Inglés</li> </ul> <p><b>4) Áreas de especialización</b></p> <ul style="list-style-type: none"> <li>➤ Derecho de Competencia y Regulación de Servicios Públicos.</li> <li>➤ Derecho Financiero.</li> </ul>
<p>Claudia Cotrina Roldán</p>	<p><b>1) Educación</b></p> <ul style="list-style-type: none"> <li>➤ Universidad de Piura (2005 - 2011)</li> </ul> <p><b>2) Experiencia laboral</b></p> <p>2.1. Abogada Corporativa en Compañía Sumitomo Metal</p>

	<p>Mining Perú S.A.C. (Desde marzo del 2018 hasta marzo del 2020)</p> <p>2.2. Compañía Minera Quiruvilca (Desde enero del 2014 a enero del 2018)</p> <ul style="list-style-type: none"><li>➤ En calidad de representante de la empresa, estuvo encargada del área legal de la oficina Trujillo de Compañía Minera Quiruvilca. Tuvo personal bajo su gestión y dirección (asistentes legales y asistentes técnicos.</li><li>➤ Se encargó del seguimiento de los procesos judiciales y administrativos que la empresa afronta al día de hoy, con especial énfasis en Derecho Laboral; Derecho Penal, Derecho Contractual y Derecho Administrativo Sancionador.</li></ul> <p><b>3) Idiomas</b></p> <ul style="list-style-type: none"><li>➤ Español, inglés, francés.</li></ul> <p><b>4) Áreas de especialización</b></p> <ul style="list-style-type: none"><li>➤ Abogada Especializada en Derecho Laboral, Corporativo, Administrativo, Civil, Penal y Derecho Minero – ambiental.</li></ul>
--	---

<p>Santos Urtecho Navarro</p>	<p><b>1) Educación</b></p> <p>a) Doctorado en Derecho</p> <p>b) Maestría en Derecho Civil Empresarial</p> <p><b>2) Experiencia laboral previa</b></p> <p>a) Director en Estudio Jurídico Santos E. Urtecho Benites Abogados.</p> <p>b) Docente en la Universidad Privada del Norte, desde marzo del 2008, de los siguientes cursos:</p> <ul style="list-style-type: none"> <li>▪ Derecho Civil (Acto jurídico, Obligaciones, Contratos).</li> <li>▪ Derecho Procesal Civil (Proceso de conocimiento, procesos especiales).</li> <li>▪ Derecho Procesal Constitucional.</li> <li>▪ Teoría general del proceso.</li> <li>▪ Argumentación jurídica.</li> <li>▪ Lógica jurídica</li> </ul> <p><b>3) Idiomas</b></p> <p>➤ Español, inglés e italiano.</p> <p><b>4) Áreas de especialización</b></p> <p>➤ Derecho civil y Derecho civil empresarial.</p>
-----------------------------------	--

## POBLACIÓN

De las 92 personas involucradas en las 47 expedientes de Indecopi, en materia de competencia desleal del periodo 2007 – 2013, se hace selección de 13 personas naturales y jurídicas representativas, entre los cuales, están:

A) 6 trabajadores de confianza.

B) 7 empleadores.

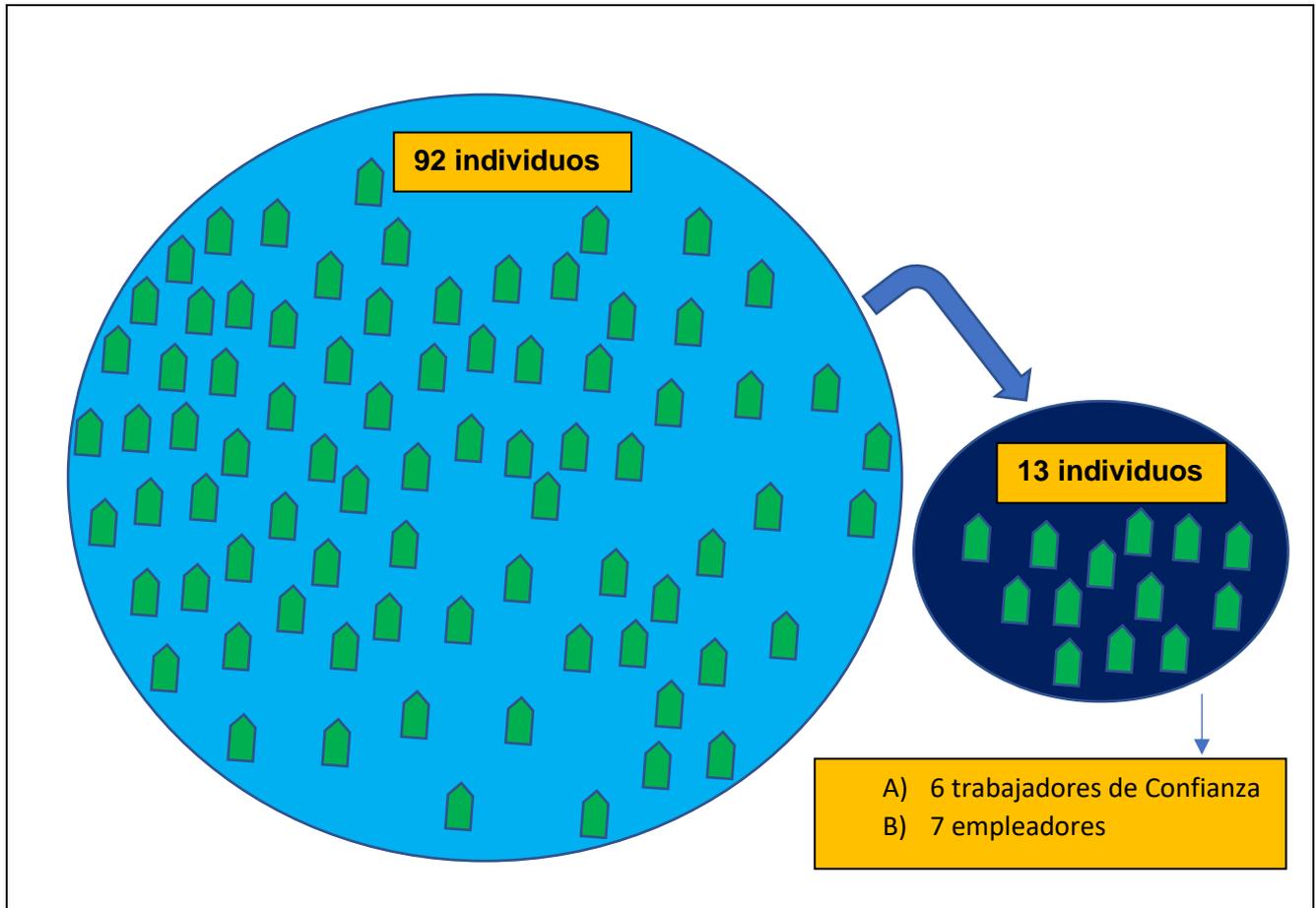
- Para ello, se seleccionó los cuatro expedientes de Indecopi.

- EXP N° 063-2007/CCD-INDECOPI
- EXP N° 297-2013/CCD-INDECOPI
- EXP N° 009-2011/CCD-INDECOPI
- EXP N° 035-2012/CCD-INDECOPI

**MUESTRA**

De una población de 92 personas representativas, se desea conocer la incidencia del espionaje corporativo en las empresas privadas de la ciudad de Lima, y para ello se necesita saber la cantidad exacta de empresas afectadas en materia de competencia desleal por actos de espionaje, e identificar a los agentes infractores que actuaron de mala fe, en beneficio propio y de terceras personas. Para ello, se realizó una revisión de 47 expedientes en materia de competencia desleal del periodo 2007 – 2013, y se hizo la selección de 13 habitantes de la ciudad de Lima, entre los cuales, están: 6 trabajadores de confianza y 7 empleadores.





EXPEDIENTES DE INDECOPI	APRECIACIONES
<ul style="list-style-type: none"> <li>1) 10-2007/CCD</li> <li>2) 25-2007/CCD</li> <li>3) 46-2007/CCD</li> <li>4) 49-2007/CCD</li> <li><b>5) 63-2007/CCD</b></li> <li>6) 59-2007/CCD</li> <li>7) 112-2007/CCD</li> <li>8) 165-2007/CCD</li> <li>9) 166-2007/CCD</li> <li>10)175-2007/CCD</li> <li>11)48-2008/CCD</li> </ul>	<p>De los 47 expedientes revisados del periodo 2007 – 2013, se puede apreciar que en los 43 casos existe mala fe mercantil y actos de sabotaje empresarial. Sin embargo, ninguno tiene relación con el supuesto de espionaje corporativo (variable 1), debido a que se aprecian otros supuestos distintos al espionaje corporativo como la inducción a la infracción contractual, riesgos de confusión para el consumidor en materia marcaría,</p>

<p>12)91-2008/CCD 13)97-2008/CCD 14)98-2008/CCD 15)137-2009/CCD 16)225-2010/CCD 17)123-2010/CCD <b>18)009 – 2011/CCD</b> 19)149-2011/CCD 20)211-2011/CCD <b>21)35-2012/CCD</b> 22)212-2013/CCD 23)232-2013/CCD <b>24)297-2013/CCD</b> 25)13-2014/CCD 26)38-2014/CCD 27)2-2015/CCD-INDECOPI-PUN 28)18-2015/CD1 29)28-2015/CCD 30)44-2015/CD1 31)77-2015/CD1 32)113-2015/CCD-INDECOPI-CUS 33)202-2015/CCD-INDECOPI-LOR 34)244-2015/CCD-INDECOPI-CUS 35)411-2015/CCD-INDECOPI-CUS 36)468-2015/CCD-INDECOPI-LAM 37)469-2015/CCD-INDECOPI-LAM 38)667-2015/CCD-INDECOPI-LAM 39)157-2016/CD1 40)182-2016/CD1 41)36-2017/CCD 42)39-2017/CCD 43)126-2017/CCD</p>	<p>monopolios o publicidad engañosa.</p> <p>Si bien es cierto, en las 43 resoluciones se presenta casos de competencia desleal en perjuicio de las empresas privadas, como la infracción a los derechos de autor, los riesgos de confusión, ante la comercialización de un servicio o producto con signos similares al del competidor directo en materia marcaria, en ningún caso, se presenta actos de espionaje, como modalidad de competencia desleal, para el apoderamiento del secreto societario (información confidencial de empresa y secretos industriales) y posterior explotación económica, u obtención indebida de ventaja estratégica competitiva en el libre mercado.</p> <p>Se han presentado otros requisitos importantes para la selección de la muestra, como la intención fraudulenta o el ánimo de lucro, en los supuestos de espionaje corporativo, donde el agente infractor se apodera indebidamente y por medios informáticos, de secretos empresariales y consecuentemente, comete la violación del secreto societario por los siguientes motivos: para obtener una ventaja estratégica indebida, para su divulgación a terceras personas, y para su explotación económica.</p> <p>Solo en 4 expedientes de Indecopi del periodo 2007 - 2013 se ha podido observar que</p>
---	--

<p>44)137-2017/CCD 45)26-2018/CCD 46)059-2019/CCD 47)0062-2020/INDECOPI-SAM</p>	<p>efectivamente ha existido un daño concurrencial negativo en perjuicio de la víctima económica (empleador), en los supuestos de violación del secreto empresarial por medio de espionaje corporativo. Asimismo, tienen vinculación con la problemática de la fuga de información confidencial de empresa en materia de propiedad intelectual por medio espionaje corporativo y los daños patrimoniales ocasionados en perjuicio de la víctima económica, por la violación del secreto empresarial, así como también la infracción del deber de guardar reserva respecto a los acuerdos de confidencialidad pactados entre el trabajador y el empleador sobre el secreto empresarial.</p> <p>Los expedientes de Indecopi seleccionados son los siguientes:</p> <p><b>a) EXPEDIENTE N° 63-2007/CCD</b></p> <p>Del expediente N° 63 – 2007, se puede apreciar que la parte denunciante (Foamflex S.A.) es propietaria de fórmulas industriales (espuma de poliuretano) para la elaboración de diversos productos comercializables (muebles, colchones, almohadas, juguetes, calzados, etc) , y que han sido utilizadas sin su autorización, por el empleado desleal Daniel Curi Rojas, quien infringió el deber de</p>
---	---

guardar de reserva en el acuerdo de confidencialidad pactado, y reveló estos secretos industriales a la sociedad comercial Muebles Lot's S.A.C.

Cabe recalcar, que luego del despido, el ex trabajador de la empresa agraviada (Foamflex S.A.) paso a trabajar a la empresa Muebles Lot's S.A.C, y empezaron a elaborar productos comercializables en base a la fórmula química de la espuma de poliuretano (secreto industrial), configurándose un supuesto atípico en materia penal de espionaje y violación de secretos industriales a favor de la empresa Muebles Lot's S.A.C, por parte del ex trabajador de confianza (Daniel Curi Rojas).

**b) EXPEDIENTE N° 35-2012/CCD**

Del expediente N° 35 – 2012/CCD, se puede apreciar que Gabriela Sedano Corzo, jefa de marketing de Belmay S.A.C, estuvo revelando fórmulas industriales de productos comercializables a otra sociedad comercial (Criteria Consultores) por medio de correos electrónicos, sin autorización de la empresa.

Entre los productos revelados por la trabajadora desleal, estuvieron los siguientes:

- i. Cremas para masaje (Fórmulas industriales N° F – 52001 Y 51602)

ii. Crema drenaje linfático corpus total  
(Fórmula N° F - 51702),

iii. Loción adaptogénica y reductora BF.

Sin embargo, la parte imputada (Gabriela Sedano Corzo), alegó que se había infringido su derecho de privacidad de las comunicaciones, porque no había dado su consentimiento para el acceso a su cuenta personal de correo electrónico, conforme al artículo 13 del T.U.O del reglamento general de la Ley de telecomunicaciones. Debido a ello, la Comisión de Indecopi declaró infundada el pedido de la parte denunciante.

Se puede apreciar que, a pesar de haber existido un acto de sabotaje empresarial por parte de la trabajadora Gabriela Sedano Corzo, queda exenta de responsabilidad penal por la existencia de vacíos legales frente a los supuestos de espionaje corporativo y revelación de información confidencial de empresa a terceras personas.

**c) EXPEDIENTE N° 009-2011/CCD**

Del expediente **N° 009-2011/CCD-INDECOPI**, se puede apreciar que el señor Alberto Sánchez Julca laboró en la empresa denunciante (Branif S.A.C), con el puesto laboral de Jefe de Planta y Producción, cargo

que le daba privilegios dentro de la compañía como acceder a fórmulas químicas para la elaboración de productos de Branif S.A.C.

Asimismo, la señora Nelly Castro Albarrán, laboró en Branif S.A.C hasta el 30 de junio del 2009, y tuvo acceso a información relevante relacionada a los aspectos comerciales de la empresa, tales como: la cartera de clientes, lista de productos y precios, proveedores, insumos, etc. Por otro lado la trabajadora, Mónica Fiorella Díaz Aliaga, se había desempeñado como vendedora de la empresa, hasta el 31 de agosto del 2009.

La empresa Branif S.A.C había acordado en los contratos de trabajo pactados con los mencionados trabajadores, cláusulas de reserva, para que no se revele información secreta de la empresa (secretos industriales) a terceras personas. Posteriormente, los trabajadores dejaron de laborar para Branif S.A.C y fundaron Promak S.A.C. Empezaron a comercializar productos con la misma fórmula química utilizada por la empresa Branif S.A.C, en los siguientes productos:

- i. Grasa dieléctrica siliconada GDS-100 1532 envase 1 Kg.
- ii. Aceite Refrigerante de Corte.
- iii Desengrasante de piezas mecánicas DPM- 101.

	<p>Se puede apreciar que la sociedad Comercial Promak S.A.C, obtuvo ventaja estratégica – indebida con la explotación económica de los secretos industriales proporcionados por trabajadores desleales, como la señorita Esther Sernaqué Acosta, quien se desempeñaba en el área de ventas de Branif S.A.C y realizaba actividades de espionaje y revelación de información confidencial de empresa a Promak S.A.C.</p> <p>La empresa Promak S.A.C , generó un daño concurrencial a la empresa agraviada (Branif S.A.C), al tener a su disposición la cartera de cliente de la sociedad comercial Branif S.A.C, y ofrecer productos comercializables similares al competidor directo, con la misma composición química, pero a menor precio.</p> <p>Asimismo, la empresa Promak SA.C. incitó a los trabajadores de la compañía Branif S.A.C. a que actuen deslealmente, y cometan infracciones contractuales, al incumplir con el deber de guardar reserva pactado, respecto a los secretos empresariales, e incentivándolos a renunciar, ofreciéndoles mejores puestos laborales. La comisión de Indecopi declaro infundada la denuncia , conforme al criterio de libre competencia y libertad de empresa.</p> <p>Se puede apreciar que, se configuró un supuesto atípico de competencia desleal, que al no encontrarse previsto en materia penal,</p>
--	---

dejo exento de responsabilidad a la empresa imputada (Promak S.A.C.) y generó daños patrimoniales, debido a las rentas dejadas de percibir por concepto de explotación económica del secreto empresarial, y daños concurrenciales por desmembramiento interno de la empresa (trabajadores desleales) y pérdida de clientes.

**d) EXPEDIENTE N° 297-2013/CCD**

La parte denunciante (Brisas Marinas S.A.C) se encarga de la comercialización de jabones de glicerina, y para esta empresa laboraba el funcionario desleal Carlos Ibañez Terrazas, quien fue descubierto in fraganti trabajando paralelamente para las empresas (denunciante e imputada). Luego de ser despedido por Brisas Marinas S.A.C, se fue a trabajar directamente con la empresa Makaya Laboratorios S.A.C., y empezaron a producir un producto idéntico a la forma de jabones de glicerina de la empresa Denunciante.

Se puede apreciar que la fórmula y el molde para la elaboración de jabones de glicerina fue sustraído ilegítimamente y sin autorización del titular, por el imputado (Carlos Ibañez Terrazas), y posteriormente fue revelado a la empresa competidora (Makaya Laboratorios S.A.C). Sin embargo, ante la ausencia de fiscalización frente a este tipo de supuestos de sabotaje empresarial (espionaje

	<p>corporativo), el trabajador obró deslealmente en beneficio propio y de terceros, al revelar el secreto empresarial susceptible de explotación económica (fórmula química de jabones de glicerina) a la empresa Makaya Laboratorios S.A.C, y pasar a trabajar a tiempo completo para la mencionada entidad, posterior al despido realizado por la empresa agraviada (Brisas Marinas S.A.C).</p> <ul style="list-style-type: none"><li>▪ Los cuatro expedientes seleccionados tienen vinculación con la variable 1 (espionaje corporativo), y la variable 2 (funcionamiento interno de las empresas privadas), al existir una perturbación de los ingresos y egresos de las empresas privadas de la ciudad de Lima, es decir, el flujo de riqueza o las rentas percibidas por concepto de explotación económica del secreto empresarial, y los costos generados en materia de seguridad informática y criminal compliance (programas de cumplimiento).</li></ul>
--	---

### 3.2.3.2. Criterios de Inclusión:

- Se escogieron cuatro expedientes de INDECOPI, de un universo de 47 expedientes. Se puede verificar que en estos expedientes se cometieron dolo e intención fraudulenta en la violación de secretos empresariales por medio de espionaje, sin embargo, por no estar tipificado el espionaje corporativo, se emitieron resoluciones del tribunal de INDECOPI, declarándolas infundadas en última instancia.

### 3.2.3.3. Criterios de Exclusión:

- ❖ Se excluyó las demás resoluciones (43 expedientes) debido a que no tenían relación con la variable 1: espionaje corporativo, al comprobarse que no existía competencia desleal de las partes imputadas por medio de espionaje, que constituya sabotaje empresarial en perjuicio de los empleadores, conforme al criterio de buena fe mercantil.

### 3.2.3.4. Instrumentos: Expedientes

EXPEDIENTES DE INDECOPI	Bien Jurídico	Parámetros	Instancias	Sujetos
A. EXPEDIENTE N° 063-2007/CCD	(1) Secreto Industrial: “Formula química”  Espuma de Poliuretano	<ul style="list-style-type: none"> <li>▪ Principio de Legalidad</li> <li>▪ Violación de Secretos</li> <li>▪ Dolus Malus</li> </ul>	<p><b>1° Instancia</b> Decisión: Infundada</p> <p><b>2° Instancia:</b> Decisión: Infundada</p>	<p><b>1° Denunciante:</b> <b>FOAMFLEX S.A.</b></p> <p><b>2° Imputado:</b></p> <ul style="list-style-type: none"> <li>○ MUEBLES LOT'S</li> </ul>

	<p>(2) Buena Fe Mercantil</p> <p>(3) Competencia Leal</p>	<p>(Malicia)</p> <ul style="list-style-type: none"> <li>▪ Animus Lucrandi (Ánimo de Lucro)</li> <li>▪ Distintividad</li> <li>▪ Confidencialidad</li> <li>▪ Competencia Desleal</li> <li>▪ Arbitrariedad</li> </ul>	<p><b>Fundamento:</b></p> <p>i. Falta de Medios Probatorios</p> <p>ii. Ausencia de tipificación del espionaje industrial</p>	<p>S.A.C.</p> <ul style="list-style-type: none"> <li>○ Ex Empleado de <b>FOAMFLEX:</b> Daniel Luis Curi Rojas</li> </ul> <p><b>2.1° Actos Desleales del Ex Empleado:</b></p> <p><b>1°</b> “Apoderamiento del Secreto Empresarial: fórmula química de la espuma de poliuretano, por medios informáticos”</p> <p><b>2° Violación del Secreto Empresarial</b> “Divulgar información confidencial referida a la fórmula química de poliuretano, y</p>
--	---	--	--	---

				<p>cederlo a la empresa imputada Muebles LOT S.A.C.</p> <p><b>3°</b> Infringir el deber de guardar reserva, al no cumplir con el acuerdo de confidencialidad suscrito con la parte denunciante.</p>
<p><b>B. EXPEDIENTE N° 297-2013/CCD-INDECOPI</b></p>	<p><b>(1) Secretos Industrial:</b></p> <p>🚩 “Fórmula química para jabones de Glicerina”</p> <p><b>(2) Buena Fe en los Negocios</b></p> <p><b>(3) Competencia Leal</b></p>	<ul style="list-style-type: none"> <li>▪ Principio de Legalidad</li> <li>▪ Dolus Malus (Malicia)</li> <li>▪ Animus Lucrandi (Ánimo de Lucro)</li> <li>▪ Competencia Desleal</li> </ul>	<p><b>1° Instancia:</b> Infundada</p> <p><b>2° Instancia:</b> Infundada</p> <p><b>Causas:</b></p> <ul style="list-style-type: none"> <li>○ Falta de Medios Probatorios</li> <li>○ Ausencia de tipificación del espionaje</li> </ul>	<p><b>1° Denunciante:</b> Química Brisas Marinas S.A.C</p> <p><b>2° Imputado:</b></p> <ul style="list-style-type: none"> <li>➤ Makaya Laboratorios S.A.C.</li> <li>➤ Carlos Ibáñez Terrazas (Empleado</li> </ul>

			industrial	<p>de la parte denunciante)</p> <p>2.1° <b>Actos Desleales del Ex Empleado:</b></p> <p>1° “Apoderamiento del Secreto Empresarial: fórmula química para jabones de glicerina, por medios informáticos”</p> <p>2° Violación del Secreto Empresarial “Divulgar información confidencial referida a la fórmula química de poliuretano, y cederlo a la empresa imputada <b>Makaya Laboratorios S.A.C.</b>”</p>
--	--	--	------------	---

				3° Infringir el deber de guardar reserva, en su condición de trabajador de confianza.
--	--	--	--	---

EXPEDIENTES DE INDECOPI	Bien Jurídico	Parámetros	Instancias	Sujetos
<b>A. EXPEDIENTE N° 035-2012/CCD-INDECOPI</b>	<p>(1) <b>Secretos Industriales:</b></p> <p><b>“Formulas químicas”</b></p> <p>🚩 Crema para Masaje Reafirmante (Fórmula N° F-51602)</p> <p>🚩 (Crema para Masaje Antiestrés (Fórmula N°</p>	<ul style="list-style-type: none"> <li>▪ Principio de Legalidad</li> <li>▪ Violación de Secretos</li> <li>▪ Dolus Malus (Malicia)</li> <li>▪ Animus Lucrandi (Ánimo de Lucro)</li> <li>▪ Distintividad</li> </ul>	<p><b>1° Instancia</b></p> <p>Decisión: Infundada</p> <p><b>2° Instancia</b></p> <p>Decisión: Infundada</p> <p><b>Fundamentos:</b></p> <p><b>Primero:</b> Vulneración del derecho al secreto de las comunicaciones de la parte</p>	<p><b>1° Denunciante:</b></p> <p>BELMAY S.A.C.</p> <p><b>2° Imputada:</b></p> <p>Gabriela Sedano Corzo – Cargo de Jefa de Marketing</p> <p><b>2.1° Actos Desleales de la Imputada:</b></p> <p>1° “Apoderamiento de Secretos Empresariales, por medios</p>

	<p>F-52001)</p> <p>🚩 Crema Drenaje Linfático Corpus Total (Fórmula N° F-51702)</p> <p>🚩 Loción Adaptogénica TH Cutis Mixto (Fórmula N° F52803)</p> <p>🚩 Reductora BF Cafeína Crema (Fórmula N° F21603)</p> <p><b>(2) Buena Fe Mercantil</b></p> <p><b>(3) “Competen cia Leal”</b></p>	<ul style="list-style-type: none"> <li>▪ Deber de Guardar Reserva</li> <li>▪ Confidenciali dad</li> <li>▪ Arbitrariedad</li> <li>▪ Sabotaje Empresarial</li> <li>▪ Competencia Desleal</li> </ul>	<p>imputada.</p> <p><b>Segundo:</b> Vulneración del Derecho a la intimidad de la parte demandada.</p> <p><b>Tercero:</b> No se suscribió un acuerdo confidencial con la parte imputada.</p> <p><b>Cuarto:</b> Ausencia de tipificación del espionaje industrial</p>	<p>informáticos”</p> <p>2° “Otorgar o ceder Información confidencial de Empresa vía correo electrónico a terceras personas.”</p> <p>3° Infringir el deber de guardar reserva, al actuar de mala fe, y sacar provecho del tiempo que estuvieron laborando para la Empresa BELMAY S.A.C, para apropiarse de información confidencial de la Empresa, sin autorización del titular.</p>
--	---	---	---	---

<p><b>B. EXPEDIENTE N° N° 009-2011/CCD - INDECOPI</b></p>	<p><b>(1) Secreto Industrial</b></p> <p>Las fórmulas químicas de sus productos</p> <p>a) Aceite Refrigerante</p> <p>b) Desengrasantes de Piezas Mecánicas.</p> <p><b>(2) Información Secreta:</b></p> <p>La información referente a</p>	<ul style="list-style-type: none"> <li>▪ Principio de Legalidad</li> <li>▪ Dolus Malus (Malicia)</li> <li>▪ Animus Lucrandi</li> <li>▪ Competencia Desleal</li> <li>▪ Sabotaje Empresarial</li> <li>▪ Buena Fe Empresarial</li> <li>▪ Deber de Guardar Reserva</li> </ul>	<p><b>1° Instancia:</b> Infundada</p> <p><b>2° Instancia:</b> Infundada</p> <p><b>Causas:</b></p> <ul style="list-style-type: none"> <li>○ Falta de Medios Probatorios</li> <li>○ Ausencia de tipificación del espionaje industrial</li> </ul>	<p><b>1° Denunciante:</b> BRANIF PERÚ S.A.C.</p> <p><b>2° Imputado:</b> PROMAK PERÚ S.A.C.</p> <p><b>Fundadores:</b></p> <p>1° Alberto Sánchez Julca</p> <p>2° Nelly Castro Albarrán</p> <p>3° Mónica Fiorella Díaz Aliaga</p> <p><b>2.1. Actos Desleales de los Fundadores:</b></p> <p>1° “Apoderamiento de Secretos Empresariales (formulas químicas de productos), por</p>

	<p>su cartera de clientes y de proveedores</p> <p><b>(3) Competencia Leal</b></p> <p><b>(4) Buena Fe Mercantil</b></p>			<p>medios informáticos”</p> <p>2° “Sacar ventaja estratégica y competitiva, al acceder a Información confidencial de Empresa, referida a clientes y proveedores de BRANIF S.A.C.”</p> <p>3° Infringir el deber de guardar reserva.</p>
--	--	--	--	--

### ANÁLISIS DE RESOLUCIONES

#### i. EXPEDIENTE Nº 063-2007/CCD

##### A. POSTURA DE PARTE DENUNCIANTE:

- La entidad denunciante Foamflex, expresó ser propietaria de las fórmulas industriales de la espuma de poliuretano, que pueden ser utilizados para la elaboración de colchones y otros productos comercializables. Asimismo, la compañía comercial alegó que la parte denunciada (Daniel Luis Curi Rojas) se apropió indebidamente del secreto industrial y lo divulgó sin su autorización expresa a la empresa Muebles Lot's para su respectiva

explotación económica, a través de la fabricación y comercialización de muebles y otros productos, a pesar de que previamente habían pactado un acuerdo de confidencialidad que prohibía el acto de poner en conocimiento la fórmula industrial del poliuretano a terceras personas. (EXPEDIENTE N° 063-2007/CCD, 2007)

- La parte denunciante argumentó que la fórmula industrial del poliuretano es muy versátil, lo que facilita la obtención de espumas con características distintivas útiles para la fabricación de una variedad de productos comercializables como muebles, calzados, juguetes, sector construcción y automotriz, sistemas hidráulicos y neumáticos, barcos, aviones, entre otros. (EXPEDIENTE N° 063-2007/CCD, 2007)

#### **B. ACUERDO DE CONFIDENCIALIDAD:**

- La parte denunciante alegó que brindó protección especial a la fórmula industrial del poliuretano por su valor comercial y a la información confidencial de empresa, a través de un acuerdo de confidencial pactado con Daniel Luis Curi Rojas (parte denunciada), en el cual se estipularon las obligaciones de guardar reserva, no divulgar a terceras personas los secretos industriales, ni utilizarlo en beneficio propio o de terceros, ni para propósitos distintos a aquellos de la compañía comercial Foamflex. Además, se estipuló que durante la vigencia o en cualquier momento, posterior a la culminación del acuerdo contractual con Foamflex, la parte denunciante no podía revelar a terceras personas los secretos industriales, comerciales e información confidencial de la entidad, ni sacar algún provecho económico de los mismos en el libre mercado. (EXPEDIENTE N° 063-2007/CCD, 2007)
- La parte denunciada dio su consentimiento en la aceptación de todos los inventos, innovaciones, descubrimientos que se generaran durante la vigencia del acuerdo contractual con FOAMFLEX S.A.C, respecto a la

exclusividad de los secretos comerciales e información confidencial, así como los ensayos y pruebas realizados a la espuma de poliuretano. (EXPEDIENTE N° 063-2007/CCD, 2007)

### **C. PUNTOS CONTROVERTIDOS:**

- La entidad Foamflex S.A.C alegó que después de un año de resuelto el contrato de locación de servicios, el denunciado Daniel Luis Curi Rojas empezó a brindar servicios en la empresa Muebles Lot's, momento a partir del cual la entidad empezó a producir y comercializar productos elaborados con espuma de poliuretano, con características similares a la compañía comercial denunciante. (EXPEDIENTE N° 063-2007/CCD, 2007)
- La empresa Muebles Lot's no producía espuma de poliuretano antes de la llegada de Daniel Curi a la empresa. Existe indicios claros que la entidad Muebles Lot's se benefició ilegítimamente con el uso de la fórmula industrial de poliuretano de Foamflex, a través de la fabricación y comercialización de muebles y variedad de productos, configurándose de esta manera la violación de secretos industriales por parte de la entidad denunciada. (EXPEDIENTE N° 063-2007/CCD, 2007)

## **ii. EXPEDIENTE N° 297-2013/CCD-INDECOPI**

### **A. POSTURA DE PARTE DENUNCIANTE:**

- La fórmula industrial de jabones de glicerina por la empresa de jabones de glicerina fue robada por el funcionario principal Carlos Ibañez Terrazas, quien realizó su divulgación a terceras personas, laborando de forma simultánea para la compañía comercial MAKAYA LABORATORIOS S.A.C, entidad que obró con malicia e intención fraudulenta al explotar

económicamente la fórmula industrial de jabones de glicerina sin autorización del titular. (EXPEDIENTE N° 297-2013/CCD-INDECOPI, 2013)

- El funcionario Carlos Ibañez Terrazas quedo descubierto in fraganti laborando simultaneamente para la empresa agraviada Brisas Marinas S.A.C, y para la empresa MAKAYA LABORATORIOS S.A.C, entidad que se vio beneficiada ilegítimamente con la fórmula industrial y que antes de contratar al mencionado agente infractor, producía otro tipo de jabones, y ahora comercializa un producto idéntico, con muchas similitudes a los jabones que comercializa la entidad agraviada. El imputado Ibañez fue cesado en su cargo laboral al ser descubierto, y quedar en evidencia su conducta desleal, maliciosa y fraudulenta. (EXPEDIENTE N° 297-2013/CCD-INDECOPI, 2013)

#### **B. PUNTOS CONTROVERTIDOS:**

- La fórmula industrial de jabones de glicerina fue sustraída por el extrabajador de confianza Carlos Ibañez, quién ejerció funciones de gerencia en la entidad denunciante y laboró simultaneamente para la empresa imputada Makaya Laboratorios S.A.C. El imputado Ibañez realizó de manera deliberada e ilegítima la divulgación de la fórmula industrial a Makaya Laboratorios S.A.C, quien sacó un provecho económico indebido a través de la fabricación y comercialización de un producto similar al de la parte agraviada Brisas Marina S.A.C. (EXPEDIENTE N° 297-2013/CCD-INDECOPI, 2013)
- La empresa denunciante Brisas Marinas S.A.C argumentó que la forma del jabón, el Molde, es de su propiedad exclusiva y la parte denunciada requiere de su autorización para su uso y explotación económica, configurándose la violación del Know How (secreto industrial) con animus lucrandi (ánimo de lucro) malicia e intención fraudulenta del agente infractor Carlos Ibañez Terrazas. (EXPEDIENTE N° 297-2013/CCD-INDECOPI, 2013)

### **C. CONTROVERSIA JURÍDICA:**

- El objeto de controversia en el presente caso se centró no solo en la presentación comercial de Makaya S.A.C similar a Brisas Marinas S.A.C, al comercializar los jabones de glicerina, lo cual generaba un riesgo de confusión en el mercado, respecto al origen empresarial del producto, sino también en el acto desleal del agente infractor Carlos Ibañez Terrazas, quien se apoderoo ilegítimamente de la fórmula industrial para su divulgación a la empresa denunciada Makaya Laboratorios S.A.C, quien sacó un provecho económico indebido con la fabricación y explotación económica de jabones con la mismas fórmulas químicas - industriales de Brisas Marinas S.A.C. (EXPEDIENTE N° 297-2013/CCD-INDECOPI, 2013)

### **iii. EXPEDIENTE N° 035-2012/CCD-INDECOPI**

#### **A. POSTURA DE PARTE DENUNCIANTE:**

- ❖ Belmay S.A.C alegó que con fecha 11 de febrero del 2011, tuvo conocimiento de que la parte denunciada (Gabriela Sedano) había estado realizando actos de espionaje, desde el correo corporativo [gabriela.sedano@boticafrancesa.com](mailto:gabriela.sedano@boticafrancesa.com) y enviando información secreta de la empresa a terceras personas, siendo que en la misma fecha, el Notario Público de Lima Gino Benvenuto Murguía elevó un acta notarial en la que había constatado de la existencia de 4 correos electrónicos con fecha 2 de febrero del 2011, enviados ilegítimamente, sin autorización del titular al correo electrónico [info@grupocriterio.com](mailto:info@grupocriterio.com), correspondiente a “Criteria Consultores”. (EXPEDIENTE N° 035-2012/CCD-INDECOPI, 2012)

#### **B. PUNTOS CONTROVERTIDOS:**

- ❖ El notario constató que, de los correos electrónicos enviados por la imputada

Gabriela Sedano, estos contienen fórmulas industriales de diversos productos fabricados por la compañía agraviada Belmay S.A.C, entre los cuales tenemos 2 cremas para masaje: Reafirmante de Coca (Fórmula N° F-51602) y antiestrés (Fórmula N° F-52001), 1 crema de Drenaje Linfático para el cuerpo (Fórmula N° F-51702), 1 loción Adaptogénica para cutis de la piel (Fórmula N° F52803) y 1 Reductora BF Cafeína Crema (Fórmula N° F21603). (EXPEDIENTE N° 035-2012/CCD-INDECOPI, 2012)

- ❖ La empresa agraviada Belmay S.A.C. petitionó a la Comisión de Indecopi que dictamine las medidas correctivas con el fin de remover los efectos negativos de la divulgación de las 5 fórmulas industriales por parte de la agente infractora Gabriela Sedano, la inscripción de la sanción respectiva en el registro de infractores y el pago de las costas y costos. (EXPEDIENTE N° 035-2012/CCD-INDECOPI, 2012)

### C. CONTROVERSIA JURÍDICA:

- ❖ La señora imputada Gabriela Sedano señaló en su defensa que la diligencia de inspección mediante el cual la empresa agraviada Belmay S.A.C había observado los correos electrónicos corporativos enviados se observó e hizo pública sin su consentimiento expreso, violentando su derecho a la privacidad de las comunicaciones. (EXPEDIENTE N° 035-2012/CCD-INDECOPI, 2012)
- ❖ **Posición de la Comisión de Indecopi:** La Comisión de Indecopi en una decisión bastante controvertida, decide declarar sin efectos legal los correos electrónicos adjuntados por la empresa agraviada Belmay S.A.C a pesar de haberse acreditado la divulgación indebida y deliberada de las fórmulas industriales a “Criteria Consultores” por medio del envío deliberado e ilegítimo de correos corporativos, siendo la postura de la Comisión que se obtuvo violentando el derecho al secreto y a la inviolabilidad de las comunicaciones y documentos privados acorde al numeral 10 del artículo 2

de la Constitución Política del Perú. (EXPEDIENTE N° 035-2012/CCD-INDECOPI, 2012)

**iv. EXPEDIENTE N° 009-2011/CCD - INDECOPI**

**A. POSTURA DE PARTE DENUNCIANTE:**

➤ **BRANIF S.A.C.** manifestó que:

(i) El imputado Alberto Sánchez Julca laboró para la empresa agraviada Branif S.A.C hasta el 31 de julio del 2009, con puesto laboral de Jefe de Planta y Producción, con facultades de acceso a fórmulas químicas, industriales que son utilizadas para la elaboración de productos comercializables de la mencionada entidad. (EXPEDIENTE N° 009-2011/CCD-INDECOPI, 2011)

(ii) Asimismo la imputada Nelly Castro Albarrán laboró para Branif hasta el 30 de junio del 2009, gozando de facultades de acceso a información confidencial vinculada a aspectos comerciales de la compañía, como la lista precios, proveedores, productos, precios, la cartera de clientes, insumos, etc. (EXPEDIENTE N° 009-2011/CCD-INDECOPI, 2011)

(iii) Por otro lado, la imputada Mónica Fiorella Díaz Aliaga se desempeñó como vendedora de la entidad hasta el 31 de agosto del 2009, gestionando también información secreta de empresa, y la entidad teniendo conocimiento de la importancia de mantener reservada los secretos societarios, estipuló cláusulas contractuales de reserva en los contratos pactados con los mencionados imputados con el fin esencial de mantener reservada dicha información. (EXPEDIENTE N° 009-2011/CCD-INDECOPI, 2011)

## **B. PUNTOS CONTROVERTIDOS:**

- Los productos comercializados de la entidad imputada Promak S.A.C tienen la misma composición química que los productos de Branif S.A.C gracias a la colaboración de los ex trabajadores de confianza de la empresa agraviada, quienes divulgaron las fórmulas químicas, industriales de manera deliberada con el fin de gozar privilegios laborales y mejores condiciones salariales en la mencionada empresa denunciada. Además la entidad agraviada señaló que, a través de análisis de laboratorio realizados por la Universidad Nacional de Ingeniería, sobre diversos productos comercializados por ambas compañías comerciales, determinó que la composición química de los productos comercializados por **Promak S.A.C** es la misma que de la mercadería de la empresa **Branif S.A.C**. (EXPEDIENTE N° 009-2011/CCD-INDECOPI, 2011)
  
- Existe indicios de que la empresa imputada Promak S.A.C venía remitiendo cotizaciones a los mismos clientes de Branif S.A.C. a través del uso ilegítimo de la cartera de clientes otorgado por los ex trabajadores de confianza, ofreciéndoles los mismos tipos de productos y a un precio menor, generando daño concurrencial y externalidades negativas a las utilidades de la entidad agraviada. Además, la empresa denunciante mencionó que Promak S.A.C estuvo induciendo a la infracción contractual a sus trabajadores, incentivándolos con mejores condiciones laborales para que incumplan con sus obligaciones contractuales y pasen a formar parte de la empresa imputada. (EXPEDIENTE N° 009-2011/CCD-INDECOPI, 2011)

## **C. CONTROVERSIA JURÍDICA:**

- La imputada Esther Sernaqué Acosta se encontraba desempeñando funciones laborales en Promak y haciendo uso ilegítimo y deliberado de la

cartera de clientes de Branif S.A.C a favor de Promak S.A.C. Además, entidad denunciante alegó que la imputada continuaba en comunicación con los trabajadores de la empresa agraviada, con el fin de seguir obteniendo indebidamente información confidencial de empresa a favor de Promak S.A.C, e induciéndolos a incumplir con sus obligaciones contractuales a través de ofrecimiento de mejores condiciones salariales. (EXPEDIENTE N° 009-2011/CCD-INDECOPI, 2011)

- **Posición de la Comisión de Indecopi:** La Comisión de Indecopi, de manera controvertida desestimó la denuncia alegando que Branif S.A.C no tiene el derecho exclusivo a desarrollar actividades económicas en el sector industrial, en función al criterio de la libre iniciativa privada y libertad de empresa, sin tomar en consideración la actuación desleal y deliberada de los imputados (ex trabajadores de confianza y Promak S.A.C) a través de la apropiación ilegítima de los secretos empresariales, el aprovechamiento económico indebido de las fórmulas químicas, industriales, y el posicionamiento en el libre mercado a través del daño concurrencial a la empresa agraviada, con el uso de la cartera de clientes, lista de proveedores, insumos y otros secretos organizacionales de la entidad afectada. (EXPEDIENTE N° 009-2011/CCD-INDECOPI, 2011)

### 3.3. Técnicas y Materiales

#### 3.3.1. Técnicas:

##### 3.3.1.1. Técnica de Recolección de Datos:

- i. **Técnica de Entrevista Escrita:** Se realizó una Entrevista escrita al Doctor Sixto Chávez Avalos, especialista en derecho de competencia y regulación de servicios públicos, para la recolección de información referida a la violación de Secretos empresariales por parte de los competidores desleales, los supuestos en los que el trabajador de confianza renuncia a la

empresa, el deber de guardar reserva de los empleados, los riesgos Empresariales que acarrea la falta de registro de los Secretos Patentables y la importancia de las Franquicias.

## **GUÍA DE ENTREVISTA – DOCTOR SIXTO CHÁVEZ:**

### **A. LA VIOLACIÓN DEL SECRETO EMPRESARIAL Y EL BALANCE ECONÓMICO DE LAS PERSONAS JURÍDICAS**

- ¿Cómo afectaría la violación de Secretos empresariales por parte de los competidores desleales, al balance económico de una Empresa (ingresos y egresos), en el supuesto que no se hayan pactado las cláusulas contractuales, que protejan esta información secreta, como en los contratos de franquicias?

### **II. EL TRABAJADOR DE CONFIANZA Y EL DEBER DE GUARDAR RESERVA:**

- En el supuesto de que el trabajador de confianza, renuncie a la empresa, y al ser contratado por otra compañía, incumple con el deber de guardar reserva, con respecto a la información secreta (Know How).
- ¿Sería pertinente una regulación jurídica en materia penal – económica, a fin de sancionar estas conductas de mala fe?

### **III. LOS SECRETOS PATENTABLES Y LA ORGANIZACIÓN DE LAS PERSONAS JURÍDICAS**

- ¿Qué riesgos Empresariales se originarían, al no están registrados los Secretos Patentables?
- ¿Qué problemas organizacionales podrían surgir para el empleador, y que desventajas tendrían en el posicionamiento de un producto, servicio, en una economía social de Mercado?

### **IV. ACUERDOS DE CONFIDENCIALIDAD Y VACIOS LEGISLATIVOS EN MATERIA PENAL**

- ¿Qué probabilidades hay de que un trabajador de confianza, cumpla con el deber de confidencialidad y de guardar reserva, ante la falta de una sanción punitiva, en materia penal?
- ¿Son garantía suficiente los acuerdos de confidencialidad, en un libre mercado y ante los avances tecnológicos y la competencia vigorosa?

### **V. IMPORTANCIA DE LAS FRANQUICIAS:**

- ¿Qué importancia tiene las Franquicias en nuestro país, como impulsores del desarrollo económico a nivel nacional?
- ¿Cuán beneficioso puede ser para el Orden Económico del Estado, una mayor implementación de este tipo de negocios, en el libre mercado?

## ENTREVISTA DR. SIXTO CHÁVEZ – CUESTIONARIO: RESPUESTAS

<p>1. ¿Cómo afectaría la violación de Secretos empresariales por parte de los competidores desleales, al balance económico de una Empresa (ingresos y egresos), en el supuesto que no se hayan pactado las cláusulas contractuales, que protejan esta información secreta, como en los contratos de franquicias?</p>	<p>El Doctor Chávez mencionó que la violación de secretos empresariales se manifestaría en pérdidas. Así también serían gastos todo aquel dinero que la empresa requiera para contrarrestar el acto desleal. Respecto a la inexistencia de cláusulas de protección, habrá que determinar si éstas son esenciales para que podamos atribuir a determinada información el carácter de secreto empresarial. Caso contrario, no habrá secreto que proteger, ni secreto empresa violentado por el acto desleal.</p>
<p>2. En el supuesto de que el trabajador de confianza, renuncie a la empresa, y al ser contratado por otra compañía, incumple con el deber de guardar reserva, con respecto a la información secreta (Know How). ¿Sería pertinente una regulación jurídica en materia penal – económica, a fin de sancionar estas conductas de mala fe?</p>	<p>El Doctor Chávez considera que el ilícito de revelar indebidamente un secreto industrial debería ser penalmente relevante, como lo son la violación de secreto bancario, secreto profesional y secreto de las comunicaciones. Bajo esa condición, resulta necesaria una sanción de esa naturaleza contra la mala fe.</p>

<p>3. ¿Qué riesgos Empresariales se originarían, al no están registrados los Secretos Patentables? ¿Qué problemas organizacionales podrían surgir para el empleador, y que desventajas tendrían en el posicionamiento de un producto, servicio, en una economía social de Mercado?</p>	<p>El Doctor Chávez considera que la falta de registro, en principio impedirá la protección del Secreto, en la vía del Ilícito de propiedad industrial. Téngase en cuenta además que la patente constituye un derecho de exclusiva que permite obtener ventaja competitiva frente a otros agentes económicos. Definitivamente estamos hablando de que la falta de registro se traducirá en mayor exposición a daño concurrencial.</p>
<p>Desde un análisis Económico del Derecho ¿Qué probabilidades hay de que un trabajador de confianza, cumpla con el deber de confidencialidad y de guardar reserva, ante la falta de una sanción punitiva, en materia penal? ¿Son garantía suficiente los acuerdos de confidencialidad, en un libre mercado y ante los avances tecnológicos y la competencia vigorosa?</p>	<p>El Doctor Chávez, entendiendo que la pregunta es qué tan eficiente es un sistema de protección del secreto empresarial, en el que no hay sanciones, considera que efectivamente el sistema es ineficiente. Ahora, habría que ponernos a considerar que tipo de protección queremos y cuál de ellos es el más efectivo: Una tutela civil, administrativa o penal frente al ilícito.</p>
<p>¿Qué importancia tiene las Franquicias en nuestro país, como impulsores del desarrollo económico a nivel nacional? ¿Cuán beneficioso puede ser para el Orden Económico del Estado, una mayor implementación de este tipo de</p>	<p>El Doctor Chávez resalta que las franquicias son muy importantes. Es una oportunidad de negocio para cualquier empresario que quiere empezar a invertir. El orden económico está constituido por normas y situaciones indispensables, sin las cuales el sistema no funciona. Destaca el hecho que hay mayor movimiento en la economía del país, más puestos de trabajo, mayor recaudación de</p>

negocios, en el libre mercado?	impuestos y si se promueven mejor, mayor gasto de inversión y de consumo, lo cual es positivo. (S. Chávez, comunicación escrita, 15 de junio del 2018).
--------------------------------	---

### **APRECIACIÓN**

De la entrevista realizada al Doctor Sixto Chávez Avalos, se puede apreciar que el espionaje corporativo como modus operandi de violación del secreto empresarial produce daños concurrenciales que se manifiestan en pérdidas económicas en perjuicio del empleador, titular de la información secreta de empresa, por dos motivos: Las ganancias dejadas de percibir, por concepto de explotación económica del secreto empresarial y los gastos generados para contrarrestar los actos sabotaje empresarial por medio de espionaje, así como también la implementación de un programa de cumplimiento o criminal compliance para la detección de irregularidades administrativas o actos desleales del agente infractor, en la cadena productiva de la empresa.

Asimismo, cabe recalcar la pertinencia de regular los supuestos de espionaje corporativo en los casos de violación del secreto empresarial, en materia penal, para evitar más agraviados, víctimas económicas por el apoderamiento indebido a través de medios electrónicos, informáticos, escritos, del secreto societario de aplicación económica y la posterior divulgación de la información secreta de empresa o explotación económica del mismo por parte del agente infractor, en beneficio propio o de terceros.

Finalmente, el espionaje corporativo genera daños concurrenciales no solo en perjuicio de las empresas privadas, sino también a nivel macro económico, del consumidor y el trabajador, porque al verse perturbado el flujo de riqueza de las

empresas afectadas por la violación del secreto empresarial, ello acarrea la reducción del presupuesto para la contratación de personal, insumos esenciales, producción de bienes, servicios al cliente, marketing e infraestructura corporativa, lo cual produce externalidades negativas en la generación de empleo en nuestro país y la calidad del producto o servicio ofrecido al consumidor, a causa de los problemas organizacionales internos y los costos generados en criminal compliance, vigilancia y seguridad informática.

## ii. Técnica de Entrevista Oral:

- Se realizó una Entrevista oral al Doctor Santos Urtecho Navarro, especialista en derecho mercantil, derecho civil contractual, para la recolección de información referida al modo de repercusión del Espionaje Corporativo en el funcionamiento de las personas jurídicas, los efectos generados, las medidas a adoptar ante esta problemática en materia de competencia desleal, y la aparición del Derecho Penal Económico como rama jurídica que podría contribuir a una mejor regulación jurídica de la violación del secreto empresarial, especialmente en los casos de espionaje corporativo.

### **GUÍA DE ENTREVISTA – DOCTOR SANTOS URTECHO:**

#### **1. EL ESPIONAJE CORPORATIVO Y EL CORRECTO FUNCIONAMIENTO DE LAS PERSONAS JURÍDICAS**

- ¿Cómo podría repercutir el espionaje empresarial, en el correcto funcionamiento de las personas jurídicas?

## 2. LOS EFECTOS DEL ESPIONAJE EMPRESARIAL

- ¿Cuáles son los efectos generados por el Espionaje corporativo?

## 3. MEDIDAS DE SOLUCIÓN, FRENTE AL ESPIONAJE CORPORATIVO

- ¿Qué medidas se podría adoptar ante la problemática del espionaje corporativo?

## 4. LA POLÍTICA CRIMINAL Y LA REGULACIÓN JURÍDICA PENAL

- ¿Sería necesario la implementación de una política Criminal, respecto al espionaje de las personas jurídicas?

### ENTREVISTA ORAL – CUESTIONARIO:

<p>a) Quería consultar su opinión acerca del tema del Espionaje Corporativo. En la parte económica. ¿Cómo podría repercutir el espionaje empresarial, en el correcto funcionamiento de las personas jurídicas?</p>	<p>- El Doctor Urtecho declaro recientemente que repercute negativamente porque hay conflicto por tema de competencia comercial, donde los participantes buscan sacar beneficio, provecho a costa de cualquier situación, y justamente el espionaje implica averiguar situaciones que, por sí, los que lo cometen no conocen, o no tienen conocimiento sobre ciertos aspectos</p>
--	---

	<p>relevantes de la empresa, como los conocimientos de carácter industrial, procedimientos y productos, que son susceptibles de explotación económica en el libre mercado.</p> <p>- Sacar ventaja ilícita e indebida, determina que el afectado, y perjudicado tenga que estructurar económicamente parte de su logística, o de su planeamiento, a fin de evitar el espionaje corporativo. Si no es en evitar, es en recuperar lo que ha perdido como consecuencia de la competencia desleal o indebida de los sujetos.</p> <p>- Entonces Daño Económico definitivamente es destinar recursos a algo que no es propiamente actividad del empleador, empleado corporativo, y esos recursos son incalculables. Porque se podrá saber que existe espionaje, pero no se podrá saber a priori, la magnitud del daño, que no solamente causa efecto inmediato, sino también permanece en el tiempo, hasta que el afectado tenga como defenderse.</p>
<p>b) ¿Cuáles son los efectos generados por el Espionaje corporativo?</p>	<p>- El Doctor Urtecho declaro recientemente que existen efectos directos sobre la persona jurídica, el primer factor, el primer riesgo es disminuir utilidades, El Segundo factor, es tener que invertir en</p>

	<p>logística y el tercer factor es el desmembramiento interno de la empresa. Que la persona jurídica quiebre, con la desaparición, disolución, liquidación. Mientras que los efectos Indirectos recaen sobre los empleados: el sistema económico, el sistema comercial, el flujo de efectivo de la empresa se ve afectado, por la pérdida de valor comercial del secreto empresarial. La repercusión es a nivel macroeconómico. Es como los delitos de corrupción de funcionarios públicos. Basta con una actividad de este tipo, para que se vaya afectando la política adoptada, el funcionamiento del sistema judicial, y la ciudadanía en general.</p>
<p>c) ¿Qué medidas se podría adoptar ante la problemática del espionaje corporativo?</p>	<p>- El Doctor Urtecho declaro recientemente que, en los casos de espionaje, además de una sanción económica, que podría considerarse como una protección de la competencia leal, se requiere una sanción punitiva, una sanción penal, para detener de cierta forma este tipo de actos desleales.</p>
<p>d) Para finalizar ¿Sería necesario la implementación de una política Criminal?</p>	<p>- El Doctor Urtecho declaro recientemente que sí es necesario, y que la Política Criminal va a tener que estar enfocada en el marco económico, o la regulación económica y en sentido general, para todos los ciudadanos, no solo para los grupos económicos, o las empresas que se dedican a actividades corporativas, porque la</p>

	<p>repercusión se da a todo nivel.</p> <p>- La política Criminal podría comprender el Derecho Penal Económico, para la adecuación del espionaje corporativo y su tipificación en materia penal, a fin de brindar una mejor protección a los titulares del secreto empresarial. (S. Urtecho, comunicación oral, 2017).</p>
--	---

### **APRECIACIÓN**

De la entrevista realizada al Doctor Santos Urtecho Navarro, se puede apreciar que efectivamente existe un problema de relevancia jurídica, ante la falta de protección en materia penal, del empleador frente a los supuestos de espionaje corporativo y violación del secreto empresarial, que acarrear problemas organizacionales al interno de las empresas privadas como gastos en logística, desmembramiento interno de la empresa y posible disolución de la compañía, por quiebra e insolvencia económica.

Asimismo, también cabe recalcar que las externalidades negativas de la competencia desleal por medio de espionaje corporativo, recaen sobre los empleados, consumidores, que forman parte del sistema comercial, y el flujo de riqueza o las rentas generadas por la explotación económica sin autorización del secreto societario. La violación del secreto empresarial a través de actos de espionaje, conlleva a la pérdida de valor comercial y estratégico del mismo, y afecta por un lado las rentas percibidas por la explotación económica del secreto societario, y, por otro lado, el adecuado proceso competitivo entre las empresas privadas, en materia de competencia desleal.

### iii. Técnica de Entrevista Escrita:

- Se realizó una Entrevista escrita a la Doctora Claudia Cotrina Roldán, especialista en derecho corporativo, para la recolección de información referida al Espionaje Corporativo como modalidad de competencia desleal, su incidencia en la cadena productiva, la imagen y buena reputación de las personas jurídicas y la violación del secreto empresarial.

#### **GUÍA DE ENTREVISTA – DOCTORA CLAUDIA COTRINA ROLDÁN:**

##### **1) EL ESPIONAJE CORPORATIVO**

- ¿Cómo podría incidir el espionaje empresarial, en los ingresos y egresos de las empresas?

##### **2) LOS TRABAJADORES DE CONFIANZA**

- ¿Cuáles son los efectos generados por mala fe de los trabajadores de confianza, al tener acceso a información secreta de la empresa?

##### **3) COMPETENCIA DESLEAL**

- ¿Por qué se da frecuentemente el espionaje corporativo como modalidad de competencia desleal?

#### 4) LA RESPONSABILIDAD SOCIAL CORPORATIVA

- ¿Como podría afectar el espionaje corporativo a la imagen y buena reputación de las empresas?

#### CUESTIONARIO – DOCTORA CLAUDIA COTRINA ROLDÁN:

<p>(a) ¿Cómo podría incidir el espionaje empresarial, en los ingresos y egresos de las empresas?</p>	<p>- Podría incidir negativamente, porque los empleadores tienen que destinar parte de sus recursos a la prevención de los ataques de espionaje, y controles de seguridad continuos, así como también cambiar la logística y reforzar el sistema de seguridad de los secretos empresariales.</p>
<p>(b) ¿Cuáles son los efectos generados por mala fe de los trabajadores de confianza, al tener acceso a información secreta de la empresa?</p>	<p>- Los efectos son negativos, porque los trabajadores de confianza sacan provecho de su puesto de trabajo, acceden a información confidencial de la empresa sin un debido control, y se ven incentivados a actuar de mala fe y sacar un provecho indebido sin autorización del secreto empresarial. En consecuencia, se</p>

	infringe la buena fe empresarial y el deber de guardar reserva.
(c) ¿Por qué se da frecuentemente el espionaje corporativo como modalidad de competencia desleal?	- Se da frecuentemente, porque no hay actualmente una fiscalización de las actividades de espionaje, y en una economía social de mercado, los agentes económicos, los empleadores, y los franquiciantes, buscan en todo momento tener una ventaja estratégica competitiva que ayude al crecimiento de sus empresas.
(d) ¿Como podría afectar el espionaje corporativo a la imagen y buena reputación de las empresas?	- Podría afectar negativamente, porque el espía infractor que obra de mala fe, puede causar un detrimento al status actual de la empresa, utilizar el secreto empresarial en contra del empleador, sobornarlo, extorsionarlo con la revelación del secreto de empresa, y en consecuencia, la información confidencial puede ser divulgada y usada indebidamente. (C. Cotrina, comunicación escrita, 2018).

### **APRECIACIÓN**

De la entrevista realizada a Claudia Cotrina Roldán, se puede apreciar que el espionaje corporativo acarrea costos en seguridad, y la ausencia de persecución penal en estos supuestos atípicos de sabotaje empresarial, posibilitan la comisión de la violación del secreto empresarial, a los espías corporativos por

autoría mediata e inmediata, configurándose el nexo causal con el resultado dañoso producido al balance patrimonial de las empresas privadas.

Asimismo, el adecuado proceso competitivo se ve perturbado, por la falta de fiscalización del espionaje corporativo, en las empresas privadas, cometiéndose actos de competencia desleal por parte de los trabajadores y terceras personas, en complicidad con los agentes económicos del mercado, personas de status socioeconómico alto y con excelente calificación profesional.

Asimismo, la falta de sanciones punitivas a los agentes infractores, por la violación del secreto empresarial, fomenta el uso indebido sin autorización del titular, de la información secreta de empresa, y su divulgación a terceras personas, con fines de lucro o para perjudicar la imagen y buena reputación de las empresas privadas.

#### **3.3.1.2. Técnica de Análisis de Datos:**

- Mediante la técnica de análisis documental, abordé aspectos principales sobre el espionaje corporativo, los secretos empresariales y las personas jurídicas en el Perú en fuentes de investigación enfocadas en su mayoría a artículos sobre el espionaje corporativo en materia de competencia desleal, el criminal compliance, la violación del secreto Empresarial, y las patentes, que fueron citados correspondientemente, así como libros virtuales sobre el tema en mención y noticias de la actualidad.

#### **3.3.1.3. Técnica de Recolección de Datos:**

- Mediante la técnica de recolección, recopilé principalmente información proveniente del Código Penal Peruano, así como también artículos especializados en materia de competencia desleal, en relación con los

secretos empresariales, contratos de franquicia, el espionaje corporativo, las personas jurídicas, el criminal compliance, los riesgos empresariales derivados del espionaje empresarial y los secretos como derecho de propiedad intelectual.

### **3.3.2. Materiales de Estudio:**

#### **i. Doctrina:**

- Para conocer las posiciones doctrinarias de los juristas que han estudiado los principios y fundamentos de los secretos empresariales, en especial la temática de las infracciones internas de las empresas, el sabotaje mercantil y la violación del Secreto Empresarial en casos de espionaje empresarial como modalidad de competencia desleal, los derechos de propiedad intelectual en relación a los secretos patentables, las franquicias y la importancia del Know How en estos modelos de negocio.

#### **ii. Jurisprudencia:**

- Con la finalidad de conocer los argumentos, criterios jurisprudenciales y posiciones del Tribunal Constitucional, respecto a el Secreto Empresarial, y su vinculación con el derecho a la intimidad en el ámbito constitucional, y del Tribunal de Defensa de la Competencia y de la Propiedad Intelectual en lo concerniente a la violación del secreto empresarial. Asimismo, se toma en cuenta criterios jurisprudenciales del Derecho administrativo sancionador, referidos a la intención fraudulenta y el grave perjuicio, adoptados por las Comisiones de INDECOPI en sus resoluciones administrativas, y que son aplicables en el ámbito penal, para el análisis de los supuestos de violación del secreto empresarial en casos de espionaje, y los problemas organizacionales que acarrear

al empleador y al franquiciante, como competidores leales en una economía social de Mercado.

### iii. Legislación Nacional y Comparada:

- Se tomo en consideración la normatividad nacional, en específico el Decreto Legislativo N° 1044 “Ley de Represión de la Competencia Desleal” que regula los supuestos de violación del secreto empresarial como modalidad de competencia desleal de los agentes económicos y demás participantes del libre mercado. También se tomó en consideración los instrumentos normativos internacionales aplicables a los supuestos de violación de secreto empresarial y mala fe de los competidores, como La Decisión N° 486 que regula el Régimen de Propiedad Industrial.
  
- Para un mayor desarrollo de la temática de Espionaje Corporativo y Violación del Secreto Empresarial, también fue objeto de estudio, los Acuerdos de la Organización Mundial del Comercio sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), que brindan protección jurídica a la información no divulgada y de carácter confidencial de los titulares e inventores, la Ley de Propiedad Industrial de México que sanciona la revelación de secretos comerciales a personas no autorizadas, el código penal español, que sanciona punitivamente la violación de los secretos empresariales por medio de espionaje y la Ley de Competencia Desleal de España - Ley 3/1991 que sanciona los actos desleales de apoderamiento por cualquier medio, del secreto empresarial, para su posterior aprovechamiento económico y sin autorización del titular.

### **3.4. Procedimiento:**

#### **3.4.1. Recolección de Datos:**

- Revisión y recopilación inicial de información mediante la técnica de análisis documental, mediante el cual, abordé los aspectos sobre el espionaje corporativo, los secretos empresariales y las personas jurídicas en el Perú.
- Seguido, mediante el mismo método; analicé en qué casos o cómo se efectúa con mayor frecuencia los casos de espionaje corporativo, para ello tuve en cuenta dos aspectos importantes, el primero, son los sujetos y entes involucrados en el correcto funcionamiento de las personas jurídicas, y segundo son los derechos afectados y daños generados en los casos de espionaje corporativo.

#### **3.4.2. Tratamiento y análisis de Datos:**

- Posteriormente, apliqué la técnica de análisis y tratamiento de datos: A través del método mencionado, encontraré, explicaré e interpretaré cual es el estado de indefensión de los empleadores, franquiciantes y los efectos generados a partir de la falta regulación jurídica en materia penal, del espionaje corporativo en el Perú, frente a los casos de sabotaje empresarial y mala fe por parte de los trabajadores y empleadores, a través del aprovechamiento económico indebido del secreto empresarial y otros datos confidenciales de la empresa, por parte de los espías corporativos, en su condición de competidores desleales.

### **3.5. Aspectos Éticos**

- Para el desarrollo de la investigación, se ha tomado en cuenta la honestidad y la responsabilidad con el profesionalismo y la orientación adecuada, la enseñanza de mi docente y mis asesores temáticos.

#### IV. RESULTADOS:

##### 4.1. PRIMEROS HALLAZGOS

###### **ENTREVISTAS:**

###### **OBJETIVO ESPECÍFICO N° 1**

###### **a) ENTREVISTA – DOCTOR SIXTO CHÁVEZ ÁVALOS**

1. ¿Cómo afectaría la violación de Secretos empresariales por parte de los competidores desleales, al balance económico de una Empresa (ingresos y egresos)?

2. ¿Sería pertinente una regulación jurídica en materia penal – económica, a fin de sancionar estas conductas de mala fe?

3. ¿Qué riesgos Empresariales se originarían, al no están registrados los Secretos Patentables?

4. ¿Qué problemas organizacionales podrían surgir para el empleador, y que desventajas tendrían en el posicionamiento de un producto, servicio, en una economía social de Mercado?

5. ¿Qué probabilidades hay de que un trabajador de confianza, cumpla con el deber de confidencialidad y de guardar reserva, ante la falta de una sanción punitiva, en materia penal?

De la entrevista realizada al doctor Chávez (2018), en la pregunta n° 1 hay coincidencia con los daños patrimoniales a las empresas privadas en materia de competencia desleal, y se aplican como criterios el espionaje corporativo, la violación del secreto empresarial y los daños económicos de carácter patrimonial en perjuicio del empleador, titular de los secretos industriales e información confidencial, por los siguientes motivos: las ganancias dejadas de percibir, por concepto de explotación económica exclusiva del secreto empresarial, la pérdida de royalties o regalías generadas por otorgamiento de licencias hacia terceras personas, para el uso autorizado y aprovechamiento económico del secreto empresarial en el libre mercado, y los gastos generados en criminal compliance o programas de cumplimiento, para la detección de conductas maliciosas, desleales de espionaje corporativo en las entidades privadas, para contrarrestar los actos sabotaje empresarial, apoderamiento y difusión indebida de secretos empresariales hacia terceras personas, por parte de los espías infractores.

<p><b>OBJETIVO ESPECÍFICO N° 2</b></p> <p><b><u>ENTREVISTA – DOCTORA</u></b></p> <p><b><u>CLAUDIA COTRINA</u></b></p> <p>1. ¿Cómo podría incidir el espionaje empresarial, en los ingresos y egresos de las empresas?</p> <p>2. ¿Cuáles son los efectos generados por mala fe de los trabajadores de confianza, al tener acceso a información secreta de la empresa?</p> <p>3. ¿Por qué se da frecuentemente el espionaje corporativo como modalidad de competencia desleal?</p> <p>4. ¿Como podría afectar el espionaje corporativo a la imagen y buena reputación de las empresas?</p>	<p>De la entrevista realizada a la doctora Cotrina (2018) en la pregunta N° 2 hay coincidencia con las obligaciones contractuales pactadas entre el trabajador de confianza y el empleador respecto a inventos, secretos empresariales, e información confidencial de empresa, así como también con el espionaje corporativo como modalidad de competencia desleal para la obtención de una ventaja estratégica competitiva en el libre mercado. Se aplican como criterios la falta de fiscalización del espionaje corporativo, en las empresas privadas, el acceso a información confidencial por parte de los trabajadores de confianza, los actos desleales de espionaje y violación del secreto empresarial, las infracciones contractuales como el deber de guardar reserva estipulado en los acuerdos de confidencialidad.</p>
<p><b>OBJETIVO ESPECÍFICO N° 3</b></p> <p><b><u>ENTREVISTA – DOCTORA</u></b></p> <p><b><u>CLAUDIA COTRINA</u></b></p> <p>1. ¿Cómo podría incidir el espionaje empresarial, en los ingresos y egresos de las empresas?</p> <p>2. ¿Cuáles son los efectos generados por mala fe de los trabajadores de confianza, al tener acceso a información secreta de la empresa?</p>	<p>De la entrevista realizada a la doctora Cotrina (2018) en la pregunta N° 3 hay coincidencia con la ausencia de persecución penal del espionaje corporativo, como eximente de responsabilidad, y se aplican como criterios la comisión de la violación del secreto empresarial por parte del trabajador espía, por medios informáticos (físicos o electrónicos), la falta sanciones punitivas frente a los supuestos atípicos de espionaje, la mala fe del trabajador de confianza, la inducción a la infracción contractual por parte de terceras personas, el uso indebido sin autorización del titular, de secretos industriales e información confidencial, y su posterior divulgación a agentes</p>

<p>3. ¿Por qué se da frecuentemente el espionaje corporativo como modalidad de competencia desleal?</p> <p>4. ¿Como podría afectar el espionaje corporativo a la imagen y buena reputación de las empresas?</p>	<p>desleales, así como también la intención fraudulenta y el ánimo de lucro del competidor desleal con la explotación económica del secreto empresarial.</p>
<p><b>OBJETIVO ESPECÍFICO N° 4</b></p> <p><b><u>ENTREVISTA – DOCTOR URTECHO:</u></b></p> <p>1. ¿Cómo podría repercutir el espionaje empresarial, en el correcto funcionamiento de las personas jurídicas?</p> <p>2. ¿Cuáles son los efectos generados por el Espionaje corporativo?</p> <p>3. ¿Qué medidas se podría adoptar ante la problemática del espionaje corporativo?</p> <p>4. ¿Sería necesario la implementación de una política Criminal, respecto al espionaje de las personas jurídicas?</p>	<p>De la entrevista realizada al doctor Urtecho (2017) en la pregunta N° 2 hay coincidencia con los efectos negativos generados por el espionaje corporativo en materia de competencia desleal. Como criterios aplicables, tenemos la pérdida del carácter reservado y exclusivo del secreto empresarial ante los actos de apoderamiento y difusión indebida de los datos confidenciales de empresa, realizados por parte de los agentes económicos desleales y trabajadores espías hacia terceras personas, la obtención indebida e ilegítima de ventaja estratégica – competitiva y beneficios lucrativos por parte de los competidores desleales, a través de la violación del secreto empresarial en perjuicio del titular, ante el descuido del empleador en materia de seguridad informática, blindaje y protección de datos reservados de empresa y programas de cumplimiento para la detección de conductas maliciosas, desleales, contrarias a la buena fe empresarial en el interior de las entidades privadas.</p>
<p><b><u>EXPEDIENTES:</u></b></p> <p>1) N° 063-2007/CCD-INDECOPI</p> <p>2) EXP N° 297-2013/CCD-</p>	<p>Del expediente seleccionado N° 063-2007/CCD-INDECOPI, se aplican como criterios la explotación económica indebida de los secretos empresariales, el dolus malus (Malicia), intención fraudulenta, el</p>

<p>INDECOPI:</p> <p><b>OBJETIVO ESPECÍFICO N° 1:</b> Especificar los efectos del espionaje corporativo, en la esfera jurídica patrimonial de las empresas privadas del periodo 2007 - 2013.</p>	<p>ánimo de lucro del agente económico desleal, la mala fe empresarial, los acuerdos de confidencialidad pactados entre trabajadores de confianza y el empleador, la infracción del deber de guardar reserva respecto a los secretos industriales y comerciales en perjuicio del empresario titular de secretos de aplicación económica, la obtención ilegítima de beneficios lucrativos por parte de agentes económicos desleales, empresas competidoras dentro de un determinado sector comercial. Asimismo, tenemos la competencia desleal existente bajo la modalidad de violación de secretos empresariales, a través del apoderamiento y divulgación indebida de secretos industriales, realizado por parte de los trabajadores espías en su condición de agentes desleales.</p> <p>Del expediente seleccionado EXP N° 297-2013/CCD-INDECOPI se aplican como criterios el deber de mantener en reserva los secretos industriales, información confidencial de empresa, la autoría inmediata del espionaje corporativo por parte de trabajadores de confianza, y autoría mediata de terceras personas, agentes económicos desleales, por medio de la incitación o inducción a los empleados de confianza, al incumplimiento de sus obligaciones laborales y contractuales pactadas con el empleador. Asimismo, tenemos también la divulgación de secretos empresariales en materia de competencia desleal, la obtención beneficios económicos y la explotación económica de secretos industriales sin autorización del titular.</p>
---	--

<p><b>EXPEDIENTE:</b></p> <p>1) EXP N° 009-2011/CCD-INDECOPI</p> <p><b>OBJETIVO ESPECÍFICO N° 2:</b></p> <p>Determinar las consecuencias de los vacíos legales existentes del espionaje corporativo, en las obligaciones contractuales pactadas entre el trabajador y el empleador.</p>	<p>Del expediente seleccionado EXP N° 009-2011/CCD-INDECOPI se aplican como criterios la violación de secretos empresariales, la inducción a la infracción contractual por parte de terceras personas, agentes económicos desleales, empleadores de empresas competidoras, el dolus malus (Malicia), ánimo de Lucro, mala fe empresarial, la infracción del deber de guardar reserva por parte de los trabajadores de confianza, respecto a los secretos empresariales, el apoderamiento indebido y difusión de secretos industriales hacia terceras personas, agentes económicos desleales, empresas competidoras, la pérdida de ventaja estratégica competitiva del empleador o titular de secretos de aplicación económica, el posicionamiento de mercado, de marcas comerciales, productos o servicios de entidades competidoras beneficiadas con la obtención ilegítima de secretos empresariales y la captación indebida de clientes en el mismo sector comercial, por parte de agentes económicos desleales, empresas competidoras, con el uso y aprovechamiento indebido de los secretos comerciales e industriales otorgados por los empleados de confianza.</p>
---	---

<p><b>EXPEDIENTE:</b></p> <p>1) EXPEDIENTE N° 035-2012/CCD-INDECOPI</p> <p><b>OBJETIVO ESPECÍFICO N° 3:</b> Determinar de qué manera el vacío del tipo penal de espionaje corporativo, exime de responsabilidad penal al trabajador espía en su condición de sujeto activo.</p>	<p>Del expediente seleccionado EXPEDIENTE N° 035-2012/CCD-INDECOPI se aplican como criterios el dolus malus (Malicia), la mala fe empresarial de los trabajadores de confianza, la infracción del deber de guardar reserva respecto a los secretos empresariales, el ciberespionaje empresarial, la divulgación de secretos de aplicación económica por parte de la empleados de confianza hacia terceras personas, agentes económicos desleales a través de la transferencia de datos confidenciales contenidos en soportes o ficheros informáticos, secretos industriales adjuntados en correos corporativos, de forma ilegítima y sin autorización del titular, el derecho a la intimidad y al secreto de las comunicaciones de los trabajadores, frente al poder de vigilancia del empleador.</p>
<p><b>EXPEDIENTE:</b></p> <p>1) EXPEDIENTE N° 009-2011/CCD-INDECOPI</p> <p><b>OBJETIVO ESPECÍFICO N° 4:</b> Especificar los efectos del espionaje corporativo, en los secretos empresariales de las empresas privadas, del periodo 2007 – 2013.</p>	<p>Del expediente seleccionado N° 009-2011/CCD-INDECOPI se aplican criterios como el dolus malus (malicia), intención fraudulenta, animus lucrandi (ánimo del lucro), la infracción del deber de guardar reserva de los trabajadores de confianza, la pérdida del carácter exclusivo y reservado de los secretos empresariales, la difusión de secretos industriales e información confidencial de empresa por parte de trabajadores desleales a terceras personas, por medios informáticos, físicos y electrónicos, la mala fe empresarial, la pérdida de ventaja estratégica –</p>

	<p>competitiva del empleador o titular de secretos corporativos de aplicación económica, la falta de un adecuado proceso competitivo en el mismo sector comercial, la explotación económica indebida de los secretos empresariales por parte de empresas competidoras, agentes económicos desleales, la captación indebida de clientes con el uso de los secretos comerciales obtenidos ilegítimamente, la variación del valor económico del secreto empresarial, la reducción de los precios de mercado, de los productos elaborados y comercializados en función a los secretos industriales obtenidos ilegítimamente.</p>
--	--

#### 4.2. RESULTADOS: HALLAZGOS

<b>4.2. RESULTADOS: HALLAZGOS</b>	
<p><b>OBJETIVO ESPECÍFICO N° 1</b></p>	<p>1) <b>Expediente:</b> Conforme al expediente N° 063-2007/CCD, se puede apreciar que el trabajador desleal de la empresa denunciante (Daniel Curi Rojas) se apodera de la fórmula química-industrial del producto (espuma de poliuretano) por medios físicos y electrónicos para su divulgación indebida a empresas competidoras (Muebles Lot's S.A.C), sin autorización del titular del secreto industrial (Foamflex S.A.C), infringiendo su deber de guardar reserva estipulado en acuerdos de confidencialidad, respecto a los secretos industriales, invenciones e información confidencial de empresa. Como consecuencias en la esfera jurídica - patrimonial de la empresa agraviada, tenemos las pérdidas potenciales de royalties o regalías generadas por otorgamiento de licencias hacia terceras personas, para el uso autorizado y explotación económica del secreto empresarial en el libre mercado, los gastos generados en</p>

criminal compliance o programas de cumplimiento, para la detección de conductas maliciosas, desleales de espionaje corporativo en el interior de la entidad privada, para contrarrestar los actos sabotaje empresarial. Asimismo, tenemos también la pérdida de secretos empresariales como propiedad industrial e intelectual exclusiva de la empresa agraviada, ante el robo y difusión indebida de datos confidenciales de la entidad hacia terceras personas, por parte de los trabajadores desleales, y la pérdida de la atribución exclusiva que tenía el empleador agraviado para la explotación económica de secretos empresariales, en materia de competencia desleal.

Asimismo, conforme al expediente N° 297-2013/CCD-INDECOPI, se puede apreciar que el trabajador de la empresa agraviada (Química Brisas S.A.C) actúa deslealmente, con malicia y animus lucrandi, al apoderarse de secretos industriales (fórmula química-industrial de glicerina) de la compañía agraviada por autoría inmediata, para su divulgación indebida a otra empresa competidora (Makaya Laboratorios S.A.C), que pertenece al mismo rubro empresarial. Ello trae daños concurrenciales negativos en las potenciales regalías a partir del otorgamiento de licencias para el uso exclusivo del secreto empresarial, la pérdida de secretos empresariales como propiedad industrial e intelectual de la empresa agraviada, la pérdida de la atribución exclusiva que tenía empleador, en el uso y explotación económica de secretos industriales (fórmula química de glicerina) y los gastos generados en criminal compliance o programas de cumplimiento para la protección de secretos de aplicación económica, de carácter reservado y el cumplimiento de la buena fe empresarial y legalidad en la entidad privada.

2) **Entrevista:** El doctor Chávez (2018), considera que el espionaje corporativo genera daños concurrenciales no solo en perjuicio de las empresas privadas, sino también a nivel macro económico, del

	<p>consumidor y el trabajador, porque al verse perturbado el flujo de riqueza de las empresas afectadas por la violación del secreto empresarial, ello acarrea la reducción del presupuesto para la contratación de personal y el servicio al cliente, lo cual produce externalidades negativas en las utilidades y la generación de empleo en nuestro país, a causa de los problemas organizacionales internos y los gastos generados en vigilancia y seguridad informática. También resalta la importancia de una sanción punitiva de las conductas de espionaje corporativo, con el fin de resguardar el valor comercial y carácter exclusivo de los secretos empresariales y patentes, a fin de fomentar la generación de empleo y el crecimiento económico a nivel nacional.</p>
<p><b>OBJETIVO ESPECÍFICO N° 2</b></p>	<p>1) <b>Expediente:</b> Conforme al expediente N° 009-2011/CCD-INDECOPI, la empresa competidora (Promak S.A.C) incita a los trabajadores de la entidad agraviada (Branif S.A.C), a incumplir con sus obligaciones contractuales (acuerdos de confidencialidad), y revelar información confidencial de la empresa (cartera de clientes, proveedores, insumos) y secretos industriales (fórmulas químicas de elaboración de productos) para obtener beneficios lucrativos y un mejor posicionamiento de su marca comercial en el libre mercado. Asimismo, los trabajadores desleales se ven incentivados a infringir el deber de guardar reserva respecto a los secretos empresariales e incumplir sus obligaciones contractuales, con el ofrecimiento de mejores condiciones salariales y beneficios lucrativos, pasando a formar parte de la sociedad comercial competidora (Promak S.A.C). La empresa competidora obtiene beneficios lucrativos indebidos de los secretos industriales otorgados por los empleados de confianza, a través de la explotación económica indebida de la misma composición química utilizada por la empresa agraviada (Branif S.A.C) y saca un aprovechamiento indebido de los secretos</p>

	<p>comerciales, como la cartera de clientes, lista de proveedores e insumos.</p> <p>2) <b>Entrevista:</b> Para Cotrina (2018), la falta de fiscalización del espionaje corporativo, en las empresas privadas, facilitan la inducción a la infracción contractual y la realización de actos de mala fe por parte de los trabajadores de confianza, quienes ante la ausencia de fiscalización y los descuidos por parte del empleador en la protección de secretos empresariales e información confidencial corporativa, realizan actos de divulgación de datos confidenciales de empresa a terceras personas y la explotación económica del secreto empresarial, sin autorización del titular, infringiendo el deber de guardar reserva que le había confiado el empleador, o habiéndose estipulado los acuerdos de confidencialidad respecto a los secretos comerciales, industriales y de aplicación económica en el libre mercado.</p>
<p><b>OBJETIVO ESPECÍFICO N° 3</b></p>	<p>1) <b>Expediente:</b> Conforme al expediente N° 035-2012/CCD-INDECOPI, se puede apreciar que la trabajadora de confianza (Gabriela Sedano) actúa deslealmente y contrario a la buena fe empresarial, sacado provecho indebido de sus facultades de acceso a información confidencial de empresa, para realizar la transferencia de secretos empresariales contenidos en soportes y ficheros informáticos, secretos industriales adjuntados en correos corporativos, de forma ilegítima y sin autorización del titular, para su divulgación indebida a terceras personas. La trabajadora desleal en su condición de espía por autoría inmediata, se ve incentivada a actuar deslealmente, ante la falta de persecución penal del supuesto atípico de espionaje corporativo y violación del secreto empresarial. Es por ello, que se puede apreciar que la trabajadora de confianza obra de mala fe e infringe el deber de guardar reserva</p>

	<p>respecto a los secretos industriales de la empresa agraviada (BELMAY S.A.C), para revelarlo indebidamente a terceras personas, sin autorización del titular.</p> <p>2) <b>Entrevista:</b> Para Cotrina (2018), se puede apreciar que la ausencia de persecución penal del espionaje corporativo, posibilita la comisión de la violación del secreto empresarial, a los competidores desleales (trabajadores y terceras personas) por autoría mediata e inmediata, en relación de causalidad con el resultado dañoso producido a las empresas privadas por el robo de secretos empresariales y difusión a terceras personas. La especialista destaca que, frente a esta disyuntiva, los trabajadores espías y terceras personas, hacen uso abusivo de su derecho de libertad de empresa, actúan de forma arbitraria y desleal en el libre mercado a través de actividades de espionaje y violación del secreto empresarial, con el fin de obtener beneficios lucrativos y una ventaja estratégica - competitiva en el mismo rubro o sector comercial que el agraviado.</p>
<p><b>OBJETIVO ESPECÍFICO N° 4</b></p>	<p>1) <b>Expediente:</b> Conforme al expediente N° 009-2011/CCD-INDECOPI, la empresa imputada (Promak S.A.C) realizó actividades atípicas de espionaje corporativo por autoría intelectual, con malicia (dolus malus) y animus lucrandi (ánimo de lucro), con la colaboración de trabajadores desleales de la empresa agraviada (Branif S.A.C), en la difusión de secretos industriales e información confidencial de empresa, por medios físicos y electrónicos, teniendo como consecuencias, en primer lugar, la pérdida del carácter reservado y exclusivo de los secreto empresariales ante los actos de apoderamiento y divulgación indebida de los datos confidenciales corporativos hacia la empresa competidora, en segundo lugar, la pérdida de ventaja estratégica – competitiva del empleador titular de</p>

	<p>secretos empresariales, como activo para el buen posicionamiento de las marcas comerciales en el libre mercado, la adulteración o cambio en la esencia de los productos elaborados y comercializados por parte de la empresa competidora, a partir de los secretos industriales obtenidos ilegítimamente. Asimismo, se realiza de manera continua el robo o apoderamiento indebido de información confidencial de empresa como secretos industriales (fórmulas químicas de elaboración de productos), secretos comerciales (cartera de clientes, proveedores, insumos), la explotación económica indebida de secretos empresariales (fórmulas químicas de aceite refrigerante; y desengrasantes de piezas mecánicas) y actos de sabotaje empresarial como la captación indebida de clientes de la empresa afectada.</p>
	<p>2) <b>Entrevista:</b> Para Urtecho (2017), las externalidades negativas del espionaje corporativo, recaen sobre los empleados, consumidores, que forman parte del sistema comercial, y el flujo de riqueza o las rentas generadas por la explotación económica del secreto societario, que pierde su carácter exclusivo y reservado ante su divulgación indebida por parte de trabajadores espías, funcionarios y socios comerciales hacia terceras personas, agentes económicos desleales o empleadores de otras entidades competidoras y la pérdida de la atribución exclusiva del secreto empresarial que tenía el empleador o titular del secreto empresarial. El especialista resalta que ello acarrea problemas organizacionales al interno de las empresas privadas como gastos en logística para contrarrestar los actos espionaje corporativo en el interior de las entidades privadas, el desmembramiento interno, declaración de quiebra e insolvencia económica de las compañías comerciales.</p>

## V. DISCUSIÓN DE RESULTADOS:

- a) Sobre el Objetivo Específico N°1: Especificar los efectos del espionaje corporativo, en la esfera jurídica patrimonial de las empresas privadas del periodo 2007 - 2013.

Como resultados tenemos que los trabajadores de confianza se apoderan de secretos industriales por medios físicos y electrónicos, para su divulgación indebida a terceras personas, teniendo como efectos la pérdida de royalties o regalías generadas por otorgamiento de licencias hacia terceras personas, para el uso autorizado y explotación económica del secreto empresarial en el libre mercado, la pérdida de secretos empresariales como propiedad industrial e intelectual exclusiva y el aumento de gastos de vigilancia, seguridad informática y criminal compliance (programa de cumplimiento) para contrarrestar y detectar los actos desleales de espionaje, contrastando con la hipótesis específica N° 1: “La falta de fiscalización del espionaje corporativo en materia penal, incide negativamente en la esfera jurídica patrimonial de las empresas privadas fiscalizadas por la Comisión de Indecopi de Lima, en el periodo 2007 - 2013”, porque se puede apreciar que los actos desleales de espionaje y violación del secreto empresarial por parte de los trabajadores de confianza, producen un perjuicio en la esfera jurídica patrimonial de las compañías privadas, al generar pérdidas potenciales de regalías de licencias de otorgamiento de secretos empresariales a terceras personas para su comercialización y uso exclusivo con autorización del titular, los gastos generados al empleador en vigilancia informática, programas de cumplimiento para las detecciones de actos de sabotaje empresarial, y en la reestructuración de parte de su logística, ante la fuga de información confidencial y secretos empresariales en materia de propiedad industrial e intelectual.

Asimismo, se aplicó el **método empírico: hipotético deductivo**, con la hipótesis específica siguiente: La falta de regulación jurídica penal del espionaje corporativo, incide en la esfera jurídica patrimonial de las empresas privadas del periodo 2007 - 2013, conforme a la revisión de los expedientes de Indecopi N°

063-2007/CCD y N° 297-2013/CCD, al verificarse que efectivamente existe un perjuicio de carácter patrimonial, hacia las empresas afectadas por las actividades de sabotaje empresarial, que acarrea gastos en logística, seguridad informática, para contrarrestar los actos desleales de espionaje, y el desmembramiento interno de las empresas privadas. Asimismo, conforme al método de **análisis jurídico**, se puede apreciar de los precitados expedientes, que los trabajadores de las empresas privadas, cometen actos desleales, mediante el apoderamiento indebido del secreto empresarial y su divulgación a terceras personas con fines de lucro, para la explotación económica del secreto industrial y el posicionamiento en el libre mercado.

Además, se aplicó el método de **interpretación jurídica - extensiva** en el expediente N° 297 – 2013/CCD – INDECOPI, donde la Comisión de Indecopi, destaca que, si bien se ha podido verificar el carácter confidencial de la fórmula química contenida en el secreto industrial, la parte denunciante no ha acreditado que el imputado haya realizado la explotación económica del secreto empresarial. Asimismo, el mencionado órgano administrativo resalta que el imputado tiene derecho a la libre iniciativa privada, en el mismo rubro o sector comercial del denunciante, conforme a la libertad de empresa, comercio e industria, amparado por el artículo 58 y 59 de la Constitución Política del Perú, por desarrollarse la actividad comercial o empresarial dentro de una economía social de mercado.

Asimismo, **la Comisión de Indecopi** en el Expediente N° 063-2007/CCD, coincide al considerar que la parte denunciante no tiene derecho exclusivo a desarrollar actividades económicas en el sector industrial. En relación con el derecho a la libertad de empresa, amparado en el artículo 58 de la Constitución Política del Perú, el mencionado órgano administrativo destaca que el imputado tiene derecho a desarrollar actividades económicas en el mismo rubro o sector comercial del denunciante y conforme a su propia conveniencia. Asimismo, respecto a los medios probatorios presentados durante el procedimiento administrativo, la parte denunciante no pudo acreditar la existencia del secreto

empresarial, dejando de esta manera, exento de responsabilidad al imputado en materia de competencia desleal.

Asimismo, se aplicó **la técnica de entrevista oral**, al Doctor Sixto Chávez, donde podemos resaltar las externalidades negativas del espionaje corporativo como las pérdidas económicas que acarrear los actos de espionaje y la divulgación del secreto empresarial a terceras personas, ante la ausencia de persecución penal, lo cual conlleva a incentivar al agente desleal a actuar de mala fe, con intención fraudulenta y animus lucrandi para la explotación económica del secreto de empresa. El supuesto atípico de espionaje corporativo requiere regulación en materia penal, por darse distintas modalidades atípicas de espionaje a través del apoderamiento del secreto empresarial por medios electrónicos, informáticos (ciberespionaje) o escritos en físico. Asimismo, el uso del correo corporativo, es otro medio por el cual el agente desleal, realiza actos de espionaje para la divulgación a terceras personas de información confidencial de la empresa, y en muchos casos de carácter comercial, susceptible de explotación económica, para la obtención ilegítima de un provecho económico indebido. El espionaje corporativo produce daños concurrenciales que se manifiestan en daños patrimoniales en perjuicio del empleador, titular de la información secreta de empresa, por los siguientes motivos: Las pérdidas potenciales en regalías de la explotación económica del secreto empresarial y los gastos generados para contrarrestar los actos sabotaje empresarial por medio de espionaje, para la detección de irregularidades administrativas o actos desleales del agente infractor, en la cadena productiva de la empresa.

Además, se aplicó **la técnica de análisis documental**, a través del cual, se puede llegar a contrastar los aspectos teóricos con los resultados obtenidos en relación con el objetivo N° 1, al determinarse conforme al punto de vista de Pinto (2007) que el robo de información confidencial de empresa o secretos industriales por medio de espionaje corporativo como modalidad de competencia desleal, acarrea pérdidas económicas en perjuicio del patrimonio empresarial del empleador, ante los actos de sabotaje empresarial como falsificar un invento a menor costo, copiando la fórmula de preparación, estrategias de fabricación,

negociaciones millonarias, robo de patentes o contratos, etc. Sin embargo, para Jarabo (2015), si bien es cierto el robo de información confidencial de la empresa y los secretos industriales en materia de propiedad intelectual, representa pérdidas económicas potenciales para las empresas privadas, el mencionado autor destaca principalmente las repercusiones significativas en cuanto a la imagen y buena reputación de las empresas privadas ante sus clientes, empleados y el público en general, debido a que estos pueden percibir que su información privada podría ser vulnerada ante la ausencia de seguridad informática y programas de cumplimiento que detecten la fuga de información ante los actos de sabotaje empresarial, generando así, un clima de incertidumbre y desconfianza.

En conclusión se acepta la hipótesis específica planteada, al demostrarse la existencia de un perjuicio de carácter pecuniario, en la esfera jurídica patrimonial de las empresas privadas de la ciudad de Lima, del periodo 2007 – 2013, traducidos en pérdidas potenciales de regalías por explotación económica de secretos empresariales, gastos en seguridad informática, gestión de ataques de espionaje y programas de cumplimiento para la detección de fuga de información confidencial y secretos industriales, frente a los actos de sabotaje empresarial de los trabajadores espías y terceras personas, bajo la modalidad de espionaje y violación del secreto empresarial.

- b) **Sobre el Objetivo Específico N°2:** Determinar las consecuencias de los vacíos legales existentes del espionaje corporativo, en las obligaciones contractuales pactadas entre el trabajador y el empleador.

Como resultados tenemos que el vacío del tipo penal del espionaje corporativo incide negativamente en las obligaciones contractuales pactadas entre el empleador y el trabajador, frente a los supuestos atípicos de espionaje corporativo, en contraste con la hipótesis específica N° 2: “Los vacíos del tipo penal de espionaje corporativo, inciden negativamente en las obligaciones contractuales de los trabajadores de las empresas privadas

fiscalizadas por la Comisión de Indecopi de Lima en el periodo 2007 – 2013”, porque se puede apreciar que el espionaje corporativo realizado por parte de los trabajadores de confianza con facultades de acceso a información confidencial de empresa y secretos industriales, sacan provecho de su categoría laboral y de la ausencia de fiscalización del espionaje corporativo, además de percibir un sistema de seguridad débil del empleador, y roban secretos industriales o de aplicación económica en el libre mercado, además de difundirlo a terceras personas, con fines de lucro o para generar un perjuicio en la imagen, y posicionamiento estratégico de la empresa agraviada, frente a los daños concurrenciales negativos generados, en materia de competencia desleal. Asimismo, cabe destacar que estos daños concurrenciales son generados por terceras personas quienes inducen a los trabajadores de las empresas privadas, a infringir su deber de guardar reserva pactado en los acuerdos de confidencialidad, respecto al secreto empresarial, a causa de la divulgación indebida del mismo por medios electrónicos (correo electrónico personal) y físicos.

Se aplicó el método empírico: **hipotético - deductivo**, a través del cual, puede contrastarse la hipótesis específica: “Los vacíos del tipo penal de espionaje corporativo, inciden negativamente en las obligaciones contractuales de los trabajadores de las empresas privadas fiscalizadas por la Comisión de Indecopi de Lima en el periodo 2007 – 2013”, con el resultado N° 2. Conforme al expediente de Indecopi N° 009-2011/CCD, se puede apreciar que efectivamente existe una incidencia negativa del espionaje corporativo en las obligaciones contractuales de los trabajadores, al darse frecuentemente la inducción a la infracción contractual en las empresas privadas del departamento de Lima, del periodo 2007 - 2013, donde los trabajadores de confianza aprovechan sus facultades de acceso a información confidencial de empresa y difunden los secretos empresariales a terceras personas y para obtener mejores beneficios laborales en otras empresas. En consecuencia, se infringe el deber de guardar reserva pactado

en los acuerdos de confidencialidad, respecto a los secretos empresariales en materia de propiedad intelectual.

Asimismo, se aplicó el método empírico: de interpretación jurídica - extensiva y la técnica de análisis documental respecto a los aspectos teóricos que contrastan con el resultado número 2, donde de acuerdo al punto de vista de Stucchi (2016), los actos desleales del trabajador en los casos de inducción a la infracción contractual, son debido a las facultades de acceso a información confidencial de empresa por parte de los trabajadores de confianza, la falta de vigilancia del empleador en la organización interna de la compañía, y el empleador es responsable de la supervisión y el control del sistema de seguridad informática, en relación con los secretos industriales y la información confidencial de la empresa.

Sin embargo, Jované (2014) difiere al sostener que el poder de vigilancia del empleador respecto a sus trabajadores se ve limitado por el derecho al secreto de las comunicaciones amparado por la Constitución Política del Perú, donde el empleador no puede invadir la esfera íntima de los trabajadores, ni acceder a sus correos personales, viéndose sus facultades de vigilancia condicionados o restringidos.

Asimismo, se aplicó la técnica de entrevista escrita a la Doctora Claudia Cotrina, y se puede apreciar que hay contrastación con el resultado N° 2, por coincidir en que los trabajadores de confianza se ven inducidos por parte de competidores desleales a incumplir con sus obligaciones contractuales pactadas con el empleador, respecto a los acuerdos de confidencialidad suscritos sobre los secretos empresariales, ante la ausencia de persecución penal del espionaje corporativo y la falta de sanciones punitivas a los agentes desleales. Además, el espionaje corporativo acarrea costos económicos al empleador, en la contrarrestación de actos de espionaje y protección de secretos empresariales e información confidencial de empresa. La falta de persecución penal, incentiva la comisión de actos de espionaje corporativo por parte de los trabajadores de confianza de las empresas y terceras

personas que actúan de manera maliciosa y desleal. Por ello, se divulga indebidamente los secretos industriales, comerciales y organizacionales a terceras personas para la obtención de una ventaja estratégica competitiva y su explotación económica. Ello afecta negativamente no solo las utilidades o el balance patrimonial del empleador, sino también el posicionamiento en el mercado y la ventaja estratégica competitiva de la empresa, con la fuga de información valiosa y confidencial.

En conclusión se acepta la hipótesis específica planteada: El espionaje corporativo incide negativamente en las obligaciones contractuales pactadas entre el empleador y el trabajador, al comprobarse que efectivamente existe inducción a la infracción contractual por parte de terceras personas hacia los trabajadores de confianza que tienen acceso a información confidencial de empresa, secretos industriales, susceptibles de explotación económica y que cuenten con una ventaja estratégica competitiva.

- c) Sobre el Objetivo Específico N°3: Determinar de qué manera el vacío del tipo penal de espionaje corporativo, exime de responsabilidad penal al trabajador espía en su condición de sujeto activo.

Como resultados tenemos que el trabajador espía se encuentra eximido de responsabilidad penal, a causa de la falta de tipificación legal de los supuestos de espionaje corporativo y la ausencia de persecución penal, teniendo como consecuencia la frecuente violación del secreto empresarial por parte de los trabajadores de confianza y terceras personas, mediante el apoderamiento del secreto de aplicación económica en el libre mercado por medios electrónicos y físicos, sin autorización del titular, para su explotación económica o su divulgación a terceras personas. Asimismo, ante la falta de fiscalización en este tipo de supuestos, el agente desleal, abusa de la buena fe contractual, en su condición de trabajador confianza en el interior de las empresas privadas, y

empieza a hacer uso de los secretos industriales e información confidencial de empresa sin autorización del titular, para obtener un beneficio económico o una ventaja estratégica competitiva, en conjunto con terceras personas.

Se aplicó el método empírico **hipotético deductivo**, a través del cual, se puede contrastar la hipótesis específica N°3: “la falta de regulación jurídica penal del espionaje corporativo exime de responsabilidad penal al trabajador espía en su condición de sujeto activo” con el resultado n°3, al apreciarse que el trabajador espía actúa arbitrariamente ante la percepción de una autoridad débil y la ausencia de una sanción punitiva en materia penal, comete actos de sabotaje empresarial por medio de espionaje, consistentes en el apoderamiento indebido del secreto empresarial por medios físicos y electrónicos y su difusión a terceras personas en perjuicio del empleador o titular agraviado.

Asimismo, conforme al expediente de Indecopi N° 035-2012/CCD, se puede apreciar que los trabajadores cometen actos desleales de espionaje en beneficio propio, para mejorar su situación laboral, gozar de mayores beneficios sociales y mejoras salariales en otras compañías, generando de esta manera un perjuicio al empleador, al tener que reestructurar parte de su logística y organización interna de la empresa, ante los actos de sabotaje empresarial del trabajador desleal en conjunto con terceras personas. Asimismo, se aplicó el método de interpretación jurídica - extensiva en el Expediente N° 035-2012/CCD-INDECOPI, donde se puede apreciar que la parte imputada por violación del secreto empresarial, actúa deslealmente y contrario a la buena fe empresarial, al sacar provecho de su condición de trabajadora de confianza y apoderase por medios físicos y electrónicos de secretos societarios, para su difusión y explotación económica en beneficio propio y de terceras personas.

Sin embargo, **la Comisión de Indecopi** en el Expediente N° 035-2012/CCD-INDECOPI, considera que el empleador no puede invadir la intimidad del trabajador ni infringir el secreto de las comunicaciones y documentos electrónicos privados, por medio de la obtención de correos electrónicos personales adjuntados por la denunciante para acreditar la violación del secreto

empresarial en materia de competencia desleal, porque se encuentra amparado por el derecho al secreto y a la inviolabilidad de las comunicaciones regulado en el numeral 10 del artículo 2 de la Constitución Política del Perú, viéndose de esta manera condicionado el poder de vigilancia del empleador, en virtud a los criterios de no injerencia y privacidad de las comunicaciones.

Se aplicó el método empírico de interpretación jurídica - extensiva y análisis documental, respecto a los aspectos teóricos contrastados con el resultado N° 3, donde Stucchi (2016) resalta principalmente la implementación de programas de cumplimiento en el interior de las empresas privadas y los acuerdos de confidencialidad estipulados en las relaciones contractuales pactadas entre el empleador y el trabajador, como mecanismos de protección de los secretos empresariales ante los ataques de espionaje corporativo, y destaca que el empleador es responsable en la gestión e implementación de medidas eficaces en su organización, en materia de vigilancia y seguridad informática. Sin embargo, Jované (2014) difiere con el punto de vista de Stucchi, al sostener que una de las limitaciones a las que se ve enfrentado el poder de dirección del empleador es precisamente cuando se ve afectada la dignidad del trabajador como persona humana. El mencionado autor destaca que la intimidad del trabajador se encuentra estrechamente ligada a la dignidad humana, en relación con los correos personales y el secreto de las comunicaciones; es decir, en la medida en que el trabajador de una empresa vea su integridad, intimidad, y pudor restringido o afectado, entonces hasta allí llega el límite al ejercicio del poder de dirección del empleador.

Se aplicó la técnica de entrevista escrita a la Doctora Claudia Cotrina, a través del cual, se puede contrastar con el resultado n° 3 obtenido, al coincidir en que la falta de fiscalización del espionaje corporativo en materia penal incentiva a que los trabajadores de confianza incumplan con sus deberes de guardar reserva con el empleador, respecto a los secretos empresariales o información confidencial de empresa que les ha sido revelados, y revelen los secretos societarios a terceras personas, sin autorización del titular o empleador. La ausencia de una

sanción punitiva en materia penal incentiva a que los trabajadores de confianza de las empresas saquen provecho de sus facultades de acceso a información confidencial y secretos empresariales, para transferir datos confidenciales por medio del correo corporativo, para divulgarlo a terceras personas. Por ello, ante los continuos avances tecnológicos y la existencia de medios telemáticos y herramientas informáticas que facilitan el modus operandi del espía infractor, se requiere reprimir punitivamente las conductas atípicas de espionaje empresarial.

En conclusión se acepta la hipótesis específica planteada: La falta de regulación jurídica penal del espionaje corporativo exime de responsabilidad penal al trabajador espía en su condición de sujeto activo, al verse posibilitado de cometer frecuentemente la violación del secreto empresarial por razón de sus facultades de acceso a información confidencial de empresa y secretos industriales, ante las bajas probabilidades de detección por parte de las autoridades, así como también la ausencia de persecución penal.

- d) Sobre el Objetivo Específico N°4: Especificar los efectos del espionaje corporativo, en los secretos empresariales de las empresas privadas fiscalizadas por la Comisión de Indecopi de Lima en el periodo 2007 – 2013.

Respecto al resultado n° 4, tenemos que el espionaje corporativo genera la pérdida del carácter reservado y exclusivo de los secretos empresariales; en segundo lugar, la pérdida de ventaja estratégica – competitiva del empleador titular de secretos empresariales, como activo para el buen posicionamiento de las marcas comerciales en el libre mercado, como consecuencia del apoderamiento indebido de secretos de aplicación económica por parte de los trabajadores de confianza y su posterior difusión a terceras personas, agentes económicos desleales y empresas competidoras. Es por ello que, el posicionamiento estratégico de la empresa en el libre mercado se ve afectada, ante la pérdida de los secretos empresariales como activos valiosos

para la obtención de ventaja estratégica competitiva, beneficios lucrativos y la competencia desleal vigorosa dentro de un determinado sector comercial.

Se aplicó el método empírico: hipotético deductivo con la hipótesis específica siguiente: la falta de regulación jurídica penal del espionaje corporativo, incide negativamente en los secretos societarios de las empresas privadas del periodo 2007 - 2013, de la ciudad de Lima en contrastación con el resultado N° 4, y se puede apreciar que, conforme al expediente de Indecopi N° 009-2011/CCD, existe una pérdida del carácter reservado y exclusivo de los secretos empresariales y la ventaja estratégica – competitiva del empleador titular de secretos empresariales, frente a los casos de espionaje corporativo y violación del secreto empresarial, porque los actos de sabotaje empresarial realizados por los trabajadores de confianza, generan un perjuicio al posicionamiento estratégico de la empresa agraviada en el libre mercado, ante el daño concurrencial por parte de los trabajadores desleales en conjunto con terceras personas de mala fe, quienes obran con animus lucrandi, realizan la explotación económica indebida de secretos empresariales obtenidos ilegítimamente y comercializan productos industriales similares a la entidad agraviada, en el mismo sector comercial.

Se aplicó el método de interpretación jurídica - extensiva en el Expediente N° 009-2011/CCD-INDECOPI, a través del cual se puede apreciar que la empresa imputada conformada por ex trabajadores de confianza, realizaron actividades atípicas de espionaje corporativo con la colaboración de trabajadores desleales de la sociedad comercial agraviada teniendo como consecuencias, en primer lugar la violación de secretos industriales (fórmulas químicas de elaboración de productos), información confidencial de la empresa (listas de clientes, proveedores, insumos) la pérdida de valor económico y estratégico de los secretos societarios, y la explotación económica de los secretos empresariales (fórmulas químicas) sin autorización del titular o agraviado.

Sin embargo, la Comisión de Indecopi en el expediente N° 009 – 2011/CCD – INDECOPI, sostiene que, conforme al derecho a la libertad de Empresa, la empresa denunciante no tiene el derecho exclusivo de desarrollar actividades económicas en el sector industrial, y la parte imputada (ex trabajadores del denunciante) puede ejercer libremente su iniciativa privada al desarrollar actividades empresariales en el mismo rubro comercial y de acuerdo a sus intereses privados en una economía social de mercado.

Se aplicó el método empírico de interpretación jurídica - extensiva y la técnica de análisis documental, respecto a los aspectos teóricos en contrastación con el resultado N° 4, de acuerdo al punto de vista de Navarro (2013), quien destaca principalmente la pérdida de ventaja estratégica competitiva por parte del empleador o titular del secreto empresarial, como consecuencia del robo de conocimiento o secreto societario de aplicación económica, frente a los actos de sabotaje empresarial por parte del espía infractor, y el posicionamiento estratégico en el libre mercado. Sin embargo, Pinto (2007) difiere, al sostener que la principal incidencia del espionaje corporativo se centra en la pérdida de valor económico del secreto industrial, susceptible de explotación económica, en un determinado rubro o sector comercial, y que genera daños concurrenciales en perjuicio del dueño o titular del secreto de aplicación económica, conforme a la libertad de empresa.

Asimismo, se aplicó la técnica de entrevista oral al Doctor Urtecho, a través del cual, se puede contrastar con el resultado n° 4 obtenido, al coincidir en que la violación del secreto empresarial en un libre mercado, ante la competencia vigorosa, genera un perjuicio al valor comercial del secreto empresarial, y afecta el flujo de riqueza o las rentas percibidas por concepto de explotación económica del secreto empresarial, ante la explotación económica indebida y sin autorización del secreto empresarial por parte de terceras personas (competidores desleales). Se produce una disminución de utilidades, a causa del espionaje corporativo lo cual puede conllevar a diversos problemas organizacionales internos dentro de la empresa, desde el desmembramiento interno, perturbación de las relaciones laborales y

comerciales a nivel organizacional por la comisión del espionaje corporativo, la extinción de vínculos de trabajo por el recorte presupuestal.

En conclusión, se acepta la hipótesis específica planteada: “el espionaje corporativo incide negativamente en los secretos empresariales de las empresas privadas del periodo 2007 – 2013, de la ciudad de Lima”, al comprobarse el agravio generado hacia el empleador o titular del secreto empresarial, cuyo negocio se ve afectado en cuanto al posicionamiento estratégico en un determinado sector comercial y a las ganancias económicas percibidas por concepto de explotación del secreto empresarial.

Respecto a la plausibilidad de las conclusiones de la presente discusión, teniendo en cuenta el conocimiento existente, existe una secuencia lógica relacionada con la temática del espionaje corporativo, al verificarse el agravio generado por el vacío del tipo penal del espionaje corporativo, en el funcionamiento interno de las empresas privadas del periodo 2007 – 2013, de la ciudad de Lima, por los daños económicos ocasionados por los agentes desleales, traducidos en gastos para contrarrestar los actos desleales, y la pérdida de ventaja estratégica – competitiva, al perder el secreto empresarial su carácter de confidencialidad, frente a la difusión a terceras personas por parte de los trabajadores de confianza.

Respecto a los hallazgos discrepantes, tenemos diversos autores que opinan por un lado que, el espionaje corporativo tiene su incidencia en la imagen y buena reputación de las empresas, y, por otro lado, opinan que el empleador no puede restringir la privacidad de sus trabajadores, conforme al secreto de las comunicaciones. Actualmente con los avances tecnológicos, el empleador tiene un poder de vigilancia que se ve restringido o limitado, por la Constitución Política del Perú.

Asimismo, se puede apreciar que existe validez interna con las variables 1 (vacío del tipo penal de espionaje corporativo) y 2 (funcionamiento interno de las empresas privadas) al existir una relación causa y efecto, respecto a la incidencia negativa del espionaje corporativo en la cadena productiva de las empresas privadas de la ciudad de Lima, del periodo 2007 – 2013, al comprobarse que existe un perjuicio en las potenciales regalías y utilidades por concepto de explotación económica de secretos empresariales, el balance patrimonial por los gastos generados en logística e infraestructura para contrarrestar los actos desleales de espionaje y el posicionamiento estratégico de las empresas privadas en un determinado sector comercial.

Los problemas surgidos fueron la determinación del costo generado por el espionaje corporativo, y la forma de reestructuración de la logística, en la organización interna de las empresas privadas, así como también las rentas y regalías dejadas de percibir por concepto de explotación económica de secretos empresariales.

Durante el estudio surgen nuevas preguntas como: ¿De qué manera el poder de vigilancia del empleador se ve restringido por el secreto de las comunicaciones? ¿De qué manera incide las nuevas tecnologías de información en el poder de vigilancia del empleador? ¿Cómo se aplicaría el test de ponderación de la pena a imponer en los supuestos de espionaje corporativo? ¿Qué circunstancias atenuantes y agravantes se aplicarían en los supuestos de espionaje corporativo?

## **VI. CONCLUSIONES:**

- 1) Globalmente, el espionaje corporativo incide negativamente en el funcionamiento interno de las empresas privadas, a causa de las conductas maliciosas y fraudulentas realizadas por parte de los trabajadores espías, empleadores y terceras personas orientadas a generar daños concurrenciales negativos a la marca

comercial, la logística empresarial y el balance patrimonial de las compañías comerciales agraviadas, y obtener beneficios lucrativos ilegítimos en función al apoderamiento y explotación económica indebida de los secretos empresariales, generando de esta manera perjuicios financieros, administrativos y organizacionales en la estructura comercial y cadena productiva de las empresas privadas.

- 2) El espionaje corporativo, acarrea potenciales pérdidas económicas en el balance patrimonial de las entidades privadas debido al robo y explotación económica de los secretos empresariales con valor comercial por parte del espía infractor para sacar un provecho económico ilegítimo a través de la comercialización de bienes y servicios en el libre mercado y su divulgación indebida a terceras personas. Asimismo, el espionaje corporativo acarrea gastos en la contrarrestación de los actos de sabotaje empresarial, la gestión de ataques de seguridad, los programas de cumplimiento para la detección de fugas de información confidencial de empresa, secretos comerciales e industriales, el fortalecimiento del sistema informático corporativo en materia de seguridad, el replanteamiento de la logística para reforzar la vigilancia interna de los trabajadores, los reajustes de presupuesto empresarial, despidos y rotación de personal.
- 3) La ausencia de fiscalización penal del espionaje corporativo genera infracciones contractuales recurrentes por parte de los trabajadores en las entidades privadas, al inducirlos al incumplimiento de sus obligaciones contractuales pactadas con el empleador, respecto al deber guardar reserva sobre la información confidencial corporativa y no divulgar los secretos organizacionales, comerciales e industriales a terceras personas. Además, los trabajadores con cargo de confianza sacan provecho de la falta de protección y blindaje informático de los datos confidenciales de la empresa; ante el descuido del empleador, apropiándose ilegítimamente y sin autorización expresa del titular, de dicha información para su posterior divulgación a terceras personas, por medio de correo corporativo, infringiendo de este modo los deberes éticos de buena fe y confidencialidad.

- 4) Los trabajadores espías quedan eximidos de responsabilidad penal, a pesar de configurarse la relación de causalidad entre el resultado dañoso generado en perjuicio del empleador o titular de los secretos empresariales e información secreta de empresa, como consecuencia de la conducta desleal y maliciosa del agente espía, al difundir los datos confidenciales corporativos a terceras personas o sacar un provecho económico indebido de los mismos, sin autorización expresa. Ante la falta de persecución penal del espionaje corporativo, los trabajadores de las entidades privadas se ven incentivados a sacar provecho de sus facultades de acceso a información confidencial de empresa, secretos comerciales e industriales, para su explotación económica o difusión a terceras personas, por medios físicos, electrónicos, soportes y ficheros informáticos, bajo la modalidad de ciberespionaje, a través del uso del correo corporativo y personal.
  
- 5) El espionaje corporativo genera la pérdida del carácter exclusivo y reservado de los secretos empresariales de las empresas privadas, como consecuencia de su explotación económica y divulgación indebida por parte de los agentes desleales y trabajadores espías hacia terceras personas, con el fin de obtener beneficios lucrativos y un mejor posicionamiento en el libre mercado. Los secretos empresariales que han sido difundidos y explotados económicamente, generan la pérdida de la atribución exclusiva del empleador o titular de los mismos, al ser comercializados en el mismo rubro de negocios por otros agentes económicos desleales y empresas competidoras. Asimismo, los conocimientos de aplicación técnica que otorgan una ventaja estratégica competitiva y facilitan el posicionamiento en el libre mercado, pierden su valor estratégico inicial al ser divulgados a terceras personas, para beneficiar ilegítimamente a otras empresas o negocios, sin autorización del titular del know how.

## VII. REFERENCIAS:

### 7.1. REFERENCIAS TEÓRICAS:

- 7.1.1. Abad, S. B. (2012). *Derecho al Secreto de las Comunicaciones. Alcances, Límites y Desarrollo Jurisprudencial*. Pensamiento Constitucional, 16 (16), 12–28.
- 7.1.2. Abanto, M. A. (1997) “*La Protección Penal de la Competencia*”, (36), 143–154.
- 7.1.3. Águila, C. y Gallardo, M., (2011). *El ABC del Derecho: Propiedad Intelectual*, EGACAL.
- 7.1.4. Abanto, M. (2006). *El Derecho Penal en una Economía de Mercado, Influencia de la Integración Económica y la Globalización*. Revista Jurídica de la Universidad Católica de Santiago de Guayaquil, (20), 101-153.
- 7.1.5. Alfaro, M. V. (2013). *El Know How y su Aplicación Práctica en el Contrato de Franquicia*. Revista Judicial, (109), 5 – 25.
- 7.1.6. Alterini, A. (1987). *Responsabilidad Civil*, Editorial Abeledo - Perrot.

- 7.1.7. Astudillo, G. (2015). *Hacia la Implementación de los Programas de Cumplimiento (compliance) en el Perú*. Temas de Derecho Penal Económico: Empresa y Compliance, (08), 234-257.
- 7.1.8. Barría, D. (2009). *El Poder de Dirección del Empresario y los Derechos Fundamentales del Trabajador*. Universidad de Chile.
- 7.1.9. Basterra, M. I. (2003) *El problema de las lagunas del derecho*. *Derecho & Sociedad*, (15), 280-291.
- 7.1.10. Benavente, H. (2012) *La Violación de Secretos de Empresa (Know How) como Modalidad de Competencia Desleal en el Perú*, 11 (15), 66-89.
- 7.1.11. Berenguer, L. (11 de abril de 2009). *Competencia en tiempos de Crisis*. [https://elpais.com/diario/2009/04/12/negocio/1239542074\\_850215.html](https://elpais.com/diario/2009/04/12/negocio/1239542074_850215.html).
- 7.1.12. Bramont, L. (1992). *Delitos Económicos y Bien Jurídico*. *Ius Et Veritas*, 3 (5), 86 – 91.
- 7.1.13. Buainain, A. y Loyola, P. (2015). *Gestión integral del Riesgo en la Agricultura*. *Mapfre*, (122), 54-63.
- 7.1.14. Bullard, A. (2012). *Comentarios a la Propuesta Metodológica Para La Determinación de MULTAS en el INDECOPI*. Bullard Falla Ezcurrea. [https://www.bullardabogados.pe/publications/wp-content/uploads/2013/02/Comentarios-BFE-a-propuesta-de-metodologia-de-multas-INDECOPI\\_16.01.13.pdf](https://www.bullardabogados.pe/publications/wp-content/uploads/2013/02/Comentarios-BFE-a-propuesta-de-metodologia-de-multas-INDECOPI_16.01.13.pdf)
- 7.1.15. Callaghan, X. (2001). *Propiedad Industrial, Teoría y Práctica*. Editorial Ramón Areces.

- 7.1.16. Chirinos, M., Fernández, L. y Sánchez, G. (2012). *Responsabilidad Empresarial o Empresas Socialmente Responsables*. Razón y Palabra, N° 81, p.1-18.
- 7.1.17. Cornejo, L. (2015). *Reglas Claras o Presunciones: El Derecho de Reserva a Razón de la Franquicia*. Pontificia Universidad Católica del Perú.
- 7.1.18. De Espona, R. J. (2017). *Consideraciones jurídicas sobre la inteligencia corporativa en el marco del sistema de seguridad nacional de España*. Revista de Pensamiento Estratégico y Seguridad CISDE, 37-44.
- 7.1.19. De Trazegnies, F. (2001). *La Responsabilidad Extracontractual*. Fondo Editorial PUCP. <http://repositorio.pucp.edu.pe/index/handle/123456789/74>
- 7.1.20. Domingo, I. (05 de mayo de 2020). *El coronavirus da alas al Ciberterrorismo para atacar Empresas y Redes Estratégicas*. Estrategias de Inversión (EI). España. <https://www.estrategiasdeinversion.com/analisis/bolsa-y-mercados/informes/el-coronavirus-da-alas-al-ciberterrorismo-para-n-447669>
- 7.1.21. Domínguez, J. (2015). *Seguridad informática Personal y Corporativa*. Universidad Politécnica Territorial del Estado Aragua.
- 7.1.22. Diario Gestión (10 de agosto del 2017). *Perú registrará US\$ 4,782 millones en pérdidas por ciberdelitos en 2017*. <https://gestion.pe/tecnologia/peru-registrara-us-4-782-millones-perdidas-ciberdelitos-2017-141411>
- 7.1.23. Diario Gestión (07 de mayo del 2018). *Perú es el Quinto País con más Alto Riesgo de Corrupción en el Mundo*. <https://gestion.pe/economia/ey-peru-quinto-pais-mas-alto-riesgo-corrupcion-mundo-233064>.

- 7.1.24. Espinoza, C. (2006). *Aspectos Contables del Contrato de Franquicia*. Actualidad Empresarial. (7). 3 – 5.
- 7.1.25. Espinoza, J. (2013). *Derecho de la Responsabilidad Civil*. Editorial Rodhas.
- 7.1.26. Espinoza, A. (2016). *Programas de Cumplimento: un Mecanismo de Autorregulación regulada para las Personas Jurídicas*. Universidad San Martín de Porres.
- 7.1.27. Estrada, A. (2015). *Dogmática Jurídica de los Delitos de Violación de Secreto Empresarial*. Universitat Pompeu Fabra.
- 7.1.28. Ferrara, F. (1929). *Teoría de las personas jurídicas*. Editorial Reus.
- 7.1.29. Fernández, R. (1996). *El Arte de la Guerra por Sun Tzu Aplicado a la Gestión Moderna de Empresas*. UCB La Paz.
- 7.1.30. Fernández, C. (2018). *La Amenaza de las Nuevas Tecnologías en los Negocios: el Ciberespionaje Empresarial*. Revista de Derecho UNED, (23), 17–52.
- 7.1.31. Fonseca, M. (2017). *La protección del secreto comercial en el contrato de franquicia internacional*. Universidad Internacional de La Rioja. <https://reunir.unir.net/bitstream/handle/123456789/6342/FONSECA%20GUERRA%2C%20MARIBEL.pdf?sequence=1&isAllowed=y>
- 7.1.32. García, P. (2016). *Las Políticas Anticorrupción en la Empresa*. Pontificia Universidad Católica de Valparaíso. (2). p. 226 – p. 228.
- 7.1.33. Gógova, S. (2015). *Inteligencia Competitiva*. Editorial Díaz de Santos. <https://corladancash.com/wp-content/uploads/2018/11/Inteligencia-competitiva-Gogova-Sonia.pdf>

- 7.1.34. Gómez, J. (1974). *El secreto industrial (Know How). concepto y protección*. Editorial Tecnos.
- 7.1.35. González, J. (1987). *Gerencia de riesgos y seguros*. Mapfre Estudios. (12). p. 35 – p.40. Madrid.
- 7.1.36. Gonzáles, J. (2011). *La competencia desleal de los empleados: responsabilidad laboral, civil y penal*. La Gaceta Jurídica. [http://www.hispacolex.com/wp-content/uploads/documents/pdf/la\\_competencia\\_desleal\\_de\\_los\\_empleados.pdf](http://www.hispacolex.com/wp-content/uploads/documents/pdf/la_competencia_desleal_de_los_empleados.pdf)
- 7.1.37. Gonzáles, M. (2014). *Fraudes en Internet y Estafa Informática*. Universidad de Oviedo. [https://digibuo.uniovi.es/dspace/bitstream/handle/10651/27824/TFM\\_Gonzalez%20Suarez,%20Marcos.pdf;jsessionid=1832ED182CB31C8988FAFEA8B087368B?sequence=3](https://digibuo.uniovi.es/dspace/bitstream/handle/10651/27824/TFM_Gonzalez%20Suarez,%20Marcos.pdf;jsessionid=1832ED182CB31C8988FAFEA8B087368B?sequence=3)
- 7.1.38. Gonzáles, D. (2014). *El riesgo y la Falta de Políticas de Seguridad Informática, una Amenaza en las Empresas Certificadas BASC*. Universidad Militar Nueva Granada. <https://repository.unimilitar.edu.co/bitstream/handle/10654/12251/ENSAYO%20FINAL.pdf;sequence=1>
- 7.1.39. Gordon, A. (07 de abril de 2020). *¿Cómo mantener una cultura de integridad durante la pandemia de COVID-19?*. [https://www.ey.com/es\\_py/forensic-integrity-services/how-to-maintain-a-culture-of-integrity-during-the-covid-19-pandemic](https://www.ey.com/es_py/forensic-integrity-services/how-to-maintain-a-culture-of-integrity-during-the-covid-19-pandemic)
- 7.1.40. Guillermo, R. Edwin, E. (14 de octubre de 2003). *El espionaje corporativo*. <https://www.gestiopolis.com/el-espionaje-corporativo/>

- 7.1.41. Gutiérrez, W. (2000). *Paciente o Consumidor. El contrato de servicio médico y la responsabilidad del médico*. PUCP.
- 7.1.42. Jakobs, G. (1997). *Derecho penal parte general: Fundamentos y teoría de la imputación*. Editorial Pons.
- 7.1.43. Jarabo, P. (08 de abril de 2015). *El Espionaje. Pasado y presente*.  
<https://apavaldeluz.files.wordpress.com/2015/05/el-espionaje-pablo-jarabodef.pdf>
- 7.1.44. Jiménez, B. Bonilla G. y Gil J. (1997). *Manual de Inteligencia Operativa Policial*. Derechos de Edición y Artes Gráficas Reservados.
- 7.1.45. Jiménez, S. (2014). *La Necesidad de Protección del Secreto Empresarial en el Mercado Interior*. Universidad de Salamanca.  
[https://gredos.usal.es/bitstream/handle/10366/125354/TFM\\_JimenezMurillo\\_Necesidad.pdf?sequence=1&isAllowed=y](https://gredos.usal.es/bitstream/handle/10366/125354/TFM_JimenezMurillo_Necesidad.pdf?sequence=1&isAllowed=y)
- 7.1.46. Jované, J. (2014). *El poder de dirección del empleador vs. el acceso de los medios tecnológicos e informáticos dentro de la empresa*, VIA IURIS, (18), 47-71. <https://www.redalyc.org/pdf/2739/273944646003.pdf>
- 7.1.47. López, R. (2009). *El delito de Espionaje Comercial: su repercusión en la pequeña y mediana empresa*. Gaceta Jurídica de Granada.  
<https://www.hispacolex.com/biblioteca/articulos-doctrinales/el-delito-de-comercial-su-repercusion-en-la-pequena-y-mediana-empresa/>
- 7.1.48. Lovejoy, K. (20 de marzo de 2020). *COVID-19: Cinco Pasos para defenderse de los Atacantes Cibernéticos Oportunistas*.  
[https://www.ey.com/es\\_cl/consulting/covid-19-steps-to-defend-against-opportunistic-cyber-attackers](https://www.ey.com/es_cl/consulting/covid-19-steps-to-defend-against-opportunistic-cyber-attackers)

- 7.1.49. Mallo, P. (2014). *Descubrimiento y Revelación de Secretos*. Universidad de Sevilla.
- 7.1.50. Massaguer, J. (2019). *De Nuevo sobre la Protección Jurídica de los Secretos Empresariales (a propósito de la ley 1/2019, de 20 de febrero, de secretos empresariales)*. Actualidad Jurídica Uría Menéndez, (51), 46 – 69.
- 7.1.51. Mercado, E. (2009). *Los Secretos Comerciales y el Know How en las Iniciativas Privadas de Inversión*. *Círculo de Derecho Administrativo*, (07), 397-406.
- 7.1.52. Mora, D. (2015). *Daniel Mora estima que habría más de 20 empresas dedicadas al espionaje industrial*. <https://gestion.pe/peru/politica/daniel-mora-estima-habria-20-empresas-dedicadas-espionaje-industrial-73416>
- 7.1.53. Molina, C. (2017). *El Poder Empresarial de Control Digital*. Universidad de Jaén. España, (3), 288-296.
- 7.1.54. Morón, E. (2002). *La Tutela Penal del Secreto de Empresa, desde una Teoría General del Bien Jurídico*, Barcelona, España, Universitat Autònoma de Barcelona.
- 7.1.55. Navarro, D. (2013). *Espionaje, Seguridad Nacional y relaciones internacionales*. Universidad del País Vasco, (14), 1-56.
- 7.1.56. Pacheco, E. (2015). *El Derecho de la Competencia en Guatemala tras la Ratificación del Acuerdo de Asociación suscrito entre la Unión Europea y Centro América*. Universidad Rafael Landívar.

- 7.1.57. Pacini, C. y Brody, R. (Abril de 2005). *Un Enfoque Proactivo para combatir el Fraude*. <https://studylib.es/doc/4851194/un-enfoque-proactivo-para-combatir-el-fraude--febrero>
- 7.1.58. Palop, F. y Vicente, J. (1999). *Vigilancia Tecnológica e Inteligencia Competitiva*. Universidad Politécnica de Valencia. [http://informecotec.es/media/15\\_Est15\\_Vig\\_Tec\\_Intelg\\_Compediti.pdf](http://informecotec.es/media/15_Est15_Vig_Tec_Intelg_Compediti.pdf)
- 7.1.59. Pinto, L. (Abril de 2007). *Espionaje Industrial*. <http://www.proyectotabano.com.mx/Reportes/Enero%202009/AIEspionajeindustrialabril-07.pdf>
- 7.1.60. Porter, M. y Kramer, M. (2006). *Estrategia y Sociedad*, Cambridge, Estados Unidos, Universidad de Harvard.
- 7.1.61. Praxedis, M. (2003). *Derecho Industrial y de la Informática*. Revista Notarial, 07 (82), 1-52.
- 7.1.62. Ramos, G. (2015). *Las Empresas Multinacionales delincuencia de cuello blanco a nivel Supranacional*. Revista de la Universidad del Zulia. 03 (06), 131-136.
- 7.1.63. Reaño, J. L. (2015) *La Utilidad de los Programas de Criminal Compliance para las Empresas que operan en Perú*. THEMIS Revista de Derecho, (68), 141-152.
- 7.1.64. Rivadeneira, M. (2010). *Los Conocimientos Técnicos Secretos y la Problemática de su Protección dentro del Régimen Jurídico Ecuatoriano*. Universidad Internacional SEK.

- 7.1.65. Rodríguez, G. M. (2014). *Dueño de tus silencios, esclavo de tus palabras: Reflexiones sobre la Protección Legal de los Secretos Comerciales*. Revista Foro Jurídico, (13), 51 – 57.
- 7.1.66. Saavedra, J. (2016). *Manual de Propiedad Intelectual y Transferencia para el Investigador*. Pontificia Universidad Católica de Valparaíso. [http://www.pucv.cl/uuaa/site/artic/20161122/asocfile/20161122160420/low\\_manual\\_investigador\\_pucv.pdf](http://www.pucv.cl/uuaa/site/artic/20161122/asocfile/20161122160420/low_manual_investigador_pucv.pdf)
- 7.1.67. Salmón, E (2012). *La Progresiva Incorporación de las Empresas Multinacionales en la Lógica de los Derechos Humanos*. PUCP.
- 7.1.68. Sanín, J. (2013). *El Secreto Empresarial: Concepto Teórico y fallas a la hora de alegar su Violación ante la Superintendencia de Industria y Comercio*. Revista de Derecho Privado. (49). 4–15.
- 7.1.69. Santiago, E. y Sánchez, J. (2017). Ciberseguridad en las Empresas. Ciencia, Tecnología y Medio Ambiente. Revista Tecnología y Desarrollo. (15). 1-33.
- 7.1.70. Stave, S. (2013) ¿Cómo el espionaje corporativo afecta el horizonte estratégico de las organizaciones, los consumidores y el mercado?”. <https://revistas.uexternado.edu.co/index.php/proyecta/article/download/3446/3170/>
- 7.1.71. Sosa, A. (2016). *Competencia Desleal y Resguardo de los Secretos*. PUCP. (68). 246 – 253.
- 7.1.72. Soto, J. (2012). *Vías de Aplicación del Derecho de la Competencia*. Universidad Autonoma de Madrid.

- 7.1.73. Stucchi, P. (30 de abril de 2016). *¿Cómo protejo mis secretos empresariales?*. <https://gestion.pe/blog/reglasdejuego/2016/04/como-protejo-mis-secretos-empresariales-2.html>
- 7.1.74. Valdés, F (2013). *Aplicación de Contra – Inteligencia Empresarial: Análisis sobre la Protección contra el Espionaje Cibernético en las Organizaciones*. Universidad de León.
- 7.1.75. Valdivia, P. (2012). *Los delitos contra los Derechos de Autor en el Perú*. Universidad Nacional Mayor de San Marcos.
- 7.1.76. Valdivia, J. (1 de Agosto de 2012). *Los empleados de confianza en la Administración Pública Peruana*. Gestión Pública y Desarrollo. [http://www2.congreso.gob.pe/sicr/cendocbib/con4\\_uibd.nsf/8224F4A8FA6EA90605257E2F0063620D/\\$FILE/revges\\_1601.pdf](http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/8224F4A8FA6EA90605257E2F0063620D/$FILE/revges_1601.pdf)
- 7.1.77. Velando, S. (06 de octubre de 2012). *Espionaje Industrial va en Aumento en Perú*. <http://commondigital.pe/index.php/locales/11354-espionaje-industrial-va-en-aumento-en-peru>
- 7.1.78. Venegas, A. (1 de Noviembre de 2016). *Espionaje Económico y Financiero como una Herramienta de la Inteligencia Estratégica, Escenarios Hipotéticos*. <https://aprenderly.com/doc/3236772/espionaje-econ%C3%B3mico-y-financiero-como-una>
- 7.1.79. Vergara, P. (2014). *Delitos Relativos a la Violación del Secreto de Empresa*, Universidad Pontificia Icai Icade.
- 7.1.80. Vilas, J (2017). *La Contrainteligencia en el sector de la Industria*. Universidad de La Rioja, (405), 133-141.

7.1.81. Villén, M. (14 de octubre de 2010). *Del hacking a la delincuencia informática actual*. <http://www5.poderjudicial.es/CVdi/TEMA08-ES.pdf>.

7.1.82. Zaffaroni, E. y Croxatto, G. (2015). *El espionaje masivo como un nuevo Crimen de Agresión*. Universidad de Buenos Aires. <http://www.derecho.uba.ar/publicaciones/pensar-en-derecho/revistas/7/el-espionaje-masivo-como-un-nuevo-crimen-de-agresion.pdf>

## 7.2. ANTECEDENTES JURÍDICOS:

- Tribunal del Indecopi (2007). Resolución recaída en el expediente N° 063-2007/CCD-INDECOPI. Foamflex S.A. contra Muebles Lot's S.A.C. 13 de junio.
- Tribunal del Indecopi (2013). Resolución recaída en el expediente N° 0297-2013/CCD-INDECOPI. Química Brisas Marinas S.A.C. contra Makaya Laboratorios S.A.C. 23 de diciembre.
- Tribunal del Indecopi (2012). Resolución recaída en el expediente N° 009-2011/CCD-INDECOPI. Branif Perú S.A.C. contra Promak Perú S.A.C. 18 de abril.
- Tribunal del Indecopi (2012). Resolución recaída en el expediente N° 035-2012/CCD-INDECOPI. Belmay S.A.C. contra Gabriela Sedano Corzo. 14 de marzo.

## 7.3. REFERENCIAS LEGALES:

- Congreso del Perú. (1991). Decreto Legislativo N° 635 – Código Penal Peruano. Diario Oficial El Peruano. Lima, Perú: Congreso de la República, 08 de abril.
- Congreso del Perú. (1984). Decreto Legislativo N° 295 – Código Civil Peruano. Diario Oficial El Peruano. Lima, Perú: Congreso de la República, 24 de julio.

- Congreso del Perú. (1993). Constitución Política del Perú de 1993. Diario Oficial El Peruano. Lima, Perú: Congreso Constituyente Democrático, 29 de diciembre.
- Congreso de España. (1995). Ley Orgánica 10/1995 - Código Penal Español. Boletín Oficial del Estado. Madrid, España: Congreso de los Diputados, 23 de noviembre.
- Congreso del Perú. (2008). Decreto Legislativo N° 1044 – Ley de Represión contra La competencia Desleal. Diario Oficial El Peruano. Lima, Perú: Congreso de la República, 25 de junio.
- Congreso del Perú. (1997). Decreto Legislativo N° 728 – Ley de Productividad y Competitividad Laboral. Diario Oficial El Peruano. Lima, Perú: Congreso de la República, 27 de marzo.
- Congreso de los Estados Unidos Mexicanos. (1991). Ley de Propiedad Industrial. Diario Oficial de la Federación. México: Congreso de la Unión, 27 de junio.
- Congreso General de los Estados Unidos Mexicanos. (2020). Ley Federal de Protección a la Propiedad Industrial. Diario Oficial de la Federación. México: Congreso de la Unión, 1 de julio.
- Congreso de España. (2010). Real Decreto 201/2010. Boletín Oficial del Estado. Madrid, España: Congreso de los Diputados, 13 de marzo.
- Comisión de la Comunidad Andina (2000). Decisión 486. Régimen Común sobre Propiedad Industrial. Lima, 14 de septiembre.

## VIII. ANEXOS:

### 8.1. ANEXO A: PROYECTO DE LEY DE ESPIONAJE CORPORATIVO

#### 8.1.1. Actores involucrados: Entidades y sujetos

INSTITUCIONES PÚBLICAS Y PRIVADAS	ROLES	ACTORES	OBJETIVOS	BENEFICIARIOS
---	-------	---------	-----------	---------------

<ul style="list-style-type: none"> <li>➤ GOBIERNOS REGIONALES</li> <li>➤ GOBIERNOS LOCALES</li> <li>➤ MINISTERIO PÚBLICO</li> <li>➤ EMPRESAS PRIVADAS</li> </ul>	<p><b>a) Fiscalía de la Nación:</b></p> <ul style="list-style-type: none"> <li>▪ Sancionar punitivamente aquellas conductas desleales, maliciosas y fraudulentas de los espías infractores en los supuestos de espionaje corporativo.</li> </ul> <p><b>b) Empleadores:</b></p> <ul style="list-style-type: none"> <li>▪ Pactar acuerdos de exclusividad respecto al uso exclusivo y explotación económica de secretos empresariales susceptibles de valorización económica.</li> <li>▪ Pactar cláusulas contractuales de la obligación de guardar reserva respecto a secretos empresariales, en acuerdos comerciales con socios y</li> </ul>	<ul style="list-style-type: none"> <li>➤ FISCALES</li> <li>➤ EMPLEADORES</li> <li>➤ TRABAJADORES DE CONFIANZA</li> <li>➤ SOCIOS COMERCIALES</li> </ul>	<p><b>1. GENERAL:</b></p> <p>Brindar Protección especial a los empleadores o titulares de secretos empresariales e información confidencial de empresa frente a los supuestos de espionaje corporativo y ciberespionaje empresarial.</p> <p><b>2. ESPECÍFICOS:</b></p> <ul style="list-style-type: none"> <li>➤ Reprimir aquellas conductas maliciosas y fraudulentas de espionaje corporativo en materia penal.</li> <li>➤ Evitar las fugas de secretos empresariales e información confidencial de empresa en los supuestos de espionaje corporativo y ciberespionaje empresarial</li> <li>➤ Sancionar punitivamente a los espías infractores, por la divulgación</li> </ul>	<ul style="list-style-type: none"> <li>➤ EMPRESARIOS</li> <li>➤ SOCIOS COMERCIALES</li> <li>➤ CIUDADANÍA EN GENERAL (CRECIMIENTO ECONÓMICO)</li> </ul>
--	--	--	--	--

	<p>contratos laborales con trabajadores de confianza</p> <p><b>c) Socios Comerciales y Trabajadores de Confianza</b></p> <ul style="list-style-type: none"> <li>▪ Cumplir con el deber de guardar reserva respecto a los secretos empresariales e información confidencial de empresa que les ha sido revelados.</li> </ul>		<p>indebida de secretos empresariales e información confidencial de empresa a terceras personas</p> <p>➤ Fiscalizar y sancionar punitivamente a los espías infractores por la explotación económica indebida y sin autorización de los secretos empresariales.</p>	
--	---	--	--	--

## 8.1.2. Capítulo I: Disposiciones Generales

### Artículo 1. Finalidad

La presente Ley tiene por objeto el velar por los empleadores, empresarios o titulares de secretos empresariales con carácter confidencial, y a tal fin, se establece la prohibición y sanción punitiva a aquellos actos de espionaje corporativo realizados por cualquier individuo en su calidad de espía infractor, quien obra con animus lucrandi, malicia e intención fraudulenta.

## **Artículo 2. Ámbito de Aplicación**

La presente ley será aplicada a aquellas conductas maliciosas o comportamientos antijurídicos de espionaje empresarial realizados por el espía infractor, que buscan generar daños concurrenciales negativos en las operaciones comerciales y administrativas de las entidades privadas y perjuicios económicos en el balance patrimonial del empleador. Asimismo, se reprimirá a aquellas conductas maliciosas orientadas a generar perjuicios financieros en los comerciantes o empresarios, a través de la apropiación ilegítima de los secretos empresariales, información secreta de empresa con valor comercial para su explotación económica indebida o divulgación a terceras personas. Además, se sancionará punitivamente aquellas conductas maliciosas del agente infractor, orientadas al apoderamiento ilegítimo de información secreta de empresa, de carácter reservado y que otorga alguna ventaja estratégica competitiva en el libre mercado.

### **8.1.3. Capítulo II: El Espionaje Corporativo**

**Artículo 3.** Se considerará como Espionaje Corporativo a aquellas conductas realizadas por cualquier individuo en su calidad de espía infractor, orientadas a la vigilancia o monitoreo ilegítimo de las actividades comerciales, laborales y administrativas de las empresas privadas para la obtención ilegítima de secretos empresariales y ventajas estratégicas competitivas en el libre mercado, realizadas a nivel interno (en el interior de las entidades) y externo (realizado clandestinamente desde otro lugar).

**Artículo 4.** Para que configure el espionaje corporativo se deberá reunir los siguientes requisitos, de acuerdo al supuesto de hecho aplicable:

- a) Debe existir una relación de causalidad entre el espía infractor o agente de espionaje y el titular de secretos empresariales, en relación con los daños económicos causados por la explotación económica ilegítima de los secretos de empresa de carácter comercial y con valor estratégico-comercial.

- b) Debe existir una relación de causalidad entre el espía infractor o agente de espionaje y el titular de secretos empresariales, en relación con los daños ocasionados de carácter no patrimonial, es decir, los disturbios, rupturas, quebrantamientos de contratos, normativas internas y los conflictos internos de intereses privados generados en el ámbito organizacional y administrativo la empresa.
- c) La Información obtenida sin autorización del titular, por el espía infractor deberá ser de carácter reservado, confidencial o en su defecto, abarcar secretos industriales, comerciales y organizacionales.

#### **8.1.4. Capítulo III: Modalidades de Espionaje Corporativo**

**Artículo 5.** El que realice actividades de inteligencia o espionaje corporativo sobre una o más entidades de manera continua con fines de obtención ilegítima de secretos comerciales, industriales y organizacionales, será reprimido con pena privativa de libertad no menor a 4 años ni mayor a 8 años, y 1360 horas de servicio comunitario.

**Artículo 6.** El individuo o agente infractor que con malicia, intención fraudulenta y animus lucrandi, induce a trabajadores de una o más entidades, a que realicen de actividades de espionaje corporativo en el interior de las empresas, será reprimido con pena privativa de libertad no menor a 3 años ni mayor a 6 años, y 991 horas de servicio comunitario.

**Artículo 7.** El trabajador que, a través de trabajo remoto o a distancia, se aproveche indebidamente del acceso al sistema informático de la entidad, para la realización de actividades de espionaje cibernético y divulgación de datos confidenciales de la empresa, será reprimido con pena privativa de libertad no menor a 2 años ni mayor a 4 años, y 580 horas de servicio comunitario.

**Artículo 8.** El individuo o espía infractor que de manera oculta, clandestina, realiza actividades de espionaje empresarial con el fin de generar daños concurrentiales

negativos en las operaciones comerciales y administrativas de una o más entidades, será reprimido con pena privativa de libertad no menor a 3 años ni mayor a 6 años.

**Artículo 9.** El trabajador o espía infractor que, realiza actos de espionaje corporativo en el interior de la empresa por medio de dispositivos electrónicos, documentos físicos y en soportes informáticos, será reprimido con pena privativa de libertad no menor a 1 años ni mayor a 3 años, y 595 horas de servicio comunitario.

#### **8.1.5. Capítulo IV: Violación del Secreto Empresarial: Secretos Industriales, Comerciales y Organizacionales**

**Artículo 9.** El individuo o espía infractor que, realice actos de apoderamiento de secretos empresariales por medios físicos y electrónicos, será reprimido con pena privativa de libertad no menor a 4 años y no mayor a 6 años.

**Artículo 10.** El trabajador o espía infractor que, a través de trabajo remoto o a distancia, realiza actos de apoderamiento u obtención ilegítima de secretos comerciales, industriales u organizacionales, será reprimido con pena privativa de libertad no menor a 4 años ni mayor a 7 años.

**Artículo 11.** El individuo o espía infractor que colabora en conjunto con terceras personas, para la divulgación y explotación económica de secretos empresariales robados u obtenidos ilegítimamente, sera reprimido con pena privativa de libertad no menor a 3 años y no mayor a 5 años.

**Artículo 12.** El espía infractor que, en concurso con terceras personas, se presta a colaborar en actos de espionaje o inteligencia, para el apoderamiento de secretos comerciales, industriales y organizacionales será reprimido con pena privativa de libertad no menor a 1 año y ni mayor a 3 años.

**Artículo 13.** El que realice actos de explotación económica del secreto empresarial a través de la comercialización de productos y servicios sin autorización del titular del mismo, será reprimido con pena privativa de libertad no menor a 3 años ni mayor a 5 años.

**Artículo 14.** El agente o espía infractor que induce con malicia e intención fraudulenta a otro individuo, al incumplimiento del deber de guardar reserva respecto

a secretos industriales, comerciales y organizacionales, será reprimido con pena privativa de libertad no menor a 2 años ni mayor a 4 años, más 480 horas de servicio comunitario.

**Artículo 15.** El agente o espía infractor que, accede a los archivos confidenciales empresariales contenidos en soportes informáticos sin autorización del titular, será reprimido con pena privativa de libertad no menor a 1 año ni mayor a 3 años.

#### **8.1.6. Capítulo V: Circunstancias agravantes de responsabilidad Penal**

##### **Artículo 16.**

Son circunstancias consideradas como agravantes las siguientes:

- a) Hacer uso de la violencia física y psicológica para la comisión del espionaje corporativo
- b) Realizar actos espionaje corporativo o inteligencia constituyendo una organización criminal o en conjunto con varias personas.
- c) Tener establecida una infraestructura tecnológica utilizada exclusivamente para la comisión de actos de espionaje corporativo.
- d) Realizar actividades de espionaje corporativo de forma frecuente y continua en el tiempo.
- e) Realizar actos de espionaje corporativo con alevosía