RESPONSABILIDAD DEL EMPRESARIO POR EL USO DE LA TECNOLOGÍA

Por: Daniel Peña Valenzuela[1]

Introducción

Es para mí un honor presentar esta ponencia en el XXXI Congreso Nacional de Derecho Comercial, evento de particular prestigio por la novedad temática, por las cualidades y la trayectoria profesional de mis colegas conferencistas y por la audiencia calificada que nos acompaña. Mi agradecimiento por la invitación a la Cámara de Comercio de Medellín para Antioquía, el Colegio de Abogados de Medellín y la Universidad Externado de Colombia por la invitación. Resalto la perseverancia de más de tres décadas de los organizadores en la búsqueda permanente de excelencia.

El tema que me corresponde tiene como escenario privilegiado a la muy admirada Capital de la Montaña, pues sin lugar a dudas, Medellín está construyendo y liderando a escala nacional la visión y la realidad, sin mayor emulación, como ciudad del conocimiento, digital e inteligente. Este ejemplo debe ser seguido

---

1 Abogado y Profesor Titular de la Universidad Externado en las Facultades de Derecho y Finanzas, y Relaciones Internacionales en pregrado y posgrado. LLM (Máster en Leyes) de la Universidad de Londres. DESS (Máster en Propiedad Intelectual, Contratos Industriales y Derecho de las Nuevas Tecnologías, Université Grenoble II). Árbitro de la Cámara de Comercio de Bogotá (lista A) y de la Organización Mundial de la Propiedad Intelectual. Socio Fundador de la firma Peña Mancero Abogados.

por otras ciudades y regiones, lo que ojalá redunde en un resultado conjunto de Colombia como un país más innovador, creativo y dispuesto a arriesgar en capital (privado y público) y trabajo para construir un entorno ávido de convertir la información en conocimiento, el saber en innovación y cambiar el futuro de las próximas generaciones.

Para iniciar, permítanme tomar las ideas planteadas por el periodista Andrés Oppenheimer en su reciente libro *Crear o Morir*[2], en el cual propone como las cinco grandes claves para impulsar la cultura de la innovación en América Latina: reorientar la educación a ese fin, modificar las leyes que la inhiben, estimular la inversión en innovación, y por último, globalizar las ideas, las creaciones y las invenciones. Todo lo anterior, dejando de lado el miedo y la estigmatización al fracaso de los emprendedores.

Las empresas colombianas están avanzando de manera paulatina en la incorporación de la tecnología en sus procesos productivos y en la utilización de las TIC como herramienta de desarrollo empresarial. Para alcanzar mayores tasas de crecimiento económico, Colombia y sus empresas deben acelerar ese proceso de transformación productiva, diversificar su base de productos para exportar y llevar a cabo un proceso de cambio estructural, o de nueva política industrial que traiga consigo el aumento de la productividad de la economía y un impulso a la innovación. En los indicadores internacionales de competitividad, Colombia no avanza de manera significativa, por el contrario, lleva varios años estancada en las mismas posiciones. En el Índice Global de Competitividad que mide el Foro Económico Mundial, no se ha experimentado un cambio significativo. En el informe "Doing Business" del Banco Mundial, pese a que Colombia se ubica entre los países del mundo que más reformas hicieron en los últimos años, su desempeño en algunos indicadores es pobre.

La innovación empresarial se expresa de varias maneras:

- En la gestión tecnológica de recursos propios o de terceros, enfocados en la invención y el desarrollo de nuevos productos y servicios, así como en la manera de hacer empresa generando nuevos modelos de negocios y arriesgando tiempo y capital en ciencia y tecnología (CyT).

2 Oppenheimer, A. (2015). *Crear o morir*. Madrid: Editorial Debate.

- En el análisis costo/beneficio de la inversión o reinversión de recursos debe primar la asunción de riesgos derivados del uso de una tecnología determinada respecto de la imitación o copia de modelos o productos ya existentes.
- La creación de tecnología propia mediante procesos de ciencia, tecnología, investigación y desarrollo, la transferencia o la recepción de conocimientos técnicos, la utilización de TIC son un imperativo para las empresas colombianas, pero cualquier uso de tecnología genera riesgos que deben ser prevenidos, detectados, analizados y en la medida de los posible, mitigados. La existencia de riesgos tecnológicos sin que se puedan mitigar o medir de manera adecuada causa retraso en la adopción de la tecnología o puede ser fuente de reclamos, acciones judiciales y potencial infracción de derechos de terceros.
- La mitigación de las causas y de los posibles costos para prevenir o asumir una eventual responsabilidad deben ser parte de las políticas, prácticas y planes estratégicos corporativos y del análisis de costos asociados al desarrollo de nuevos productos y servicios.
- La definición correcta del grado de responsabilidad de los administradores puede ser un incentivo para asumir determinados riesgos y en últimas acelerar la adopción de nuevas tecnologías en el ámbito empresarial, favoreciendo la competitividad y la productividad.

En este escrito se abordan los supuestos de la responsabilidad empresarial en la era digital, de la innovación y de la tecnología, y las fuentes específicas de esa potencial responsabilidad. Se toma como base el hecho de que los administradores tienen deberes generales y específicos, así como un rol fundamental de liderazgo en diseño, planeación y cumplimiento legal asociado a las estrategias de TIC, innovación, protección de la propiedad intelectual, ciencia, investigación y tecnología al interior de las empresas. Se analiza el papel de los nuevos cargos que se deben crear en las entidades para tal efecto, como los Gerentes de Innovación y Desarrollo, Jefes de Seguridad Informática, Vicepresidentes de Información y Tecnología, entre otros. Además de los deberes propios de sus cargos, estas actividades pueden originar responsabilidad legal frente a la empresa, los terceros, los reguladores y las autoridades. En los últimos dos eventos, en caso

de incumplimiento de obligaciones establecidas por la regulación o por las leyes. Finalmente se abordarán tópicos especiales de responsabilidad por el uso de la tecnología en el ámbito empresarial y la definición del grado de responsabilidad en uso de la tecnología.

1. Supuestos de la responsabilidad empresarial en la era tecnológica

La relación entre las empresas y la tecnología ha cambiado en las últimas décadas de manera dramática, como consecuencia de un incremento notable en el uso de las Tecnologías de la Información y las Comunicaciones (TIC) en los modelos de negocios de las empresas "Internet", y como nuevo canal para las actividades mercantiles de las empresas tradicionales. Las grandes y medianas empresas han venido incorporado, de manera paulatina, sistemas de información como redes y aplicaciones móviles corporativos para sus equipos de trabajo, ERP (Enterprise Resource Planning), CRM (Costumer Resources Management), platafomas y aplicaciones integradas de computación en la nube, y en general, soluciones tecnológicas para sus procesos internos como manejo de personal, análisis de información, contabilidad, inventarios, entre otros; y también para la relación con proveedores, distribuidores y clientes. Esos sistemas de información incorporan el licenciamiento de programas de ordenador, la integración de bases de datos y aplicaciones móviles, y almacenamiento de información en la nube. Así mismo, el uso y el aprovechamiento de internet, páginas web y redes sociales para difundir información empresarial y realizar actividades de publicidad y mercadeo digital, lo que se ha convertido en una necesidad para consolidar y ampliar mercados y como respuesta al cambio generacional con nuevos consumidores, en su mayoría nativos digitales. La masificación en el uso de toda clase de TIC debe beneficiar, de manera preponderante, a las pymes que pueden obtener frutos más significativos de la revolución digital por la disminución de costos en la adquisición de equipos, soluciones y herramientas informáticas. Las Pymes tienen acceso a TIC que hasta hace poco se limitaban a las grandes y medianas con el apoyo del gobierno; Mediante programas de cooperación o con sus propios recursos y propósitos de innovación también incorporan de manera paulatina los recursos TIC.

Según Confecámaras, los obstáculos que deben ser superados por la industria colombiana incluyen "bajos niveles de innovación y emprendimiento y se ha trabajado para lograr mejorar esos indicadores, las cámaras de comercio, como actores del Sistema Nacional de Competitividad e Innovación, trabajan integralmente con instituciones públicas y privadas, precisamente con programas y proyectos que buscan generar espacios que dinamicen la innovación en el país. Actualmente, las cámaras cuentan con 46 programas de cultura y gestión de innovación que han llegado a más de 14.700 beneficiarios. Asimismo, la Red de Cámaras de Comercio trabaja en alianza con la Superintendencia de Industria y Comercio, en procesos de capacitación en temas de propiedad intelectual"[3]. La ANDI coincide en que los temas que abarca la agenda industrial deben incluir "una estrategia de ciencia, tecnología, innovación y emprendimiento, políticas y programas para atraer inversión y lograr la transferencia de tecnología"[4].

Más allá de herramientas y soluciones informáticas, los avances en las TIC han puesto a la información en el centro de la generación de valor, no solamente para las empresas del sector de comunicaciones sino también para las organizaciones que entienden que la información es base de la innovación, del mejor servicio al cliente, de la adquisición de nuevos mercados, desmaterialización de sus productos y servicios, de la internacionalización y de la optimización de sus procesos. La información en sus diversas facetas con valor comercial, en ocasiones secretos empresariales o comerciales, la información técnica y científica patentada, y los datos personales.

También se evidencia como resultado de la influencia determinante de las TIC, la electronificación del derecho mercantil, (para utilizar la original expresión del profesor Rafael Illescas[5]), que en Colombia se aprecia con la utilización y reconocimiento jurídico de las comunicaciones electrónicas en el ámbito empresarial, incluyendo la celebración de los contratos electrónicos, la validez de la

3 Domínguez, Julián. La dinámica de la industria colombiana y sus desafíos en Revista Doing Business, n.° 81, septiembre del 2014.

4 Mac master, Bruce. Trabajo Conjunto para impulsar la Industria en el país, n.° 81, septiembre del 2014.

5 Illescas, Rafael. La electrónificación del derecho de sociedades mercantiles, en particular de los derechos del socio y los órganos sociales, en Memorias del III Congreso Internacional de Derecho Comercial. Colegio de Abogados Comercialistas y Cámara de Comercio de Bogotá, 2013.

firma electronica y de la firma digital, la desmaterialización de los títulos valores y de los documentos transferibles y la posibilidad de utilizar medios electrónicos para llevar a cabo las asambleas, juntas y consejos directivos, así como la posibilidad de llevar los libros de comercio y registrarlos ante las cámaras de comercio por medios electrónicos, entre otros.

Como consecuencia de la utilización masificada de las TIC, en el interior de las empresas surgen interrogantes respecto de (i) el alcance de la responsabilidad de las empresas en internet y de las empresas tradicionales que utilizan los medios electrónicos como nuevo canal de comunicación y transaccional con los usuarios y consumidores, (ii) la responsabilidad en cabeza de los sujetos tradicionales que integran las organizaciones, en particular las responsabilidades de los administradores de las compañías y de los empleados, (iii) las responsabilidades asignadas a los nuevos roles y cargos que surgen en las empresas como los de CIO (Chief Information Officer), CISO (Chief Information Security Officer), CTO (Chief Technology Officer), de los Webmaster y de los Community Manager, y que tienen bajo su control el contenido de páginas web corporativas, los perfiles de redes sociales y la estrategia del manejo de la información digital, (iv) la variedad de los tópicos y materias específicas de tecnología utilizadas en las empresas que pueden generar diversos riesgos y causas de responsabilidad.

1.1 La aparición de tecnologías emergentes para uso empresarial

Hasta hace poco, las tecnologías que se utilizaban al interior de las empresas estaban confinadas a un número reducido, el licenciamiento de los programas de computador y en algunos casos, bases de datos con información sobre empleados, clientes y proveedores. El inventario de TIC en el ámbito empresarial ha aumentado la lista de una manera significativa para incluir, entre otras, a tecnologías emergentes, por ejemplo, las siguientes:

1. Páginas web corporativas
2. Nombres de dominio de internet y direcciones IP
3. Internet y comercio electrónico
4. Desmaterialización documental, comunicaciones electrónicas, mensajes de datos y documentos electrónicos (pagarés y facturas electrónicas)

5. Redes sociales con perfiles comerciales
6. Tecnologías vestibles
7. Tecnologías y aplicaciones móviles
8. Analítica de grandes volumenes de datos (*Big Data*)
9. Mercadeo y publicidad digital (*eMarketing*)
10. Posicionamiento reputacional (SEO) y marcario en línea (*eBranding*) en buscadores de internet
11. Computación en la nube
12. Virtualización
13. Robótica, impresoras 3D, drones, videovigilancia e Inteligencia Artificial

Todas estas nuevas tecnologías, TIC, se utilizan cada vez con más frecuencia en las empresas, ya sea adaptándolas a modelos de negocios específicos de empresas digitales, también, a las empresas tradicionales donde exploran, investigan, prueban e incorporan a sus procesos productivos, de mercadeo, promoción y logísticos las tecnologías emergentes.

Muchas de estas nuevas tecnologías no tienen regulación legal en cuanto a su explotación y uso comercial, con lo cual se generan inquietudes y obstáculos prácticos, así como costos de transacción para su utilización debido a la incertidumbre sobre las bases y límites a la responsabilidad legal que puede traer consigo su utilización.

La historia demuestra que la mayoría de tecnologías emergentes surge con propósitos de experimentación, académicos y militares, pero pronto comienza su explotación comercial, con el fin de lograr mayor eficiencia en los procesos comerciales e industriales[6].

La revolución informática surge como consecuencia, entre otras, de la masificación comercial del *software*. Luego con la telemática y las comunicaciones surge la revolución de Internet y el comercio electrónico. Internet da lugar a nuevos cambios y progresos como el Internet social con la Web 2.0 y las redes sociales que permiten una interactividad global de miles de millones de usuarios. Ahora se

6 Ceruzzi, Paul. A History of Modern Computing, Mit Press, Boston, 2003.

anticipa que el Internet de las cosas, la robótica y la inteligencia industrial pueden introducir una nueva revolución industrial en la cual la producción a la medida, la aparición de nuevos materiales y la masificación de las impresoras 3D puede cambiar los factores y variables tradicionales de la producción industrial[7].

1.2 *Nuevos roles y cargos relacionados con las TIC al interior de las empresas*

La revolución TIC es individual y empresarial. La cultura digital propicia la aparición de usuarios generadores de contenidos, cada uno de nosotros acumula la condición de consumidor digital, usuario de servicios TIC y ciudadano digital. Esas tres dimensiones individuales son distintas en el primer mundo y en los países emergentes por las condiciones de acceso a la red y de alfabetización digital. La otra faceta de la revolución TIC es la empresarial, fruto de la relevancia de los sistemas de información al interior de las empresas, así como de la especialización y sofisticación de las funciones que cumplen los mismos la cual ha obligado a las empresas a reorientar su visión respecto de la gestión, manejo y administración interna de las TIC y de la información. Las empresas, usualmente, tienen dos opciones: a) ampliar sus departamentos (interno de sistemas y TIC) vinculando a expertos en internet, redes sociales y en soluciones informáticas, y capacitar o profesionalizar en las tecnologías emergentes a los recursos humanos bajo el control de la vicepresidencia de tecnologia, y b) contratar la tercerización de servicios informáticos con proveedores mediante contratos de *outsourcing* y acuerdos de niveles de servicios (SLA). Ambos modelos pueden dar lugar a responsabilidad, no por el hecho de que se encargue a terceros el procesamiento de la información o la propiedad de los equipos una empresa transfiere la responsabilidad. De hecho, es relevante la manera cómo se establecen, en los contratos de *outsourcing,* las cláusulas de confidencialidad, los niveles de seguridad y servicios y la responsabilidad en caso de eventos que afecten la integridad y seguridad de la información. En el caso de los datos personales, de manera expresa se establecen en la ley 1.581 del 2012, los deberes de los responsables y encargados del tratamiento de la información personal con el fin de que se no diluyan las cargas y las obligaciones de cada uno de ellos. En el caso de los productos

7 Anderson, Chris. Makers The New Industrial Revolution, Crown Business, Nueva York, 2012.

o servicios digitales no se debe dejar de lado que la responsabilidad entre productor y distribuidor frente al consumidor, la novedad del formato no afecta la regla general de solidaridad.

Uno de los desarrollos más interesantes, y a la vez más preocupantes, en el entorno empresarial es el hecho de que la revolución digital propicia que los usuarios de tecnologías sean generadores de contenidos. Esta vocación creadora de los empleados coincide con la entrada en el mundo laboral de la generación del milenio, es decir, jóvenes nativos digitales de la era tecnológica que comienzan a ingresar a las empresas como nueva fuerza de trabajo. Esta tendencia de usuarios creativos agrega nuevos temas jurídicos a los tradicionales, los cuales partían del papel del empleado como usuario pasivo de tecnología con relevancia del monitoreo en las empresas de herramientas como el correo electrónico y la navegación de la red global, durante las horas laborables. Las actividades de los empleados (ahora también usuarios generadores de contenidos) en redes sociales que presentan opiniones, revelan información propia y de la compañia, interactúan con otros empleados mediante las redes sociales pueden generar responsabilidad para la empresa por infracción a los derechos de terceros o de la propia empresa respecto a contenidos digitales y que puedan afectar la reputación corporativa a escala global y en tiempo real[8].

Además de los ingenieros de sistemas que tradicionalmente controlaban el funcionamiento cotidiano de los sistemas de información, realizaban labores de mantenimiento, atención al usuario (help desk) y almacenamiento de copias de seguridad (backup), diversas profesiones y oficios irrumpen en el ámbito empresarial con múltiples capacidades como el diseño de contenidos digitales, la programación de aplicaciones, el mercadeo y la publicidad digital, la comunicación de mensajes en el ecosistema digital, análisis de grandes volúmenes de datos y periodismo por medios electrónicos, blogueros, e incluso, psicología del consumidor en línea.

Desde el punto de vista jerárquico, el principal rol en la cúspide de la estrategia de la información en una empresa lo cumple el Chief Information Officer

8 Rallo Artemi y Martínez Ricard. Derecho y Redes Sociales, Civitas Thomson Reuters, Madrid, 2013.

CIO[9], quien es el encargado a nivel directivo de la planificación de la estrategia respecto de la gestión y valor agregado que debe generar la información para una organización. La gestión, el tratamiento y la administración de la información incluye de manera preponderante la determinación y la valoración de los riesgos y las políticas de mitigación de estos, así como las directrices en seguridad informática. Entre las principales cualidades o habilidades que debe tener un CIO se encuentran: a) la orientación de la relación de la tecnología con los negocios, b) determinar y encaminar los beneficios de la tecnología de la información hacia los problemas y retos del modelo de negocio de la empresa, c) identificar y evaluar las nuevas tecnologías que sean beneficiosas para el negocio, d) capacitación en seguridad informática, administración de costos y riesgos, e) facilidad para comunicarse y entenderse con clientes internos que no sean técnicos y f) la habilidad para traducir al lenguaje gerencial la terminología técnica.

La visión estratégica se construye a partir de una clasificación o segmentación de la información que permita determinar su valor comercial, y también para el modelo de negocio específico, el ciclo de vida de la información entre su recolección y tratamiento final, la explotación de los resultados y su almacenamiento por el tiempo que sea adecuado. Desde el punto de vista legal, esta clasificación del valor de la información debe tener como base la definición de si se trata de una información confidencial, pública, comercial o personal (datos personales públicos, semiprivados, privados, sensibles), así como del régimen legal que abarca a la información respectiva, el cual define los deberes legales y tecnológicos en cuanto a su reserva, acceso, tratamiento, actualización y transferencia a terceros (dentro y fuera del territorio nacional).

Otro rol que ha aparecido con el uso de las TIC en la empresas es el web master, quien es la persona responsable del mantenimiento y la programación de un sitio web, entre otros de los contenidos de la página, y de la operatividad, programación y mantenimiento de la disponibilidad de la información, y si es el caso, de las transacciones electrónicas. El web master tiene a su cargo clasificar y determinar, de acuerdo con las politicas de la empresa, la información que se va a publicar en la página web, y tener certeza de la titularidad de derechos de la empresa sobre los contenidos digitales para evitar reclamos posteriores de los

9 También denominado CTO Chief Technology Officer con alcance más amplio

empleados o terceros. También debe tener a su cuidado la actualización de la información para que no se afecte la integridad o actualidad de los datos.

También aparece el community manager[10], quien es la persona encargada de gestionar, construir y moderar a los usuarios de las redes sociales y las comunidades virtuales en torno a una empresa. Este cargo tiene un perfil dentro de las empresas que pretenden obtener reconocimiento y reputación con base en las conversaciones sociales y la comunicación con los consumidores, usuarios y seguidores en línea. A nivel micro, es el encargado de manera dinámica de generar los contenidos de las redes sociales y de que la estrategia digital corresponda a los mensajes de publicidad, imagen corporativa y valores empresariales, y que permita una coherencia entre los contenidos móviles en las distintas plataformas, así como evitar que la información pueda afectar la imagen, buen nombre y reputación de terceros. Tiene el papel de observar a la competencia, generar publicidad a favor de las marcas propias, pero sin generar competencia desleal o infracciones marcarias.

Las funciones específicas de cada uno de estos cargos debe estar definida en los documentos de estrategia y política que se defina por el CIO, el manual de funciones y en el organigrama de la empresa para definir sus actividades, sus deberes, limitaciones en con base en lo anterior el grado de responsabilidad como garantes de la integridad y autenticidad de la información empresarial.

1.3 *La innovación, la ciencia aplicada y la transferencia de tecnología*

La innovación es la base de nuevos productos y procedimientos que optimicen los procesos industriales, disminuyan costos y habiliten la entrada a mercados diferentes de los tradicionales, incluyendo mercados internacionales. Para lograr innovar se debe contar con la voluntad política al más alto nivel de la empresa para transformar la manera de percibir un negocio e incorporar una visión a largo plazo.

La planeación de procesos de innovación requiere un conocimiento del *estado de la técnica y vigilancia* de las tecnologías utilizadas en un determinado sector o ramo industrial o comercial, la contratación de vigilancia tecnológica,

10 La integración de medios digitales, redes sociales y aplicaciones móviles ha modificado y ampliado el rol del community manager para nominarlo como Digital Strategist o Estratega digital.

asistencia a ferias nacionales e internacionales, contratación de expertos o conocedores que puedan generar informes sobre la tecnología puede ser objeto de investigación o adoptarse, entre otras.

El proceso de desarrollo de una tecnología propia acarrea costos que se deben sopesar en cuanto a la inversión y a la tasa de retorno a mediano y largo plazo. De manera inmediata se debe evaluar si las tecnologías que se van a investigar y desarrollar serán novedosas y originales, y por ende, susceptibles de apropiación y protección por derechos de propiedad intelectual e industrial. Así mismo, si el riesgo de infringir derechos de terceros es por lo menos mínimo o inexistente.

Al definir la política de ciencia e innovación al interior de una empresa se debe definir que todo el personal involucrado ceda los derechos de autor y de propiedad industrial sobre los desarrollos e inventos a favor de la entidad con el fin de que los resultados obtenidos le pertenezcan.

En caso de que la innovación por medios propios sea imposible, se puede acudir a la transferencia tecnológica de terceros, para lo cual se debe hacer un estudio pormenorizado de la capacidad y trayectoria del socio tecnológico del que se va a recibir el conocimiento. Así mismo, evaluar la tecnología que se va a recibir desde la óptica de su protección nacional e internacional, así como de la adecuación de la misma para los propósitos de la empresa receptora. Es recomendable que se utilicen documentos y contratos para definir la modalidad de transferencia de tecnología, las tecnologías involucradas, los derechos y los deberes de las partes, las prohibiciones y las restricciones de uso, la posible exclusividad territorial, la responsabilidad en caso de infracción a los derechos de terceros, la ley aplicable, los métodos de resolución de controversias, entre otras.

1.4 *Los modelos de negocio como estándar de la responsabilidad de la empresa*

La responsabilidad de la empresa en relación con la tecnología depende de su objeto social y de las actividades principales y secundarias que lleve a cabo. En este sentido, las empresas se pueden clasificar en:

1. Empresas que prestan servicios de TIC, como por ejemplo, los prestadores de servicios de internet que permiten el acceso, el *hosting* o la publicación de información o los proveedores de pagos y facturación electrónica.

2. Empresas tradicionales con canales de comercialización o publicidad de sus productos y servicios por medios electrónicos.

3. Empresas digitales o 'de internet' con modelos de negocio electrónico propios de la economía digital, dirigidos al consumidor (B2C) o entre consumidores (C2C), como tiendas virtuales de bienes intangibles, por ejemplo música digital, libros electrónicos, agencias de publicidad digital, buscadores de internet, agregadores de contenidos digitales, portales de intercambio de bienes y servicios, martillos en línea y plataformas o pasarelas de pago.

4. Empresas que participan en esquemas de financiamiento de emprendimiento o de instrumentos de cofinanciación y empresas vehículo de proyectos de aceleración de empresas[11].

5. Centros de investigación tecnológica, *clusters* y esquemas de trabajo creativo o de investigación compartida.

La responsabilidad de los administradores y empleados en cada uno de los tipos de empresas reseñados depende de los siguientes factores:

1. La regulación general de las TIC. En Colombia, la ley 1.341 del 2009 establece la intervención del Estado en las actividades y el sector TIC con habilitación general para la prestación de servicios de TIC con la obligación de registrarse ante el Ministerio de las Tecnologías de la Información, MinTICs, y el pago de una contraprestación al Fondo MinTIC. Estas normas configuran los deberes y las obligaciones de las empresas que son proveedores de servicios y redes TIC como servicios públicos a cargo del estado, pero que pueden ser prestados por particulares.

2. Las reglas generales aplicables de manera transversal a las actividades mercantiles que se pueden aplicar por analogía a los bienes inmateriales, como pueden ser la protección de datos personales, normas de competencia aplicadas a los mercados digitales, derechos de autor en la era digital, nombre y enseña comercial, y nombres de dominio de internet. Estas normas tradicionales permiten la determinación del régimen de propiedad y explotación de bienes inmateriales.

11 El Ministerio de Comercio Industria y Turismo ha creado el programa INNpulsa Colombia para incentivar desde el Estado el ecosistema de emprendimiento e innovación.

3. Leyes y reglamentos aplicables al entorno digital y a la equivalencia de funciones y efectos jurídicos como la ley 527 de 1999, la cual se aplica a la prueba digital, a las actividades de comercio electrónico y los contratos electrónicos, las entidades de certificación digital, entre otras. Estas normas han sido introducidas en el ordenamiento jurídico colombiano (y casi en todos los países del mundo) con el fin de responder a la primera etapa de utilización de medios electrónicos para actividades con relevancia mercantil. Por ejemplo, en relación con la responsabilidad se pueden resaltar los deberes y las obligaciones de los suscriptores de certificados digitales en cuanto a la diligencia y cuidado, respecto de las claves privadas así como la información que deben entregar sobre cualquier cambio a las entidades de certificación. Así mismo, los deberes y las responsabilidades en cuanto a Políticas de Certificación para entidades certificadoras y el cumplimiento de los requisitos de acreditación.

4. Regulaciones específicas de internet para los proveedores de servicios de internet como las relacionadas con los derechos de los usuarios en los contratos de acceso, los estándares de las tecnologías de acceso como la banda ancha, deberes en cuanto a la no discriminación de contenidos y neutralidad en la red, la lucha universal contra la pornografía infantil, la defensa contra la piratería o infracción de derechos de propiedad intelectual[12]o la retención de información de los usuarios sobre el tráfico en la red.

5. Regulaciones sectoriales de actividades específicas cuando se llevan a cabo utilizando canales digitales como la banca electrónica, la television digital, IPTV, juegos de azar, actividades profesionales, ventas de medicamentos en cuanto a estándares de seguridad informática o límites en la prestación de ciertos servicios.

6. Normas sobre protección de la propiedad intelectual, derechos de autor y propiedad industrial.

7. Regulación de transferencia tecnológica, *know how*, asistencia técnica y servicios técnicos de reparación y mantenimiento.

12 Peña Valenzuela, Daniel. Responsabilidad de los Proveedores del Servicio de Internet en relación con la Propiedad Intelectual, Universidad Externado de Colombia, Bogotá, 2013

1.5 *El diseño e implementación de la estrategia digital en una empresa debe estar a cargo de los administradores*

La estrategia o agenda digital bajo la planificación del CIO y con la responsabilidad de ejecución por el web master, el community manager o el estratega digital debe ser parte del plan de acción de las empresas de cualquier tamaño: grande, mediana o pyme que pretenda a) competir en el Mercado de manera adecuada, b) implementar la gestión de innovación, ciencia y tecnología, c) ingresar en nuevos mercados aprovechando la eliminación o disminución de las barreras, d) entrar en un proceso de internacionalización y e) insertarse en la economía digital y en la sociedad de la información para aprovechar la globalización en ciernes.

El contenido y el plan de acción de las estrategias digitales empresariales incluye actividades como las siguientes:

1. La presentación de la empresa en páginas web y redes sociales

2. La desmaterialización documental y de procesos internos y externos

3. La utilización de medios electrónicos para publicitar sus productos y servicios.

4. La utilización de comunicaciones electrónicas para las comunicaciones internas y externas de la empresa.

5. El uso del canal de comercio electrónico para la comercialización de productos y servicios.

6. El uso de las redes sociales como Twitter, Facebook, Linkedin, YouTube, Instagram para expresar opiniones, publicación electrónica de videos institucionales, eventos corporativos y fotografías digitales, para mercadeo de productos, para comunicados a los clientes.

7. Almacenamiento de información en la nube.

8. Analítica de la información recaudada en medios digitales sobre clientes y consumidores.

9. La utilización de aplicaciones móviles para presentar funcionalidades a los clientes y consumidores.

El diseño, la planeación y la puesta en funcionamiento de las estrategias digitales hacen parte de las actividades bajo el control y la responsabilidad de las juntas directivas, los administradores y el CIO por la importancia estratégica y comercial de la información y por los riesgos que traen consigo para la reputación y para el desempeño operativo de las empresas.

Los principales riesgos para las empresas con la digitalización de sus actividades y la desmaterialización de documentos y los procesos son:

1. La pérdida de acceso y la disponibilidad a la información corporativa.

2. La repudiación por los destinatarios a las comunicaciones electrónicas y mensajes de datos enviadas por la empresa a terceros.

3. La aplicación por analogía de normas o regulaciones tradicionales a las actividades por medios electrónicos.

4. La afectación a derechos fundamentales de terceros como la intimidad, la protección de datos personales, la libre expresión y el libre desarrollo de la personalidad.

5. El ejercicio por los consumidores en línea de los nuevos derechos como el derecho de información reforzada, el derecho de retracto y la reversion de pagos, en los cuales cuentan con gran discrecionalidad para invocarlos por el mero rechazo a los productos o servicios.

6. Incurrir en sanciones administrativas por falta de cumplimiento de regulaciones.

7. La violación de normas sobre secretos empresariales, propiedad industrial e intelectual, competencia desleal o abuso de posición dominante.

8. La violación de *covenants* y compromisos contractuales contraídos con terceros.

9. La dificultad en determinar correctamente la identidad digital de los consumidores y contratantes por ser relaciones en ausencia y a distancia.

10. Falta de integridad y autenticidad en las comunicaciones electrónicas

11. Incertidumbre sobre el régimen de responsabilidad aplicable a la empresa y sus funcionarios en la era digital.

12. La inseguridad informática, los incidentes y los ataques cibernéticos.

13. Atentados a la integridad de los negocios, fraude informático, injuria y calumnia, utilizando redes sociales o afectación de la reputación en línea.

14. Las regulaciones aplicables en terceros países a las actividades en línea.

15. Desconocimiento de jueces y árbitros sobre las nuevas categorías tecnológicas y dificultad para adjudicar derechos o para que las decisiones sean aplicables[13].

Para mitigar los riesgos enunciados, los administradores pueden generar, adoptar e implementar entre otros: políticas de gestión y manejo de tecnología e innovación tecnológica (programas de ordenador y patentes, entre otras), programas de seguridad y aseguramiento de información, políticas de manejo adecuado de datos personales y privacidad, políticas de gestión, términos y condiciones para la contratación electrónica, políticas de gobernanza y manejo de gestión de mensajes de datos y comunicaciones electrónicas, incluyendo generación, almacenamiento, transmisión y políticas de seguridad informática y de certificación digital.

2. Fuentes específicas de responsabilidad de la empresas en la era digital

2.1 Contenido y alcance de la obligación en materia tecnológica

En el entorno empresarial la obligación que genera una responsabilidad de incumplimento puede estar vinculada a los siguientes supuestos:

a. Deber de las empresas y los empresarios de actuar de buena fe y con lealtad commercial.

b. Deber general y objetivo de prevención de riesgos.

c. Deber de cumplimiento de las regulaciones sobre la fabricación y distribución de productos y servicios.

d. Deber de cumplimiento de las noras asociadas a la tecnología, por ejemplo, la propiedad intelectual, propiedad industrial, protección de datos personales, ciencia y tecnología y transferencia de tecnología, entre otros.

13 Peña Valenzuela, Daniel. Responsabilidad Jurídica en la web 2.0 y en las Redes Sociales en Anuario de Responsabilidad Civil y del Estado. Ediciones Unaula, Medellín, 2014.

e. Deber de cuidado y diligencia respecto de las cosas bajo su control.

f. Deber derivado del contenido específico derivado de contrato o convención tecnológica particular.

La primera aproximación a la obligación en materia de tecnología es que se trata de una obligación de medio y no de la consecución de resultado específico alguno. No obstante, precisamente para lograr que sea un objetivo específico el que determine el alcance del cumplimiento, las partes interesadas deben precisar las especificaciones técnicas, los parámetros tecnológicos, las definiciones, los niveles de servicios y todo lo que delimite la prestación de dar, hacer o no hacer.

Los grados de responsabilidad dependen de lo pactado, de la conducta de las partes y de la creciente tendencia a considerar una responsabilidad objetiva por el uso de tecnología o por lo menos invertir la carga de la prueba sobre la atribución y la ocurrencia del daño. La otra base de la responsabilidad en tecnología se deriva del daño causado por las cosas a cargo de un sujeto, entendiendo por cosas, los sistemas de información, las aplicaciones y las redes. En el caso del almacenamiento y la custodia de la información propia y de terceros y el uso de herramientas, máquinas y dispositivos (*hosting* o *cloud computing*, por ejemplo) implica un riesgo, y en el ambiente creciente de inseguridad informática, se podría encaminar a su clasificación como una actividad peligrosa.

En el reciente caso, bajo investigación internacional, que afecta a la compañía alemana Volkswagen, en el cual se acusa a la compañia de haber colocado motores con *software* que falsificaba los datos de las emisiones contaminantes en vehículos fabricados por esta compañía y con sus marcas, se aprecia la necesidad de vigilar y controlar el uso de innovaciones, ya que en este caso el objetivo de la tecnología era engañar a las autoridades[14].

En Colombia:

> Los administradores responderán solidaria e ilimitadamente de los perjuicios que por dolo o culpa ocasionen a la sociedad a los socios o a terceros. No estarán sujetos a dicha responsabilidad, quienes no hayan tenido

14 http://www.spiegel.de/wirtschaft/unternehmen/volkswagen-affaere-das-droht-martin-winterkorn-a-1055302.html, consultado el 1 de octubre del 2015.

> conocimiento de la acción u omisión o hayan votado en contra, siempre y cuando no la ejecuten. En los casos de incumplimiento o extralimitación de sus funciones, violación de la ley o de los estatutos, se presumirá la culpa del administrador (Código de Comercio)[15].

De acuerdo con esta normativa, el uso de la tecnología en una empresa puede generar responsabilidad de los administradores y de la empresa frente a terceros, y si existe conocimiento de la acción u omisión. En el evento que el uso de la tecnología se realice en extralimitación de funciones y se cause un daño, se presumirá la culpa de los administradores. Con lo que se realza el papel fundamental de definir el binomio: tecnología y deberes de los administradores, así como los compromisos de estos últimos en las políticas de adopción, vigilancia, control, explotación y uso de tecnologías propias y de terceros.

2.2 *Expansión de las fuentes normativas de responsabilidad por el uso de tecnología en las empresas*

Desde la perspectiva de la competividad y productividad de las empresas es un paradigma indiscutible que el presente y el futuro está enmarcado en creación, adopción, adaptación e incorporación de tecnología. Este nuevo modelo de negocio es el resultado de la inserción de la economía colombiana en el proceso de globalización en curso. Con el fin de copar esa necesidad, las empresas se ven abocadas a diversas actividades: (i) se deben adoptar tecnologías en los procesos productivos, (ii) invertir en innovación, investigación y conocimiento, (iii) incorporar los procesos de adquisición y transferencia de tecnología en las estrategias a corto, mediano y largo plazo, (iv) capacitar a los equipos de trabajo en tecnologías y en monetización de la explotación tecnológica, (v) crear *clusters* tecnológicos y cadenas de colaboración en proyectos tecnológicos, (vi) crear condiciones favorables para el emprendimiento digital y apoyar las empresas con capital de riesgo.

Como ejemplo de este nuevo ecosistema de emprendimiento, se encuentra la Corporación Ruta N, creada por la Alcaldía de Medellín, UNE y EPM con el fin de facilitar la evolución económica de la ciudad hacia negocios intensivos en

15 Artículo 200 del Código de Comercio.

ciencia, tecnología e innovación de una manera incluyente y sostenible. El principal objetivo es que en el año 2021, Medellín esté posicionada como la ciudad más innovadora de América Latina.

La responsabilidad en el ámbito empresarial por el uso de TIC se rige por las reglas de responsabilidad que provienen de la legislación civil y mercantil, así como de leyes específicas como el Estatuto del Consumidor y la Ley de Protección de Datos Personales[16]. En el caso de sectores regulados de manera específica, la responsabilidad frente al consumidor por servicios de banca en línea y los propios servicios TIC. En cuanto a la infracción a derechos por la utilización de *software*, invenciones, diseños industriales, bases de datos, el fundamento, el Régmen Andino de los Derechos de Autor y Derechos Conexos (Decisión 351 de 1993) y el Régimen Común de la Propiedad Industrial (Decisión 486 del 2000).

La norma rectora es el artículo 1.341 del Código Civil que establece:

> El que ha cometido un delito o culpa, que ha inferido daño a otro, es obligado a la indemnización, sin perjuicio de la pena principal que la ley imponga por la culpa o el delito cometido. Las TICs pueden ser utilizadas por directivos y empleados de mala fe o con dolo para causar daños y perjuicios a terceros. La mala intención puede ser en el uso mismo de la tecnología o de la información para afectar y perjudicar o de manera deliberada y conciente la infracción de las reglas que atribuyen titularidad y protección a los derechos respecto de la tecnología. También la responsabilidad puede originarse en la negligencia a la luz del artículo 2.356 del Código Civil que establece: por regla general todo daño que pueda imputarse a malicia o negligencia de otra persona, debe ser reparado por ésta.

De acuerdo con nuestra ley mercantil:

> Los administradores deben obrar de buena fe, con lealtad y con la diligencia de un buen hombre de negocios. Sus actuaciones se cumplirán en interés de la sociedad, teniendo en cuenta los intereses de sus asociados. En el cumplimiento de su función los administradores deberán:1. Realizar los esfuerzos conducentes al adecuado desarrollo del objeto social. 2. Velar por el estricto cumplimiento de las disposiciones legales o estatutarias. 3.Velar

16 Peña Valenzuela, Daniel. La Responsabilidad Civil en la Era Digital. Universidad Externado de Colombia, Bogotá, 2007

> porque se permita la adecuada realización de las funciones encomendadas a la revisoría fiscal. 4. Guardar y proteger la reserva comercial e industrial de la sociedad. 5. Abstenerse de utilizar indebidamente información privilegiada. 6. Dar un trato equitativo a todos los socios y respetar el ejercicio del derecho de inspección de todos ellos. 7. Abstenerse de participar por sí o por interpuesta persona en interés personal o de terceros, en actividades que impliquen competencia con la sociedad o en actos respecto de los cuales exista conflicto de intereses, salvo autorización expresa de la junta de socios o asamblea general de accionistas[17].

En la Sociedad por Acciones Simplificada, se amplió subjetivamente la responsabilidad de los administradores, así:

> Las reglas relativas a la responsabilidad de administradores contenidas en la Ley 222 de 1995, les serán aplicables tanto al representante legal de la sociedad por acciones simplificada como a su junta directiva y demás órganos de administración, si los hubiere. Parágrafo. Las personas naturales o jurídicas que, sin ser administradores de una sociedad por acciones simplificada, se inmiscuyan en una actividad positiva de gestión, administración o dirección de la sociedad, incurrirán en las mismas responsabilidades y sanciones aplicables a los administradores[18].

En la exposición de motivos del proyecto de ley de reforma del régimen de sociedades, se establece:

> Por ello se propone un trasplante jurídico de la regla del buen juicio de los negocios, de ascendencia anglosajona. Esta regla de conducta se basa en la concepción que ve en la labor de los administradores sociales, una función rigurosamente económica, consistente en la asunción razonada de riesgos que puede conducir a la innovación empresarial y a la creación de riqueza, por ello, la regla implica que los jueces no han de inmiscuirse en las decisiones de negocios adoptadas por los administradores, siempre y cuando que en ellas no medie conflicto de interés o ilegalidad. Se trata de una especie de presunción de hecho, según la cual, se considera adecuada la conducta del administrador por las decisiones relacionadas

17 Artículo 23 de la Ley 222 de 1995.

18 Artículo 27 de la Ley 1.258 del 2008.

> con los negocios sociales, a menos que estén presentes las situaciones irregulares aludidas[19].

Esta norma propuesta es más proclive a la asunción de riesgos por los empresarios, incluyendo los relacionados con la creación de innovación y la adopción y uso de tecnologías en el entorno corporativo.

El CIO como administradores pueden tener responsabilidad societarios, pero en todo caso tienen que asumir la responsabilidad profesional, en la medida de sus funciones y deberes con los parámetros fijados por la sociedad como por sus calidades y formación profesional y tecnológica. Lo anterior, enmarcado en el deber de defender y cuidar los intereses de la empresa y de los accionistas u omitir el cumplimiento de sus funciones en particular la de adoptar políticas y medidas adecuadas, para prevenir y evitar los riesgos para la empresa asociados al uso de tecnología y de explotación de la información propia o de terceros.

Cada uno de los aspectos relacionados con la planificación e implementación de la agenda de desarrollo y e implementación de TIC en una empresa pueden originar responsabilidad en los distintos niveles de una empresa. La responsabilidad en caso de los directivos de las empresas, se refieren a la inexistencia de políticas que no se apliquen correctamente, ausencia de 'voluntad política', que no se dispongan de medios, herramientas y personal adecuado e idóneo para aplicarlas. Lo anterior, reiteramos, en concordancia con el Código de Comercio que establece que:

> Los administradores responderán solidaria e ilimitadamente de los perjuicios, que por dolo o culpa ocasionen a la sociedad, a los socios o a terceros. No estarán sujetos a dicha responsabilidad, quienes no hayan tenido conocimiento de la acción u omisión o hayan votado en contra, siempre y cuando no la ejecuten. En los casos de incumplimiento o extralimitación de sus funciones, violación de la ley o de los estatutos, se presumirá la culpa del administrador (Código de Comercio)[20].

Las políticas relacionadas con el uso de tecnología y en particular de TIC, hacen referencia al cumplimiento de normas, regulaciones generales y específicas,

19 Exposición de motivos reforma del Código de Comercio Proyecto de Ley 070 del 2015.

20 Artículo 200 del Código de Comercio.

autorizaciones, habilitaciones, acreditaciones y estándares técnicos (nacionales, internacionales o de autorregulación) relacionados con los siguientes tópicos:

1. Manejo y gestión de propiedad intelectual e industrial, innovación y transferencia de tecnología.

2. Sistemas de Gestión, Administración y Seguridad de los Sistemas de Información, bases de datos y herramientas tecnológicas utilizados por la empresa.

3. Políticas de seguridad documental, retención documental, archivo y gestión de pruebas digitales y computación forense.

4. Política de recaudo, recolección, tratamiento de datos personales, y Estudio de Impacto de Privacidad

5. Política de medidas tecnológicas de protección de información confidencial, secreto empresarial e información reservada.

6. Política de prueba, evidencia y trazabilidad de las transacciones electrónicas con consumidores.

7. Políticas de PQR, *help desk* y atención a los usuarios y consumidores relacionados con derechos del consumidor, privacidad y protección de datos.

2.3 *El uso del 'software' autorizado y licenciado como base de la tecnología en la empresa*

Los programas del ordenador son protegidos por los derechos de autor en cuanto a su forma plasmada en el código fuente, en la descripción del programa y el material auxiliar. En relación con sus funciones, de manera asociada a otras invenciones, el programa del ordenador puede ser protegido por medio de las patentes de invención.

La utilización de los programas de computador (sistema operativo y aplicaciones) como *software* propietario, o sea, con un titular de derechos de autor con propósitos de explotación onerosa y con ánimo de lucro se ha masificado en las empresas y representa la aproximación más tradicional entre la tecnología y la empresa. En materia de utilización de programas de computador, las sociedades

comerciales deben contar con las respectivas licencias de uso para cada uno de los equipos que posea y para las casas matrices, subsidiarias y filiales, si las tienen. Los usos de los programas deben circunscribirse a los autorizados, expresamente en el contrato de licencia de uso, y cumplir con las restricciones previstas, por ejemplo, la prohibición de realizar ingeniería inversa. La licencia debe encontrarse vigente el momento de la utilización de los programas y abarcar el territorio en el que esté ubicado el licenciatario o sus equipos[21].

La explotación de los programas de ordenador ha desarrollado diversos modelos de negocios, entre otros, los paquetes corporativos, las descargas en línea y la utilización de la nube para facilitar las aplicaciones. La lucha contra la piratería imperante y la necesidad de que las medidas para prevenir las infracciones sean efectivas, propiciaron que se establezca la responsabilidad legal de los administradores como principales encargados de la dirección y políticas de la compañía. La obligación legal de presentar, como parte del informe de gestión, el cumplimiento de las reglas de propiedad intelectual no debe ser una actividad mecánica de cumplimiento, sino la expresión de la diligencia en las políticas y control del cumplimiento de la ley. En particular, respecto del licenciamiento o autorización de uso y explotación de los derechos de autor que protegen los programas de ordenador[22].

La diligencia de los administradores puede acreditarse por la implementación de una política efectiva de gestión y cumplimiento de la propiedad intelectual que incluya auditorías constantes sobre el uso adecuado de las tecnologías y de las herramientas informáticas por los empleados y la utilización de las herramientas informáticas adecuadas para que no se puedan descargar y almacenar programas sin autorización.

Toda utilización del programa de computador debe estar legitimada por una autorización previa y expresa del autor o de los titulares[23], de lo contrario infringe el derecho de autor y se incurrirá en una actividad ilegal que trae consigo

21 Peña Valenzuela, Daniel. Software Libre y Software Propietario. Impacto jurídico, económico y cultural en Colombia, Universidad Externado de Colombia. Bogotá, 2014.

22 El artículo 47 de la Ley 222 de1995 modificado por la Ley 603 de 2000, que hace parte del Código de Comercio, impone a las sociedades comerciales presentar en sus informes de gestión: "el estado de cumplimiento de las normas sobre propiedad intelectual y derechos de autor por parte de la sociedad", *so pena* de ser sancionada por parte de la Superintendencia de Sociedades.

23 Artículo 54 de la Decisión Andina 351 de 1993.

sanciones civiles y penales. En materia penal, la legislación colombiana tipifica como delitos acciones como la violación a los derechos morales del autor; la defraudación a los derechos patrimoniales del autor, la cual se configura cuando se reproduce, utiliza, alquila por cualquier medio una obra entre ellas el soporte lógico sin autorización previa y expresa del titular, y la violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones, como por ejemplo eludir o superar las medidas tecnológicas adoptadas para restringir los usos no autorizados[24].

En materia civil, la Ley 23 de 1982 y el Código General del Proceso faculta a los titulares de obras que consideren vulnerados sus derechos, para iniciar acciones civiles por medio de un proceso verbal ante los jueces civiles o ante la Dirección Nacional de Derecho de Autor que tiene funciones jurisdiccionales.

Con las Tecnologías de la Información y las Comunicaciones, y como consecuencia de la arquitectura de Internet como sistema de información distribuido con una amplia gama de intermediarios o proveedores de servicios de diversa índole, se ha generado una polémica aún no resuelta respecto al grado de responsabilidad que deben asumir. Las alternativas pueden ser el régimen de responsabilidad tradicional, un tratamiento atenuado con excepciones y limitación de responsabilidad, la liberación de cualquier responsabilidad por mandato legal y la determinación por materias, por ejemplo, en cuanto a delitos, atentados a la libre expresión o propiedad intelectual[25].

2.4 *El uso de tecnología amparada por patentes de invención o 'know-how'.*

El derecho de propiedad industrial más asociado a la explotación y uso de la tecnología en las empresas es el derecho a las patentes de invención. El administrador debe asegurarse que en la elaboración y manufactura de los productos, sus procesos tecnológicos y de innovación no se están infringiendo patentes de terceros.

---

24 Titulo VIII, artículos 270 a 272 del Código Penal (Ley 599 del 2000).

25 Peña Valenzuela, Daniel. Responsabilidad de los Proveedores de Servicios de Internet en materia de Propiedad Intelectual, Universidad Externado de Colombia. Bogotá, 2014.

Los administradores deben propender por la protección de las invenciones que lleven a cabo sus empleados, los centros de investigación e innovación mediante el registro de las patentes por las oficinas de propiedad industrial, en Colombia, la Superintendencia de Industria y Comercio. Este registro se debe realizar en relación con cada uno de los territorios a los cuales se quiera exportar los productos o procedimientos amparados por estos derechos de propiedad industrial. Con la protección, se evita que el producto exportado pueda infringir derechos de terceros que demanden perjuicios, soliciten el decomiso en los puntos de comercialización o medidas en frontera.

Los derechos de propiedad industrial conferidos con una patente de invención otorgan a su titular el derecho de impedir a terceras personas que no tengan su consentimiento, realizar cualquiera de los siguientes actos: a) cuando en la patente se reivindica un producto: i) fabricar el producto; ii) ofrecer en venta, vender o usar el producto; o importarlo para alguno de estos fines; y, b) cuando en la patente se reivindica un procedimiento: i) emplear el procedimiento; o ii) ejecutar cualquiera de los actos indicados en el literal a), respecto a un producto obtenido directamente mediante el procedimiento.

El titular de una patente tendrá derecho a ejercer acción judicial por daños y perjuicios por el uso no autorizado de la invención o del modelo de utilidad durante el periodo comprendido entre la fecha en que adquiera carácter público y pueda ser consultada la solicitud respectiva y la fecha de concesión de la patente. El resarcimiento solo procederá con respecto a la materia cubierta por la patente concedida, y se calculará en función de la explotación efectivamente realizada por el demandado durante el periodo mencionado.

Para efectos de calcular la indemnización de daños y perjuicios se tomarán en cuenta, entre otros, los criterios siguientes: a) el daño emergente y el lucro cesante sufrido por el titular del derecho como consecuencia de la infracción; b) el monto de los beneficios obtenidos por el infractor como resultado de los actos de infracción; o c) el precio que el infractor habría pagado por concepto de una licencia contractual, teniendo en cuenta el valor comercial del derecho infringido y las licencias contractuales que ya se hubieran concedido.

Como consecuencia del Tratado de Libre Comercio suscrito, y en vigencia con los Estados Unidos de América, se aprobó la Ley 1.648 del 2013, por medio de la cual se implementan procedimientos judiciales civiles para obtener

mayor información de los infractores, solicitar la destrucción de productos e implementos destinados a la infracción, e implementar el sistema de tasación de perjuicios. Esta ley permite al demandante, al momento de presentar la demanda por infracción marcaria, elegir el sistema de indemnización que le permita, de manera más eficiente, la reparación de los daños causados, entre: (i) el sistema de indemnizaciones preestablecidas o (ii) el sistema de reglas generales sobre prueba de la indemnización de perjuicios. El Ministerio de Comercio, Industria y Turismo reglamentó la ley mencionada[26]. Este decreto señala que el demandante puede optar por el primer sistema, caso en el cual no tendrá que probar la cuantía de los daños causados. Bajo el sistema de indemnizaciones prestablecidas, la tasación de los perjuicios se sujetará al criterio y determinación del juez, la cual se fijará entre tres (3) salarios mínimos legales mensuales vigentes (SMLMV) y un máximo de cien (100) SMLMV, por cada marca infringida. En el evento en el que en el mismo proceso se incluya la pretensión de la infracción de varias marcas, el juez fijará un monto por separado por cada signo distintivo vulnerado. El juez puede superar el límite de los cien (100) SMLMV e incrementarlo hasta doscientos (200) SMLMV, cuando: (i) dentro del proceso de infracción marcaria y a petición de la parte demandante, el juez haya declarado la notoriedad de la marca infringida, (ii) se demuestre la mala fe del infractor, (iii) se ponga en peligro la vida o la salud de las personas, por ejemplo con licores o productos farmacéuticos adulterados, y (iv) se constate la reincidencia del infractor sobre la misma marca. El juez en la sentencia que ponga fin al proceso, puede fijar el monto de la indemnización con base en las pruebas aportadas al proceso, la duración e impacto de la infracción, su amplitud, cantidad de productos infractores y el alcance geográfico. En el caso de que el demandante escoja el sistema tradicional sobre prueba de los perjuicios debe probar cada uno de los daños y perjuicios causados con la infracción.

Las acciones por infracciones de propiedad intelectual se pueden presentar ante los jueces civiles o ante la Superintendencia de Industria y Comercio que tiene funciones jurisdiccionales.

26 Decreto 2.264 del 2014 del Ministerio de Comercio, Industria y Comercio.

2.5 *La extracción o el acceso abusivo de información que hacen parte de registros de bases de datos*

Las bases de datos se protegen por los derechos de autor como una compilación en cuanto a la selección y disposición particular y específica de elementos que permiten un orden de búsqueda, tablas e índices que permiten la organización de la información. El contenido de las bases de datos se protege en la medida que la información, obras o datos estén amparadas como bienes inmateriales por normas especiales. Pueden ser, entre otras, obras protegidas por el derecho de autor, información confidencial o secretos empresariales e información personal. En esos tres casos, además de la base de datos como tal, se protegen la información en cuanto a su uso, explotación, acceso o uso no autorizado, según el caso.

El alcance y restricciones del acceso al contenido de las bases de datos se determina por contratos en los que se definen los derechos y deberes de los usuarios. Los límites en cuanto al uso de la información para un propósito distinto a la mera consulta. Los terceros no pueden acceder a las bases de datos o a los sistemas de información sin autorización, de lo contrario, pueden incurrir en responsabilidad penal por acceso abusivo a un sistema de información y asumir la responsabilidad civil en caso de que causen perjuicios[27]. En el artículo 269a del Código Penal se establece el *Acceso abusivo a un sistema informático*. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

2.6 *El recaudo, la recolección, el tratamiento, las transferencias, la transmisión de datos personales*

Las TIC son las tecnologías de la información y el mercadeo digital, la comunicación y la interacción con los usuarios y consumidores se pueden potenciar con el conocimiento de los datos personales, sus tendencia y perfiles. La

27 Peña Valenzuela, Daniel. Derecho de la Seguridad de los Sistemas de Información. Construcción de parámetros para el concepto de ciberdelito en XXXII Jornadas Internacionales de Derecho Penal. Derecho Penal Económico y de la Empresa, Universidad Externado de Colombia, 2010.

gestión deficiente y el mal uso de las bases de datos electrónicas que incorporan datos personales pueden acarrear responsabilidad para los administradores y las empresas, en caso de que no se respeten las reglas sobre la protección de datos personales, ocurran incidentes que generen el acceso no autorizado por terceros y por ende, el incumplimiento de los principios de finalidad y circulación restringida. Este régimen de protección, desde el punto de vista material, abarca, de acuerdo con la Ley 1.581 del 2012, al dato personal, una clase de información específica que es definido como "cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables".

En la ley se establece el cumplimiento de los deberes de las empresas cuando actúan como responsables o encargados del tratamiento de los datos personales y la obligación de registro de las bases de datos y de las políticas de protección de los datos personales. Según la Ley 1.581 del 2012, el encargado del tratamiento es la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento y el responsable del tratamiento: es la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos o el tratamiento de los datos.

La protección de la información personal hace referencia a las distintas etapas y actividades relacionadas con el ciclo de existencia y explotación de los datos personales, principalmente el recaudo, la recolección, el tratamiento, las transferencias y la transmisión de datos personales. Respecto a cada una de esas etapas, el responsable del tratamiento de datos personales tiene el deber de información respecto del titular con el siguiente alcance:

a) Al momento de solicitar la autorización, debe informar de manera clara y expresa, el tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo.

b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes.

c) Informar los derechos del titular (entre otros, conocer, actualizar y rectificar sus datos personales, solicitar prueba de la autorización otorgada al responsable del tratamiento, ser informado por el responsable del

tratamiento o el encargado del tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales y presentar ante la Superintendencia de Industria y Comercio quejas por infracciones).

d) La identificación, dirección física o electrónica y teléfono del responsable del tratamiento.

e) El responsable del tratamiento deberá conservar prueba del cumplimiento de sus deberes y, cuando el titular lo solicite, entregarle copia.

Los incidentes de seguridad son eventos en que se exponen y ponen en riesgo los datos personales con la consecuencia de que pueden ser utilizados, destruidos, divulgados o tratados, violando los límites de la autorización otorgada por el titular. La causa de la responsabilidad no proviene de una acción imputable a la empresa sino la negligencia en la puesta en marcha y aplicación de medidas y políticas de seguridad informática que garanticen la circulación restringida y la confidencialidad de los datos personales. Los efectos son, por una parte, la imposición de sanciones administrativas por las agencias de protección de datos, en Colombia, la Superintendencia Delegada de Protección de Datos Personales y, por otra, la indemnización de perjuicios que pueda declarar un juez en favor de los titulares de los datos personales.

La Superintendencia, en el 2015, expidió las guías para la demostración del principio de responsabilidad demostrada en material de protección de respecto de una mayor orientación en el camino de construir un Programa Integral de Gestión de Datos Personales, y está dirigida a quienes estén sometidos al cumplimiento del régimen general de protección de datos personales y sean vigilados por la Superintendencia de Industria y Comercio.

El concepto de responsabilidad demostrada, aplicada al tratamiento de datos personales, tiene más de tres décadas. En 1980, las guías para la protección de la privacidad y los flujos transfronterizos de datos personales introdujeron el concepto anglosajón de "Accountability", donde se hace énfasis en el rol del responsable del tratamiento como el obligado a implementar medidas dentro de la organización con el fin cumplir con el resto de principios de la "Data Protection". Algunas autoridades de protección de datos en el mundo han publicado guías que le permiten a las organizaciones cumplir con la ley e implementar ese alto estándar dentro de su gestión operativa.

En septiembre de 2013, la OCDE publicó la versión revisada de las guías sobre la protección de la privacidad y los flujos transfronterizos de información que originalmente habían sido publicados en 1980. Las guías de OCDE recogen un principio fundamental conocido como responsabilidad demostrada (accountability), según cual una entidad que recoge y hace tratamientos de datos personales debe ser responsable del tratamiento efectivo de las medidas que implementen los principios de privacidad y protección de datos. En la versión del 2013 de las guías se establece un aparte nuevo sobre la implementación del principio de responsabilidad demostrada. En este sentido, y según lo dispuesto por las guías, los responsables del tratamiento deben contar con un programa integral de gestión de datos personales y estar preparados para demostrarle a la autoridad la implementación efectiva de esas medidas en la organización.

En las normas de protección de datos en Colombia se establece el criterio de la responsabilidad demostrada como una obligación de los responsables del tratamiento que deben estar en capacidad de demostrar, a petición de la Superintendencia de Industria y Comercio,[28] que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1.581 del 2012.

La norma establece de manera específica que estas medidas se deben adoptar teniendo en cuenta diversos factores que son propios de cada organización, entre los que se encuentran su tamaño y naturaleza jurídica, la naturaleza de los datos tratados, el tipo de tratamiento al que se someta la información y los riesgos que implique para los titulares para la recolección y posterior uso y circulación de esos datos. Las políticas internas efectivas que se implementen deberán garantizar que en la organización exista una estructura administrativa proporcional a la estructura del responsable para implementarlas, que se adopten mecanismos internos para poner en práctica las políticas que incluyan herramientas de implementación, entrenamiento y programas de educación y la adopción de procesos para la atención de reclamos y consultas de los titulares[29].

La Superintendencia de Industria y Comercio podrá imponer a los responsables del tratamiento y encargados del tratamiento las siguientes sanciones:

28 Artículo 26 del Decreto 1.377 del 2013.

29 Artículo 27 del Decreto 1.377 del 2013.

a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) Salarios Mínimos Mensuales Legales Vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.

b) Suspensión de las actividades relacionadas con el tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar.

c) Cierre temporal de las operaciones relacionadas con el tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio.

d) Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles.

La Superintendencia de Industria y Comercio debe tener en cuenta la existencia de medidas y políticas adecuadas de protección de datos bajo los principios de responsabilidad, demostrada en el momento de evaluar la imposición de una sanción. El énfasis de la protección de la información personal tiende hacia un modelo que privilegia la gestión del riesgo y la asignación de responsabilidad en cabeza del responsable del tratamiento.

De acuerdo con la Ley 1.273 del 2009 sobre Delitos Informáticos, la violación de datos personales está tipificada como hecho punible en Colombia, en los siguientes términos:

> El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 Salarios Mínimos Legales Mensuales Vigentes.

Esta conducta debe ser mirada de manera detallada en relación con la Ley 1.266 y con el proyecto de ley en revisión de la Corte Constitucional, con el fin de determinar el bien jurídico tutelado, los ingredientes normativos, los deberes de los sujetos con deberes de protección de los garantes de los bienes tutelados y la punibilidad establecida.

2.7 *La seguridad tecnológica el estándar de diligencia de los empresarios*

La seguridad tecnológica es una obligación para todas las empresas que utilicen tecnología y que tengan información propia o de terceros que sea relevante, que tenga protección legal o valor económico. Con los mecanismos, las herramientas y las políticas que se planeen y adopten en relación con los sistemas de información, se debe garantizar la protección y preservación de la características y cualidades de la información como la integridad, el acceso, la usabilidad, la confidencialidad, la autenticidad y el no repudio.

Además de las normas legales, existen normas de autorrregulación sobre estándares de seguridad informática como la ISO 27001, la cual es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe la manera de gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada con base en la norma británica BS 7799-2. La norma ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública. Proporciona una metodología para implementar la gestión de la seguridad de la información en una organización y permite que una empresa sea certificada, con lo cual una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en la organización en cumplimiento con la norma ISO 27001. La norma ISO 27001 se ha convertido en la principal norma global para la seguridad de la información.

La garantía de disponibilidad y usabilidad de la información digital para ser utilizada para defender la posición del empresas en procesos judiciales y administrativos. Los empleados son usuarios generadores de contenido digital con lo cual se debe reforzar su compromiso con la empresas de ser responsables respecto del contenido que publiquen en sitios web y redes sociales. En caso de que las opiniones o contenidos solo comprometan la responsabilidad de la empresa, esta consigna debe constar de manera expresa. Hasta hace poco, las herramientas informáticas y equipos eran de propriedad exclusiva de las empresas y bajo el control centralizado, pero con la tendencia de utilización de sus propios equipos (traer su propio equipo BYOC) es importante separar la información del equipo.

La información es de la empresa, así el equipo le pertenezca al empleado. Esto también es aplicable a la seguridad e integridad de la información en las comunicaciones móviles de las fuerza de ventas en puntos remotos.

La seguridad informática de las organizaciones busca lograr el mayor nivel posible de confiabilidad y aseguramiento de sus arquitecturas, de los sistemas de información, así como evaluar el nivel dificultad requerido por los atacantes para ingresar y vulnerar las medidas de protección. Las entidades buscan incrementar la confianza de sus clientes, y comprender que la seguridad es un problema de tecnología, de riesgos y de las diferentes maneras de gestionarlos y mitigar sus efectos.

Los Sistemas de Gestión de Seguridad de la Información (SGSI) son el medio más eficaz de minimizar los riesgos, identifican y valoran los datos y sus riesgos, considerando el impacto para la organización, y se adoptan los controles y procedimientos más eficaces y coherentes con la estrategia del modelo de negocio.

La gestión y administración de la seguridad de la información permite garantizar: la confidencialidad, con el fin de asegurar que solo quienes estén autorizados puedan acceder a la información; la integridad, para asegurar que la información y sus métodos de proceso son exactos y completos; y la disponibilidad, en el sentido de que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

En el caso de las entidades financieras, los parámetros de seguridad informática, así como las medidas, herramientas tecnológicas y equipos que se requieren para garantizar la integridad, autenticidad y disponbilidad de información. Además de las normas generales enunciadas, se aplica la Circular Externa 052 del 2007 sobre requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios y el Anexo de la Circular 42 del 2012 sobre requerimientos mínimos de seguridad y calidad para la realización de operaciones

2.8 *La prevención y protección de los derechos de los consumidores como estándar de diligencia en el comercio electrónico*

En el caso de que se utilice el canal electrónico para realizar ventas a distancia o transacciones de comercio electrónico, el empresario debe tener en cuenta las reglas establecidas de manera especial para proteger al consumidor en el entorno

digital en la Ley 1.480 del 2011 como: el derecho de retracto, el deber de información reforzada, los deberes de los portales de contacto, los derechos de niños y adolescentes y la reversión de pagos.

La información que el proveedor de comercio electrónico debe proporcionar al consumidor en relación con los bienes o servicios, el medio de publicación digital de la oferta y las transacción electrónica misma, incluye lo siguiente:

a) Informar en todo momento de forma cierta, fidedigna, suficiente, clara, accesible y actualizada su identidad, especificando su nombre o razón social, Número de Identificación Tributaria (NIT), dirección de notificación judicial, teléfono, correo electrónico y demás datos de contacto.

b) Suministrar en todo momento información cierta, fidedigna, suficiente, clara y actualizada respecto de los productos que ofrezcan. En especial, deberán indicar sus características y propiedades, tales como el tamaño, el peso, la medida, el material del que está fabricado, su naturaleza, el origen, el modo de fabricación, los componentes, los usos, la forma de empleo, las propiedades, la calidad, la idoneidad, la cantidad, o cualquier otro factor pertinente, independientemente de que se acompañen de imágenes, de tal forma que el consumidor pueda hacerse una representación lo más aproximada a la realidad del producto.

También se deberá indicar el plazo de validez de la oferta y la disponibilidad del producto. En los contratos de tracto sucesivo, se deberá informar su duración mínima.

Cuando la publicidad del bien incluya imágenes o gráficos del mismo, se deberá indicar en qué escala está elaborada dicha representación.

c) Informar, en el medio de comercio electrónico utilizado, los medios de los cuales disponen para realizar los pagos, el tiempo de entrega del bien o la prestación del servicio, el derecho de retracto que le asiste al consumidor y el procedimiento para ejercerlo, y cualquier otra información relevante para que el consumidor pueda adoptar una decisión de compra libremente y sin ser inducido en error.

Igualmente deberá informar el precio total del producto, incluyendo todos los impuestos, costos y gastos que deba pagar el consumidor para

adquirirlo. En caso de ser procedente, se debe informar adecuadamente y por separado los gastos de envío.

d) Publicar en el mismo medio y en todo momento, las condiciones generales de sus contratos, que sean fácilmente accesibles y disponibles para su consulta, impresión y descarga, antes y después de realizada la transacción, así no se haya expresado la intención de contratar.

Previamente a la finalización o terminación de cualquier transacción de comercio electrónico, el proveedor o el expendedor deberá presentar al consumidor un resumen del pedido de todos los bienes que pretende adquirir con su descripción completa, el precio individual de cada uno de ellos, el precio total de los bienes o servicios y, de ser aplicable, los costos y gastos adicionales que deba pagar por envío o por cualquier otro concepto y la sumatoria total que deba cancelar. Este resumen tiene como fin que el consumidor pueda verificar que la operación refleje su intención de adquisición de los productos o servicios ofrecidos y las demás condiciones, y de ser su deseo, hacer las correcciones que considere necesarias o la cancelación de la transacción. Este resumen deberá estar disponible para su impresión o descarga.

La aceptación de la transacción por parte del consumidor deberá ser expresa, inequívoca y verificable por la autoridad competente. El consumidor debe tener el derecho de cancelar la transacción hasta antes de concluirla.

Concluida la transacción, el proveedor y el expendedor deberá remitir, a más tardar, el día calendario siguiente de efectuado el pedido, un acuse de recibo del mismo, con información precisa del tiempo de entrega, precio exacto, incluyendo los impuestos, gastos de envío y la forma en que se realizó el pago.

Queda prohibida cualquier disposición contractual en la que se presuma la voluntad del consumidor o que su silencio se considere como consentimiento, cuando de esta se deriven erogaciones u obligaciones a su cargo.

e) Mantener en mecanismos de soporte duradero la prueba de la relación comercial, en especial de la identidad plena del consumidor, su voluntad expresa de contratar, de la forma en que se realizó el pago y la entrega real y efectiva de los bienes o servicios adquiridos, de tal forma que garantice la integridad y la autenticidad de la información y que sea verificable por la autoridad competente, por el mismo tiempo que se deben guardar los documentos de comercio.

f) Adoptar mecanismos de seguridad apropiados y confiables que garanticen la protección de la información personal del consumidor y de la transacción misma. El proveedor será responsable por las fallas en la seguridad de las transacciones realizadas por los medios por él dispuestos, sean propios o ajenos.

Cuando el proveedor o expendedor dé a conocer su membrecía o afiliación en algún esquema relevante de autorregulación, asociación empresarial, organización para resolución de disputas u otro organismo de certificación, deberá proporcionar a los consumidores un método sencillo para verificar dicha información, así como detalles apropiados para contactar con dichos organismos, y en su caso, tener acceso a los códigos y prácticas relevantes aplicados por el organismo de certificación.

g) Disponer en el mismo medio en que realiza comercio electrónico, de mecanismos para que el consumidor pueda radicar sus peticiones, quejas o reclamos, de tal forma que le quede constancia de la fecha y hora de la radicación, incluyendo un mecanismo para su posterior seguimiento.

h) Salvo pacto en contrario, el proveedor deberá haber entregado el pedido a más tardar en el plazo de treinta (30) días calendario a partir del día siguiente a aquel en que el consumidor le haya comunicado su pedido.

La Superintendencia de Industria y Comercio puede imponer, previa investigación administrativa, las siguientes sanciones:

1. Multas hasta por dos mil (2.000) Salarios Mínimos Mensuales Legales Vigentes al momento de la imposición de la sanción.

2. Cierre temporal del establecimiento de comercio hasta por 180 días.

3. En caso de reincidencia y atendiendo a la gravedad de las faltas, cierre definitivo del establecimiento de comercio o la orden de retiro definitivo de una página web, portal en Internet o del medio de comercio electrónico utilizado.

4. Prohibición temporal o definitiva de producir, distribuir u ofrecer al público determinados productos. El productor podrá solicitar a la autoridad competente, el levantamiento de esta sanción previa la demostración de que ha introducido al proceso de producción las modificaciones que aseguren el cumplimiento de las condiciones de calidad e idoneidad.

5. Ordenar la destrucción de un determinado producto, que sea perjudicial para la salud y seguridad de los consumidores.

6. Multas sucesivas hasta de mil (1.000) Salarios Mínimos Legales Mensuales Vigentes, por inobservancia de órdenes o instrucciones mientras permanezca en rebeldía.

Es importante resaltar que, además de la responsabilidad de la empresa como tal, cuando se compruebe que administradores, directores, representantes legales, revisores fiscales, socios, propietarios u otras personas naturales han autorizado o ejecutado conductas contrarias a las normas contenidas en la Ley 1.480 del 2011, se les pueden imponer multas hasta por trescientos (300) Salarios Mínimos Legales Mensuales Vigentes al momento de la imposición de la sanción y la prohibición de ejercer el comercio hasta por cinco (5) años, contados a partir de la ejecutoria de la sanción.

2.9 *El respeto de la identidad digital, la reputación y los signos distintivos de terceros*

La publicidad en línea y el mercadeo digital son la nueva frontera en la divulgación de mensajes corporativos, de creación de valor para marcas tradicionales y nuevas, tanto en páginas web como en las redes sociales. La creación de contenidos digitales publicados en diversas plataformas y formatos. Así mismo, la posibilidad de interacción con consumidores y el uso de la información que se recolecta para determinar perfiles, tendencias y preferencias puede ser fuente valiosa de conocimiento y potencializar modelos de negocios.

Estas nuevas herramientas digitales generan obligaciones respecto a respetar los derechos de los titulares de marcas en el entorno digital, utilizar nombres de dominio que no correspondan a signos distintivos ajenos, evitar la competencia desleal por medios electrónicos, abstenerse de usar contenidos digitales protegidos a nombre de terceros y el uso no autorizado de marcas en internet. La injuria y la calumnia encuentran en internet un amplificador de sus efectos negativos y perjudiciales, y por ende, agravan la conducta punible así como su sanción.

El uso de las redes sociales trae consigo un canal de comunicación de los valores y las opiniones de la empresa, de sus directivos y funcionarios. En la medida que las redes sociales se han convertido en la forma en que se expresa

la libertad de expresión comercial. En junio de 2011, los relatores especiales de la ONU y la CIDH, de manera conjunta con sus colegas de la Organización para la Seguridad y la Cooperación en Europa (OSCE) y la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP), emitieron la Declaración Conjunta sobre Libertad de Expresión e Internet. Esta declaración señala que si bien la libertad de expresión, incluso a través de internet, no tiene carácter absoluto, deben formularse enfoques específicos para responder a contenidos ilícitos que, al mismo tiempo, reconozcan las características singulares de internet y su capacidad de promover el goce de la libertad de expresión. La declaración señala que no se debe exigir a los intermediarios controlar el contenido generado por usuarios y enfatiza la necesidad de protegerlos respecto de cualquier responsabilidad, siempre que no intervengan específicamente en los contenidos o cuando se nieguen a cumplir una orden judicial que exija su eliminación. La declaración expresa, además, que la competencia respecto de causas vinculadas con contenidos de internet debería corresponder exclusivamente a los Estados donde tales causas presenten impactos directos y genuinos.

Asimismo, toda limitación a la libertad de expresión, incluyendo aquellas que afectan la expresión en internet, debe establecerse por ley de manera clara y precisa, debe ser proporcionada a los fines legítimos perseguidos y debe basarse en una decisión judicial, fruto de un proceso contradictorio. En este sentido, la legislación sobre internet no debe incluir definiciones amplias y vagas, ni afectar de manera desproporcionada a sitios web y servicios legítimos. Los comentarios que se hacen en las secciones abiertas al público en *blogs*, páginas web o plataformas deben ser opiniones que no afecten de manera ilegítima imagen, personalidad, integridad, veracidad u honor de terceros.

Conclusiones

1. Las empresas de todos los tamaños, pymes y grandes, tienen grandes desafíos para lograr aprovechar las bondades de la innovación, de la ciencia, de los desarrollos tecnológios propios, de la transferencia de tecnología, de la incorporación de las TIC y de la economía digital. En este proceso de creación y adopción de conocimientos nuevos, también deben detectar, prevenir y mitigar los riesgos que implica el uso de las tecnologías para sus actividades mercantiles.

2. La Información, la innovación, la creación de conocimiento y la transferencia y recepción de tecnología son los paradigmas del siglo XXI que están transformado la sociedad y el ámbito empresarial. El derecho comercial asume de manera paulativa ese desafío mediante la adecuación del derecho informático, propiedad intelectual e industrial, derecho del emprendimiento y de la seguridad de la información, entre otros.

3. Las empresas de tecnología y del ecosistema digital tienen un grado de responsabilidad derivado de regulaciones legales a sus actividades por desempeñar el servicio público de prestación de servicios y provisión de redes TIC.

4. El uso de tecnologías propias o de terceros deben estar amparados por derechos propietarios como patentes de invención, modelos de utilidad y diseños industriales o ser el resultado de transferencia o licencia de tecnología.

5. Las empresas tradicionales que utilizan tecnología para sus actividades mercantiles deben ser conscientes de la responsabilidad que tienen por el hecho de que llevan a cabo transacciones mediante comercio electrónico o que ofrecen sus productos y servicios por medios electrónicos a consumidores

6. La información es el nuevo bien inmaterial que tienen los empresarios para moldear sus modelos de negocios y como canal de relacionamiento con proveedores, contratistas, consumidores y usuarios, lo cual obligue a determinar y mitigar los riesgos por el uso y explotación de la información propia y de terceros.

7. El régimen de responsabilidad de los administradores por sus funciones y por la extralimitación de las mismas debe diferenciar la asunción de riesgos en el marco de la innovación y la adopción de tecnologías en el curso normal de las actividades de la empresa y las actividades que impliquen ilegalidad o conductas dolosas. El actual proyecto de reforma del régimen societario propuesto por el gobierno que incluye reglas renovadas respecto a la responsabilidad de los empresarios es una excelente oportunidad para seguir ese camino.

8. La confidencialidad y el secreto empresarial son categorías contractuales y legales que requieren medidas y prácticas jurídicas y contractuales para garantizar su eficacia y cumplimiento.

9. Los datos personales son una categoría de información que tiene protección constitucional, legal y regulatoria, con una amplia jurspruden-cia de la Corte Constitucional y con la Superintendencia de Industria y Comercio como Autoridad Nacional de Protección de Datos. Los derechos de acceso, rectificación, cancelación y oposición deben ser cumplidos *so pena* de que exista una sanción administrativa, indemnización de perjuicios e incluso la comisión del delito de violación de datos personales.

10. Las empresas deben definir los nuevos roles que cumplen empleados y contratistas en relación con la información de la empresa, desde el nivel directivo hasta las personas que tienen contacto directo con los consumidores y usuarios.

11. La seguridad de la información compete a todos los niveles de una entidad u organización. Los directivos deben facilitar el cumplimiento de la estrategia y políticas de seguridad de la información y proyectar esos deberes a todos los funcionarios. En las negociaciones con terceros, se deben establecer las obligaciones contractuales para que se cumplan los estándares de seguridad de la información.

12. Las empresas deben definir el rol de los nuevos empleos y funciones al interior de la empresa para utilizar y explotar las nuevas herramientas informáticas y de internet, entre ellos los de del CIO, CISO, CTO, el web master y el community manager.

13. El uso de las tecnologías puede acarrear responsabilidad para los empresarios. Las tecnologías pueden utilizarse de mala fe y con dolo para causar daños y perjuicios a terceros. La mala intención puede ser en el uso mismo de la tecnológia como herramienta para afectar y perjudicar o de manera deliberada y conciente la infracción de las reglas que atribuyen titularidad y protección a los derechos respecto de la tecnología.

14. En la era digital, se produce la integración de funciones, la desmaterialización de procesos y documentos, métodos de control y vigilancia electrónica, nuevos canales electrónicos de comunicación y de intercambio de productos y servicios (comercio electrónico B2C y B2B) que generan.

15. Las empresas deben adoptar políticas para el manejo y gestión de propiedad intelectual, innovación y transferencia de tecnología, sistemas de gestión y administración de la seguridad de los sistemas de información utilizados por la empresa, políticas de seguridad documental, retención documental, archivo y gestión de pruebas digitales y computación forense, política de recaudo, recolección, tratamiento de datos personales, políticas y medidas tecnológicas de protección de información confidencial y política de trazabilidad de las transacciones electrónicas con los consumidores.