RESPONSABILIDAD CIVIL DERIVADA DE LA RUPTURA DE DEBERES U OBLIGACIONES DE PROTECCION DE INFORMACION PERSONAL

ANA CAROLINA GÓMEZ ARIAS
ERIKA BOTERO ARISTIZÁBAL

UNIVERSIDAD EAFIT
FACULTAD DE DERECHO
MEDELLÍN
2016

RESPONSABILIDAD CIVIL DERIVADA DE LA RUPTURA DE DEBERES U OBLIGACIONES DE PROTECCION DE INFORMACION PERSONAL

ANA CAROLINA GÓMEZ ARIAS
ERIKA BOTERO ARISTIZÁBAL

Trabajo de grado presentado como requisito para optar el título de Abogado

Asesora
Estefanía Gómez Arias
Abogada Especialista en Responsabilidad Civil y Seguros

UNIVERSIDAD EAFIT
FACULTAD DE DERECHO
MEDELLÍN
2016

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Medellín, julio de 2016

TABLA DE CONTENIDO

INTRODUCCIÓN

En las últimas décadas del Siglo XX y comienzos del Siglo XXI la sociedad se ha visto inmersa en una era digital debido al gran desarrollo de las tecnologías que han cambiado la concepción de la comunicación, de la comercialización, el consumo, entre otras, logrando modificar varias esferas de la misma. Una de las grandes novedades que presentó la tecnología fue el Internet, el cual es definido hoy en día como una red de redes descentralizada de carácter internacional que permite la comunicación simultánea entre diferentes ordenadores ubicados en cualquier parte del mundo y por medio de la cual se puede compartir información.

El Internet actualmente es un fenómeno mundial que se encuentra presente en el día a día de la mayoría de población, de acuerdo con las cifras de Internet WorldStats cuya página web que se cita a nota al pie[1] a noviembre de 2015, el 46.4% de la población mundial es usuaria de Internet lo que corresponde a un aumento del 832.5% de usuarios entre los años 2000 a 2015. Es evidente el gran auge que ha tenido este espacio en el Siglo XXI y la razón por la cual se le ha llamado era digital, abarcando no solo la vida de las personas naturales sino en gran escala a las personas jurídicas, las cuales han desarrollado sus ideas de negocio con ayuda del Internet.

El Internet ha sido una herramienta que ha facilitado el desarrollo de las civilizaciones, el mundo de los negocios y de los gobiernos, razón por la cual es una red que contiene gran información personal, financiera y confidencial. Es por

[1] http://internetworldstats.com/stats.htm

[2] Para efectos de esta monografía se le denominará delincuente informático a toda persona o grupo de personas que cometa uno o varios delitos informáticos. En esta definición se encuentran incluidos, entre otros, los hackers, crackers, carders y piratas de software. Por hacker se entiende un individuo que se especializa en obtener acceso no autorizado a sistemas informáticos; así mismo un pirata de software es quien distribuye o recoge softwares informáticos protegidos con

esto que es atractiva para los delincuentes informáticos[2] que buscan obtener la información que se recolecta allí, exponiéndola a múltiples riesgos como los ataques cibernéticos que se llevan a cabo por delincuentes informáticos por medio de las armas cibernéticas, tales como virus informáticos o malware, gusanos, troyanos, entre otros.

Las consecuencias de su uso pasan desapercibidas, sobre todo, por los ciudadanos quienes están inadvertidos de que son potenciales víctimas de incidentes por el uso de esta, debido a que su información personal o crediticia puede ser conocida por personas inescrupulosas que desean manejar esta información de manera fraudulenta.

Los riesgos cibernéticos en la actualidad son uno de los principales riesgos empresariales a nivel mundial debido al aumento de los casos en que se ha presentado ataques cibernéticos y al auge que este medio ha producido en el desarrollo de los negocios; es así como las empresas han visto la necesidad de tomar medidas para protegerse de dichos ataques, los cuales consisten en el robo de información de las empresas, ya sea con un objetivo de espionaje corporativo, robo de número de tarjetas de crédito y débito de sus clientes, u otros. Al mismo tiempo otro de los objetivos de estos ataques es el robo de la información confidencial de gobiernos u organizaciones internacionales, por lo cual éstos también se encuentran en la misma posición de los empresarios, es decir, buscando proteger su información.

[2] Para efectos de esta monografía se le denominará delincuente informático a toda persona o grupo de personas que cometa uno o varios delitos informáticos. En esta definición se encuentran incluidos, entre otros, los hackers, crackers, carders y piratas de software. Por hacker se entiende un individuo que se especializa en obtener acceso no autorizado a sistemas informáticos; así mismo un pirata de software es quien distribuye o recoge softwares informáticos protegidos con copyright (Tomado de: MEYER, Gordon R. The social organization of the computer underground. NORTHERN ILLINOIS UNIV DE KALB, 1989. Pág 15). Por otro lado cracker es aquella persona que se infiltra en sistemas informáticos ilegalmente con el fin de robar, modificar o destruir información (Tomado de: SERRANO BUITRAGO, Edison Raúl, et al. La práctica de delitos informáticos en Colombia. 2015. Pág 15). Finalmente por el término carders se entiende los sujetos que utilizan de forma ilegal tarjetas de crédito (Tomado de: ROSTECK, Tanja S. Hackers: rebeldes con causa. 2005)

De acuerdo a la relevancia del tema, esta monografía busca darle una mirada jurídica al asunto desde la perspectiva de las consecuencias jurídicas que se puedan presentar al materializarse un riesgo asociado a la información personal, en especial, en el ámbito de los sistemas informáticos, entre éstos riesgos están: el acceso, la manipulación, manejo, pérdida o robo de información o datos personales.

Se debe aclarar que este trabajo se centrará en los riesgos cibernéticos en los que pueda verse afectada la información personal (tanto de personas naturales como de personas jurídicas). Con especial énfasis en aquella que se encuentre en medios virtuales, en contraposición a aquellos físicos.

En el marco de lo anterior, este trabajo tiene como objetivo exponer a grandes rasgos el desarrollo del Internet, los riesgos que se pueden presentar respecto a la información personal que se encuentre en la red, la normatividad colombiana que se ha desarrollado al respecto, la responsabilidad civil que se pueda presentar en caso de una eventual vulneración de información personal y una breve mirada de los delitos informáticos y transnacionales. Antes de pasar a enunciar la división del texto, es relevante indicar que este trabajo no pretende profundizar en todos los riesgos cibernéticos sino en aquellos en los cuales se pueda ver vulnerado el derecho fundamental a la intimidad personal y al buen nombre contemplado en el Artículo 15 de la Constitución Política de Colombia de 1991, ni se pretende indicar cuál debe ser la regulación correspondiente al respecto sino analizar la regulación actual del tema.

Una vez hecha esta salvedad, se pasa a enunciar el contenido de la monografía que estará dividido en cinco secciones. En la primera de ellas se expone la era digital, en aras de contextualizar al lector sobre el fenómeno que se está viviendo y sus características, así como las definiciones de los términos relevantes para

este estudio respecto al uso de información digital. Esta primera sección funde las bases para el desarrollo y entendimiento de la segunda sección, en la cual se presenta el objetivo del trabajo. Esta sección profundiza en aspectos generales y específicos de la responsabilidad civil y en la regulación de la protección de datos en Colombia, así como de la responsabilidad que se configuraría por el incumplimiento de esta.

En la tercera sección, debido a la falta de jurisprudencia colombiana en relación a los ataques cibernéticos, se acudió a jurisprudencia y casuística Norteamericana e Inglesa para analizar el trato que estos países le han dado a estas situaciones, ya que en razón de la frecuencia y magnitud de sus eventos los han tenido que enfrentar constantemente y tienen cierta evolución jurídica y práctica frente al tema. Los casos prácticos que serán presentados en esta sección serán posteriormente analizados de forma breve en contraste con la regulación colombiana. Este análisis enriquece al trabajo en la medida que nos permite dar una mirada a los eventos que se han dado en otros sistemas jurídicos y permite conocer el trato que se le han dado a estos para así extraer los elementos que podrían complementar el sistema jurídico colombiano en este ámbito.

La cuarta sección trata de la responsabilidad penal por delitos informáticos, qué sucede cuando son transnacionales, debido a que estas dos responsabilidades (civil y penal) pueden surgir simultáneamente frente a un mismo hecho imputable. Este capitulo no pretende estudiar exhaustivamente la responsabilidad penal que pueda surgir por la ocurrencia de estos delitos informáticos, sino aproximar al lector a estos en cuanto a la relación entre ambas responsabilidades respecto al supuesto de hecho. La última sección enunciara las conclusiones pertinentes del presente estudio.

1. ERA DIGITAL

Con el fin de contextualizar al lector abogado acerca del fenómeno que se está viviendo en la actualidad llamado era digital, a continuación se presentará brevemente la historia del Internet al ser la herramienta principal por medio de la cual la era digital ha logrado desarrollarse, igualmente las definiciones técnicas necesarias para el entendimiento del mundo digital, así como también se nombrarán algunos de los usos que se le han dado al Internet en los que se ven reflejados los riesgos cibernéticos, los cuales también serán abordados para su conocimiento y comprensión.

1.1 HITOS DEL INICIOS DEL INTERNET

"*La cultura es uno de los grandes carriles de las autopistas del conocimiento en las sociedades post-industriales. En este plano estamos en tránsito desde la sociedad que da más prioridad a los sistemas, redes y aparatos de la información, o a la propia información como ítem, que al conocimiento, los contenidos, la cultura y el aprendizaje*"[3].

En el último cuarto del siglo XX, una revolución tecnológica centrada en torno a la información transformó el modo de vivir de la sociedad. En todo el planeta se ha constituido una economía global dinámica, enlazando a la gente, a los entes y a las actividades valiosas de todo el mundo mientras se desconecta de las redes de poder y riqueza a los pueblos y territorios carentes de importancia desde la perspectiva de intereses dominantes. Una cultura de la virtualidad real, constituida en torno a un universo audiovisual cada vez más interactivo y cambiante ha calado

[3]ELGUEZABAL, R. Z. Estructuras de la comunicación y la cultura: Políticas para la era digital. Editorial Gedisa. 2011. p. 25.

la representación mental y la comunicación, integrando la diversidad de culturas en un hipertexto electrónico[4]. El hoy llamado Internet.

Su importancia radicó en ser un mecanismo que propagaba la información en una velocidad no antes vista hasta la época y que logró convertirse en un medio indispensable de comunicación entre los individuos independientemente de su localización geográfica[5]. Esta revolución dio como resultado la era digital que se vive desde finales del Siglo XX hasta la actualidad.

En el libro "*Cyber Security 2.0 & The History of the Internet"* del profesor Michael J. Woodrow se encuentran los principales hitos de la historia del Internet que se presentarán brevemente a continuación:

- En los años 50 como consecuencia del Proyecto RAND surgió un método de conectar computadoras que consistía en permitir a las terminales conectarse a través de largas líneas alquiladas con la ayuda de un computador central.
- J.C.R. Licklider fue quien comprendió la necesidad de una red mundial. Este se refería a una red de muchos ordenadores conectados mediante líneas de comunicación de banda ancha con avances en el guardado y adquisición de información. Este era el objetivo del Internet. Relacionar a computadores que pudieran intercambiar información. En 1962 Licklider creó un grupo informal dentro de la oficina de procesamiento de información (DARPA) del Departamento de Defensa de los Estados Unidos con el fin de desarrollarla, finalmente esta red se denominó ARPANET y era utilizada para funciones estatales. Esta fue la red que finalmente se convirtió en el Internet.

[4]CASTELLS, M. La era de la información: economía, sociedad y cultura, Vol. 3. siglo XXI. 2004. p. 25.
[5]LEINER, B. M., CERF, V. G., CLARK, D. D., KAHN, R. E., KLEINROCK, L., LYNCH, D. C.& WOLFF, S. Una breve historia de internet. Primera y segunda parte, 1999. p. 1.

- En la década de los 70 nació la red UUCPnet, creada por dos estudiantes de la Universidad Duke. Esta red nació con el objetivo de transferir noticias y mensajes entre universidades pero luego su software se hizo público.
- En 1978, aparecieron los protocolos TCP/IP[6]. En 1983, estos fueron los únicos protocolos aprobados en ARPANET.
- La década de 1980 fue crucial ya que en esta se implementaron las tecnologías que se reconocerían como las bases de la moderna Internet. Junto con DARPA, la National Science Foundation (NSF) se involucró fuertemente en la investigación en Internet y empezó un desarrollo como sucesor de ARPANET. En 1986 esto resultó en la primera red de banda ancha diseñada específicamente para usar TCP/IP, llamada NSFNet su función era conectar y proveer acceso a una cantidad de supercomputadores establecidos por la NSF para usos investigativos y educativos. El Internet surgió entonces como la fusión entre ARPANET y NSFNet, definido como cualquier red que usase el protocolo TCP/IP.
- En 1990 ARPANET se disolvió y TCP/IP la sustituyó como también a la mayor parte de los protocolos de grandes redes de ordenadores.
- En esta misma época se introdujo la World Wide Web[7] por Tim Berners-Lee[8], esta red informática ha permitido a los usuarios acceder fácilmente a información distribuida a través del mundo[9].

---

[6] Los dos protocolos más importantes son los que dan nombre a toda la familia: IP ("Internet Protocol") y TCP ("Transmission Control Protocol"). El protocolo IP es una red de conmutación de paquetes en la que la información a transmitir es fragmentada en trozos o paquetes, mientras que el protocolo TCP se encarga de subsanar las posibles deficiencias para conseguir un servicio de transporte de información fiable de cara a las aplicaciones. Tomado de: SANZ, Miguel Ángel. A, B, C de Internet. *RedIRIS-Boletín de la red nacional de I+ D*, 1994, vol. 28, p. 15-30.

[7]"En informática, la World Wide Web (WWW) o red informática mundial es un sistema de distribución de documentos de hipertexto o hipermedios interconectados y accesibles". Recuperado de: vía Internet.https://es.wikipedia.org/wiki/World_Wide_Web.

[8]BIANCHINI, A. Conceptos y definiciones de hipertexto. Reporte Técnico Interno. Departamento de Computación y Tecnología de la Información, Universidad Simón Bolívar. Caracas. 1999. .pág 2. Disponible en: http://ldc. usb. ve/~ abianc/hipertexto. pdf.

[9]LEINER, B. M., CERF, V. G. CLARK, D. D., y otros, Op cit. p 16

Todo comenzó con la idea de una red de computadoras diseñada para permitir la comunicación general entre usuarios de varias computadoras, desde allí la evolución ha sido constante y notoria. En sus inicios el correo electrónico fue el uso principal que se le dio al Internet[10].

Otra clasificación que se le ha dado a la evolución de esta red consiste en la diferenciación de cuatro etapas de su funcionamiento. La web 1.0 es conocida como la web de cognición, la web 2.0 como la de comunicación, la 3.0 como la de cooperación y la 4.0 como la de integración.

La Web 1.0 nació como un espacio de lectura de información principalmente, a su predecesora se le añadió la opción de escritura, por su parte la Web 3.0 o "*web semántica*" quería facilitarle la vida a los usuarios con contenidos que se leían por el mismo computador. Por último la 4.0 o webOS que tiene interacciones inteligentes, una web para leer, escribir y ejecutar. Esta web alcanza una participación importante en redes online pues intervienen en el gobierno, distribución, participación, colaboración de sectores clave como la industria, la política y la comunidad en general[11].

La definición que se tendrá en cuenta de Internet para continuar con el presente escrito, es la propuesta por la Corte Suprema de Estados Unidos, "*una red internacional de computadoras interconectadas, que permite comunicarse entre sí a decenas de millones de personas, así como acceder a una inmensa cantidad de información de todo el mundo"*[12]*.*

Una vez identificados los períodos más relevantes en cuanto a la historia del Internet y con el fin de comprender los tecnicismos del mundo digital que serán

[10]"Cyber Security 2.0 & The History of the Internet". 2014.Pág 18. Michael J. Woodrow
[11]AGHAEI, S., NEMATBAKHSH, M. A., &FARSANI, H. K. Evolution of the world wide web: from Web 1.0 to Web 4.0. International Journal of Web & Semantic Technology, 2012. vol. 3,1, p.1-10.
[12]HOCSMAN, Simón Heriberto. Negocios en Internet. Editorial Astrea. 2003. p. 224.

utilizados a lo largo de este escrito, a continuación se hará un estudio de los conceptos básicos que van a permitir entender el mundo del Internet y sus aspectos más importantes, al ser estos ajenos al lenguaje jurídico y al uso común.

1.2 Definiciones Relacionadas con el Uso de la Información Digital

Al hacer el estudio de la protección de datos personales en el contexto de la información digital no se puede dejar de lado que el mundo de la tecnología tiene un lenguaje técnico, que se hace necesario detallar para comprender a cabalidad el ámbito de protección de la regulación colombiana en esta esfera y el objetivo de este trabajo.

Para empezar, el riesgo de un sistema informático es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del Sistema Informático, causando un impacto en el dueño de la información, el riesgo es característico para cada amenaza y cada sistema, pudiéndose disminuir tomando las medidas adecuadas; mientras que es llamado un incidente de seguridad, a cualquier evento que tenga, o pueda tener como resultado, la interrupción de los servicios suministrados por un Sistema de Información y/o pérdidas físicas, de activos o financieras. En otras palabras la materialización de una amenaza, al siempre existir riesgos, es posible que se materialice.[13]

Un sistema de información es definido como "*todo sistema utilizado para generar, enviar, recibir, archivar, conservar o procesar de alguna otra forma mensajes de datos*"[14]. Así como el término cloud o nube se utiliza para hacer referencia de manera indistinta a Internet, Intranet, Extranet, es decir, a redes digitales o empresariales con capacidad de transmisión, lo que lleva a que la computación en

[13]MELIÁN, J. M. M. Riesgos cibernéticos. Cuadernos de estrategia, 2003. No.120, p.131.

[14] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 527 de 1999. Artículo 2 (agosto, 18,1999). por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Diario Oficial 43.673. Bogotá.

la nube sea una expresión que se refiere al almacenamiento y procesamiento de información, con base en una lógica de coordinación en Internet[15].

El término Big Data también ha empezado a ser utilizado a medida que más y más datos están siendo almacenados por el gobierno, compañías y personas en el marco de una vida interactiva cada vez más ocupada. Este concepto se refiere a la "*recolección masiva de información sobre clientes, ciudadanos, y empresas. Se presenta como una nueva generación del mercadeo digital en que se utilizan las capacidades de captura de datos en línea y en los dispositivos móviles con el fin de lograr mejor conocimiento de las tendencias de consumo y en general de los hábitos de navegación o uso de aplicaciones*[16]". Y por supuesto las TIC[17], que se trata de una gama amplia de servicios, aplicaciones y tecnologías que utilizan diversos tipos de equipos y de programas informáticos, que generalmente se transmiten a través de las redes de telecomunicaciones[18]. O en palabras más simples, "*son un conjunto de productos y servicios, utilizados por medio de un equipo informático o electrónico que sirven para generar, transmitir y recibir información, y para ello se valen de cualquier red o infraestructura existente*"[19].

Con el fin de salvaguardar la información, aparece la palabra ciberseguridad[*20*], la cual se define por la Unión Internacional de Telecomunicaciones (UIT) como el conjunto de herramientas, políticas, directrices, conceptos de seguridad, métodos de gestión de riesgos, acciones, practicas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Por otro lado, por activos se entiende los dispositivos informáticos,

[15] PEÑA VALENZUELA, Daniel y BAZZANI MONTOYA, Juan David. Aspectos legales de la computación en la nube. Universidad Externado de Colombia. 2012.p.15.
[16] Ibid., p.84.
[17] Tecnologías de la Información y las Comunicaciones.
[18] COMISIÓN AL CONSEJO Y AL PARLAMENTO EUROPEO .Comunicado de 14 de diciembre de 2001.
[19] Occit., RINCON, p. 3.
[20] Relacionado a la ciberseguridad, se conoce la ciberdefensa que trata de proteger al Estado de amenazas cibernéticas. Es decir, tienen un foco distinto pero con un objetivo común.

los servicios-aplicaciones, los sistemas de comunicaciones y en general la totalidad de información transmitida o almacenada en el ciberentorno[21].

De igual modo, el desarrollo legislativo ha permitido identificar definiciones de conceptos con gran importancia para esclarecer la normatividad respecto a la recolección de información o datos personales y generar un mayor uso de los medios electrónicos desde años atrás.

El comercio, con el desarrollo del Internet, ha llegado a tener una categoría propia llamada comercio electrónico que se conoce como el intercambio de información entre personas que da lugar a una relación comercial, consistente en la entrega en línea de bienes intangibles en un pedido electrónico de bienes[22] y el importante mensaje de datos o información digital que la Ley 527 de 1999 define como "*la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax*", es decir, es un concepto global en cuanto a comunicación e información digital. Y por su parte el Intercambio Electrónico de Datos (EDI) es "*la transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto[23]".* En relación a lo anterior, la información reservada se dice que es la información de alta sensibilidad que debe ser conocida por un reducido grupo de personas por su criticidad para el desarrollo de un trámite[24].

[21] Op cit., RINCON, p. 427
[22] Ibid., p.11.
[23] Op cit, COLOMBIA, Ley 527 de 1999. Artículo 2.
[24]Op cit., RINCON, p.133

1.3 USOS DEL INTERNET

Con el Internet y su capacidad para llegar a millones de personas en el mundo, la posibilidad de comprar, vender y saber los datos de las dos partes de la relación comercial en el mismo momento, cambió el dogma de negocio establecido en la publicidad, las ventas por correo y muchas más áreas. La web fue una red revolucionaria, la cual podía juntar compradores y vendedores sin relación previa de manera fluida y con bajo costo, desde allí su desarrollo y acogida no se ha detenido.

Cada vez Internet tiene más usuarios y más cabida en la vida diaria de la población. La mayoría de las personas usan constantemente Internet sin ser conscientes de ello; no sólo se está tomando la vida personal de cada uno, también las empresas cada vez se interconectan y dependen más de las redes. La facilidad de intercambio de información que el Internet ha generado tiene consecuencias. A medida de que avanza la tecnología también lo hace la susceptibilidad a ser atacada y un asalto sorpresivo es fatal si se hace en la esfera correcta. El fenómeno que ha generado la era digital es un tema de revisión global, debido a que el Internet ha interconectado al mundo en una forma en la que muchas veces no se necesita hablar de zonas geográficas pues mientras estés conectado, desaparece lo tangible.

Las estadísticas de uso de internet, tanto nacionales como regionales, permiten determinar una tendencia clara sobre los principales usos de la red por parte de los usuarios, los cuales corresponden a funciones tradicionales, las principales son: búsqueda de información, correspondencia por email y uso de las redes sociales.[25]

[25]MARTIN, P. E. Inseguridad Cibernética en América Latina: Líneas de Reflexión para la evaluación de riesgos, 2015. p. 6.

En Colombia en el año 2014, según el Banco Mundial, había 52,6 usuarios de Internet por cada 100 personas[26], mientras que para el 2015 esta cifra había aumentado a 59.1% usuarios de Internet correspondiente a 28,475,560 personas, demostrando la fuerza que tiene el Internet para conseguir usuarios de su red.

De acuerdo a Internet WorldStats[27], entre el año 2000 a 2015 los usuarios de Internet han aumentado en un 832.5%, es decir, que para el año 2015 habían 3,366,261,156 usuarios de Internet en todo el mundo. El mayor número de usuarios de Internet se encuentran en el continente de Asia, con un 48.2%, continuando con Europa con 18%, Latino América 10.2%, África 9.8%, Norte América 9.3%, correspondiéndole un 87.4% de ese porcentaje; Medio Oriente y Oceanía suman el 4.5% faltante.

Debido al gran auge de esta red, aparece el concepto de *persuative computing*[28], pues la sociedad se encuentra ante un cambio de paradigma de uso del Internet, al pasar de conectarse puntualmente a estar siempre conectada gracias a los dispositivos móviles como el Smartphone. Anteriormente eran incompatibles el uso del teléfono y la utilización del Internet, hoy en día existe un teléfono que además de móvil, tiene Internet para múltiples funciones, entre estas, llamar gratuitamente.

Nuevas tecnologías como la impresión 3D, los *werables*, que son ropa y complementos que adquieren conectividad y capacidad de procesamiento, suponen una evolución del Internet, por ejemplo hacía el Internet de las Cosas, el ámbito personal que convierte a objetos de uso cotidiano en aliados, se ha desarrollado principalmente en forma de relojes inteligentes y dispositivos de

[26]BANCO MUNDIAL. Usuarios del internet (por cada 100 personas). Recuperado de: http://datos.bancomundial.org/indicador/IT.NET.USER.P2
[27]INTERNET WORLD STATS. *World internet usage and population statistics* november 30, 2015 – update. Recuperado de : http://internetworldstats.com/stats.htm
[28]Computación Obicua.

monitoreo de la salud[29], haciendo cada vez la vida más fácil pero al mismo tiempo volviendo a las personas más y más dependientes del Internet, lo que supone al mismo tiempo un incremento en el uso de los dispositivos susceptibles de ataques cibernéticos en busca de información digital.

El robo de información, la suplantación electrónica, el fraude, el bullying, la pérdida de privacidad y la difamación, son algunas de las formas de estar expuestos ante este espacio que no es posible controlar, cuya magnitud y complejidad está más allá del manejo de un simple usuario, es por esto que se debe ahondar un poco acerca de estos.

1.4 RIESGOS CIBERNÉTICOS

Debido al gran auge que ha tenido el Internet en la sociedad y el avanzado desarrollo de este, ha logrado volverse indispensable en la vida de las personas y a su vez ser una herramienta fundamental para el manejo de empresas y Gobiernos; por lo anterior, es un instrumento en el cual se concentra la información confidencial de estos sujetos, volviéndose un foco de atracción de amenazas y ataques con el objetivo de obtener la información que se recolecta allí, exponiéndola a múltiples riesgos.

La privacidad es hoy en día uno de los derechos que más se busca proteger y el hecho de que una red abierta como el Internet, que almacena las bases de datos de Gobiernos y empresas, no ofrezca un alto grado de seguridad de la información complica el progreso del comercio electrónico, lo cual lleva a que en la actualidad se busquen medidas para salvaguardar dichos datos, las cuales deben ser adoptadas por dos vías: técnica y jurídica.

[29]TELEFÓNICA, F. La Sociedad de la Información en España 2013: siE *13*. Fundación Telefónica. Prólogo. 2014.

Los criminales informáticos utilizan diferentes medios para lograr sus objetivos, dentro de estos se encuentran los *virus informáticos*[30]*, "Su finalidad es controlar al ordenador para poder hacer una copia de sí mismo. Se trata de un aparato reproductor. Una vez ejecutado el programa con el virus, se reproduce en una copia exacta, etc. Se trata de un sistema perfecto de serialidad al infinito. Así, el virus es un sistema reproductor de sí mismo en forma automática, un Ara (auto-reproductor-automático)."*[31] El primer virus fue creado por el investigador Robert Thomas Morris, en el año 1972, el cual desafiaba a la comunidad informática de que se le cazara.

Desde 1972, los virus informáticos han sido el principal arma de los criminales informáticos[32] con el fin de robar o manipular indebidamente la información que tengan los ordenadores, destruir información, dañar hardware, controlar el ordenador y todos aquellos que se encuentren conectados por una red, entre otros. A este tipo de actuaciones de los criminales se les denomina ataques cibernéticos.

Otras de las armas cibernéticas más utilizadas para cometer estos delitos son los gusanos, que no son más que programas independientes que pasan de una computadora a otra; y los troyanos que son fragmentos de códigos que se ocultan en los programas y desempeñan funciones no deseadas.[33]

Los ataques cibernéticos son una amenaza latente de todos aquellos que utilizan Internet y el "*crecimiento sostenido del mercado negro de la información, funciona como motor que impulsa una importante masa de ataques informáticos,*

[30]Fred Cohen, en 1983, denominó por primera vez a los programas que pudieran modificar otros programas y auto-replicar, como *virus informático.*
[31]VILCHEZ, Lorenzo. La construcción social del virus informático. En: Revista Signo y Pensamiento, Universidad Javeriana. 2000
[32] Ibid, p. 225
[33] Ibid, p. 225

principalmente destinados a obtener bases de datos con información personal"[34], además de otorgar la facilidad de que el delincuente informático opere desde cualquier lugar del mundo.

Los ataques cibernéticos pueden tener como finalidad:

> *"1. Tener acceso a la red sin autorización. 2. Destrucción de información y de recursos de la red. 3. Introducción o modificación de información. 4. Revelación de la información. 5. Causación de interrupciones o de un mal funcionamiento de la red de servicios. 6. Robo de información y recursos de la red. 7. Denegación de servicios recibidos o de información enviada o recibida. 8. Manifestación de estar entregando la provisión de servicios que no han sido administrados o de haber enviado o recibido información no recibida".*[35]

Es posible que este objetivo se logre con un solo ataque o por el contrario se requiera de varias intromisiones para lograr lo que se propuso.

Estos ataques cibernéticos buscan lograr vulnerar cada una de las esferas de la seguridad informática, como lo son (i) la integridad, la cual busca que la información enviada a sus destinarios llegue sin haber sufrido alteraciones, se afecta con la modificación de la información por parte de los atacantes; (ii) la disponibilidad implica que las partes autorizadas tengan la posibilidad de tener un acceso constante y continuo a la información, se vulnera por medio de la interrupción al acceso de la información o su destrucción; (iii) la característica de confidencialidad de la información requiere que esta no pueda ser leída, copiada, modificada o revelada sin la debida autorización y principalmente no pueda ser interceptada por terceros ajenos a esta; y por último (iv) la autenticidad exige que se pueda verificar quien es el emisor de la información, la cual se quebranta con la introducción de objetos falsificados en el sistema.[36]

---

[34]TEMPERINI, Marcelo Gabriel Ignacio. Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte.
[35]HOCSMAN, Op cit., p. 232.
[36]Ibid

Alrededor de estas esferas de la seguridad informática debe y efectivamente gira, como se detallará más adelante, la regulación de la protección de la información personal en medios digitales. El hecho imputable, presupuesto esencial de la responsabilidad civil, constituirá finalmente en la perturbación de alguno de estos elementos.

Dado a que una de las principales intenciones del delincuente informático es producir un daño en el sistema, se ha requerido el desarrollo de mecanismos para protegerse y defenderse de estos ataques. El mecanismo por excelencia lo denominan antivirus, el cual es la manera más común de prevenir algunos de los daños informáticos, que actúa "*reconociendo el problema apenas se inserta en la computadora y en el sistema, impidiendo que este propague sus efectos*"[37].

Aunque la finalidad del antivirus es prever los daños que generan los ataques cibernéticos no logra ser suficientes para detener a estos delincuentes, lo cual exige que los blancos de estos ataques (personas naturales, jurídicas, organismos gubernamentales y organizaciones globales) deban centrar su mayor atención en generar medidas dentro de su propia organización que eviten que estos criminales logren su objetivo.

La importancia de esta investigación radica en que en países más desarrollados que Colombia se han presentado ataques cibernéticos con perjuicios tan grandes que afectan no solo a la víctima como tal sino también la confianza en el uso del Internet, tanto por las sumas económicas que involucra, como por la vulneración al buen nombre de la persona, además de generar un lucro cesante por parte de las empresas cuando sus canales virtuales, que contienen información personal, son infiltrados. Durante el desarrollo del trabajo, como un ejemplo de esto, se referirán casos de Estados Unidos e Inglaterra para el tema de estudio.

[37] Ibid., p.244.

2. FUENTES DE RESPONSABILIDAD DERIVADA DEL USO DE LA INFORMACIÓN EN MEDIOS DIGITALES

Una vez descrita la importancia del Internet en las relaciones privadas y de negocios de ésta era digital y habiendo estudiado los eventos que han ocurrido en países como Inglaterra y Estados Unidos, en donde se han presentado robos de información que ponen en jaque la intimidad de las personas, su información confidencial e incluso un cese de negocio a las empresas víctimas de ese ataque. Procederemos a analizar cuál es el bien jurídico protegido por la regulación Colombiana frente a la materialización de un riesgo cibernético y posteriormente cuál es la regulación existente en Colombia enfocada en proteger la información y su tratamiento, dirigida tanto a prevenir que esta sea vulnerada como a proporcionarle consecuencias jurídicas a los comportamientos o hechos que la afecten; y para finalizar se revisarán dos fuentes de responsabilidad: la civil y la penal a la luz de la materialización de estos eventos.

2.1 NORMATIVIDAD COLOMBIANA DEL DERECHO FUNDAMENTAL A LA INTIMIDAD Y BUEN NOMBRE POTENCIALMENTE GENERADORA DE RESPONSABILIDAD CIVIL

Como eje fundamental de este estudio se encuentran los derechos fundamentales a la intimidad y al buen nombre, ya que pueden ser fácilmente vulnerados en el entorno de las prácticas tecnológicas y el Internet. Se les debe dar entonces, en primer lugar, una mirada para entender cuál es su verdadero contenido.

El artículo 15 de la Constitución Política de Colombia es el que contiene el derecho a la intimidad, el texto dice lo siguiente:

> **"***Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que*

se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley

Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley"[38].

Este derecho es particularmente importante en cuanto al uso del Internet, pues como se ha visto, las violaciones a bases de datos personales y bancarios, afectan la intimidad y hasta el buen nombre de las personas cuya información se ve comprometida. La misma Constitución le impone un límite al Estado en la intervención caprichosa de la intimidad de los ciudadanos y a su vez le asigna el deber de intervenir y emprender acciones con el fin de que no sean objeto de manipulación por parte de terceras personas. Este artículo además consagra el derecho al *habeas data*[39], la Corte Constitucional lo definió *como "el derecho que otorga la facultad al titular de datos personales de exigir de las administradoras de esos datos el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de su divulgación, publicación o cesión, de conformidad con los principios que regulan el proceso de administración de datos personales".* Así mismo, ha señalado que este

---

[38] COLOMBIA. Constitución Política. Artículo 250: (…)*En ejercicio de sus funciones la Fiscalía General de la Nación, deberá: (…) 2. Adelantar registros, allanamientos, incautaciones e interceptaciones de comunicaciones. En estos eventos el juez que ejerza las funciones de control de garantías efectuará el control posterior respectivo, a más tardar dentro de las treinta y seis (36) horas siguientes, al solo efecto de determinar su validez* (…) Esto con el fin de buscar elementos materiales probatorios, evidencia física, búsqueda y ubicación de imputados, indiciados o condenados. No podrán interceptarse comunicaciones del defensor y solamente se puede hacer por 6 meses, salvo orden del fiscal, que será posteriormente sometida a control por el juez de control de garantías (artículo 235 Código de Procedimiento Penal).

[39] El derecho de habeas data se encuentra actualmente regulado parcialmente por la Ley 1266 de 2008 en los temas concernientes al carácter financiero, comercial, de servicios y de terceros países.

derecho *"tiene una naturaleza autónoma que lo diferencia de otras garantías con las que está en permanente relación, como los derechos a la intimidad y a la información"*[40].

Estos derechos hacen parte de una serie de regulaciones que quieren abarcar y reafirmar todos los ámbitos de la protección a la información[41], intimidad y buen nombre de las personas. Es por esto que también tienen cabida en instrumentos de derecho internacional tales como el artículo 5º de la Declaración Americana de los Derechos y Deberes del Hombre que establece que "*toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar"* o el artículo 11 de la Convención Americana de los Derechos Humanos que por su parte dice que nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación, así como que tiene derecho a la protección de la ley contra estos últimos, que es equivalente en su texto al artículo 17 del Pacto Internacional de los Derechos Civiles y Políticos.

En cuanto a su carácter de derecho fundamental, muchas sentencias así lo afirman, tales como la T 405/07, T 437/04 y por supuesto la sentencia C 640 de 2010, la cual hace especial énfasis en el derecho a la intimidad y dice que "*desde 1992 la Corte Constitucional reconoció el derecho a la intimidad como un derecho fundamental que permite a las personas manejar su propia existencia como a bien lo tengan con el mínimo de injerencias exteriores".* Se habla de este como un derecho general, extrapatrimonial, inalienable e imprescriptible, tanto frente al Estado como a los particulares*,* es decir que solo por el hecho de ser persona se

[40]COLOMBIA. Corte Constitucional. Sentencia C-1011 de 2008. Magistrado Ponente: Jaime Córdoba Triviño.
[41]Constitución Política. "*ARTICULO 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación (…)"*

es titular de este derecho. Es tan grande su alcance que se entiende casi como un derecho absoluto y es que su finalidad es la de asegurar la protección de intereses morales, estando estrechamente ligado a la dignidad humana pues se deduce de esta y se considera que *"su titular no puede renunciar total o definitivamente a la intimidad pues dicho acto estaría viciado de nulidad absoluta".* Sus límites, según esta corporación, no son más que lo derechos de los demás y el ordenamiento jurídico[42].

En cuanto a la honra, se ha dicho que es un derecho que está relacionado con el valor intrínseco de los individuos frente a la sociedad y frente a sí mismos, parecido al buen nombre pues comparten parte de su significado al ser la estimación que tienen los demás miembros de la sociedad de una persona a quien conocen y tratan. El buen nombre se ha definido como *"la reputación, o el concepto que de una persona tienen los demás*", este puede ser vulnerado por particulares o por el Estado y puede ser amparado mediante acción de tutela[43].

En la sentencia T 406 de 1992 (M.P. Ciro Angarita Barón) se enumeran los requisitos que debe cumplir un derecho para que se entienda como fundamental, estos son: *"1) Conexión directa con los principios constitucionales; 2) Eficacia directa y 3) Contenido esencial".* Se entiende que los derechos constitucionales fundamentales no solamente se determinan porque la Constitución los mencione, sino también por su importancia para la realización de los principios y valores que se consagran en la misma y por la conexidad con otros derechos fundamentales, esta última interpretándose en cada caso concreto[44].

---

[42] COLOMBIA. Corte Constitucional. Sentencia C 640 de 2010. Magistrado Ponente: Mauricio González Cuervo.

[43] COLOMBIA. Corte Constitucional. Sentencia C-489/02. Magistrado Ponente: Rodrigo Escobar Gil.

[44] COLOMBIA. Corte Constitucional. Sentencia T 473 de 1992. Magistrado Ponente: Ciro Angarita Barón.

"La intimidad, el buen nombre y la honra son derechos constitucionalmente garantizados, de carácter fundamental, lo cual comporta, no sólo que para su protección se puede actuar directamente con base en la Constitución cuando a ello haya lugar, a través de la acción de tutela, sino que, además, de las propias normas constitucionales se desprende la obligación para las autoridades de proveer a su protección frente a los atentados arbitrarios de que sean objeto"[45].

Sin embargo, el problema radica es en la materialización de las normas más que en la falta de regulación. Si bien el tratamiento que se le ha dado a estos derechos es valioso y adecuado, sobre todo al considerarlos como fundamentales debido a que por su importancia lo ameritan, lo realmente significativo es que en el marco de la justicia del Estado se les esté dando el tratamiento judicial y administrativo necesario.

Es por esto que en Colombia se ha hecho un esfuerzo por regular la materia y proteger al titular de la información y tratar de adelantarse en materia normativa, a posibles realidades que en el mundo han demostrado ser fatales.

Ahora se identificarán los aspectos de la regulación de protección de datos personales en el ordenamiento jurídico colombiano que puedan tener relevancia en relación a los robos de información cibernética, esta se encuentra contenida en diferentes normativas que serán presentadas a continuación. En estas se busca reconocer cuáles son las obligaciones que se encuentran en cabeza de quienes manejan las bases de datos con información personal o crediticia; cuáles podrían ser las consecuencias de su incumplimiento; las definiciones y principios rectores del manejo de datos personales; los derechos de los titulares de la información; qué se debe entender por dato personal; cuál es el manejo adecuado que se le

[45]CORTE SUPREMA DE JUSTICIA**.** Sala De Casación Civil**.** Magistrado Ponente: Ariel Salazar Ramírez. Radicación: 11001310300320030066001. Bogotá D. C., cinco (5) de agosto de dos mil catorce (2014).

debe dar a la información personal; de qué se trata el Registro Nacional de Base de Datos, entre otros, reconociendo el aporte de cada una de las normas en este tema.

Al final de este recuento se hará un índice cronológico de la normatividad colombiana en el que se sintetizará el propósito de cada una frente al tema de la información personal.

2.1.1 Ley 527 de 1999

Por medio de esta Ley se *"define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales",* desarrollo legislativo que estuvo a la vanguardia con la era digital que se estaba comenzando ha desarrollar para el siglo XXI.

Por medio de esta Ley se reconoció jurídicamente el mensaje de datos o información digital, prohibiendo que se le niegue la validez, fuerza obligatoria o efecto jurídico a una información por el solo hecho de estar en forma de mensaje de datos, además pretendió que un requerimiento de firma se entienda satisfecho como mensaje de datos pero en realidad el objetivo principal de la Ley es el de otorgarle valor probatorio al mensaje de datos. Dando a entender que no porque un requisito jurídico no conste en papel debe ser rechazado, el derecho debe adaptarse a las necesidades de la sociedad y desde la creación de los computadores, la evolución acelerada de la tecnología hizo que leyes como estas tuvieran que ser creadas para estar a la vanguardia. Los mensajes de datos tienen una innegable importancia en el contexto de la sociedad actual, son el soporte electrónico con base en el cual se sustentan y se prueban las relaciones que se establezcan en los entornos electrónicos[46].

[46]RINCÓN CÁRDENAS, Erick. Derecho del Comercio Electrónico y de Internet. 2 ED. 2015.

2.1.2 Ley Estatutaria 1266 de 2008

Esta ley estatutaria por tratar derechos fundamentales fue la ley por medio de la cual se regularon temas como el habeas data y el manejo de información contenida en bases de datos. Su objetivo era desarrollar los preceptos del artículo 15 de la Constitución, así como los del artículo 20[47], en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países. Esta se aplica a la información personal contenida en un banco de datos de cualquier entidad, salvo las utilizadas internamente o por el DAS, la Fuerza Pública y las Cámaras de Comercio.

Establece definiciones que permiten identificar quién es el titular de la información[48], qué es un dato personal[49], un dato público[50], semiprivado[51] y privado[52], elementos que son de relevancia a la hora de identificar si los recolectores de información personal están cumpliendo con los parámetros de la protección de datos personales.

Esta ley establece en su artículo cuarto los principios de la administración de datos, los cual son:

---

[47] **"**Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación..." Subrayado fuera de texto.

[48] Artículo 3. "Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley".

[49] Artículo 3. "Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados".

[50] Artículo 3. "Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas".

[51] Artículo 3. "Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley."

[52] Artículo 3. "Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular."

1. Principio de veracidad o calidad de los registros o datos. La información debe ser veraz, completa, exacta, actualizada, comprobable y comprensible, no pueden registrarse o divulgarse datos parciales, incompletos, fraccionados o que induzcan a error;

2. Principio de finalidad. La administración de datos personales debe tener una finalidad legítima de acuerdo con la Constitución y la ley, esta se le debe informar al titular de la información antes o durante la autorización si esta es necesaria o siempre que el titular solicite información al respecto;

3. Principio de circulación restringida. *"Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley".* A su vez la administración de datos personales está limitada por la naturaleza de los datos, de las disposiciones de la presente ley y por los principios de la administración de datos personales especialmente por el de temporalidad de la información y la finalidad del banco de datos;

4. Principio de temporalidad de la información. "*La información del titular no podrá ser suministrada a usuarios o terceros cuando deje de servir para la finalidad del banco de datos*";

5. Principio de interpretación integral de derechos constitucionales. Este principio busca que esta ley se interprete de acuerdo a la protección de los derechos constitucionales de los titulares especialmente el hábeas data, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información;

6. Principio de seguridad. La información se deberá manejar con las medidas técnicas que sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado;

7. Principio de confidencialidad. Todas las personas naturales o jurídicas, no públicas, que intervengan en la administración de datos personales están

obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma[53].

Estos principios son un derrotero de cómo se debe manejar la información contenida en bases de datos, identificándose que están dirigidos a la protección de los derechos fundamentales del titular de la información, pretendiendo que la información no pueda ser conocida por terceros no autorizados.

Además, establece tácitamente quiénes se encuentran autorizados para recibir la información que se encuentra recolectada en las bases de datos, indicando que únicamente (i) los titulares, personas debidamente autorizadas por estos y sus causahabientes mediante el procedimiento previsto por esta ley; (ii) los usuarios de la información[54] (dentro de ciertos parámetros); (iii) cualquier autoridad judicial, previa orden judicial; (iv) entidades públicas del poder ejecutivo, cuando el conocimiento de dicha información esté relacionada directamente al cumplimiento de alguna de sus funciones; (v) órganos de control y demás dependencias de investigación disciplinaria, fiscal, o administrativa, cuando esta sea necesaria para

---

[53] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1266 (31, diciembre, 2008). por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario oficial, Bogotá , 2008.

[54] Artículo 3. *"El usuario es la persona natural o jurídica que, en los términos y circunstancias previstos en la presente ley, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información. El usuario, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. En el caso en que el usuario a su vez entregue la información directamente a un operador, aquella tendrá la doble condición de usuario y fuente, y asumirá los deberes y responsabilidades de ambos".*

una investigación en curso; (vi) otros operadores de datos[55] cuando se cuente con autorización del titular o cuando sin ser necesaria la autorización del titular el banco de datos de destino tenga la misma finalidad o una finalidad que comprenda la que tiene el operador que entrega los datos. Es importante resaltar que esta Ley establecía que "*si el receptor de la información fuere un banco de datos extranjero, la entrega sin autorización del titular sólo podrá realizarse dejando constancia escrita de la entrega de la información y previa verificación por parte del operador de que las leyes del país respectivo o el receptor otorgan garantías suficientes para la protección de los derechos del titular*", sin embargo en el año 2012 fue modificado por la Ley 1581[56]; y por último (vii) a otras personas autorizadas expresamente por la ley[57].

La Superintendencia de Industria y Comercio (para la protección de datos personales) y la Superintendencia Financiera (para los usuarios, fuentes u operadores que son vigilados por esta entidad) son las encargadas de vigilar el cumplimiento de la Ley y se encuentran facultadas para imponer multas, suspender, clausurar temporalmente o indefinidamente las actividades de los bancos de datos en caso de que se viole alguna de las disposiciones consagradas en la Ley y con base en los criterios para graduar las sanciones establecidas en el

---

[55] Artículo 3. "*Se denomina operador de información a la persona, entidad u organización que recibe de la fuente datos personales sobre varios titulares de la información, los administra y los pone en conocimiento de los usuarios bajo los parámetros de la presente ley. Por tanto el operador, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. Salvo que el operador sea la misma fuente de la información, este no tiene relación comercial o de servicio con el titular y por ende no es responsable por la calidad de los datos que le sean suministrados por la fuente".*

[56] Únicamente se podrán transferir los datos personales a bases de datos extranjeras cuando la Superintendencia de Industria y Comercio lo permita en cada caso, teniendo en cuenta que la regulación de los terceros países deben cumplir "*con los estándares fijados por la Superintendencia de industria y Comercio sobre la materia*" que no pueden ser menores a los establecidos por la Ley. No obstante, se excluye la prohibición cuando el titular autorice la transferencia, por regulación de tratados internacionales, transferencias bancarias o bursátiles, cuando sea necesario en la etapa precontractual o para la ejecución de un contrato entre el titular y el responsable del tratamiento, o para salvaguardar derechos en procesos judiciales o el interés público.

[57] Artículo 5.

artículo 19[58]. Dentro de las funciones encargadas a estas dos entidades se encuentra el deber de "*velar porque los operadores y fuentes cuenten con un sistema de seguridad y con las condiciones técnicas suficientes para garantizar la seguridad y actualización de los registros, evitando su adulteración, pérdida, consulta o uso no autorizado conforme lo previsto en la presente ley"*, en relación con obligación de los operadores, fuentes y usuarios de las bases de datos de tener la seguridad debida para conservar la información que tienen en su poder.

2.1.3 Ley 1341 de 2009

A través de esta Ley se dictan los *"principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones",* es decir, es la Ley de las Telecomunicaciones.

En el Título VI "*Régimen de Protección al Consumidor",* se establece como derechos de los usuarios de los servicios de telecomunicación el de *"Recibir protección en cuanto a su información personal, y que le sea garantizada la inviolabilidad y el secreto de las comunicaciones y protección contra la publicidad indebida, en el marco de la Constitución Política y la ley."*

2.1.4 Ley 1480 de 2011 o Estatuto del Consumidor

El estatuto del consumidor abre un espacio para la protección de datos personales dentro del marco del comercio electrónico, esta normatividad tiene importancia en

[58]Artículo 19. "*Criterios para graduar las sanciones. Las sanciones por infracciones a que se refiere el artículo anterior se graduarán atendiendo los siguientes criterios, en cuanto resulten aplicables: a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley. b) El beneficio económico que se hubiere obtenido para el infractor o para terceros, por la comisión de la infracción, o el daño que tal infracción hubiere podido causar. c) La reincidencia en la comisión de la infracción. d) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio. e) La renuencia o desacato a cumplir, con las órdenes impartidas por la Superintendencia de Industria y Comercio. f) El reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar"*

la medida que el comercio electrónico está creciendo cada vez más y no es posible que se desarrolle sin que se vea involucrada información personal.

Se puede decir que a simple vista el comercio electrónico tiene muchas ventajas, como facilitar el intercambio comercial satisfaciendo tanto a consumidores ansiosos como a oferentes ambiciosos pero no es posible negar la inseguridad frente a los datos personales en esta figura, además de las complicaciones que se presentan cuando el intercambio es imperfecto. Podría decirse que el miedo principal de los consumidores en el comercio electrónico es el robo de sus datos crediticios o la estafa. Existen otros riesgos como: el riesgo de suplantación de identidad, el riesgo de alteración de información electrónica, el riesgo de ausencia de confidencialidad, entre otros[59].

El Estatuto del Consumidor se creó para proteger al consumidor[60] en sus relaciones de consumo, esta normatividad trae un capítulo específico para la protección de este en el comercio electrónico (Capítulo VI) y establece una serie de estrictas obligaciones para los proveedores y expendedores[61] ubicados en el territorio nacional que ofrezcan productos utilizando medios electrónicos, estas sin perjuicio de las demás directrices de la Ley.

En su artículo 50 se reglamenta la protección de los datos personales en el comercio electrónico específicamente, indicando que se debe mantener en mecanismos de soporte duradero la prueba de la relación comercial, en especial de la identidad plena del consumidor, entre otros, así como adoptar mecanismos

---

[59] Ibid, pp- 129-130.

[60] Esta ley entiende por consumidor o usuario a "t*oda persona natural o jurídica que, como destinatario final, adquiera, disfrute o utilice un determinado producto, cualquiera que sea su naturaleza para la satisfacción de una necesidad propia, privada, familiar o doméstica y empresarial cuando no esté ligada intrínsecamente a su actividad económica. Se entenderá incluido en el concepto de consumidor el de usuario"*

[61] Esta misma ley entiende como proveedor o expendedor a "*quien de manera habitual, directa o indirectamente, ofrezca, suministre, distribuya o comercialice productos con o sin ánimo de lucro".*

de seguridad apropiados y confiables que garanticen la protección de la información personal del consumidor y de la transacción misma, se entiende que el proveedor será responsable por las fallas en la seguridad de las transacciones realizadas por los medios dispuestos por él, sean propios o ajenos. Se reafirma la importancia de la protección de la información.

Así mismo en el artículo 61 se entablan una serie de sanciones que la Superintendencia de Industria y Comercio puede imponer, posteriormente a una investigación administrativa (respetando el debido proceso), por no acatar las normas del Estatuto, entre otros. Las sanciones van desde multas por 2000 salarios mínimos mensuales legales vigentes hasta el cierre temporal del establecimiento de comercio hasta por 180 días, graduándola con criterios como el daño causado a los consumidores, la disposición de buscar o no una solución adecuada para los mismos o el grado de diligencia y cuidado con el que hubieran atendido sus deberes.

Estas sanciones administrativas son distintas a las que pueden llegar a imponerse en un proceso judicial por responsabilidad civil, donde también se podrá llegar a responder por el incumplimiento de una norma de esta ley. Se quiere resaltar que el Estatuto habla específicamente de la seguridad de la información personal del consumidor y de la transacción, haciendo responsable al proveedor por las fallas de la seguridad, es claro todo esto en el escenario del comercio electrónico. No podría entonces el proveedor excusarse por sus fallas de seguridad por algo menor a una causa extraña o una causal de justificación, se trata de una responsabilidad objetiva y se entiende esto por la forma en la que está estructurada la norma. Se establece que se hace responsable al proveedor por las fallas sin dejar espacio al establecimiento de una culpa, es decir, se le da el tratamiento de una obligación de resultado[62] donde si no hay fallas no se

[62] *"(…) mientras que cuando estamos en presencia del incumplimiento de una obligación de resultado, el demandante se encuentra relevado de la prueba de la culpa y el demandado no*

responderá pero si en caso de que estas existan. Esto es razonable si se tiene en cuenta que el consumidor es en últimas la parte débil del contrato.

El amparo a la seguridad de los datos en este escenario es compatible con la tendencia de protección de datos personales que se ha venido dando en Colombia; se denota el deseo por salvaguardar la integridad, disposición, confidencialidad y autenticidad de la información personal.

En caso de querer entablar un proceso judicial por el incumplimiento de la obligación retratada se puede acudir a la figura de la acción de grupo si se presenta un perjuicio para veinte personas o más, pero principalmente a la acción de protección al consumidor consagrada para casos individuales. Mediante esta acción se deciden "*los asuntos contenciosos que tienen como fundamento la vulneración de los derechos del consumidor por la violación directa de las normas sobre protección a consumidores y usuarios".*[63]

Puede fallar el caso en cuestión tanto la Superintendencia de Industria y Comercio como el juez civil dependiendo de las reglas de competencia. "*La Superintendencia de Industria y Comercio tiene competencia en todo el territorio nacional y reemplaza al juez de primera o única instancia competente por razón de la cuantía y el territorio*"[64].

2.1.5 Resolución No. 76434 de 2012

Mediante esta Resolución la Superintendencia de Industria y Comercio indicó las instrucciones de la protección de datos personales en relación con la Ley 1266 de 2008, estableciendo repetidamente que las entidades que administren bases de

---

*puede exonerarse de responsabilidad demostrando diligencia y cuidado, sino una causa extraña".*CORTE SUPREMA DE JUSTICIA. Sala de Casación Civil. Magistrado Ponente: Arturo Solarte Rodríguez. Radicado: 20001-3103-005-2005-00025-01. Bogotá D.C., cinco (5) de noviembre de dos mil trece (2013).

[63] Artículo 56.

[64] Artículo 58.

datos deberán cumplir con un protocolo para asegurar la información y tener certeza que quien la reciba se encuentre autorizado por el titular o por la ley. Además contempla la posibilidad que tienen dichas entidades a tener la información en la Web para que aquellos que se encuentren autorizados puedan acceder a ella, "*siempre y cuando se cuenten con las debidas seguridades para verificar la identidad del titular e impedir la pérdida, alteración o uso no autorizado o fraudulento de los registros".*

2.1.6 Ley Estatutaria No. 1581 de 2012

Esta Ley buscó establecer un marco general para la protección de datos personales en aras de salvaguardar los derechos constitucionales de toda persona a la intimidad personal, familiar, al buen nombre, así como el derecho a la información. Está dirigida a las bases de datos que tengan información personal susceptible de tratamiento ya sea por entidades públicas o privadas; su campo de aplicación es el territorio colombiano y en caso de que la información sea tratada por quien no este domiciliado en el territorio colombiano pero que por tratados internacionales le sea aplicable esta legislación.

Excluyó de su aplicación las bases de datos (i) domésticas o de uso personal; (ii) las que tengan como finalidad la seguridad y defensa nacional; (iii) las que tengan información de inteligencia; (iv) las dirigidas a información periodística y contenidos editoriales; (v) las reguladas por la Ley 1266 de 2008 (es decir, la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países); y (vi) las reguladas por la Ley 79 de 1993. Sin embargo, estableció que los principios en los que se fundamenta la Ley son aplicables a todas las bases de datos, incluidas las mencionadas anteriormente.

Los principios de la protección de datos personales son en principio los consagrados en la Ley 1266 de 2008 y agrega otros como:

1. Principio de legalidad en materia de Tratamiento de datos. El tratamiento de datos personales debe cumplir con las disposiciones de la ley y las demás que la reglamenten.

2. Principio de libertad. El titular de la información debe dar previa autorización para que su información pueda ser obtenida o divulgada, salvo mandato legal o judicial que lo autorice.

3. Principio de transparencia. Derecho del titular de los datos personales de obtener información sin restricción acerca de los datos que le interesa.

4. Principio de acceso y circulación restringida. Agrega al principio de circulación restringida de la Ley 1266 de 2008, que únicamente el personal autorizado por el titular o quien haga sus veces podrá realizar el Tratamiento de los datos.

5. Principio de seguridad. Complementa el principio de seguridad que contemplaba la Ley 1266 de 2008, estableciendo el *"deber de manejar con las medidas técnicas, humanas y administrativas, que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso o autorizado o fraudulento.*[65]*"*

La Ley identifica a tres sujetos: (i) el titular de la información que es una persona natural; (ii) el encargado del tratamiento puede ser una persona natural o jurídica del sector público o privado que realiza el tratamiento de datos personales por cuenta del tercer sujeto denominado responsable del tratamiento; (iii) este último es la persona natural o jurídica que decide sobre la base de datos y su tratamiento (recolección, almacenamiento, uso, circulación o supresión). Se debe entender que datos personales para esta ley es "*cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas y determinables.*[66]*"*

[65] Artículo 4.
[66] Artículo 3.

Es importante mencionar acerca de esta ley que identificó categorías de datos especiales que deben tener un trato diferenciado a las demás categorías, se encuentran consagradas en el Título III y entre ellas están (i) los datos sensibles, que son *"aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos."*, este listado presentado por el legislador no se debería entender como taxativo, ya que lo que se puede interpretar de la intención del legislador era proteger todos aquellos datos que hagan parte de la vida personal del titular, prohibiendo su tratamiento salvo: que sus titulares hayan dado autorización; en caso necesario de salvaguardar un interés vital cuando haya incapacidad del titular y con autorización de su representante legal; sean tratados por organismos sin ánimo de lucro en ejercicio de una actividad legítima; sean necesarios en un proceso judicial o su tratamiento tenga una finalidad histórica, estadística o científica; y (ii) en cuanto a los datos de los niños, niñas y adolescentes, el tratamiento de estos datos está prohibido salvo los que tengan carácter de públicos.

Respecto a los datos personales, estos pueden ser tratados, ya sea porque el titular otorgo autorización o porque no se requiere de autorización previa como es el caso de: los datos públicos; frente a una situación de urgencia médica o sanitaria; los relacionados con el registro civil del titular; los autorizados por la ley para fines históricos, estadísticos o científicos; o los requeridos por entidad pública o administrativa en ejercicio de las funciones legales o por orden judicial.

Los datos personales solo pueden ser suministrados a los titulares, sus representantes legales o causahabientes, entidades públicas o administrativas o a

los terceros autorizados ya sea por el titular o por la ley. En caso de que estos se suministren a personas diferentes a las mencionadas, se entenderá que tanto el responsable del tratamiento como el encargado del mismo incumplieron los preceptos establecidos en esta Ley y estarán sujetos a la sanción que la Superintendencia de Industria y Comercio en ejercicio de sus funciones de vigilancia a las personas de naturaleza privada les imponga, la cual puede ir desde una multa (no superior a 2.000 smlmv) hasta el cierre definitivo de *"la operación que involucre el tratamiento",* sanciones que determinará la Delegatura para la Protección de Datos Personales con base en los criterios para graduar la sanción establecidos en el artículo 24[67] de la Ley. Si el incumplimiento de la Ley se da por parte de una autoridad pública será la Procuraduría General de la Nación la encargada de realizar la respectiva investigación.

Dentro de los deberes de los responsables del tratamiento, consagrado en el artículo 18, se encuentra la obligación de exigir condiciones de seguridad y privacidad de los datos personales al encargado del tratamiento y tanto a este como al encargado del tratamiento se les exige informar a la SIC[68] o quien haga sus veces, de las violaciones a la seguridad o cuando existan riesgos en la administración de los datos del titular y "*conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento."*

---

[67] *"Artículo 24. Criterios para graduar las sanciones. Las sanciones por infracciones a las que se refieren el artículo anterior, se graduarán atendiendo los siguientes criterios, en cuanto resulten aplicables:*
a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley.
b) El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción.
c) La reincidencia en la comisión de la infracción.
d) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio.
e) La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio.
f) El reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar."
[68] Superintendencia de Industria y Comercio.

Por último, es importante recordar que modificó la transferencia de datos a terceros países consagrada en la Ley 1266 de 2008, indicando que únicamente se podrán transferir los datos personales a bases de datos extranjeras cuando la SIC lo permita en cada caso, teniendo en cuenta que la regulación de los terceros países deben cumplir "*con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia*" que no pueden ser menores a los establecidos por la Ley. No obstante, se excluye la prohibición cuando el titular autorice la transferencia; por regulación de tratados internacionales; transferencias bancarias o bursátiles; cuando sea necesario en la etapa precontractual o para la ejecución de un contrato entre el titular y el responsable del tratamiento; o para salvaguardar derechos en procesos judiciales o el interés público.

2.1.7 Decreto 1377 de 2013

Para reglamentar parcialmente la Ley anterior, el Gobierno promulgó en el año 2013 el Decreto 1377 que trata aspectos relacionados con la autorización del tratamiento por parte del titular, políticas de tratamiento de las bases de datos por parte de los Responsables y Encargados, como debían ejercer el derecho a la información los titulares, transferencias de datos personales y respecto a la rendición de cuentas, cuál debía ser la responsabilidad demostrada frente al tratamiento de datos personales.

El Decreto define como transferencia *"cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del tratamiento y se encuentra dentro o fuera del país."* y a la transmisión como el *"tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable."* Establece que frente a la transferencia internacional de datos personales se regirá bajo lo estipulado en la

Ley 1581 de 2012 y reguló respecto a las transmisiones internacionales de información personal que se dan entre Responsables y Encargados, que para que éstos últimos realicen el tratamiento no será necesario la autorización por parte del titular para que se permita la transmisión, siempre y cuando se cumpla con la celebración de un *contrato de transmisión de datos personales* entre el Encargado y el Responsable, en el cual se deberá establecer detalladamente por parte del responsable del tratamiento las obligaciones, actividades, alcances del tratamiento con las que deberá cumplir el Encargado. A su vez en dicho contrato se deberá comprometer a cumplir con la finalidad del tratamiento de los datos personales que autorizo el titular, la política de tratamiento del Responsable (que en virtud de este Decreto debe acoger todo Responsable del tratamiento) y las leyes aplicables. Por disposición del Decreto, el Encargado del tratamiento tiene tres obligaciones como mínimo (i) realizar el tratamiento conforme a los principios de protección de datos personales; (ii) velar por la seguridad de las bases de datos; y (iii) confidencialidad en relación al tratamiento dado.

Otro aspecto novedoso que reglamenta el Decreto es la figura de la "*responsabilidad demostrada"* frente al tratamiento de datos personales*,* que consiste en que los responsables de tratamiento deberán demostrar, en caso de que la Superintendencia de Industria y Comercio lo solicite, el cumplimiento de todas las medidas exigidas por la Ley 1581 de 2012 y este Decreto, incluyendo en el informe *"los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares (…) deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas."*

En caso de que en el informe presentado a la SIC no se demuestre que se está cumpliendo con las obligaciones y deberes exigidos por estas normativas, habrá lugar a las sanciones correspondientes en el caso concreto.

2.1.8 Decreto 886 de 2014

El artículo 25 de la Ley 1581 de 2012 delegó al Gobierno Nacional la reglamentación del Registro Nacional de Bases de Datos[69] que debe ser administrado por la Superintendencia de Industria y Comercio. En cumplimiento de este mandato y del impuesto por la Corte Constitucional en la Sentencia C-748 de 2011 en la cual se estudió la constitucionalidad de dicho artículo, el Gobierno Nacional a través del Decreto 886 de 2014 reglamentó el Registro Nacional de Bases de Datos.

La Corte Constitucional estableció que dicho Registro *"debe permitir a cualquier persona determinar quién está haciendo tratamiento de sus datos personales para de esa forma garantizar que la persona pueda tener un control efectivo sobre sus datos personales al poder conocer clara y certeramente en qué bases se manejan sus datos personales. Por ende, el Gobierno Nacional tendrá en su labor de reglamentación que acudir a los estándares internacionales y a la experiencia de otros Estados en la materia para lograr que la finalidad antes descrita de este registro se cumpla"*[70].

El Decreto reglamenta la información mínima que debe tener el Registro Nacional de Bases de Datos, al cual se deben inscribir todas las bases de datos que tengan datos personales sujetos a tratamiento por parte de personas naturales o jurídicas, ya sea que se encuentren domiciliadas en Colombia o que se les aplique la regulación colombiana y que les sea aplicable la Ley 1581 de 2012.

Es obligación del Responsable del tratamiento inscribir cada una de las bases de datos, las cuales deben ir identificadas de acuerdo a la finalidad para la cual

---

[69] Decreto 886 de 2014: *"Directorio público de las bases de datos personales sujetas a Tratamiento que operan en el país, administrado por la Superintendencia de industria y Comercio y de libre consulta para los ciudadanos."*

[70] COLOMBIA. Corte Constitucional. Sentencia C-748 de 2011. Magistrado Ponente: Jorge Ignacio Pretelt Chaljub.

fueron creadas y se debe establecer si el tratamiento es manual (cuando la información se tiene de manera física) o automatizada (se tiene almacenada en herramientas informáticas). Además de identificar los medios por cuales los titulares pueden ejercer sus derechos, la identificación tanto del Responsable como del Encargado de los datos personales, la base de datos y su finalidad, así como su forma y política de tratamiento.

2.1.9 Circular Externa No. 02 del 2015

La Superintendencia de Industria y Comercio por medio de la Circular Externa No. 02 del 3 de noviembre de 2015 impartió instrucciones respecto al Registro Nacional de Bases de Datos creado por medio del artículo 25 de la Ley 1581 de 2012 y regulado por el Decreto 886 de 2014, dirigido únicamente a los Responsables del tratamiento de datos personales que fueran personas jurídicas de naturaleza privada o sociedades de economía mixta y la cual se habilitó desde el 9 de noviembre de 2015, tres años después de que se facultara a la SIC para administrar el Registro Nacional Público de Bases de Datos.

Por medio de esta Circular Externa se adicionó información que se debe incluir al registro en el Sistema Integral de Supervisión Inteligente (SISI). Teniendo en cuenta que solo se debe inscribir dicha información y no propiamente los datos personales que tengan en sus bases de datos. Los Responsables del tratamiento deben registrar (i) la clasificación de los datos almacenados en cada base de datos; (ii) las medidas de seguridad y controles que serán tomados por el Responsable para garantizarle a los titulares de la información la protección de sus datos personales; (iii) en caso de que se presente transmisión internacionales de datos personales se deberá dar la información del destinatario, ya sea como Responsable o Encargado del tratamiento y si la información transmitida fue permitida por la SIC o no requería autorización de esta entidad; (iv) si se presenta una cesión o transferencia nacional de la base de datos el cesionario Responsable del tratamiento deberá informar dicha cesión; y (v) se deberá registrar las

novedades que se presenten en relación con la base de datos respecto a los reclamos que presenten los titulares o la violación de los códigos de seguridad de las bases de datos que se lleguen a presentar, dentro de los 15 días hábiles siguientes a la ocurrencia del incidente y se incluye la obligación del Responsable de informarle a los titulares de los datos personales el suceso.

A pesar de que el Decreto 886 de 2014 había establecido que una vez habilitado el Registro Nacional de Bases de Datos se podría realizar la inscripción de la base de datos dentro del mismo año, la Superintendencia sugirió un cronograma en el cual deben registrar las personas jurídicas privadas o las sociedades de economía mixta sus bases de datos a partir de los dos últimos dígitos del NIT, generando inquietud en estas entidades de cuál sería la consecuencia de incumplir con la inscripción de la base de datos en las fechas asignadas por la SIC.

Una vez presentada la normatividad colombiana en relación a la protección de la información personal, es propio entrar a advertir los diferentes aspectos que se hacen evidentes al analizar el desarrollo por parte del ordenamiento jurídico en este tema.

Principalmente, es de resaltar el hecho de que Colombia por medio de la Ley 527 de 1999 haya comenzado a regular los mensajes de datos, el comercio electrónico y las firmas digitales, logrando de esta manera incentivar el uso de la tecnología, hasta el punto de que el nuevo Código General del Proceso estableciera que es posible el envío de memoriales a los juzgados por medio del correo electrónico, presumiéndose la autenticidad de la firma digital. Esto demuestra el gran auge que tiene la tecnología en todos los ámbitos de la sociedad y la importancia que tiene que los legisladores identifiquen la necesidad de que esta actividad que involucra a un gran porcentaje de los campos de la vida del ser humano, debe ser regulada

de una forma eficiente para evitar los riesgos a los que están expuestos todos aquellos que hacen uso del Internet.

Colombia ha considerado el derecho al Habeas Data y Protección de la Información Personal dentro de los fundamentales y es por esto que ha entrado a establecer un marco normativo general dentro del cual se pretende proteger en gran medida los datos personales que son entregados por su titular a terceros. Sin embargo, al buscar una protección tan estricta olvida la eficacia de su regulación, principalmente por la definición tan amplia que se le otorga a un dato personal, como *"cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables"*[71]. Esta definición entonces llega a confundir con aquella del dato que tenga relación con una persona, incluyendo entre esos a la grabación que realizan las cámaras de seguridad de un aeropuerto, una empresa, las de vías públicas, entre otras; indicando entonces que todos los Responsables del tratamiento de ese *dato personal* deberá solicitar autorización previa al titular de la información para poder grabarlos, situación que genera múltiples complicaciones a las personas naturales o jurídicas que sean responsables del tratamiento de los datos personales y generando quizás un incumplimiento masivo de la regulación de la Protección de la Información Personal. Este es una situación que al pasar el tiempo es posible que se convierta en una bola de nieve, debido a que genera cargas exorbitantes y difíciles de cumplir en cabeza del Responsable del tratamiento de la información.

Con respecto a la figura de Responsabilidad Demostrada que crea el Decreto 1377 de 2013, es posible que a la hora de exigirse a los Responsables del tratamiento que se cumpla con esta exigencia, sea más notable identificar los problemas que se presenten en el cumplimiento de la regulación acerca de los

[71] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1581 de 2012. Artículo 3. (octubre, 7, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá: Diario Oficial 48587 de octubre 18 de 2012.

datos personales, además de que no existe explícitamente regulado cuáles son las condiciones de seguridad y privacidad bajo las cuales los encargados y responsables del tratamiento de datos deben cumplir, lo que genera inseguridad jurídica y un amplio margen de interpretación, por lo cual es necesario que se identifique específicamente estas medidas de seguridad y así evitar un posible fraude a la ley. El incumplimiento de esta obligación además de ser potencialmente generadora de responsabilidad civil, también lo es de multas administrativas por parte de la SIC.

Otra situación que llama la atención es la demora de la Superintendencia de Industria y Comercio para habilitar el Registro Nacional de las Bases de Datos, ya que incluso, hasta el momento, para las entidades públicas y personas naturales que sean responsables del tratamiento de datos personales no se encuentra habilitado el respectivo registro, generando de tal forma una demora aún mayor a la ya presentada. Concluyéndose que quizás durante el tiempo que se demore la habilitación del registro para estas entidades o personas naturales que realicen tratamiento de datos personales, sea posible que se encuentren vulnerados los derechos fundamentales de miles de personas titulares de tales datos personales. Sin embargo, la creación de este Registro es de gran importancia para el avance de la regulación de datos personales y una forma de control para el titular de la información, siempre y cuando sea cumplida la obligación del registro.

Luego de identificar el desarrollo de la normatividad por parte de Colombia para proteger la información personal que es recolectada por personas naturales o jurídicas y que se encuentran tanto en bases de datos físicas como en medios electrónicos, es claro afirmar que el país se ha empeñado en crear un orden normativo que logre proteger el derecho fundamental a la intimidad y buen nombre, estableciendo que quienes recolecten información deben otorgar la seguridad debida a los titulares de la información personal, evitando así que se logre por parte de terceros acceder a la información que se encuentran en esas

bases de datos generando daños que pueden ser de gran dimensión para una sociedad como Colombia que va en desarrollo.

Sin embargo, se debe agregar que a pesar del empeño de Colombia en crear un marco normativo que busque salvaguardar la información personal de los riesgos a los cuales está expuesta, debe velar por el cumplimiento de este marco por parte de los sujetos que tienen el manejo de la información, en este caso por medio de la Superintendencia de Industria y Comercio. Esta entidad es la encargada tanto de vigilar el cumplimiento de las directrices impuestas a los Responsables y Encargados del tratamiento de datos personales como de la administración del Registro Nacional de Bases de Datos.

2.2 ÍNDICE CRONOLÓGICO DE LA NORMATIVIDAD COLOMBIANA

Por medio de la tabla 1, se pretende hacer un breve resumen cronológico de las normas señaladas anteriormente, en el cual se explique el objetivo principal de estas en relación con la protección de datos personales.

Tabla 1. Índice Cronológico

Regulación	Año de Expedición	Objetivo
Constitución Política de Colombia	1991	Se estableció como Derecho Fundamental el derecho a la intimidad personal y al buen nombre, el cuales el eje central de toda la regulación que pretende proteger este derecho.
Ley 527	1999	Esta Ley comienza a regular temas propios de la era digital, como lo son los mensajes de

Regulación	Año de Expedición	Objetivo
		datos, las firmas digitales y el comercio electrónico.
Ley 1266	2008	Es la primera Ley que regula la protección al derecho fundamental de la intimidad personal y buen nombre, reglamentando propiamente las bases de datos que contienen información financiera y crediticia de persona natural o jurídica, buscando directamente que esta información personal no pueda ser conocida por terceros no autorizados. Establece sanciones en caso de que se violen algunas de las disposiciones consagradas en la Ley.
Ley 1341	2009	La Ley de las Telecomunicaciones establece un régimen de protección al consumidor, indicando que todos los usuarios de las telecomunicaciones tienen derecho a recibir protección en cuanto a su información personal, asegurándose que su información no va a ser violada y estará protegida contra la publicidad indebida.
Decreto 2952	2010	Incluye al mensaje de datos como un mecanismo idóneo para reportarle al usuario de información financiera o crediticia (regulada por la Ley 1266 de 2008) la información negativa.
Ley 1480	2011	Regula la protección de datos personales en el ámbito del comercio electrónico.

Regulación	Año de Expedición	Objetivo
Resolución No. 76434	2012	La Superintendencia de Industria y Comercio indicó a las entidades que administran bases de datos de información personal, la obligación de cumplir con protocolos para asegurar que esta información solo pueda ser conocida por los autorizados para ello, ya sea por el titular o por la Ley.
Ley 1581	2012	Estableció un marco general sobre el cual debe ser tratada la información personal, excluyendo de su aplicación a la información financiera y crediticia regulada por la Ley 1266 de 2008. Establece como un deber de los encargados y responsables del tratamiento de la información, el de conservar la información bajo parámetros de privacidad necesarios para impedir su robo, pérdida, adulteración, uso o acceso no autorizado. Consagra sanciones en caso de que no sean acogidas las disposiciones impuestas.
Decreto 1377	2013	Regula aspectos de políticas de tratamiento de la información que debe ser implementada ya sea por Encargados o Responsables de la información personal, transferencias de datos personales, responsabilidad demostrada y la forma en que los titulares de la información pueden ejercer su derecho a la información.

Regulación	Año de Expedición	Objetivo
Decreto 886	2014	Regula la información mínima que debe contener el Registro Nacional de Bases de Datos creado por la Ley 1581 de 2012, la cual debe ser administrada por la Superintendencia de Industria y Comercio.
Circular Externa No. 2	2015	La Superintendencia de Industria y Comercio impartió instrucciones para el Registro Nacional de Bases de Datos incluyendo información que se debe inscribir, la cual no es propiamente la información personal que este sujeta a tratamiento.

Fuente: Elaboración de las autoras

Una vez estudiada la regulación colombiana que pretende la protección de la información personal para así salvaguardar el derecho fundamental a la intimidad personal, estudiaremos en el título siguiente la responsabilidad civil que se pueda derivar de un ataque cibernético en el que se vea afectada la información personal de personas naturales o jurídicas; indicando conceptos y características esenciales de la responsabilidad civil en Colombia y su relación con los derechos fundamentales mencionados anteriormente.

2.3 ASPECTOS GENERALES DE LA RESPONSABILIDAD CIVIL

2.3.1 Conceptos de la Responsabilidad Civil en el Ámbito de Estudio

La responsabilidad civil es un ámbito importante en el derecho y su estudio requiere de un análisis detallado. El uso del Internet no es una excepción, como cualquier otra actividad es propensa a generar responsabilidad de parte de usuarios, operadores, Encargados y Responsables del tratamiento de la

información personal o crediticia y es por esto que se deben estudiar sus aspectos generales y algunos más específicos.

La Corte Constitucional sostiene que en Colombia se mantiene una concepción dualista de la responsabilidad civil, que no se puede confundir el tratamiento que se le da a una y a otra responsabilidad pues están reguladas de manera autónoma e independiente, se originan en causas o fuentes diversas y sus prescripciones en materia de reparación no son coincidentes. Las define desde la siguiente óptica:

- La responsabilidad civil contractual (Artículos 1602 a 1617 del Código Civil Colombiano) como aquella que resulta de la inejecución o ejecución imperfecta o tardía de una obligación estipulada en un contrato válido. Es decir, se ubica en el contexto de un derecho de crédito de orden privado, que solo obra en el campo exclusivo y limitado de las partes del contrato y respecto de los perjuicios nacidos de ese negocio jurídico[72].

- En tanto que la responsabilidad civil extracontractual (Artículos 2341 a 2360 del Código Civil Colombiano), también denominada delictual o aquiliana, es aquella que tiene origen en un *"hecho jurídico",* ya se trate de un delito o de un ilícito de carácter civil[73].

Para efectos del presente escrito se tendrán en cuenta estas definiciones de responsabilidad civil contractual y extracontractual. Sin embargo, es importante conocer otros puntos de vista y definiciones que se le han dado a estos conceptos. Por ejemplo, para el autor Juan Manuel Díaz Granados "*Conceptualmente la responsabilidad contractual, tiene lugar por el incumplimiento de una obligación preexistente; en la extracontractual el daño no se causa por el incumplimiento de una obligación previa nacida de un contrato[74]".* Por otro lado, algunos consideran que aunque la responsabilidad extracontractual no surge de un contrato, puede surgir de una obligación de distinta índole entre víctima y responsable como una

[72]COLOMBIA. CORTE CONSTITUCIONAL. Sentencia C-1008 de 2010. Magistrado Ponente: Luis Ernesto Vargas Silva.
[73]Ibid.
[74]DIAZ GRANADOS, J. M. El seguro de responsabilidad. Universidad del Rosario. 2006. p. 65.

obligación alimentaria por ejemplo, y la responsabilidad contractual por su parte relacionarse a obligaciones nacidas o relacionadas al contrato. Paralelamente Mariano Yzquierdo Tolsada considera que en la responsabilidad civil contractual podemos hablar de un deber jurídico incumplido, derivado de la ley que regula la naturaleza del contrato en cuestión o al pacto entre las partes, gracias a la autonomía de la voluntad tan importante en el ámbito de los contratos[75].

El análisis en el cual se enmarcará la responsabilidad civil por vulneración de información personal en medios digitales, se centrará en primer lugar en los sujetos considerados víctimas (aquel que sufre el hecho dañoso) o responsables (aquel en quien recae la obligación de indemnizar el daño que le cause a la víctima por medio de una conducta ilícita[76]), posteriormente en cuáles pueden ser los hechos imputables, el nexo de causalidad y los daños que se presentarían como consecuencia de estos hechos.

Para identificar a los sujetos es necesario acudir a la normatividad de protección de datos personales, trayendo a colación la definición que se da de dato personal en la Ley 1581 de 2012, como "*cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables",* así como la otorgada por la Ley 1266 de 2008 *"cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica".*

A partir de las definiciones anteriores, se concluye que todo sujeto que tenga acceso o conocimiento autorizado de un dato personal podrá ser responsable por violación a deberes contractuales o legales en relación a estos. Lo anterior es problemático en cuanto es una concepción muy amplia de un dato personal por lo

[75] YZQUIERDO TOLSADA, M., Sistema de Responsabilidad Civil Contractual y Extracontractual. Ed. Dykinson. Madrid, 2001. P. 35-36.
[76] TAMAYO JARAMILLO, J. Tratado de Responsabilidad Civil. Tomo I. Legis Editores. 2009. p. 8.

que puede ser contraproducente a la finalidad de la normatividad proteccionista de este tipo de datos.

Las víctimas serán entonces los titulares de la información digital, los cuales tienen derechos[77] a su favor de acuerdo a la normatividad presentada, además de que su información personal no se puede disponer por terceros sin su autorización salvo excepciones legales. Adicionalmente en caso de que el tratamiento de su información no esté cumpliendo con los parámetros legales y constitucionales convenidos al respecto, el titular podrá exigir la eliminación de dicha información con autorización de la SIC.

Por su parte el responsable podría ser toda persona natural o jurídica que recolecte datos personales en medios digitales y que no cumpla con las directrices establecidas para su tratamiento, sea en la ley o en contratos. Se debe resaltar que dentro de esta categoría se encuentran las personas que cometan delitos informáticos.

De acuerdo a la legislación y a las obligaciones impuestas en cabeza de ciertas personas, los Encargos del tratamiento y Responsables del tratamiento serían los sujetos con más posibilidades de ser llamados a responder por la vulneración de

---

[77] *Artículo 8° Ley 1581 de 2012. "Derechos de los Titulares. El Titular de los datos personales tendrá los siguientes derechos: a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado; b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley; c) 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; d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen; e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución; f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento".*

los datos personales puesto que el Responsable del tratamiento es aquella persona natural o jurídica que decide sobre la recolección, almacenamiento, uso, circulación o supresión de la base de datos y su tratamiento. Este sujeto también podría cumplir al mismo tiempo la función del Encargado del tratamiento, quien es la persona natural o jurídica que realiza efectivamente el tratamiento de datos personales, como se dijo anteriormente. Se debe recalcar que para que alguno de estos dos sujetos tenga acceso a la información personal debe mediar autorización del titular, pero se establece en la ley que el Encargado realiza el tratamiento de los datos personales por cuenta del Responsable del tratamiento.

Este aparte tiene importancia en cuanto a que la obligación de protección de datos frente al titular, está en cabeza del Responsable del tratamiento y en caso de que el Encargado incumpla con algunos de sus deberes, es el Responsable el llamado a indemnizar los perjuicios sufridos por la víctima pues a su cuenta delegó su función. La delegación no lo desprende de sus obligaciones respecto al titular y será posible que el Responsable le reclame al Encargado por su culpa y los perjuicios que debió pagar.

Cabe recordar que entre las obligaciones del Responsable se encuentran entre otras: garantizar al titular, el pleno y efectivo ejercicio del derecho de hábeas data; Informar al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada; conservar la información otorgada por el titular bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; Suministrar al Encargado del Tratamiento, únicamente datos cuyo tratamiento esté previamente autorizado; informar a la SIC cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares. A su vez entre los deberes del Encargado se encuentran: permitir el acceso a los datos únicamente a las personas que pueden tener acceso a ellos; realizar oportunamente la actualización, rectificación o supresión de los datos en los

términos de la ley; abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la SIC; entre otras, algunas de las cuales también son otorgadas al Responsable.

Paralelamente los proveedores dentro del contexto del comercio electrónico podrán ser responsables por las obligaciones que les atribuye el artículo 50 del Estatuto del Consumidor anteriormente mencionado. Sin embargo, la vulneración de la intimidad, de la honra y del buen nombre de las personas puede ser llevada a cabo por cualquier persona, aunque conozca los más mínimos datos personales o no los conozca y busque averiguarlos sin la debida autorización.

En otro orden de ideas el objetivo de la responsabilidad civil es la reparación de los daños causados con ocasión del hecho imputable, se trata principalmente de devolver a la víctima a la situación en la que estaba antes del incidente, pero con una diferencia en el caso de la responsabilidad contractual, pues en este escenario solamente se van a indemnizar los perjuicios que se pudieran prever o que se previeron al momento celebrar el contrato salvo que hubiera dolo o culpa grave (se asemeja al dolo en la jurisdicción civil) o que se hubiera estipulado así por las partes de acuerdo a la autonomía privada, por lo que no existe el principio de reparación integral atribuible a la responsabilidad extracontractual.

La división entre responsabilidad civil contractual y extracontractual en Colombia fue creada por una decisión legislativa pura. Personas que sufrieron un daño y deberían tener derecho a ser reparadas, no lo han sido a raíz de la no satisfacción de requisitos procesales y “sustanciales” que se han otorgado a una u otra responsabilidad. Si en el fondo el objetivo de la responsabilidad civil es la reparación de daños antijurídicos, el hecho de exigir el encuadramiento de la responsabilidad en contractual o extracontractual siendo su frontera borrosa en muchos casos, además entorpece la justicia y otorga una vía abierta a la

equivocación de jueces y demandantes, así como a la audacia de demandados que buscan refugiarse en esto para obstaculizar el pago debido.

Es trascendental esta concepción dualista en la medida que en el caso específico del robo de información personal en medios digitales se hace necesaria la diferenciación entre una y otra responsabilidad, dependiendo del origen de la relación. Si esta es entablada en el contexto de un contrato y se incumple una obligación establecida en el mismo acerca de la seguridad de los datos personales; o si por el contrario procede de una relación ocasional en virtud de la cual se entrega información personal y por mandato legal esta debe ser salvaguardada por la otra parte.

Consecuente con esto se diferenciará también en uno y otro caso la reparación recibida por la víctima. En el caso en el que sea una indemnización por incumplimiento de una obligación contractual solamente se repararían los perjuicios previsibles (salvo las excepciones mencionadas anteriormente), mientras que frente a un evento de responsabilidad extracontractual se repararían los perjuicios tanto previsibles como imprevisibles, siempre que se logre demostrar por la víctima la existencia de estos con las características necesarias para que sean indemnizables; esta diferenciación podría dar lugar a que en un caso de responsabilidad extracontractual la cuantía a indemnizar por parte del responsable sea mayor.

Sin embargo, a pesar de la concepción dualista que rige en Colombia, para identificar la carga probatoria en uno u otro régimen es necesario acudir al Código General del Proceso en su artículo 167, el cual establece que le *"Incumbe a las partes probar el supuesto de hecho de las normas que consagran el efecto jurídico que ellas persiguen. (…)".* De lo anterior se interpreta que sin distinción alguna del régimen de responsabilidad civil que se aplique al caso en concreto, en principio le recaerá al demandante la carga probatoria de los elementos de la responsabilidad

civil que pretenda demostrar, a excepción de algunos casos regulados en el ordenamiento colombiano que exigen una carga probatoria disímil a la consagrada en este artículo, verbigracia, el caso de responsabilidad por actividades peligrosas; la responsabilidad del deudor de un cuerpo cierto cuando este perece o se extravía estando este en mora y el supuesto de la presunción de culpa del civilmente responsable cuando se prueba la culpa del directamente responsable.

Otro de los aspectos por los cuales esta concepción dualista es esencial en el tema de estudio hace referencia al principio de no opción presente en el ordenamiento jurídico colombiano, definido por el Profesor Javier Tamayo Jaramillo:

> *"(…) la víctima no puede acudir indistintamente a los principios aplicables a la responsabilidad civil contractual o los aplicables a la responsabilidad civil extracontractual. O mejor, el juez no puede aplicar indistintamente, en tales circunstancias uno u otro régimen de responsabilidad. Corresponde, pues, determinar si el daño que se debate entre las mismas parte se deriva de la inejecución de un contrato válidamente celebrado entre ellas, en cuyo caso de puede aplicar única y exclusivamente la responsabilidad contractual, o si el contrato no existió o existiendo, el daño no se deriva de la inejecución, caso en el que la responsabilidad aplicable será necesaria y exclusivamente la extracontractual"*[78]

Esta concepción dada por el Profesor Tamayo tiene sentido en la medida en la que el juez es un sujeto imparcial que dirige el proceso judicial a partir de las pretensiones y excepciones que presentan las partes en el litigio, recayendo en él el deber de igualdad[79] entre estas, respetando su derecho de defensa sin lugar a favorecimiento a una de las partes, derecho que podría verse vulnerado en caso de que el juez redirigiera la demanda a uno u otro régimen que en últimas fuera el

[78] Op. cit, TAMAYO. p 137.

[79] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1564 de 2012. Artículo 42. Numeral 2.Por medio del cual se expide el Código General del Proceso y se dictan otras disposiciones. Bogotá D. C.

aplicable al caso concreto y que haya sido alegado desde un principio por la parte interesada.

En este mismo sentido, al ordenamiento jurídico diferenciar la responsabilidad civil contractual y extracontractual, la naturaleza de sus acciones, sus consecuencias disimiles, la prueba en cada una de ellas, el tratamiento de la culpa y los términos de prescripción, se puede interpretar que la intención es que el trato legal o judicial de cada uno de los regímenes no se confundiera o se asemejara[80]. A pesar de que la jurisprudencia ha variado respecto[81] al principio de no opción la tendencia de este órgano ha sido el reconocimiento de este principio y la exigencia del encuadramiento de la demanda en uno de los dos regímenes.

No obstante, el principio de la no opción no es absoluto debido a que existen supuestos en los que la diferenciación no es necesaria o se encuadra de igual forma en ambos regímenes de responsabilidad como es la excepción del incumplimiento del contrato y delito penal[82]. Por ejemplo, en caso de que el deudor contractual incumpla el contrato al no brindar la seguridad debida a la información personal que se le fue suministrada por el acreedor y a la vez comete un delito penal (violación de datos personales) cuyo resultado es un daño, el acreedor puede optar por demandar al deudor ya sea por responsabilidad contractual por el

---

[80] CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN CIVIL. Magistrado Ponente: José Fernando Ramírez Gómez. Expediente No. 6430. Bogotá D. C., once (11) de septiembre de dos mil dos (2002).

[81] CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN CIVIL. Magistrado Ponente: Pedro Lanfont Pianetta. Expediente 2461. Bogotá D. C., diecinueve (19) de abril de mil novecientos noventa y tres (1993); CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN CIVIL. Magistrado Ponente: Carlos Esteban Jaramillo Schloss. Expediente No. 5999. Bogotá D. C., diecinueve (19) de febrero de mil novecientos noventa y nueve (1999); CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN CIVIL. Magistrado Ponente: Nicolás Bechara Simancas. Expediente No. 6129. Bogotá D. C., veintinueve (29) de julio de dos mil dos (2002); CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN CIVIL. Magistrado Ponente: José Fernando Ramírez Gómez. Expediente No. 6430. Bogotá D. C., once (11) de septiembre de dos mil dos (2002); CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN CIVIL. Magistrado Ponente: Jorge Santos Ballesteros. Expediente No. 7001. Bogotá D. C., diecinueve (19) de noviembre de dos mil dos (2002).

[82] Op cit, TAMAYO. p. 139.

incumplimiento de este o puede pedir la indemnización de los daños que se le hayan ocasionado por la comisión del delito penal por responsabilidad extracontractual.

En la responsabilidad civil aparecen otras clasificaciones de responsabilidades más específicas y que a veces no corresponden exactamente a la concepción dualista de la responsabilidad, como lo es la responsabilidad de los profesionales. En este campo no es relevante la estipulación contractual de las obligaciones como tal puesto que estas se encuentran previamente reguladas en la ley o por los principios de la lex artis, esto se debe a que aun si se determina por el juez la inexistencia o invalidez del contrato celebrado, la víctima podrá reclamar por vía extracontractual. Esta clasificación se presenta frente a una situación en la cual el Encargado o Responsable de la información personal sea una persona natural o jurídica profesional que tenga conocimientos suficientes como para que se le pueda exigir mayor diligencia y cuidado en la protección de la información que se le suministra por parte de su titular, verbigracia Bancolombia o Apple.

Sin embargo, como se dijo anteriormente la jurisprudencia ha sido oscilante en cuanto al reconocimiento del principio de la no opción. Esto conlleva a que en la responsabilidad civil que pueda surgir en el ámbito de protección de datos personales sobre todo en casos fronterizos, en los que se tiene duda sobre si se configura dentro de uno u otro régimen, se torne inseguro jurídicamente para la víctima el logro de sus objetivos. La razón de esto es que a la hora de iniciar la acción indemnizatoria dependerá del arbitrio judicial que la demanda se encamine al régimen de responsabilidad adecuado para el caso en cuestión.

Como se desarrollará más adelante, al igual que en el caso de la responsabilidad de los profesionales cuando tienen conocimientos relacionados a la protección de datos personales, en el caso en el que se estipule contractualmente una obligación que coincida con una consagrada en la regulación de la protección de

información personal en un contrato celebrado con un sujeto no profesional en este aspecto, la víctima tendrá que someterse al régimen especial de la responsabilidad contractual. Por otro lado, en la situación en la que el juez durante el transcurso del proceso considere que existía una obligación implícita de protección de datos personales en el contexto de ese contrato y la víctima haya direccionado sus pretensiones hacía el campo de la responsabilidad extracontractual, la decisión de tal proceso se verá afectada por el arbitrio del juez. No obstante, si el juez sigue la línea jurisprudencial de la Corte en este tema sus pretensiones fracasarían.

Por otro lado en la responsabilidad civil extracontractual puede imputarse responsabilidad por el hecho propio, por el hecho ajeno (se está llamado a responder en virtud de una relación de dependencia, subordinación, por haber elegido o vigilado mal a los empleados, en los casos que diga la ley) o por riesgo de las cosas o actividades peligrosas (tiene que ver con el concepto de guarda, debe responder la persona que tenía la dirección y control sobre la actividad o la cosa). En cuanto en responsabilidad civil contractual, se responde por el hecho ajeno, el hecho propio o por las cosas o instrumentos (las fallas de las cosas o instrumentos propias carecen del elemento exterioridad, por lo que se debe responder por estas).

Una vez identificados los regímenes de responsabilidad y los aspectos relevantes para hacer un estudio de la responsabilidad civil que pueda surgir de la vulneración de datos personales, la cual se puede presentar mediante adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de estos, a continuación se indicará cuál es el régimen de responsabilidad civil que se le aplicará a aquellos que se determinen como responsables.

Los regímenes de responsabilidad civil en los que se encuadran la vulneración de datos personales son: el general de la responsabilidad extracontractual cuando se

incumple un deber legal; el especial de la responsabilidad contractual cuando la vulneración se presenta en un contexto contractual en el que se incumplan las obligaciones contractuales o se cumplan de forma tardía o imperfecta; otro de los regímenes en el cual se puede enmarcar esta responsabilidad es en el de la responsabilidad de los profesionales, por el tipo de experticia que tienen y al no cumplir con los presupuestos de la lex artis.

A partir de lo anterior se debe esclarecer que el hecho imputable en el entorno de la protección de los datos personales puede ser determinado por el régimen de responsabilidad subjetiva u objetiva según el caso. Responsabilidad subjetiva cuando el hecho imputable es necesariamente la culpa, mientras que responsabilidad objetiva es cuando no es necesaria la demostración de una culpa pues por el incumplimiento de una obligación contractual o legal específica se invierte la carga de la prueba, pudiéndose exonerar el demandado únicamente demostrando una causa extraña o causal de justificación. Es importante aclarar que el deber legal o la obligación contractual que se rija por responsabilidad objetiva es excepcional y es por su naturaleza, por precepto legal o por pacto entre las partes, que se le otorga esta característica.

2.3.1.1 Elementos integrantes de la responsabilidad civil.

En primer lugar se establecerán los elementos estructurales de la responsabilidad civil, los cuales se dividen en la culpa, el daño y el nexo de causalidad. Se indicarán sus definiciones y posteriormente se abarcará más a fondo aquellos presupuestos que requieran un análisis más detallado de cara al objeto de estudio, como es el tema del daño y los perjuicios.

- **Hecho imputable**. La Corte Constitucional afirma que la teoría general de la responsabilidad civil en el ordenamiento jurídico colombiano es de tradición culpabilista, es decir, el elemento subjetivo es uno de los pilares fundamentales

a tener en cuenta al momento de valorar el cumplimiento o incumplimiento de las obligaciones (sean contractuales o legales), y el alcance de la indemnización[83]. Este elemento subjetivo se ha definido como falta de diligencia y cuidado (sea en forma de acción u omisión) que en responsabilidad contractual se deduce del incumplimiento de un contrato y en la responsabilidad extracontractual en la violación de un deber general de comportamiento.

Existen eventos en los que la culpa se presume y no se debe demostrar, tales como el régimen de actividades peligrosas o el de cosas que son peligrosas en sí mismas o se encuentran en un estado de anormalidad. Tales supuestos no se relacionan con el tema del presente estudio, por lo que no serán posteriormente analizados.

Por otro lado, en la responsabilidad civil existe además de la responsabilidad subjetiva, aquella objetiva siendo esta última excepcional. En la responsabilidad objetiva no se debe establecer una culpa, el solo incumplimiento de los preceptos legales o contractuales invierte la carga de la prueba teniendo que demostrar por parte del supuesto responsable una causa extraña o causal de justificación. Sin embargo, en el caso de la protección de datos personales se presenta uno de estos supuestos en el Estatuto del Consumidor. Dicha hipótesis es la relativa a la obligaciones de resultado, en las que el deudor se obliga a cumplir con una obligación[84] y si no la cumple debe responder, salvo que demuestre causa extraña o causal de justificación.

Adicionalmente, la responsabilidad de los profesionales puede contar con elementos de juicio extra o en algunos casos los elementos tradicionales son más estrictos, por ejemplo se le exige máxima diligencia y cuidado a los

[83] Op cit., CORTE CONSTITUCIONAL.
[84] Tal y como se estableció en la sección 2.1.4.

profesionales pues por esta característica se espera un desempeño acorde y mejor al de alguien que tenga un conocimiento promedio del tema, es decir, solo se pueden exonerar demostrando una causa extraña, causal de justificación o ausencia de culpa.

Por su parte el artículo 1604 del Código Civil trae un criterio subsidiario en materia de responsabilidad contractual, estableciendo que dependiendo de la onerosidad o gratuidad del contrato, los acreedores y deudores (en lo que deban cada uno) deben responder por cierta culpa o tener cierta diligencia y cuidado recíprocamente, a saber: en los contratos onerosos, donde las dos partes del contrato obtienen un beneficio, se debe responder hasta por culpa leve, es decir, como lo hubiera hecho un buen hombre de familia o por una culpa grave. En los contratos gratuitos, donde solo hay beneficio para el acreedor, el deudor solo debe responder por culpa grave, es decir, debe una mínima diligencia y cuidado, al contrario de los contratos en los que solo obtiene beneficio el deudor, responde hasta por la más mínima culpa, culpa levísima, esto significa que debe tener el máximo de diligencia y cuidado.

Este aparte es importante pues los requisitos de la responsabilidad pueden atenuarse o hacerse más exigentes de acuerdo a la persona que cometa la culpa y a las características de la relación contractual, si es que se tiene una. No deberá tener, en principio, la misma diligencia Facebook que ofrece un servicio gratuito, a Whatsapp que ha cobrado su servicio en múltiples ocasiones y así debe ser, no es el mismo beneficio el recibido por cada una de parte del suscriptor. Esto tiene sentido en cuanto no se deben desconocer ciertos elementos en cada caso concreto, que cambien el panorama jurídico y den equilibrio y coherencia al sistema.

En este orden de ideas en cuanto al hecho imputable en el tema de estudio, se representa por medio de una culpa, es decir falta de diligencia y cuidado, por

violación ya sea de una obligación legal por ejemplo violar derechos fundamentales o directrices consagradas en normas como la Ley 1581 de 2012, como por incumplir una obligación establecida al respecto en un contrato o cumplirla de forma tardía o imperfecta. También por no brindar el resultado en la obligación específica del artículo 50 del Estatuto del Consumidor, es decir, brindar la seguridad exigida por esta norma.

Tal y como se menciono anteriormente, en el supuesto especifico de violación de deberes de protección de información personal se puede presentar la responsabilidad de profesionales, a estos se les exige una diligencia y cuidado mayor a la de una persona promedio que no tenga conocimiento la protección de datos personales pues por sus conocimientos deberían responder de acuerdo a la lex artis y a su experticia en salvaguardar dicho bienes. El grado de diligencia y cuidado en los contratos también puede variar, sea por el pacto entre las partes o el beneficio que se reporte a cada una de estas, entre otros.

Se puede afirmar que la violación de la regulación de datos personales se materializa (i) con el incumplimiento de un deber legal en lo que acarrearía una responsabilidad extracontractual sin la existencia de un contrato; (ii) por el incumplimiento total, parcial o tardío de un contrato en el que se pactaron obligaciones específicas en este sentido o que esta obligación esté relacionada con el objeto del contrato; (iii) por el incumplimiento de una obligación implícita en el contrato relacionada a este ámbito; (iv) por la afectación de un deber legal al respecto que se quebrante con ocasión de un contrato.

La anterior enunciación se fundamenta en una concepción de la responsabilidad contractual, en la que se considera que esta responsabilidad solo surge frente al incumplimiento total, parcial o tardío de una obligación expresa en el contrato, sea principal o accesoria, o de una obligación implícita en el mismo. Esto haciendo alusión a que el incumplimiento de un deber legal

que no se enmarque en el incumplimiento de obligaciones tanto principales como accesorias del contrato pero si tuviera relación con la ejecución de este, encuadraría en el numeral (iv) mencionado anteriormente.

Con el fin de identificar a fondo los hechos imputables que se puedan generar en relación a los deberes u obligaciones de protección de la información personal, se considera apropiado revisar este elemento de la responsabilidad civil a partir de la ejemplificación de casos que se puedan presentar:

1) María es empleada de la sociedad colombiana Montañas S.A., a pesar de tenerlo prohibido, decidió descargar música de Internet desde el computador que le fue designado en su trabajo durante la jornada laboral. Como consecuencia de la descarga gratuita de música en Internet, el computador de María fue infectado por un malware el cual logró expandirse a la red de la empresa, ocasionando la pérdida de información de los proveedores de la compañía generando así una violación de los deberes de protección de información personal suministrada por estos proveedores por parte de Montañas S.A.

   En este caso se podría configurar responsabilidad extracontractual por el hecho ajeno en cabeza de Montañas S.A. en relación al hecho imputable debido a que (i) es el empleador de María y por lo tanto se encuentra bajo su cuidado; (ii) la compañía es la civilmente responsable por la violación de los deberes legales[85] que tenía a su cargo, tal y como se establece en el artículo 2347 del Código Civil; (iii) los datos personales que se vieron afectados fueron suministrados a la compañía en ocasión a un contrato entre el proveedor y Montañas S.A.; (iv) María es la directamente responsable al ir en contra de la prohibición expresa

[85] Deberes que fueron mencionados en la sección 2.1.

de la empresa (culpa); (v) una vez sea demostrada la culpa de María se presume la culpa de Montañas S.A.; (vi) Montañas S.A. deberá responder frente a los proveedores por los daños causados; y (vii) Montañas S.A. posteriormente podrá repetir contra María por lo pagado.

2) Spotify Premium cobra $11.499.00 pesos mensuales a sus suscriptores por el acceso a su base de datos musical. Juan se suscribe a la cuenta Premium adhiriéndose a los términos y condiciones como también a las políticas de privacidad del contrato en las cuales la compañía se obliga a no suministrar la información proporcionada por los suscriptores a terceros no autorizados. Luego de cinco meses de ser usuario de Spotify Juan comienza a recibir llamadas de una entidad bancaria ofreciéndole sus servicios, por lo cual Juan comienza a investigar la razón por la que la dicha entidad tiene en su poder sus datos personales y descubre que Spotify vendió tanto sus datos como los de los otros usuarios a dicha entidad.

   Este supuesto se encuadra en el régimen de responsabilidad civil contractual. A pesar de que la Ley 1581 de 2012 y sus normas complementarias prohíben el suministro de información personal a terceros no autorizados por el titular, al haberse celebrado un contrato entre las partes en el cual se estipuló expresamente esta obligación accesoria, la responsabilidad se enmarca en este régimen especial. Por lo cual será Spotify la llamada a indemnizar los perjuicios sufridos por Juan.

   En este mismo orden de ideas, se hace necesario identificar que la obligación en cabeza de Spotify de no suministrar la información de Juan a terceros no autorizados es una obligación de resultado al ser una

obligación de no hacer[86]. Esto implica que Spotify no se obligó a desplegar todos los medios posibles para intentar no suministrar la información personal de Juan (lo cual se configuraría en una obligación de medios), por el contrario se obligó al resultado de no suministrar dicha información.

Al ser una obligación de resultado la culpa no es relevante, pues la sola frustración del resultado invierte la carga de la prueba en cabeza de Spotify de demostrar ya sea: que en realidad si se logro el resultado; una causa extraña o una causal de justificación.

3) Almacenes Éxito S.A. ofrece a sus empleados del área de mercadeo una bonificación por cumplimiento de metas, entre las cuales se establecía la de atraer nuevos clientes para que adquirieran la tarjeta de crédito que ofrece dicha compañía. Pedro es un empleado del área de mercadeo de Almacenes Éxito S.A., que en vista de que pocos de sus clientes adquirían la tarjeta de crédito y con deseo de obtener la bonificación mensual decidió hackear la cuenta de correo electrónico de 20 de sus amigos de la red social Facebook, que aún no tenían relación contractual con la compañía. Con la información obtenida del hackeo de los correos electrónicos, Pedro aumento la lista de sus clientes potenciales y se comunico con ellos para ofrecerle los servicios de la empresa.

   Los usuarios de las cuentas de correo al cuestionarse porqué Almacenes Éxito S.A. contaba con sus datos personales presentaron un derecho de petición a esta compañía solicitando una explicación. La sociedad al resolver la petición conoció el hackeo que realizó Pedro

[86] Las obligaciones contractuales se dividen en dar, hacer o no hacer.

para obtener dichos datos. Almacenes Éxito S.A. al responder la petición les ofreció un acuerdo económico con el fin de que los peticionarios no demandarán por el hackeo de información realizado por parte de su empleado.

Frente a este supuesto de hecho con respecto del hecho imputable se pudo haber entablado, en caso de haber iniciado un proceso judicial, una responsabilidad civil extracontractual por el hecho propio de la persona jurídica Almacenes Éxito S.A. El artículo 2349 del Código Civil establece responsabilidad por el hecho propio de las personas jurídicas por sus empleados al no haberlos vigilado o elegido correctamente, siempre que el daño sea con ocasión de las funciones que se le delegaron. Esto debido a que una vez demostrada la culpa del trabajador da lugar a una presunción de culpa en cabeza de la compañía de que eligió o vigiló de forma deficiente a su empleado.

Sin embargo, recaerá en cabeza de Almacenes Éxito S.A. demostrar la ausencia de culpa ya sea demostrando que eligió y vigilo correctamente o que en tal ocasión no tenía medio de prever o impedir que Pedro actuará de tal manera. Así como una causal extraña o una causal de justificación.

En el supuesto en el que Almacenes Éxito S.A. fuera condenada a indemnizar a las víctimas, está podría repetir contra Pedro por las sumas pagadas a los afectados con su actuación, siempre y cuando se demuestre la culpa de Pedro y los demás requisitos de la responsabilidad civil.

- **El daño.** Es necesario que exista un daño como aquella vulneración al derecho o interés jurídico (sobre este punto hay confusión). El profesor Javier Tamayo

Jaramillo establece que por el *"daño civilmente indemnizable entendemos el menoscabo de las facultades jurídicas que tiene una persona para disfrutar un bien patrimonial o extrapatrimonial"*[87]. Por su parte, para Juan Manuel Díaz Granados, el daño es simplemente la afectación de una persona en su dimensión patrimonial o extrapatrimonial[88].

Para que se configure un daño se requiere que esa cosa o situación afectada por el hecho imputable esté protegida por el orden jurídico, es decir, que sea un bien jurídico[89]. A su vez, es necesario que sea una afectación efectiva y real pues el simple riesgo no es suficiente para reclamar una indemnización que no se haya materializado.

Por otro lado, frente a este elemento se hace necesario que se haya causado por otra persona, ya sea natural o jurídica, diferente a la víctima. Debido a que esto se podría configurar dentro de uno de los presupuestos de causa extraña, la cual será estudiada más adelante.

Sin embargo, la concepción de daño que se ajusta a los criterios de este trabajo es aquella vulneración a un derecho. Más adelante se tratara la discusión sobre daño y perjuicio; cuál es el daño o perjuicio que resultaría de una afectación de información personal y cómo se indemniza.

Este presupuesto es clave en cuanto a que la legislación colombiana ha permitido la reparación de la afectación a derechos fundamentales aún sin ninguna repercusión material, por lo que no habría impunidad por el simple hecho de que el daño no se hubiera manifestado en el mundo físico. Al ser un concepto tan relevante para el presente estudio se hace necesario que su

[87] Op. Cit., TAMAYO. p. 247.
[88] Op. cit., DIAZ GRANADOS. p.101.
[89] TAMAYO JARAMILLO, J. Tratado de Responsabilidad Civil. Tomo II. Legis Editores. 2009. p. 329.

análisis se lleve a cabo más adelante, tanto en forma general como en concreto, una vez se hayan visto los demás elementos de la responsabilidad civil.

- **Nexo de causalidad.** El tercer elemento de la responsabilidad es el nexo de causalidad, este presupuesto se manifiesta en la causación de un daño a una persona por el hecho imputable de otra. Sin embargo, su concepción abarca un requisito adicional, se trata de que aquella persona causante del daño deba ser idónea jurídicamente hablando para responder por este en la medida de que la ley le imponga ese deber.

  Es importante establecer que no se entenderá que existe causalidad entre el hecho de una persona y el daño cuando no sea posible establecer que jurídicamente es causa de este, pues la sola manifestación física del daño y el hecho no supone la existencia de la causalidad (sin que esto suponga afirmar que no pueden coincidir una y otra). La causalidad jurídica se trata del reconocimiento del ordenamiento jurídico de un hecho imputable como fuente generadora del daño.

  Para su determinación se encuentra apoyo en las teorías de la causalidad como la causalidad adecuada, la causa próxima, la equivalencia de las condiciones, entre otras, para determinar si la culpa del supuesto responsable fue efectivamente la causa del daño. El juez es quien en últimas decidirá si así es.

  El nexo causal se divide en dos líneas, la primera es el nexo entre la culpa y el daño, que la conducta anormal de un sujeto es causante del daño a otro, es decir a la víctima. Es obligado a la indemnización quien por haber cometido delito o culpa, ha inferido daño a otro, al paso que los perjuicios tanto los previsibles como los imprevisibles deben ser consecuencia inmediata o directa

de no haberse cumplido la obligación o de haberse demorado su cumplimiento[90]; y el segundo, relacionado a si esa conducta es reprochable al autor del hecho, algunos autores lo llaman antijuridicidad, es decir, que la conducta del agente sea antijurídica, significando esto que carece de justificación a la luz del ordenamiento jurídico[91] y esta es la razón por la que es reprochable, o si por el contrario se ve exonerado tanto por una causal de justificación como el estado de necesidad, como por una causa extraña que tiene que tener las características de exterioridad, imprevisibilidad, irresistibilidad.

El elemento exterioridad comprende un evento que se entiende fuera del ámbito de control del responsable, debe tratarse de un suceso extraño a este, ajeno a su voluntad y con el que no debe existir ninguna relación causal[92]; por imprevisibilidad se entiende una situación que consta de tres características: (i) poca normalidad y frecuencia; (ii) poca probabilidad de realización; y (iii) carácter excepcional y sorpresivo. "*Prever, que en el lenguaje usual significa ver con anticipación, tiene en la tecnología culposa la acepción de conocer lo que vendrá y precaverse de sus consecuencias, o sea, prevenir el riesgo, daño o peligro, guardarse de él y evitarlo*"[93] y por irresistibilidad, un acontecimiento que no fue posible evitar a pesar de haber desplegado todos los medios posibles para que no ocurriera, "*consiste en que haya sido absolutamente imposible evitar el hecho o suceso aludido, no obstante los medios de defensa empleados por el deudor para eludirlo"*[94].

Existen tres clases de causa extraña consagradas en el ordenamiento jurídico, estas son:

---

[90]BALLESTEROS, J.S. Instituciones de responsabilidad civil. Tomo 3. vol. 21). Pontificia Universidad Javeriana. 1996). p.13.
[91]Op cit., DIAZ GRANADOS, p. 61.
[92]Ibid, p.85.
[93]Ibid., p.86.
[94]Ibid., p.89.

1. La fuerza mayor o caso fortuito es el hecho imprevisto o que no es posible resistir, como un naufragio, un terremoto, un incendio, el apresamiento de enemigos, los actos de autoridad ejercidos por un funcionario público, entre otros (artículo 64 del Código Civil) o circunstancias donde existe un constreñimiento que hace que la persona prácticamente se sienta obligada a incumplir el contrato o el deber general y en razón de esto lo hace.
2. La culpa exclusiva de la víctima hace referencia a un acto anormal de la propia víctima que sea la causa de su daño, pero tiene que ser la única causa para que se entienda que el responsable no tiene que repararla;
3. El hecho exclusivo de un tercero trata de que el acto de un tercero fue en realidad la causa del daño, no en parte, si no la causa total del daño, por lo que se exoneraría al supuesto responsable.

En el estudio de la configuración de la causa extraña es necesario evidenciar la existencia de diligencia y cuidado de aquel que la alega, pues el hecho de tener que prever y resistir implica desplegar ciertas conductas de diligencia y cuidado, que en caso de no realizarse no podría prosperar esta excepción. Estas conductas son determinadas y especificas con aquello que se pretende aludir como causa extraña.

En los casos de afectación de la información personal se podrán dar supuestos de causa extraña, sin embargo, hay que ser cuidadoso con su planteamiento debido a la facilidad con la que se enmascarar una culpa en una de las clases de causa extraña.

Por ejemplo en el caso en el que en el comercio electrónico el proveedor cumpla con las medidas de seguridad establecidas por el Estatuto pero el consumidor no siga con las directrices impuestas por el proveedor para el seguimiento de las mismas y haya un suceso en el que se afecte la seguridad

de dicha información, es probable que se pueda configurar a favor del proveedor una causa extraña en la modalidad de culpa exclusiva de la víctima, y este no tenga que responder por el incidente. Por el contrario no podrá exonerarse el proveedor si incumple con las medidas de seguridad que la Ley le impone, alegando que fue un empleado suyo quien estaba encargado de su implementación pues al no cumplirse con el requisito de exterioridad no es posible aducir una causa extraña por el hecho exclusivo de un tercero.

En este orden de ideas el nexo de causalidad se tendrá que establecer entre uno de los llamados a responder con el hecho imputable, es decir, que esta persona efectivamente haya cometido una culpa, la cual tiene que ser la causante del daño que se alega haber sufrido por parte de la víctima y esta culpa debe ser reprochable a el autor del hecho, es decir, que la ley le imponga el deber de responder por los daños causados a la víctima.

Por otra parte, en el ámbito de estudio a partir de la prueba de la culpa no se presume que esta culpa fue la causa del daño, por lo que sería necesario demostrar el nexo de causalidad frente a este aspecto. No obstante, la prueba de la culpa genera una presunción de que esta es imputable al sujeto al que se le atribuye, por lo que deberá emplear los medios de defensa disponibles para desvirtuar dicha presunción.

En aras de analizar los problemas de nexo de causalidad que se pueden presentar respecto a la violación de deberes u obligaciones de protección de información personal, se hará alusión a supuestos de hecho en los cuales se rompa la causalidad, como el siguiente:

Una aplicación digital guarda información de la localización de sus usuarios y los recorridos que estos realizan desde el momento mismo en que descargan la aplicación por medio de tiendas virtuales, y aceptan los términos y

condiciones que la aplicación contiene. Un grupo de personas no identificadas ingresan a la locación de la empresa propietaria de la aplicación y amenazan a uno de los ingenieros informáticos que posee la clave para acceder a la red de la aplicación, por lo cual este accede a entregar la información que le exigen por miedo a las represalias de los atacantes contra él.

Esta información es finalmente vendida en el mercado negro y logra llegar a manos de delincuentes informáticos que realizan transacciones con la información obtenida, generando perjuicios para los titulares de la información.

En cuanto al nexo de causalidad alegado por los usuarios de la aplicación, es desvirtuado por parte de la empresa propietaria por medio de la causal de fuerza mayor. Dado que fue una amenaza a uno de sus empleados sin posibilidad de prever o resistir, al haber sido realizada por terceros ajenos a la compañía y al haber comprometido la integridad física de sus empleados.

En este mismo orden de ideas, otro supuesto de hecho que podría revelar los problemas que surgen del nexo de causalidad se hará alusión a la teoría de la equivalencia de las condiciones. Esta teoría por si misma podría llevar a conflictos en cuanto a la conveniencia de su resultado y al objetivo axiológico de la responsabilidad.

Por ejemplo, frente a un caso en el que Martín accede a información personal de sus compañeros de trabajo sin su autorización y la conserva en su ordenador personal. Simón, un compañero de trabajo de Martín, ingresa al computador personal de su compañero con el fin de conocer su información personal, y al percatarse de que Martín tiene información tanto de el como de sus otros compañeros decide expone esta información en una red social informando sobre las actuaciones de Martín, sin más consecuencias que esta divulgación.

De acuerdo a la teoría de la equivalencia de las condiciones si se suprime un hecho de la cadena causal y sin ese hecho el daño igual se sigue produciendo, ese hecho no es causa del daño; por el contrario, si una vez suprimido este hecho el daño no se produce, el hecho se considera causa del daño. En el caso concreto, si Simón no hubiera hackeado el computador de Martín y expuesto la información que este contenía, la violación a los datos personales de sus compañeros igual se hubiera producido, por lo que la actuación de Simón no se entiende causa del daño.

Por el contrario, frente a la actuación de Martín, sin su actuación la afectación a los datos personales de los compañeros de trabajo no se hubiera presentado. De esto se concluiría, a raíz de esta teoría, que Martín sería el responsable por la vulneración a la información personal, quedando Simón exonerado de indemnizar los perjuicios sufridos por las víctimas a pesar de su actuación indebida, representando un problema en cuanto a esta teoría en relación con el elemento de causalidad.

Otro problema que se puede presentar en cuando al nexo de causalidad, el cual es aplicable al tema de estudio, es el de la teoría de autor desconocido en un grupo conocido. Esta establece la problemática que se da en cuanto a la prueba del nexo causal puede verse dificultada en casos en los que el autor pertenece a un grupo determinado de personas, sin que se pueda saber quién de ellas fue la causante del daño[95] (por ejemplo un grupo de empleados de una compañía dentro del cual necesariamente tiene que estar el causante del daño pero no se sabe cuál de estos fue específicamente el responsable).

[95] Op. cit., TAMAYO, p. 269.

Debido a la complejidad del mundo digital y la posibilidad del anonimato en esta esfera, esta problemática adquiere importancia, aunque se queda corta, en cuanto a que los hackers en la normalidad hacen parte de un grupo desconocido, por lo que las soluciones que pueden llegar a plantearse para esta teoría quedarían cortas frente a estos supuestos.

2.3.1.2 Distinción entre daño y perjuicio.

En cuanto al elemento daño, este tiene que tener ciertos requisitos para que sea indemnizable, tales como ser directo, es decir, causado directamente de la conducta del responsable[96]; lícito como aquel daño que se puede reclamar del demandado pues es objeto de protección por parte del Estado y va conforme a la ley, contrario por ejemplo a alegar la reposición de un carro robado; y real o cierto "*cuando en efecto ha acaecido o se sabe que acaecerá*", es decir, se sabe que produce o producirá un menoscabo para la víctima[97].

- Clasificación de los daños

Los daños propiamente dichos se dividen en (i) materiales, los cuales afectan a cosas físicas de la víctima; (ii) corporales, que afectan a la persona en su integridad física; y por último (iii) los inmateriales, no tienen una sede material sobre la cual reflejarse, como por ejemplo la afectación al buen nombre de una persona[98], siendo uno de los posibles daños que se pueden configurar dentro del ámbito de estudio.

A pesar de que la clasificación anterior es la que se inclina el presente estudio, existen diversas clasificaciones tanto en la doctrina como en la jurisprudencia con

[96] Op cit., DIAZ GRANADOS, p.103
[97] Ibid., p.101.
[98] Clasificación del profesor Fernando Moreno Quijano.

diferencias de todo tipo, por ejemplo el autor Juan Manuel Díaz Granados propone una clasificación de daños que atiende a distintos criterios, verbigracia por un lado habla de los daños previsibles e imprevisibles (relacionándolos con la responsabilidad contractual y la extracontractual respectivamente), los previsibles como aquellos que pudieron preverse al momento de la celebración del contrato y los imprevisibles como aquellos que siempre serán indemnizados; sigue con los daños a las cosas y a la integridad corporal, refiriéndose al origen del perjuicio, entendiendo que los eventos o conductas pueden causar deterioro o destruir cosas tangibles (bienes) o intangible (propiedad intelectual) pero también causar lesiones o muerte a personas. Por último, se refiere al daño patrimonial o extrapatrimonial, refiriéndose a si se afectó la esfera patrimonial o extrapatrimonial de la víctima[99].

Por otro lado, en el Tratado de Responsabilidad Civil del Profesor Javier Tamayo se hace alusión a la diferenciación entre daño patrimonial y extrapatrimonial dependiendo del bien jurídico sobre el que recaiga de forma inmediata la acción dañina. Adicionalmente, hace referencia a la clasificación del doctor Juan Carlos Henao que sostiene que todos los daños son patrimoniales pues todos los bienes y derechos, tengan contenido económico o no, conforman el patrimonio de una persona[100].

- Diferencia entre daño y perjuicio

Retomando lo dicho anteriormente, se hará una distinción sobre la confusión que se puede suscitar entre lo que se denomina daño y lo que se denomina perjuicio en una u otra esfera. Estos conceptos suelen usarse indistintamente en el lenguaje jurídico, pudiendo llevar a malentendidos, cuando en realidad, el perjuicio es el menoscabo de un interés jurídicamente protegido como consecuencia del

[99] Op cit., DIAZ GRANADOS, p. 104.
[100] Op. cit., TAMAYO, p. 470, 472, 473.

daño y el daño se puede entender como la afectación de un derecho (sin ser pacífico), sin embargo, es importante señalar que a veces un daño puede ser un perjuicio a su vez pero no es lo común. Un ejemplo para darle más claridad a la diferenciación sería: dos carros chocan, pues uno de los conductores se quedó dormido mientras manejaba el automotor, la víctima no salió herida del accidente pero su auto, además de necesitar cambio de algunas puertas y latas, no prendía. Por esta razón al propietario del auto le tocó utilizar medios de transporte públicos para asistir al trabajo durante el mes en el que el automotor se encontraba en el taller y pagar el arreglo de este. Este es un caso en el que se evidencian daños (el carro no prende y hay que cambiarle piezas) y perjuicios (el tener que sufragar dinero para desplazarse al trabajo, lo que antes podía hacer en su carro y por pagar el arreglo).

El mismo concepto de "daño emergente" puede crear confusión, pues aunque en su nombre tiene la palabra daño, es en realidad un perjuicio. Uno de los casos en los que no se diferencia el daño y el perjuicio o se puede decir que el daño configura un perjuicio al mismo tiempo es el caso del daño inmaterial que se ha llegado a reconocer por parte de la Corte Suprema de Justicia. Este daño ha sido denominado por esta misma Corte como daño a bienes jurídicos de especial protección constitucional, que cuando se ven afectados se lesiona tanto un derecho como un interés jurídico y se tutela, así no se materialice físicamente.

Esta misma Corte diferencia entre perjuicios patrimoniales (el mismo Código Civil contiene dos de estos, los más tradicionales, que son el daño emergente y lucro cesante[101]) y no patrimoniales, extrapatrimoniales o daños a la persona (como los llama la misma), expresa que "*son especies de perjuicio no patrimonial –además*

[101]*"ARTICULO 1614. DAÑO EMERGENTE Y LUCRO CESANTE. Entiéndase por daño emergente el perjuicio o la pérdida que proviene de no haberse cumplido la obligación o de haberse cumplido imperfectamente, o de haberse retardado su cumplimiento; y por lucro cesante, la ganancia o provecho que deja de reportarse a consecuencia de no haberse cumplido la obligación, o cumplido imperfectamente, o retardado su cumplimiento".*

del daño moral– el daño a la salud[102], a la vida de relación, o a bienes jurídicos de especial protección constitucional tales como la libertad, la dignidad, la honra y el buen nombre, que tienen el rango de derechos humanos fundamentales"[103].

Sobre este aparte se identifica una particularidad, la Corte denomina como perjuicio no patrimonial, la afectación a los bienes jurídicos de especial protección constitucional, que tienen el rango de derechos humanos fundamentales. Pero acabamos de decir que son daños inmateriales al mismo tiempo, esta es una muestra tanto de la doble característica pues son daños y perjuicios al mismo tiempo, como de la confusión que se puede dar si no se conoce a fondo el porqué de su denominación a veces como daño y a veces como perjuicio.

A su vez, se debe hacer énfasis en que esta decisión es novedosa en la medida en que es la primera decisión judicial por parte de la máxima corte de la jurisdicción ordinaria que reconoce los daños/perjuicio con los que se afectan los derechos fundamentales. Razón por la cual aún no es posible afirmar que esta Corte sostenga la posición adoptada en esta sentencia, serán necesarias posteriores reiteraciones al respecto para poder proyectar los resultados al invocar pretensiones en aras de perseguir su indemnización.
Lo mismo sucede con la pérdida de oportunidad o chance[104], este concepto puede darse bien como daño inmaterial pudiendo tener perjuicios patrimoniales (no lucro cesante) o extrapatrimoniales; siendo el mismo daño un perjuicio; o puede ser un perjuicio patrimonial o extrapatrimonial derivado de un daño corporal o material.

---

[102] Es aquel "quebranto a la integridad psicofísica o a la salud, con prescindencia de sus efectos económicos sobre la capacidad productiva de la víctima ".
[103]CORTE SUPREMA DE JUSTICIA**.** SALA DE CASACIÓN CIVIL**.** Magistrado Ponente: Ariel Salazar Ramírez. Radicación: 11001310300320030066001. Bogotá D. C., cinco (5) de agosto de dos mil catorce (2014).
[104] La pérdida de la oportunidad, se da cuando el responsable priva a la víctima de la posibilidad de adquirir un beneficio o de evitar un perjuicio, nunca se sabrá si la víctima lo iba a poder lograr pero el responsable suprimió la posibilidad de que así fuera.

Existe una diferencia entre la indemnización del perjuicio patrimonial y el extrapatrimonial y es que la del perjuicio patrimonial tiene como fin remediar el detrimento económico sufrido por la víctima, mientras que la del otro, no cumple una función resarcitoria en sentido estricto, pues ningún bien material es equiparable al valor de la dignidad humana[105]. Por ejemplo, el daño emergente es susceptible de reparación por una suma única y no periódica, a diferencia del lucro cesante que se conforma de la diferencia entre la utilidad y los gastos o la suma devengada proveniente de la prestación de un servicio, sea o no laboral.

Por su parte el daño moral (que se debería llamar en realidad perjuicio moral al tratarse de un daño y no de un perjuicio) es la lesión de la esfera sentimental y afectiva de la víctima, que corresponde a su órbita subjetiva e interna y que se expresa en dolor, sufrimiento espiritual y/o aflicción[106]. Tal como el daño a la vida en relación (sucede lo mismo con este perjuicio) que es la afectación de la actividad social de la persona, en su fuero externo, se dice que *"el daño a la vida de relación es conceptualmente distinguible del patrimonial y del daño a la salud, y puede coincidir con uno u otro, o presentarse cuando ambos están ausentes"*[107].

Mientras tanto el daño a los bienes personalísimos de especial protección constitucional que constituyen derechos humanos fundamentales, afirma la Corte que, aunque no encaja dentro de las categorías tradicionales en que se subdivide el *daño extrapatrimonial*, no interesa, pues es una especie autónoma cuya existencia y necesidad de reparación no se pone en duda. Este daño se ha definido como *"el agravio o la lesión que se causa a un derecho inherente al ser humano, que el ordenamiento jurídico debe hacer respetar por constituir una manifestación de su dignidad y de su propia esfera individual".*[108]

---

[105] Ibid.
[106] Ibid.
[107] Íbid
[108] Op cit, CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN CIVIL. Magistrado Ponente Ariel Salazar Ramírez.

2.3.1.3 Daños a bienes jurídicos de especial protección constitucional

Este daño-perjuicio específico tiene alta trascendencia para el tema de estudio de este trabajo, por lo que será abordado de una forma más profunda. Tiene importancia en cuanto el artículo 15 de la Constitución, que establece el derecho a la intimidad, buen nombre y honra, se ha reconocido como uno de estos bienes personalísimos de especial protección constitucional.

La sentencia del 5 de agosto de 2014[109], de la Corte Suprema de Justicia, Sala de Casación Civil, muestra un análisis de lo que se entiende por este daño y sus características, en general y en concreto pues el caso se relacionaba con el derecho al buen nombre. Este fallo judicial es de especial importancia para el tema de estudio dado que no existe jurisprudencia que toque directamente esta temática y a pesar de que no hace alusión al derecho a la intimidad se entiende que el derecho al buen nombre se encuentra intrínsecamente ligado a este. Así mismo, como se dijo anteriormente, al ser la primera decisión judicial que reconoce este daño/perjuicio adquiere importancia y debe ser revisada con detenimiento.

En primer lugar se entiende como incuestionable que la Constitución y los instrumentos internacionales que hacen parte del bloque de constitucionalidad ordenan la protección de los derechos fundamentales de la persona humana. Debido a esto deben ser objeto de protección y exigibilidad en el campo del derecho civil, siendo resarcibles en los casos en los que sean seriamente vulnerados, lo que es opuesto a una simple molestia, que no se tutela.

[109] Respecto a esta sentencia, el Magistrado Luis Armando Tolosa Villabona aclaró su voto al establecer que a pesar de estar de acuerdo con que se debe reconocer la indemnización de la afectación a un bien de especial protección constitucional, no compartía que este fuera categorizado dentro de los daños no patrimoniales necesariamente, al considerar que generaba problemas teóricos y prácticos como por ejemplo un obstáculo innecesario en la tasación y resarcimiento de la afectación a los derechos fundamentales.

En cuanto a la reparación la sentencia señala que los jueces son los que tienen que tomar una decisión razonable en cada caso acerca de si la medida de reparación es integral, equitativa, suficiente, necesaria y adecuada para consolar a la víctima, por la pérdida de un bien inestimable en dinero, para reivindicar su derecho fundamental y para reparar el agravio o la ofensa infligida a su dignidad. Además, debe determinar si el resarcimiento que se reclama por este concepto no se halla comprendido en otro rubro susceptible de indemnización, como el perjuicio patrimonial, el moral, a la salud, o a la vida de relación, con el fin de evitar un doble resarcimiento de la misma obligación. Pues se pueden dar tres casos: tanto que coincidan como que no o que el actor únicamente reclame la indemnización del daño a los bienes jurídicos esenciales al individuo porque su interés se centra en la reivindicación de su dignidad.

Hay una parte importante de la sentencia que ilustra específicamente a lo que se refería la no distinción de daño y perjuicio, en este caso relacionándolo con el derecho al buen nombre que era el tema de la sentencia (del 5 de agosto de 2014, de la Corte Suprema de Justicia, Sala de Casación Civil) y dice:

> *En cuanto al menoscabo del derecho al buen nombre, hay que admitir que el daño se configura cuando se demuestra la violación culposa de ese bien jurídico, sin que se requiera la presencia de ninguna otra consecuencia. Es decir que una vez acreditada la culpa contractual y la vulneración de la garantía fundamental como resultado de ese incumplimiento, se tiene por comprobado el detrimento al bien superior que es objeto de la tutela civil, y en ese momento surge el interés jurídico para reclamar su indemnización, porque el daño resarcible se identifica con el quebranto que sufre el derecho de estirpe constitucional*[110].

[110] Op cit, CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN CIVIL. Magistrado Ponente Ariel Salazar Ramírez.

Esto demuestra una evolución en la jurisprudencia colombiana, ya que se han resguardado valores constitucionales más allá de la filosofía sino en la práctica jurídica aún sin consecuencias materiales, siendo coherentes con los fines del Estado y un sentido de justicia.

Este daño/perjuicio se repara en virtud de principios de reparación integral y de equidad, al no tener un equivalente monetario específico el juez es quien lo determina. Cabe decir que la esfera reservada de la persona se valora con base a criterios extrínsecos, con prescindencia de la consideración subjetiva que cada quien tenga sobre su propio honor, intimidad o imagen; esto es determinado por la trascendencia que el ordenamiento jurídico le concede a los bienes esencialmente personalísimos, los cuales en Colombia gozan de un privilegio superior al ser consagrados expresamente como garantías fundamentales.

A su vez deben valorarse las circunstancias particulares de cada caso (en el supuesto del robo de información por ejemplo, conceptos como la cantidad de datos, la sensibilidad de los mismos, si se trata de información de personas vulnerables como niños, etc. deben alterar la forma de reparación) y las condiciones personales de la víctima, pues son las que permiten a la jurisprudencia adaptar los criterios objetivos a las situaciones concretas de cada realidad, estos son por ejemplo la intensidad de la lesión y la duración del perjuicio, junto a otras condiciones que le ayuden al juez a determinar equitativamente del monto del resarcimiento.

Verbigracia, en el caso concreto la Corte indicó:

> *"(…) se logra constatar que el daño sufrido por los demandantes corresponde al menoscabo de un derecho superior; que el perjuicio se prolongó por más de cuatro años; que se trata de personas con estudios universitarios cuyo desenvolvimiento profesional y social depende, en gran parte, de su buen*

nombre; y que mantenían frecuentes relaciones comerciales con entidades crediticias y establecimientos de comercio, ante los cuales su reputación financiera sufrió un grave deterioro."

De acuerdo a lo anterior, esta organización tasó una indemnización a cada uno de los afectados de $20.000.000 de pesos, lo que ofrece un lineamiento de los factores a tener en cuenta por el juez para cuantificar este perjuicio y el monto que se le puede llegar a otorgar a las víctimas por este concepto, teniendo siempre presente que los principios de reparación integral y equidad.

Es innegable que a la jurisprudencia colombiana le falta unificarse en varios tópicos, en el tema de daños y perjuicios se encuentran múltiples nombres y clasificaciones para un mismo concepto y esto crea confusión e inseguridad jurídica pues a la hora de demandar, el precedente escogido por el juez reinará aún si existe otro que difiera y será en parte un asunto de azar. Por otro lado, la resistencia al acogimiento de la responsabilidad objetiva en muchos casos, disfrazándola de una responsabilidad subjetiva con presunción de culpa parece quedarse sin cimientos. La evolución del derecho ha apuntado sobre este concepto y aunque pueda sonar estricto, en algunos casos es más acorde con el objetivo de la responsabilidad civil como en el caso de responsabilidad por cosas o por actividades peligrosas.

Una vez revisado el elemento daño en el contexto general, se hace necesario representarlo en el ámbito del presente estudio, dado que es el presupuesto que caracteriza a la responsabilidad civil que pueda surgir de la afectación a los datos personales que infringe el derecho a la intimidad, el derecho al buen nombre o a la honra.

Tal y como se menciono anteriormente, la Corte Suprema de Justicia promulgó el primer fallo reconociendo que el solo hecho de no respetar el derecho a la intimidad, buen nombre y honra se puede llegar a considerar un daño y un

perjuicio al mismo tiempo, sin la necesidad de tener repercusión en el patrimonio del titular de la información.

En caso de que esta posición de la Corte Suprema de Justicia sea acogida en la actualidad (dado que un solo fallo no es suficiente para afirmar que es la posición actual de la organización) podría repercutir en gran magnitud en los posteriores sucesos en los cuales se vea afectada la información personal. Dado que podría llamar la atención de aquellas personas Encargadas y Responsables del tratamiento de esta información, en cuanto podrían verse afectadas económicamente por la violación de la seguridad de los datos que tienen a su cargo, aun si no se establecen pérdidas pecuniarias al respecto. Lo anterior acarrearía en que ya no se sería necesario encajar el daño en un daño futuro sino que se trataría propiamente de un daño actual.

Sin embargo, de haberse manifestado en el patrimonio se deberá indemnizar y en todos los daños que pretendan ser resarcidos se deben demostrar previamente el nexo de causalidad y las características exigidas para que un daño sea reparado.

En conclusión, frente al supuesto de afectaciones a las obligaciones o deberes de protección de datos personales siempre se representará en un daño inmaterial, pues nunca se verá afectado directamente un bien físico del titular de la información ni su cuerpo físico como tal. Es disímil en el caso de los perjuicios que a raíz de la afectación de tales deberes u obligaciones sufren consecuencias tanto económicas (daño emergente y lucro cesante), como de la esfera intima del sujeto (daño moral y daño en vida en relación) o la pérdida de una oportunidad o chance.

Lo anteriormente expuesto será aplicable en los casos en los que la persona quiera que se le indemnice los perjuicios que se le causaron a raíz del daño a los bienes de especial protección constitucional, los cuales podrían ser el derecho a la intimidad, el buen nombre y la honra. Estos perjuicios no deben presentarse en

todos los casos de afectación a los bienes de especial protección constitucional, ya que sin su existencia también puede reclamarse la indemnización que surja de la sola afectación a este al ser un daño y al mismo tiempo un perjuicio.

Es relevante recordar que en frente a una responsabilidad extracontractual los daños que se deberán indemnizar por parte del responsable son tanto los previsibles como los imprevisibles, a diferencia de la responsabilidad contractual en la cual únicamente se deberán indemnizar los previsibles, salvo dolo, culpa grave o pacto expreso entre las partes.

A continuación, se hará una breve alusión a los supuestos de hecho mencionados en el elemento de hecho imputable y se mencionarán nuevos supuestos con el fin de identificar los daños que se pueden presentar en estas situaciones.

1) Frente al supuesto de hecho No. 1[111] algunos de los perjuicios que pudieron haber sufrido los proveedores de Montañas S.A. son por ejemplo:
   a) Daño/perjuicio de los bienes de especial protección constitucional, al verse afectado su derecho a la intimidad.
   b) En caso de que su información personal haya sido utilizada por los ciberdelincuentes para acceder a su información financiera y obtener dinero de estas, se podría reclamar un daño emergente por estas sumas.
   c) En caso en que los proveedores se vieran en la necesidad de invertir en la seguridad digital de su propia red, frente ataques cibernéticos

[111] María es empleada de la sociedad colombiana Montañas S.A., a pesar de tenerlo prohibido, decidió descargar música de Internet desde el computador que le fue designado en su trabajo durante la jornada laboral. Como consecuencia de la descarga gratuita de música en Internet, el computador de María fue infectado por un malware el cual logró expandirse a la red de la empresa, ocasionando la pérdida de información de los proveedores de la compañía generando así una violación de los deberes de protección de información personal suministrada por estos proveedores por parte de Montañas S.A.

por parte de los mismos delincuentes cibernéticos que atacaron a Montañas S.A. El capital que fue invertido para evitar los ataques se enmarcaría dentro del daño emergente que sufrieran los proveedores, siempre que sean sumas razonables y necesarios.

2) En el supuesto de la cuenta Premium de Spotify[112] el perjuicio que es probable que se presente es el de daño/perjuicio al derecho fundamental a la intimidad personal, lo cual se configuraría dentro de la categoría de los bienes de especial protección constitucional.

3) Daniel hacia parte del un proceso de selección de la compañía Pinar S.A.S., en el cual se encontraba en el último filtro junto con otros dos candidatos para ser escogido en el cargo de Auxiliar Administrativo. Luisa la exnovia de Daniel actuando dolosamente envío a la Directora de recursos humanos de Pinar S.A.S. una evidencia de que Daniel durante su período universitario había sido sancionado por fraude. Debido a esto, Daniel fue descartado del proceso de selección.

   Los perjuicios que se podrían alegar por parte de Daniel en un eventual proceso contra Luisa son:

   a) Daño/perjuicio de los bienes de especial protección constitucional, al verse afectado su derecho a la intimidad y al buen nombre.

[112] Spotify Premium cobra $11.499.00 pesos mensuales a sus suscriptores por el acceso a su base de datos musical. Juan se suscribe a la cuenta Premium adhiriéndose a los términos y condiciones como también a las políticas de privacidad del contrato en las cuales la compañía se obliga a no suministrar la información proporcionada por los suscriptores a terceros no autorizados. Luego de cinco meses de ser usuario de Spotify Juan comienza a recibir llamadas de una entidad bancaria ofreciéndole sus servicios, por lo cual Juan comienza a investigar la razón por la que la dicha entidad tiene en su poder sus datos personales y descubre que Spotify vendió tanto sus datos como los de los otros usuarios a dicha entidad.

b) Pérdida de la oportunidad o chance: aunque Daniel no tenia la certeza de ser escogido en el cargo de Auxiliar Administrativo tenía el 33. 33% de oportunidad de obtenerlo y por los documentos enviados por Luisa perdió dicha oportunidad.

De esta manera se identificaron todos los elementos constitutivos de la responsabilidad civil por vulneración a los datos personales en el contexto de los medios digitales.

2.4 ACCIÓN DE GRUPO

Teniendo en cuenta lo anterior, frente a un supuesto de hecho en el cual se presente una violación a los deberes u obligaciones de protección de información personal que afecte a una número apreciable de personas, sería posible acudir a la Ley 472 de 1998 la cual desarrolla el artículo 88[113] de la Constitución Política Colombiana.

Esta Ley consagra la acción de grupo por medio de la cual una pluralidad de personas (mínimo 20), constituida como grupo, puede acudir ante la justicia para reclamar la reparación del daño actual ocasionado a un derecho subjetivo de cada uno de los miembros de ese conjunto de personas, cuando el daño sea para todos producido por una misma causa. En este caso en concreto sería por la violación al deber u obligación de proteger la información personal. Está acción se ejercería

[113] Constitución Política de Colombia de 1998. Artículo 88: *"La ley regulará las acciones populares para la protección de los derechos e intereses colectivos, relacionados con el patrimonio, el espacio, la seguridad y la salubridad públicos, la moral administrativa, el ambiente, la libre competencia económica y otros de similar naturaleza que se definen en ella.*
También regulará las acciones originadas en los daños ocasionados a un número plural de personas, sin perjuicio de las correspondientes acciones particulares.
Así mismo, definirá los casos de responsabilidad civil objetiva por el daño inferido a los derechos e intereses colectivos."

con la finalidad de obtener el reconocimiento y pago de las indemnizaciones de los perjuicios sufridos por las víctimas.

La parte activa de la acción podría ser (i) cualquier persona que haga parte del grupo; (ii) el defensor del pueblo; y (iii) los personeros municipales y distritales en nombre de cualquier persona que lo solicite o que se encuentre en situación de desamparo o indefensión. Estos sujetos harían parte en el proceso judicial junto con los posibles agraviados que puedan surgir de este. Se interpondría contra el particular o entidad pública que presuntamente sería la responsable por la violación de la protección de datos personales, este sujeto debe ser determinado para entablar la acción pero se consagra la posibilidad de si existen otros posibles responsables el juez de primera instancia ordenará su citación al proceso.

Agregando a lo anterior, el fallo favorable de una acción de grupo no sólo tiene efecto de cosa juzgada frente a quienes hicieron parte en el proceso sino que podría llegar a beneficiar a personas que no fueron parte dentro de este, siempre y cuando sean parte del grupo interesado y no hubieran manifestado oportuna y expresamente la decisión de excluirse del grupo y de los resultados del proceso.

Por último, esta acción tiene un trámite preferencial y sumario para el juez, y exige que sea presentada durante los dos años siguientes a la fecha en que se causó el daño o cesó la acción vulnerable causante del mismo.

Como lo exige el artículo 206 del Código General del Proceso, cada una de las personas que conforman el grupo deberán realizar el respectivo juramento estimatorio de la indemnización que se pretende, discriminando cada uno de los conceptos y excluyendo los daños extrapatrimoniales del juramento, es decir, excluiría el daño/perjuicio a los bienes con especial protección constitucional cuando estos no tengan repercusión económica.

3. CASOS RELEVANTES EN ESTADOS UNIDOS E INGLATERRA

3.1. DATA BREACH" EN OTROS PAÍSES

En la actualidad se ha vuelto un método común el acudir a jurisprudencia extranjera para estudiar el análisis que hacen los tribunales de otros países acerca de un tema específico, en busca de conocer los argumentos en los que fundamentan sus decisiones logrando identificar novedosos razonamientos que logren ser de gran valor en la construcción de legislaciones e incluso decisiones judiciales en otros países.

Debido a que en Colombia no se han dado decisiones por parte de las altas cortes ni por entidades administrativas en relación a la pérdida de información personal por el uso de internet (ataque cibernético), es propio acudir a países con una mayor experiencia como Estados Unidos o Inglaterra en los cuales se han dado gran cantidad de casos de "*Data Breach"* y con grandes dimensiones en cuanto al número de víctimas y datos involucrados en los ataques. Estos países no son los únicos que han sufrido ataques cibernéticos en su territorio nacional, sin embargo, al ser del sistema jurídico del common law tienen un avance jurisprudencial importante que demuestra como en la práctica se manejan estos temas y es útil para el desarrollo del trabajo visto desde un contexto internacional.

Este estudio se realizará frente a casos prácticos pues es este el vacío en el ordenamiento jurídico colombiano y la especialidad propia del sistema jurídico de los países seleccionados. Esta recopilación de casos tiene como fin el de (i) identificar cómo se dan los ataques cibernéticos; (ii) cuál es su dimensión; (iii) cuál es el manejo que le dan las entidades internacionales a estos casos; (iv) en los que se haya desarrollado jurisprudencia al respecto identificar el trato judicial que se le ha dado a estos, en busca de conocer los argumentos en los que

fundamentan las decisiones de los tribunales extranjeros y reconocer aquellos aplicables al ordenamiento jurídico colombiano. Una vez presentado cada uno de los casos se presentará una breve conexión con la normatividad colombiana, para comenzar a identificar las diferencias y similitudes que tiene este ordenamiento jurídico con el de Estados Unidos e Inglaterra.

Los criterios que se tuvieron en cuenta para la escogencia de los casos de ataques cibernéticos que se detallarán a continuación, son (i) la cantidad de datos de información digital (personal o crediticia) afectados por estos asaltos. (ii) la cuantía de los perjuicios presentados en las pretensiones de las demandas o que hayan sido identificados por las autoridades administrativas de estos países. (iii) número de víctimas.

A lo largo de este análisis, se estudiarán algunos casos que aunque no tienen como consecuencia una indemnización propia de la responsabilidad civil, denotan la intención y regulación de los ordenamientos jurídicos de estos países en sancionar este tipo de ataques y tratar de prevenirlos, imponiendo por ejemplo, una multa por parte de una entidad administrativa.

3.1.1. CASOS RELEVANTES EN ESTADOS UNIDOS

El sistema de Estado Federal de Estados Unidos permite que exista diversa legislación, tanto Federal como Estatal, respecto a la protección de datos y el manejo de información. A nivel estatal, el órgano que está encargado de vigilar e investigar la violación de las leyes dirigidas a la protección de datos es el Federal Trade Commission (FTC), creado en 1914 para prevenir la competencia desleal dentro del comercio. En 1975 se le otorgaron facultades para adoptar normas que regulen el sector comercial.

Dentro de la regulación federal de protección de datos personales, se encuentran, entre otras:

1. *The Federal Trade Commission Ac*t (15 U.S.C. §§41-58), es una ley federal que regula la protección al consumidor en relación a las políticas de privacidad y seguridad de datos en línea, regula sanciones a las empresas en caso de no cumplir las directrices que se plantean en la ley.[114]

2. Consumer Privacy Protection Act[115] – S. 1158, busca garantizar la privacidad y seguridad de la información personal en aras de evitar que aquella que se catalogue como confidencial sea robada, como lo son las cuentas financieras, nombres de usuarios, contraseñas, entre otras, y evitar el mal uso de la información.[116]

3. Data Broker Accountability and Transparency Act, S. 668, regula a los "*Data Brokers"*[117]*,* estableciéndoles procedimientos para la recolección de la información que recogen, el tratamiento de seguridad que deben tener para salvaguardar la información y establecen mecanismos para que las personas puedan conocer la información personal que los "*Data Brokers"* tienen de cada uno.[118]

[114]https://www.ftc.gov/es/enforcement/statutes/federal-trade-commission-act
[115]"*To ensure the privacy and security of sensitive personal information, to prevent and mitigate identity theft, to provide notice of security breaches involving sensitive personal information, and to enhance law enforcement assistance and other protections against security breaches, fraudulent access, and misuse of personal information."*
[116]https://www.congress.gov/bill/114th-congress/senate-bill/1158/text
[117]"*Commercial entity that collects, assembles, or maintains personal information concerning an individual who is not a customer or an employee of that entity in order to sell or provide third party access to the information."*
[118]https://www.congress.gov/bill/114th-congress/senate-bill/668

4. Student Digital Privacy and Parental Rights Act - HR 2092 es un proyecto de ley que pretende prohibir a los sitios web y aplicaciones vender información personal de terceros.

Al ser Estados Unidos una de las grandes potencias del mundo y al estar en su territorio domiciliadas empresas de un nivel internacional relevante, se ha visto inmerso en varios casos de *"Data Breach",* como:

CASOS:

(i) Consumidores vs la compañía Target[119].

Uno de los casos más importantes que se ha dado en Estados Unidos fue el experimentado por la compañía con sede en Minneapolis, Minnesota, Target Corp. (ahora en adelante "Target"), a finales del año 2013. Según los demandantes un grupo de hackers ubicados en Europa del Este comenzaron a investigar las compañías retailers[120], logrando identificar falencias en el sistema de uno de los subcontratistas de Target, Fazio Mechanical Services (en adelante "Fazio"), que tenía acceso virtual a ciertas partes de la red de Target. "*Target gave Fazio the credentials to use for electronic billing, contract submission, and project management purposes*", los hackers se encargaron de robar la información de las credenciales otorgadas a Fazio debido al ineficiente sistema de seguridad que este tenía en su empresa, ya que contaba con un sistema de antivirus gratuito y Target no le exigió ningún requisito de seguridad para acceder a su red.

[119]*"Re: Target Corporation Customer Data Security Breach Litigation*". MDL No. 14-2522 (PAM/JJK) Memorandum, Order and Complaint.
[120]Empresas comerciales que hacen parte de la cadena de consumo, son las que finalmente tienen el contacto con el consumidor.

Tal y como se estableció en el memorial de la Corte del Distrito de Minnesota, *"The hole that left Target exposed to the hackers is called a ´segmentation issue´, which is a situation where computer systems within a network that should not be connected for security reasons are in fact connected. According to industry experts, there should never be a route between a network for an outside contractor (such as Fazio) and the network for payment data".* Además, los hackers lograron obtener la información de los clientes de Target por medio de un virus que cargaron en varias cajas registradoras de las tiendas de Target; cada vez que los usuarios pagaban sus productos con tarjetas, este virus guardaba el número de la tarjeta e información financiera adicional del cliente; posteriormente, el virus enviaba la información recolectada a los computadores de los hackers, ubicados en Rusia.

Al permitir que sus contratistas accedieran a su red sin exigirles un nivel de seguridad en sus sistemas y tener acceso a toda la información de sus clientes, esta llegó al mercado negro, en el cual se vendió la información de tarjetas de crédito y débito. *"According to The New York Times: On Dec. 11, one week after hackers breached Target's systems, Easy Solutions, a company that tracks fraud, noticed a ten to twentyfold increase in the number of high-value stolen cards on black market web sites, from nearly every bank and credit union".* El gran auge que logró obtener la venta de información de unas 330.000 tarjetas de crédito y débito emitidas por bancos de Europa, Asia, Latinoamérica y Canadá generó alerta en las entidades financieras que finalmente llamaron la atención de Target y del Departamento de Justicia de Estados Unidos.

Target incurrió en varios errores al intentar frenar el robo de información, ya que a pesar de que tuvo múltiples oportunidades para prevenir el ataque,

ignoró las alertas que se le presentaron[121] y se demoraron varios días en identificar el robo de información personal de sus clientes, teniendo en cuenta que es una compañía que recolecta toda la información posible de sus clientes y debía prevenir este tipo de hechos. En el proceso ante la Corte de Minnesota se estimó que la infracción causada por los hackers tuvo un costo aproximado de 18 billones de dólares, entre los costos de Target y las entidades financieras involucradas.

Los consumidores iniciaron una acción de grupo frente a la jurisdicción del Estado de Minnesota, el cual tiene un Acta Estatal de Tarjetas de Plástico de Minnesota, la S. 325E.64 "*Access Devices; Breach Of Security*", que impone el deber a las personas o compañías de no retener información de pago de las transacciones de sus clientes más de 48 horas[122]. Adicionalmente, establece la sanción en que incurren quienes violen el deber.

> *"Subd. 3.Liability. Whenever there is a breach of the security of the system of a person or entity that has violated this section, or that person's or entity's service provider, that person or entity shall reimburse the financial institution that issued any access devices affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders, including but not limited to, any cost incurred in connection with:(1) the cancellation or reissuance of any access device affected by the breach;(2) the closure of any deposit, transaction, share draft, or other accounts affected by the breach and any action to stop payments or block transactions with respect to the accounts;(3) the opening or reopening of any deposit, transaction, share draft, or other accounts affected by the breach;(4) any refund or credit made to a cardholder to cover the cost of any*

---

[121] "*Despite receiving multiple warnings from government and industry security experts, its own employees, and even its own computer security system, Target took no actions to protect its customers' sensitive data"*

[122] S.*325E.64 "Access Devices; Breach Of Security": "Subd. 2. Security or identification information; retention prohibited. No person or entity conducting business in Minnesota that accepts an access device in connection with a transaction shall retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction. A person or entity is in violation of this section if its service provider retains such data subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction".*

unauthorized transaction relating to the breach; and(5) the notification of cardholders affected by the breach. The financial institution is also entitled to recover costs for damages paid by the financial institution to cardholders injured by a breach of the security of the system of a person or entity that has violated this section. Costs do not include any amounts recovered from a credit card company by a financial institution. The remedies under this subdivision are cumulative and do not restrict any other right or remedy otherwise available to the financial institution"[123].

Dando lugar a que la Corte considerara que la compañía "*retaining the card security code data, the PIN verification code number, and/or the full contents of Target customers' magnetic stripe data in violation of the statute*" había actuado negligentemente al no eliminar la información y en proveer la seguridad suficiente para que los hackers accedieran a la información.

"Target concedes that classwide proof is available as to the existence of a duty and breach of that duty, but argues that Plaintiffs cannot rely on such classwide proof to establish injury or causation. Target contends that Plaintiffs' injuries here are ´risk of future harm´ injuries that are not cognizable or susceptible of classwide proof. (…) the risk of future harm is a possibility that one's financial information might at some point in the future be misused, and the injuries the Plaintiffs allege to have suffered".

Por lo cual la Corte consideró que no era un caso en el cual los demandantes debieron haber sufrido un daño, *"This is not a ´future harm´. This is a cost borne at the time of the breach and as a result of the breach."*

Finalmente, las partes en el proceso llegaron a un acuerdo en el que Target se comprometió a pagar 10 millones de dólares a los miembros de la acción de grupo y a los representantes de dicha acción sus servicios de forma adicional.

Dicho acuerdo consistió en que Target se comprometía a pagar a los miembros de la acción de grupo dependiendo de la capacidad de documentar sus daños. Los demandantes con prueba documental de sus pérdidas fueron reembolsados con un máximo de diez mil dólares, entre los que se incluía los daños que padecieron y el tiempo que los sufrieron (10 dólares por hora). Los accionantes que no tuvieran

[123]S. 325E.64 "Access Devices; Breach Of Security", se puede consultar en el siguiente link: https://www.revisor.mn.gov/statutes/?id=325E.64

pruebas documentales de sus daños podían recibir la misma cantidad que aquellos que si la tuvieran, pero únicamente después de que fueran pagados los primeros y los "*Service Awards"* que la Corte estableciera. El acuerdo también requería que la empresa mejorara sus prácticas de seguridad de la información de forma significativa.

Adicionalmente, Target se comprometió a pagar los gastos administrativos y de notificación del acuerdo, así como los gastos de representación judicial por más de 6 millones de dólares. Estos valores no hacían parte de los diez millones de dólares[124].

En este caso, se puede evidenciar que en cuanto a la información financiera, el incumplimiento de normas como la de no retener información de pago más de 48 horas, da lugar a sanciones severas como que el que incumpla debe reembolsar a la institución financiera por la cancelación o re-emisión de cualquier dispositivo de acceso afectado por la infracción; cualquier reembolso o crédito hecho a un cliente para cubrir los costos de cualquier transacción no autorizada relacionada con la infracción y la notificación a los clientes afectados por la violación, entre otros, que puede llegar a tener un gran costo económico.

En Colombia, no existe la obligación en cabeza de aquellos que recolecten información personal o crediticia de sus usuarios de informar la violación a los códigos de seguridad y la existencia de riesgos en la administración de estos datos, pero si se debe notificar a la autoridad administrativa correspondiente que esté a cargo de la vigilancia del tratamiento de datos personales como se evidenció anteriormente. Así como tampoco está establecido un tiempo límite de retención de información de las transacciones (en la cual se encuentran datos personales y crediticios), sino que debe estar siempre autorizado por el titular.

[124]*"Re: Target Corporation Customer Data Security Breach Litigation*". MDL No. 14-2522 (PAM/JJK) Memorandum, Order and Complaint. Document 645.

Por otro lado, las personas naturales o jurídicas que recolecten información personal siempre deben contar con mecanismos de seguridad para salvaguardarla, ya sea que se encuentre en medios físicos o electrónicos. Esto implica un deber de diligencia y cuidado como el de no brindar acceso a terceros no autorizados a la información recolectada pues esto se encuentra prohibido en la regulación colombiana.

En este caso la Corte de Minnesota consideró que no se trataba de una situación en la que se hubiera configurado un daño futuro, sino que ya se había materializado el daño en razón de la violación de seguridad vulnerando la protección de los datos personales y desde que esta se produjo, lo cual es compatible con la legislación colombiana en este tema tal y como se pudo identificar.

(ii) Ashley Madison[125]

Otro de los casos de "Data Breach" que ha generado mucha polémica y en el cual se han visto vulnerados los datos de millones de personas en todo el mundo, fue el robo de información de los usuarios de Ashley Madison, un sitio web que promociona conseguir una relación extramarital, mediante un servicio de citas para personas casadas.

Un grupo de hackers que se hacen llamar "The Impact Team" robó la información de aproximadamente 33 millones de clientes del sitio web de infidelidades, con la intención de presionar a la empresa canadiense AvidDatingLife Inc., propietaria del sitio web, a que cerrara la página o se publicaría la información robada. Debido a la falta de importancia que le dio la

[125]Noticia publicada en el Diario El Confidencial, España, 19 de agosto de 2015. Disponible en http://www.elconfidencial.com/tecnologia/2015-08-19/hackers-publican-los-datos-de-millones-de-adulteros-de-la-web-ashley-madison_976016/

empresa canadiense a las amenazas, los hackers publicaron información de millones de personas, la cual podía ser descargada BitTorrent[126].

La información revelada incluía nombres de usuarios, teléfonos, correos, transacciones bancarias, los cuatro últimos dígitos de las tarjetas de crédito, entre otros; lo cual permitía identificar a los usuarios del sitio web que incita a ser infiel.

Uno de los mayores problemas que se van a presentar en el litigio, que aún esta en etapa inicial, estará relacionado con los clientes que pagaban $19,00 USD al sitio web para que se eliminara todos los datos relacionados con su usuario, los cuales, según declaración de los hackers no era efectivamente eliminado de las bases de datos del sitio web.

Este es uno de los casos en los cuales el robo de información afecta directamente el buen nombre de las personas, su vida personal y profesional, ya que es información a la que puede acceder todo el público y puede afectar matrimonios y familias y permitirá conocer cuál es el trato que le dará los jueces norteamericanos al tema.

De este caso se concluye que no se debería tener que pagar una suma de dinero para que aquel que recolecte la información personal elimine dicha información de sus bases de datos, por el contrario tal y como se evidencia en la legislación colombiana, se necesita una autorización para disponer de esta información y por petición de su titular debe ser eliminada cuando este lo solicite, cuando su tratamiento no se adecue al ordenamiento jurídico, por ejemplo violando el derecho fundamental a la intimidad.

[126]Software para intercambio de archivos.

(iii) Consumidores vs.Sony Gaming Networks.

En el mes de abril de 2011 se presentó una violación de los datos personales de los usuarios de PlayStation, *"On May 2, 2011, Sony Online Entertainment LLC ("SOE") announced that an unauthorized person or persons had perpetrated an illegal and unauthorized attack on the SOE network, and that certain SOE accountholder information appeared to have been accessed as a result of the unauthorized intrusion ("the SOE Intrusion") (together with the PSN Intrusion, the "Intrusions"). Services on both the PSN and the SOE networks were suspended and unavailable to accountholders for a period of approximately two to three weeks until operations were restored on the networks by on or about May 15, 2011."*[127]

La acción de grupo fue adelanta por la Corte Distrital del Sur de California, tribunal que inicialmente inadmitió la acción propuesta por el grupo, con base en la defensa de Sony al establecer que la presentación de daños por parte de los demandantes había sido incorrecta por presentar una acción de grupo con daños individualizados y concretos (buscando que se les indemnizaran). Dichos daños se alegaba que habían sido causado por el hecho de haberse esparcido incorrectamente su información, argumentando que esto incrementaba el riesgo de daño futuro a cada uno de los miembros de la acción. Sustento que interpretó la Corte que lograba cumplir con el requisito de daño futuro para generar responsabilidad de acuerdo a la Constitución de Estados Unidos, pero no bajo las leyes de California; permitiéndoles entonces a la parte accionante modificar la acción presentada.[128]

[127] Acuerdo entre Sony Gaming Networks y Customer Data Security Breach Litigation.Corte Distrital del Sur de California. Case 3:11-md-02258-AJB-MDD. Disponible en http://docs.ismgcorp.com/files/external/Sony_Settlement_061614.pdf.Página 2.
[128] *Ibid.*

Luego de dos años de conversaciones entre las partes, Sony se motivó, en aras de evitar costos en el litigio, a llegar a un acuerdo con los accionantes por 15 millones de dólares pero advirtió que seguía negando las acusaciones. Este acuerdo solo incluía a las personas domiciliadas en Estados Unidos y que se vieron afectadas por el ciberataque[129].

Entre los múltiples compromisos de Sony con sus demandantes se encontraba: recibir un pago equivalente a cualquier "*PlayStation Wallet Credit*" que no hubiera sido usado, siempre y cuando en la cuenta hubiera dos dólares de crédito o más; por otro lado se ofrecían una serie de beneficios categorizados, entre los cuales se encontraban: el "*Theme Benefit*" que consistía en descargar gratis tres temas de "*PlayStation 3*"; el "*Game Benefit*" que otorgaba la posibilidad al usuario de descargar un juego de "*PlayStation 3"* o de "*PlayStation Portable*" sin ningún cargo; el ""*PlayStation Plus New Suscription Benefit"* que, como su nombre lo dice, podía generar sin ningún costo una nueva suscripción a "*PlayStation Plus*"; así como el "*Qriocity User Benefit"* que permitía a su beneficiario disfrutar de un mes de música ilimitada gratis en este servicio.[130]

El desastre de Sony cruzó fronteras, afectando a personas de todo el mundo, incluyendo de Gran Bretaña. ICO (La Oficina del Comisionado de Información en Gran Bretaña) impuso una multa de 250,000 euros por la infracción de datos[131].

En este caso, es notable que en la jurisprudencia estadounidense, se presentan dificultades respecto a la aplicación de leyes estatales o federales,

[129]"All Persons residing in the United States who had a PlayStationNetwork account or sub-account, a Qriocity account, or a Sony Online Entertainment account at any time prior to May 15, 2011"
[130] Op. cit., ps. 15-24.
[131] Recuperado de: http://www.techworld.com/security/uks-11-most-infamous-data-breaches-2015-3604586/

las cuales frente algunos hechos se contradicen o puede presentarse que una sea más proteccionista que la otra, por lo que del razonamiento del juez y de la habilidad del abogado dependen en mucha parte la victoria en un caso, lo que a veces satisface la ley federal, no lo hace con la estatal o al contrario.

Las leyes de California, al igual que las leyes de Colombia, no aceptan la indemnización de perjuicios con base en la causación de un daño futuro. Los demandantes debieron establecer desde el principio la materialización de un daño por la violación de la seguridad de los datos personales en la plataforma de Sony.

(iv) Szpyrka vs. LinkedIn Corporation

Katie Szpyrka, una de las usuarias de la cuenta Premium de LinkedIn (sitio web), inició una acción del grupo en contra de la compañía propietaria del sitio web debido a que el 6 de junio de 2012 "*hackers infiltrated LinkedIn´s servers and accessed database(s) containing its users´ PII* (personal identifiable information)*. After retrievind this data, the hackers publicy posted over 6 millon LinkedIn users´password online. Because LinkedIn used insufficient encryption methods to secure the user data, hackers were able to easily decipher a large number of the passwords.*[132]"

El litigio se llevo a cabo en la Corte Distrital del Estado de California, con una pretensión aproximada de $5.000.000,00 USD, basadas en que al ingresar a LinkedIn y registrarse como usuario en la página web, adquirieron una cuenta Premium de un valor entre $19.95 dólares americanos hasta $99.95 dólares americanos mensuales, la cual ofrecía proteger toda la información que los

[132]Corte Distrital del Norte de California.Szpyrka vs. LinkedInCorporation. Case5:12-cv-03088-EJD. 2012. Disponible en http://recruitingdaily.com/wp-content/uploads/sites/6/2015/02/Szpyrka-v-Linkedin-Complaint.pdf

usuarios registraran en el sitio, "*using industry standard protocols and technology*[133]". A su vez se alegaba por la demandante que la razón de la afiliación a la cuenta Premium era la seguridad adicional que brindaba respecto a la cuenta gratuita. La accionante se fundamentó en esta promesa para demostrar la negligencia por parte de LinkedIn al no proteger la información de la forma esperada de acuerdo al contrato celebrado entre los usuarios Premium y LinkedIn, ya que según estudios se comprobó que el método usado por los cibercriminales es un método común llamado "SQL injectión".

Finalmente, la Corte consideró que como los Acuerdos de Uso y las Políticas de Privacidad eran iguales tanto para la cuenta Premium como para la gratuita, no era un caso *"where consumers paid for a product, and the product they received was different from the one as advertised on the product's packaging",* por lo cual rechazó las pretensiones de los accionantes[134]. Sin embargo, al no cumplir con la protección prometida, se le condeno a pagar $1.25 millones de dólares americanos a los usuarios Premium que tuvieran vigente su suscripción entre marzo 15 de 2006 y el 7 de junio de 2012, por considerar demostrada la negligencia de la compañía al proteger la información personal de los usuarios[135].

Este caso se enmarca en un incumplimiento contractual debido a que LinkedIn se obligaba en los términos del contrato a usar protolocos y tecnología de un estándar industrial y los delincuentes informáticos penetraron el sistema utilizando un método común, es decir, el sitio web no cumplió con la calidad prometida para su sistema de seguridad de información. Esta fue la razón que en últimas hizo que LinkedIn tuviera que asumir costos de reparación, al ser

[133]Ibidem

[134]Black, J. (2013). Developments in Data Security Breach Liability. *Bus. Law.*, *69*, 199-206.

[135] Corte Distrital del Norte de California.Szpyrka vs. LinkedInCorporation. Case5:12-cv-03088-EJD. 2012. Class Action Settlement Agreement. Disponible en: https://www.linkedinclassactionsettlement.com/Documents/SettlementAgreement.pdf

iguales los estándares de las cuentas onerosas y gratuitas por lo que los alegatos de los accionantes en cuanto a la causa por la cual contrataron se quedó sin fundamentos. Con fundamento en estas razones, en Colombia se le hubiera otorgado el mismo tratamiento a este caso, enmarcándolo en un incumplimiento contractual.

(v) Consumidores vs. HannafordBrothers Co.[136]

Este ataque cibernético duró desde el 7 de diciembre de 2007 hasta el 10 de marzo de 2008 y consistió en filtración de un malware (tipo de virus informático) en más de 300 servidores de las tiendas de esta compañía, el cual extraía la información de tarjetas débito y crédito de los clientes que pagaban en las cajas registradoras por este medio de pago; fueron aproximadamente 4.2 millones de tarjetas de crédito y débito comprometidas. Los afectados presentaron acción de grupo contra la compañía, litigio que fue llevado a la Corte Distrital de Maine, la cual decidió que debido a la negligencia de la compañía y el incumplimiento del contrato implícito que tenía con sus clientes, esta debía indemnizar los daños previsibles que fueron causados[137].

De este caso se puede resaltar que la negligencia y el incumplimiento del contrato pueden llevar a tener que reparar daños causados, con otra similitud a la legislación de Colombia y es que se condenó a reparar daños previsibles.

(vi) El conocido banco JpMorgan Chase también fue objeto de una demanda por mal manejo de datos consecuente a la pérdida masiva de datos financieros de sus clientes, específicamente de tarjetas de crédito. La demanda se dio con un anuncio de Jp Morgan Chase (Septiembre 2006) en el que dijo que sin

[136] Corte Distrital de Maine. Hannaford Brothers Co. Customer Data Security Breach.Case 2:08-MD-1954-DBH. 2013. Disponible en http://www.med.uscourts.gov/Opinions/Hornby/MDL/MDL1954_2013_03_20_ORDER11.pdf
[137] Op cit., BLACK, pp.199-206.

intención había desechado muchas "*tapes*" de computador que contenían información personal de 2.6 millones clientes con tarjetas de crédito, por lo que en febrero 17 de 2009 James Willey interpuso una demanda de acción de grupo en su beneficio y en el de todas las personas afectadas por la pérdida de datos por violación del FCRA (The Fair Credit Reporting Act) que regula la disposición de información de consumidores. A su vez la Oficina del Contralor (OCC por sus siglas en inglés) establece que los bancos deben "*properly dispose of any consumer information it maintains or otherwise possesses*".

La Corte del Distrito de Nueva York encontró la reclamación estatal de los demandantes insuficiente pues fallaron en alegar daños actuales, un elemento requerido para cada reclamación. Mientras la Corte notaba que "*emotional damages*" podían ser suficientes bajo la FCRA (ley federal), sostuvo que *"in state information loss cases (…) the risk that plaintiff's data may be misused because it has been lost is not a cognizable harm".* La Corte, además no consideró que los costos de protección contra robos de identidad fueran una forma de daño y rechazó la reclamación estatal de los demandados en este campo también.

Pero han habido cortes que en casos similares no han tenido el mismo razonamiento, el Séptimo Circuito de Pisciotta, encontró que "t*he injury-in-fact requirement can be satisfied by a threat of future harm or by an act which increase[es] the risk of future harm*". La Corte de Caudle estuvo de acuerdo con esta reflexión, citando a Pisciotta y a casos de daños ambientales para soportarlo[138], demostrando que no hay uniformidad en el tema y menos cuando cada estado tiene una legislación distinta.

[138]"*Federal Court Dismisses Data Breach Class Action Brought Against J.P. Morgan Chase Based on Federal Preemption*".ALAN CHARLES RAUL, EDWARD McNICHOL AS, MICHAEL F. McENENEY, AND KARLF. KAUFMANN. "*Privacy & Data Security Law Journal".* October 2009.

A pesar de que el caso de JpMorgan Chase no se caracteriza por un ataque cibernético es relevante debido a que esta entidad financiera pudo haber sido responsable por no haber dispuesto apropiadamente de la información de sus clientes, sin embargo, no se demostraron daños actuales, ya que la Corte no consideró que los costos de protección contra robos de identidad fuera una forma de daño. A su vez tampoco consideró que lo fuera el riesgo de que la información desechada pudiera ser usada de forma inapropiada en el futuro y por esto no prosperó el cargo. Frente a esto también hubo una tensión entre la ley federal y la estatal, si se hubiera juzgado bajo la ley federal el daño moral hubiera sido suficiente para que se tuviera que responder, pero como se juzgó bajo la estatal (Nueva York) no lo fue.

A partir de esta decisión se podría decir que es necesario el elemento daño para aducir responsabilidad pero aparecen casos disimiles, como las Cortes de Claude o Pisciotta, que sostienen que el requisito de daño puede ser satisfecho por una amenaza de daño futuro o por un acto que incremente el riesgo de daño futuro, por lo que se demuestra que hay inseguridad jurídica y que probablemente los demandantes van a tratar de utilizar las normas de competencia a su favor para demandar en Estados cuyos jueces tengan el razonamiento que más les convenga. A su vez se ha planteado por algunos autores[139] que un problema común es exactamente ese, si la posibilidad de un daño futuro satisface el requisito de daño contenido en la Constitución de Estados Unidos, siendo el problema más relevante en cuanto a responsabilidad por pérdida o robo de información personal y crediticia en este país.

Considerando este caso de cara a la legislación colombiana, se identifican similitudes en cuanto a que los costos de protección contra robos de identidad no se consideran un daño, sino una carga para los titulares. Además la

[139] BLACK, John. Developments in data security breach liability. *Bus. Law.*, 2013, vol. 69, p. 200.

posibilidad de que en el futuro la información desechada pueda ser usada de forma inapropiada, no genera un daño para el ordenamiento jurídico colombiano, se requiere que este sea real y actual. Como se ha dicho anteriormente no se ampara el daño futuro.

Frente a la eliminación inapropiada de información por parte de JpMorgan Chase, es importante advertir que en caso de que esto suceda en Colombia esta compañía estaría incumpliendo con el deber de tomar todas las medidas necesarias para que la información que se les ha autorizado manejar no pueda ser adquirida por terceras personas no autorizadas por el titular; lo cual podría enmarcarse en una culpa. A pesar de que en este país se necesita que haya un daño para la configuración de una responsabilidad civil, la violación al derecho fundamental a la intimidad se ha llegado a considerar como un daño inmaterial, como se explicó anteriormente.

Los "Data Breaches" en Estados Unidos han ido aumentado con el pasar de los años, lo cual ha generado preocupación tanto en el país como en las compañías que son vulnerables a este tipo de ataques, ya que de acuerdo a una encuesta realizada por Ponemon Institute en la que se identificó que para el año 2012, el costo que generaba la violación de datos era $5.4 millones de dólares o $188 dólares por cada dato que sea robado. Además en el 2012, muchas compañías y Estados fueron víctimas de los ataques de los hackers, como fueron los casos de Global Payments, Inc que fue víctima del robo de 1.5 millones de números de tarjetas; Nationwide Mutual Insurance de 1.1 millones de cuentas; y hasta el Estado de Carolina del Sur fue víctima de los ataques cibernéticos en el cual fue robada la información de 3.6 millones de números de seguridad social y 387.000 números de tarjetas de crédito y débito del Estado.[140]

[140] Ibid.

Generalmente, en los casos de robo de información de datos personales, las cortes estadounidenses centran su atención en el cumplimiento del requisito de daño que establece el ordenamiento jurídico federal de Estados Unidos, dado que se cuestiona lo siguiente: *"a frequent issue has been whether the possibility of future injury in the absence of actual harm is enough to satisfy the Article III "injury in fact" requirement."*[141] De la cual existen diferentes decisiones dependiendo de las cortes de los distritos que deban conocer los casos.

3.1.2. CASOS RELEVANTES EN INGLATERRA

Reino Unido cuenta con una entidad encargada de velar por la protección de los datos: el Information Commissioner's Office (ICO), creado a instancias del Acta de Protección de Datos de 1998, esta normativa es la más importante y la más citada en las demandas de violaciones de datos personales en este país.

En cuanto a la legislación de la protección de datos, se encuentran, entre otras:

1. Acta de Protección de Datos de 1998, transposición de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de la Unión Europea. Se trata de la ley de mayor relevancia en la materia y que establece los fundamentos jurídicos para manejar información en el Reino Unido, ya que proporciona los instrumentos para que los ciudadanos se sientan más protegidos en cuanto a datos personales se refiere.

2. Acta de Libertad de Información de 2000, que otorga a los ciudadanos y a las organizaciones el derecho a solicitar información sobre los datos que reposan en instituciones públicas de Inglaterra, Gales e Irlanda del Norte y de instituciones privadas de Escocia.

[141] Ibid.

3. Regulaciones de Comunicaciones Privadas y Electrónicas (Directiva CE) de 2003, que es la transcripción de la Directiva 2002/58/CE.

4. Regulación de Información Ambiental de 2004, transposición de la Directiva 2003/4/EC, que atañe únicamente a datos relativos a información medioambiental[142].

Según el Gobierno de Gran Bretaña, el Acta de Protección de Datos de 1998 dictamina cómo la información personal debe ser usada por organizaciones, compañías y el Gobierno. Aquellos que manejen información deben seguir ciertos principios: usar la información de forma legal y justa; para ciertos propósitos específicos, es decir, de forma limitada; almacenarla no más del tiempo necesario; no transferir la información fuera de la zona económica de la Unión Europea sin protección adecuada; asegurarla; usarla de forma adecuada; manejarla de acuerdo a los derechos de protección de datos de las personas[143]. Esto es compatible con los principios del manejo de datos personales y crediticios en Colombia.

En varios litigios de este país se reclama que se reparen daños causados por la violación de esta Acta (en adelante DPA), nos detendremos en tres de ellos:

(i) David Paul Johnson vs Medical Defence Union[144]

En Marzo de 2007, se estudió el caso de una demanda que interpuso el médico David Paul Johnson contra su asegurador Medical Defense Union para que lo compensara de acuerdo al artículo 13 del Acta de Protección de Datos de 1998,

[142] Báez, M. C. T., & Báez, T. (2010). Aproximación A La Protección De Datos Personales En España, Inglaterra Y Francia Como Ejercicio De Derecho Comparado Previo A Una Traducción. *Contribuciones a las Ciencias Sociales*, (2010-03).
[143] Recuperado de: https://www.gov.uk/data-protection/the-data-protection-act
[144] [2007] EWCA Civ 262; (2007) 96 BMLR 99; The Times, 10 April 2007. Recuperado de: http://www.5rb.com/wp-content/uploads/2013/10/Johnson-v-MDU-CA-28-Mar-2007.pdf

por supuestamente procesar de forma desleal sus datos personales. Según el demandante al haber hecho un procesamiento de esta forma, su contrato fue terminado de manera unilateral por parte de la aseguradora. Dijo David que se seleccionó material de sus datos personales por la aseguradora para revisar sus riesgos, lo que conllevó a tomar la decisión pero que se hizo de una forma incorrecta y alega que la terminación del contrato causó gran daño a su reputación. Se determinó por la Corte Suprema de Justicia Sala Civil, División Chancery, que la selección manual de datos antes de su procesamiento automático no era procesamiento a la luz del DPA[145], que no se probó que de haber tenido otra política de manejo de información se hubiera llegado a otra conclusión pero lo más importante fue que se entendió por el juez que Johnson no había sufrido ninguna pérdida pecuniaria y por lo tanto no se podían reparar los daños por aflicción bajo el artículo 13 del DPA[146]. Esto da una luz a la interpretación de este artículo que no es implícita por su sola lectura, se afirma por el juez que se necesita que haya daño pecuniario para que haya "*distress damage"*[147]*.* En este caso también se dijo que no se debió haber tratado un daño a la reputación como una violación del DPA, sino que se debía haber tratado como difamación.

---

[145] "*´processing´, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including— (a) organisation, adaptation or alteration of the information or data, (b)retrieval, consultation or use of the information or data, disclosure of the information or data by transmission, dissemination or otherwise making available, or (d)alignment, combination, blocking, erasure or destruction of the information or data".*

[146] "*Compensation for failure to comply with certain requirements. (1)An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage. (2)An individual who suffers distress by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that distress if— (a)the individual also suffers damage by reason of the contravention, or (b)the contravention relates to the processing of personal data for the special purposes. (3)In proceedings brought against a person by virtue of this section it is a defence to prove that he had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned".*

[147] Daño moral.

De lo relatado se desprende que en Gran Bretaña es necesario una pérdida pecuniaria para reclamar lo que se podría entender como daño moral si se está solicitando el amparo bajo el acta mencionada anteriormente, además de identificar que los daños que afecten la reputación de la persona no deben tratarse por manejo de datos personales y su protección sino por normas referentes a la difamación.

Del caso anterior lo relevante para el presente estudio es identificar que en esta ocasión se consideró que para indemnizar el daño moral se necesitaba la configuración de un daño pecuniario, supeditándola a esta. En Colombia no se le da el mismo tratamiento, el daño moral debe ser consecuencia tanto de un daño material como de un daño corporal o inmaterial, al igual que lo debe ser el "daño pecuniario". Además en cuanto a la pérdida de reputación, se establecería una afectación al buen nombre de la persona, daño que se ha podido reclamar en algunos procesos de responsabilidad civil.

(ii) Vidal-Hall vs Google Inc[148].

En Corte Suprema de Justicia, División Queen´s Bench, con juzgamiento del día 27 de marzo de 2015, se pusieron en duda los requisitos del artículo 13 del DPA para pedir daño por aflicción.

El caso consistía en que los demandantes eran tres personas que usaron el navegador de Apple para acceder a Internet durante un tiempo determinado; ellos argumentan que Google guardó información privada (uso de navegador) sin que ellos supieran o tuvieran posibilidad de consentir y que después usó su información para fines comerciales. Los reclamos de los demandantes fueron en Inglaterra y Gales por mal uso de información privada, abuso de confianza y

[148] [2015] EWCA Civ 311.

violaciones del DPA, incluyendo compensación por aflicción del artículo 13 del DPA.

El juez anterior falló a favor de los demandantes en cuanto a sus pretensiones, por lo que la Corte Suprema estaba decidiendo la apelación del caso hecha por Google, la cual rechazó. La Corte se pronunció diciendo que el mal uso de información privada es distinto a abuso de confianza, que el DPA había intentado implementar la Directiva 95/46/EC de la Unión Europea y que el artículo 23 de esta directiva[149] permitía la compensación del "perjuicio". Por otro lado, el juez define que los términos legales en la legislación de la Unión Europea tienen un significado autónomo, al cual se le debe dar efecto armónico a través de las leyes de los estados miembros[150]. El problema radica en que se afirma que no se pueden pensar como compatibles el artículo 23 de la directiva y el 13.2 del DPA, al exigir este último la existencia de otro daño para que se indemnice un daño moral, además de ir en contra de los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea (EUCFR)[151].

Tal y como se dice expresamente en el texto: "*The present case falls on the Benkharbouche rather than the Chester[152] side of the line. What is required in order to make section 13(2) compatible with EU law is the disapplication of section 13(2), no more no less. The consequence of this would be that compensation*

[149] "*Responsabilidad 1. Los Estados miembros dispondrán que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Directiva, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido. 2. El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño".*

[150] Recuperado de: www.5RB.com

[151] "*Artículo 7. Respeto de la vida privada y familiar. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones. Artículo 8. Protección de datos de carácter personal. 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedarán sujeto al control de una autoridad independiente."*

[152] Precedentes Judiciales.

would be recoverable under section 13(1) for any damages suffered as a result of a contravention by a data controller of any of the requirements of the DPA. No legislative choices have to be made by the court". Esto quiere decir que se puede reclamar cualquier daño surgido por violación del DPA pero también reafirma que se necesita un daño, sin importar si es de aflicción, pecuniario u otro.

En este caso, a diferencia del anterior, se distingue el abuso de confianza del mal uso de información privada, lo cual es acorde a la legislación colombiana y se explicó que para respetar la ley de la Unión Europea se debía desaplicar el requerimiento de la existencia de otro daño para pedir daño moral y en consecuencia, se podría pedir cualquier daño por la violación del DPA. Demostrando la supremacía de la ley de la Unión Europea y otra vez, la contradicción a la que se puede llegar con decisiones jurisprudenciales. Esta decisión es acorde a la línea regulatoria de responsabilidad civil en Colombia por violación a la normatividad de protección de datos personales.

(iii) Nationwide Building Society.

Este es uno de los casos más conocidos en Inglaterra, se remonta a 2006 cuando un computador encriptado de un empleado de la compañía Nationwide Building Society, puso en riesgo la información personal de 11 millones de ahorradores[153].

La FSA (Autoridad de Servicios Financieros) multó a la empresa por 980,000 mil euros por el incidente de seguridad de la información. Como dijo la misma FSA en 2007[154], se tomaron acciones rápidas para mandar un mensaje claro y firme a todas las empresas sobre la importancia de la seguridad de la información,

[153] Recuperado de: http://www.techworld.com/security/uks-11-most-infamous-data-breaches-2015-3604586/
[154] Recuperado de: http://webarchive.nationalarchives.gov.uk/20130301170532/http:/www.fsa.gov.uk/pages/library/communication/pr/2007/021.shtml

además de que este suceso ocurrió cuando el Gobierno y la FSA estaban haciendo campañas y tomando medidas para resaltar la importancia de este asunto. Nationwide falló en la efectividad de sus sistemas y controles de manejo de riesgos de seguridad de la información, en especial el riesgo de robo o pérdida de información y fue sólo hasta que ocurrió el incidente del robo (el cual pasó inadvertido por 3 semanas constituyendo un error adicional) que se dieron cuenta de la problemática. La empresa ni siquiera sabía que el computador contenía información confidencial y a los crímenes financieros a los que estaban expuestos más de 11 millones de datos de clientes.

Margaret Cole, una de las directoras del FSA, se pronunció diciendo:

> *"Nationwide is the UK's largest building society and holds confidential information for over 11 million customers. Nationwide's customers were entitled to rely upon it to take reasonable steps to make sure their personal information was secure.*
>
> *Firms' internal controls are fundamental in ensuring customers' details remain as secure as they can be and, as technology evolves, firms must keep their systems and controls up-to-date to prevent lapses in security"*[155].

Sin embargo, la FSA reconoció que Nationwide cooperó en el curso de la investigación y tomó varias acciones para mejorar esta falla, tales como: tomar varias medidas adicionales para incrementar la seguridad en sus cuentas; informar a los clientes de la pérdida de información; afirmar su política de reembolsar a cualquier cliente que hubiera sufrido una pérdida financiera como resultado del incidente; y hacer una revisión exhaustiva de sus controles y procedimientos de seguridad de la información.

Como señal de esta misma cooperación, Nationwide llegó a un acuerdo con FSA en una etapa temprana de la investigación por lo que le hicieron un descuento del

[155] Ibid.

30% de la multa, que de no haber existido, a la empresa le hubiera tocado pagar 1.4 millones de euros por la violación del principio número tres de los Principios para los Negocios de FSA.

No se habían registrado hasta el momento de la penalidad crímenes financieros en razón de la infracción de datos. Como dijo la FSA, Nationwide tenía una práctica general y era separar la información a lo largo de sus sistemas. La información de la cuenta como el balance, el número PIN y la contraseña no estaban almacenados junto al nombre del cliente, su dirección y números de cuentas, lo que reducía el riesgo en caso de que algo pasara. Sin embargo, fallaba por ejemplo en monitorear las descargas de mucha información en dispositivos portables, por lo que tenía control limitado del uso y almacenamiento de información en estos dispositivos, incrementando el riesgo de un crimen financiero. Las políticas además tenían inconsistencias y no priorizaban, problemas críticos eran tratados igual a los comunes, en adición a la falta de entrenamiento del personal. La FSA reconoce que los riesgos no pueden ser erradicados completamente pero si manejados, también que Nationwide siguió algunas de sus recomendaciones como administración de fugas, sistemas de gestión de acceso y configuración pero le faltó en ciertos puntos.

De este caso se puede extraer que no solo la rama judicial puede sancionar por este tipo de incidentes en Gran Bretaña, ya que fue una autoridad administrativa la que multó y que las fallas en la seguridad de la información y la reacción tardía ante estas pueden dar lugar a multas de varias cifras. Es similar al caso de la Supertindencia de Industria y Comercio y de la Superintendencia Financiera en Colombia que son autoridades administrativas con facultades para sancionar en ciertos casos por infracción de deberes de protección de información personal.

Las multas impuestas por una autoridad administrativa no corresponden a una sanción propia de la responsabilidad civil, se dan de forma independiente. Debido

a que estas se presentan cuando una entidad administrativa inicia un proceso de investigación por violación a deberes legales, concluyendo el incumplimiento por parte de la persona natural o jurídica sobre la cual recaía el deber y decide sancionarla cuando es de su competencia hacerlo. En el caso de multas administrativas no se necesita daño, el solo hecho de la infracción da lugar a estas, como en este caso y en el de Sony (caso de PlayStation identificado anteriormente).

4. DELITOS INFORMÁTICOS Y TRANSNACIONALES

Falta tratar una problemática común en los ataques cibernéticos o incidentes (como se les ha llamado) y es cuándo se da uno de estos en el contexto de dos o más países distintos, cuándo tiene repercusiones en Colombia pero no fue desarrollado aquí, ¿cuál es la normatividad aplicable?, ¿quién debe juzgar a los responsables?, ¿qué consecuencias hay para ellos?, ¿qué tipo de delito es ese que se cometió?

Este apartado no pretende hacer un estudio exhaustivo de los delitos informáticos, simplemente aproximar al lector a estos en cuanto el delito penal es un hecho imputable para la responsabilidad civil generador de indemnización. El acercamiento sin embargo se va a presentar desde el punto de vista nacional e internacional en cuanto sea relevante para la legislación colombiana.

El derecho internacional y el nacional han querido llenar los vacíos que se han presentado a lo largo del tiempo y siguen haciendo esfuerzos para reforzar cada vez más la condena de estos delitos, pues el crecimiento sostenido del mercado negro de la información, el incremento de tecnología disponible, combinado con el escaso conocimiento sobre cómo protegerse de los posibles delitos que se pueden sufrir a través de las nuevas tecnologías otorga a los delincuentes una ventaja y funciona como motor que impulsa a que se den ataques informáticos,

principalmente destinados a obtener bases de datos con información personal. De acuerdo a uno de los estudios de mayor relevancia mundial en delitos informáticos, para el año 2012 se revelaba que "*por cada segundo 18 adultos son víctimas de un delito informático, lo que da como resultado más de un millón y medio de víctimas de delitos informáticos cada día, a nivel mundial"*[156].

En primer lugar se va a definir qué es un delito informático y decir que no hay consenso sobre esto, muchas definiciones se encuentran y con características disimiles. El autor Erick Rincón Cárdenas, en su libro "*Derecho del Comercio Electrónico y de Internet"* dice que si bien estos encuadran dentro de los delitos tradicionales tipificados en el ordenamiento jurídico, se les ha definido como informáticos por la única razón de que son realizados a través de redes, medios electrónicos o similares[157]. Esta concepción es distinta a la de Julio Téllez Valdez quien clasifica a los delitos informáticos en base a dos criterios: (i) Como instrumento o medio: las conductas criminales que se valen de los computadores como método, medio o símbolo en la comisión del ilícito. Por ejemplo: falsificación de documentos vía computarizada como tarjetas de crédito. (ii) Como fin u objetivo: las conductas criminales que van dirigidas contra un computador, accesorios o programas como entidad física. Por ejemplo: destrucción de programas por cualquier medio[158].

El profesor alemán Klaus Tiedemann tiene una tesis, la cual hace hincapié en la necesidad de diferenciar entre los delitos informáticos de carácter económico (cuando se produce un perjuicio patrimonial) y los que atentan contra la privacidad (mediante la acumulación, archivo y divulgación indebida de datos en los sistemas informáticos)[159].

---

[156]Op cit, TEMPERINI, M. G. I., p. 1.
[157]Op cit. RINCÓN, p. 429.
[158] BORGUELLO Cristian F. Tesis "seguridad informática: sus implicancias e implementación*".* 2001. p. 4.
[159]Op cit. RINCÓN,15**.** p. 432.

Por otro lado la ONU también tiene su propia clasificación y distingue 3 tipologías de delitos informáticos:

1. "*Fraudes cometidos mediante manipulación de computadores*": entre estos se encuentran la manipulación de datos de entrada y salida y la manipulación de programas. En cada caso, lo que se trata es de poner datos falsos en un sistema u obtenerlos de este de forma ilegal.
2. "*Falsificaciones informáticas*": se trata de usar los computadores como elemento para falsificar dinero, cuentas bancarias, entre otros.
3. "*Daños a datos computarizados*": aquí se ubican los virus, las bombas lógicas[160], los gusanos, accesos no autorizados, etc. Se trata, en general, de programas o acciones que dañan la información en un sistema determinado[161].

Esta organización señala a su vez un asunto de mucha importancia, que ya se ha detectado y es que los delitos informáticos constituyen una nueva forma de crimen trasnacional y que su combate requiere de una eficaz cooperación internacional concertada. Sin embargo habla de los problemas de esta, entre los cuales están:

1. Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos y de su definición legal.
2. Falta de especialización entre las diferentes leyes procesales nacionales acerca de la investigación de estos delitos.
3. Carácter trasnacional de muchos delitos cometidos mediante el uso de computadores.

[160]*"Una bomba lógica es una parte de código insertada intencionalmente en un programa informático que permanece oculto hasta cumplirse una o más condiciones preprogramadas, en ese momento se ejecuta una acción maliciosa". (https://es.wikipedia.org/wiki/Bomba_l%C3%B3gica)*
[161]Op cit. RINCÓN, pp.431-432.

4. Ausencia de tratados de extradición, de acuerdos de ayuda mutua y mecanismos sincronizados que permitan la cooperación internacional[162].

Estas son dificultades a la hora de sancionar conductas tanto en un proceso penal como en un proceso de responsabilidad civil, por lo que es necesario solucionarlo por los Estados con apoyo de organizaciones internacionales.

En el Código Penal, Ley 599 de 2009, existe la estructura del tipo penal de "*violación ilícita de comunicaciones*", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "*Acceso abusivo a un sistema informático*" en el artículo 195, siendo materia de modificación posterior[163].

Colombia desde 2009 creó la Ley 1273, *"por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos", y se preservan integralmente los sistemas que utilicen las tecnologías de la información y comunicaciones, entre otras disposiciones".* Se optó por reformar el código penal existente, como una de las formas de tratar el tema y no por crear una ley especial al respecto, pero lo importante del asunto es que se le preste más atención a estas conductas delictivas cuyas consecuencias pueden ser graves, en términos económicos y sociales.

Así mismo Colombia fue el primer país de América Latina en adoptar estrategias para la prevención de los delitos electrónicos, esto lo logro a través de la

[162]Ibid, p.433.
[163]Documento Conpes 3701 de 2011.

aprobación del Conpes 3701 de 2011[164], el cual buscaba generar lineamientos de política en ciberseguridad y ciberdefensa.

En este se establece que el gobierno nacional entiende la importancia de la seguridad de la información y que por esto se adoptaron estrategias de ciberseguridad y ciberdefensa como política pública en el plan nacional de desarollo2010-2014 "*prosperidad para todos*" como parte del plan Vive Digital.

También dice este documento que de enero a diciembre de 2009 (con base en la Ley 1273/09) "*se atendieron 575 delitos informáticos, que van desde el acceso abusivo a un sistema informático (259) hasta el hurto por medios informáticos y semejantes (247), la interceptación de datos informáticos (17), la violación de datos personales (35), la transferencia no consentida de activos (8), la suplantación de sitios Web (5), el daño informático (3) y la obstaculización ilegítima de un sistema informático (1)".*Y que de igual forma, durante el 2010, la cantidad de delitos informáticos y contravenciones por estos fue de 995, teniendo el hurto por medios informáticos el mayor incremento al pasar de 247 a 502, por lo que se detecta no solo un aumento en la comisión de este tipo de crímenes, si no también que para el gobierno nacional los delitos informáticos son aquellos que vulneran el bien jurídico "*de la protección de la información y de los datos",* generalmente cometidos por medios electrónicos y contra sistemas informáticos.

El documento Conpes 3701, mencionado anteriormente, reconoce al Convenio sobre la ciberdelincuencia de Budapest, 2001, como uno de los instrumentos internacionales más importantes en el tema. Este convenio dispone una serie de delitos que deberían adoptarse a nivel nacional en caso de ratificar este instrumento, de los cuales Colombia ya cuenta con varios. También normativas en temas como cooperación internacional, normas procesales y extradición, en general es muy completo. Según la Cancillería, Colombia se adhirió pero se

[164]Op cit., RINCON, p.429.

encuentra en consultas para adelantar los trámites conducentes a la aprobación legislativa.

Mirando más la normatividad nacional, se va a analizar la Ley 1273 de 2009. Esta ley, además de regular lo mencionado anteriormente, añadió al Código Penal un título (VII BIS) denominado "*De la Protección de la información y de los datos*".

Primero se enmarcan delitos que se entiende que atentan contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, delitos como (i) el acceso abusivo a un sistema informático (mencionado anteriormente), este delito ya existía en el Código Penal pero se modificó por esta ley, se entiende que se comete cuando una persona sin autorización o por fuera de lo acordado con otra, accede a un sistema informático o se mantiene dentro del mismo contra la voluntad del legitimado; como la (ii) obstaculización ilegítima de un sistema informático o red de telecomunicación, que consta de impedir u obstaculizar, sin facultad para ello, el funcionamiento o acceso normal a un sistema informático, a los datos informáticos allí contenidos o a una red de telecomunicaciones; también está (iii) la interceptación de datos informáticos que sería interceptar, sin orden judicial previa, datos informáticos en su origen, destino o en el interior de un sistema informático o las emisiones electromagnéticas provenientes de uno de estos que los transporte. Por otro lado está el (iv) daño informático (como delito) que equivale a destruir, dañar, borrar, deteriorar, alterar o suprimir datos informáticos o un sistema de tratamiento de información, sus partes o componentes lógicos, todo esto sin estar facultado para ello. También el (v) uso de software malicioso, uno de los más comunes y menos sancionados podría decirse, se trata de producir, traficar, adquirir, distribuir, vender, enviar, introducir o extraer del territorio nacional, software malicioso u otros programas de computación de efectos dañinos, sin estar facultado para ello.

No se puede olvidar la (vi) suplantación de sitios web para capturar datos personales que continúa la línea de la protección de datos, este delito consiste en diseñar, desarrollar, traficar, vender, ejecutar, programar o enviar páginas electrónicas, enlaces o ventanas emergentes sin estar facultado para ello y con objeto ilícito, así como el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza. Y la (vii) violación de datos personales, se da cuando una persona obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros[165], archivos, bases de datos o medios semejantes, sin estar facultado para ello y para provecho propio o de un tercero.

Por último, están el (viii) hurto por medios informáticos y semejantes y (ix) la transferencia no consentida de activos. El primero consiste en apoderarse de una cosa mueble ajena manipulando un sistema informático, una red de sistema electrónico, telemático[166] u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, esto superando medidas de seguridad informáticas, con el propósito de obtener provecho para sí o para otro; y el segundo se comete cuando una persona consigue la transferencia no consentida de cualquier activo en perjuicio de un tercero, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, al igual que se sanciona a la persona que fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito anterior, o de una estafa.

En el caso de la suplantación de sitios web para capturar datos personales y en la transferencia no consentida de activos hay una particularidad y es que hay cierta

---

[165] *"Un archivo o fichero informático es un conjunto de bits que son almacenados en un dispositivo".(*https://es.wikipedia.org/wiki/Archivo_(inform%C3%A1tica)

[166] *"Ciencia que reúne y combina las posibilidades técnicas y los servicios de la telecomunicación y la informática".* (http://www.wordreference.com/definicion/telem%C3%A1tico).

multa y tiempo en prisión pero desde que la conducta no constituya un delito sancionado con pena más grave, además, en el caso de la primera, la pena se agravará de una tercera parte a la mitad, si para consumarlo la persona ha reclutado víctimas en la cadena del delito y en el caso del segundo si la conducta tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad. Así como en la obstaculización ilegítima de un sistema informático o red de telecomunicación que también hay cierta multa y tiempo en prisión, desde que la conducta no constituya un delito sancionado con pena más grave.

Todos los delitos descritos anteriormente tienen sanciones de multa y prisión, cada uno con sus propias características (casi todos con pena de prisión de 48 a 96 meses), salvo la Interceptación de datos informáticos y el hurto por medios informáticos y semejantes que no tienen multa. Es decir, por más “irrelevante” que pueda parecer una conducta delictiva por relacionarse por ejemplo, con un blog sin visitantes, puede llegar a ser condenada una persona a prisión por este, pues desde el 2009 el Código Penal está tomando en serio las intromisiones a los datos, a la información y a sus sistemas.

Este aspecto se ve reflejado en la responsabilidad civil en el sentido en el que se puede dar lugar a multas administrativas por el incumplimiento de una norma o de una obligación contractual, independientemente del resarcimiento derivado de un proceso de responsabilidad civil. Así mismo se puede reparar los perjuicios sufridos por parte de la víctima por medio de un incidente de reparación integral cuando se ha condenado penalmente al responsable, sin exclusión de la condena que se hubiera establecido en este.

Todos estos delitos están consagrados en un mismo título, que también contiene circunstancias de agravación punitiva del delito (que aumentarán de la mitad a las tres cuartas partes en caso de cometerse). Si la conducta se realizó:

"1. *Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.*
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales".

Por otro lado, un punto importante es, el artículo 2 de esta ley, que adiciona a las circunstancias a mayor punibilidad del Código un numeral, el de la utilización de medios informáticos, electrónicos o telemáticos para la realización de conductas punibles, es decir, todos los delitos del Código se pueden ver castigados más fuertemente por la utilización de medios electrónicos etc. para su ejecución, entendiéndose como más grave el cometer un delito a través de estos medios que en circunstancias normales y tradicionales, algo sumamente revelador en cuanto la percepción del legislador sobre esta forma de delinquir y una forma de tratar de desestimular el uso indebido de estos.

Si bien se dice que los jueces municipales van a conocer de los delitos contenidos en este título (artículo 3), no se puede dejar un asunto de lado y es que estos delitos son cometidos generalmente en un país pero manifestándose sus consecuencias en otro y es aquí donde entra a jugar la concepción de delito transnacional. "*Esta característica de transnacionalidad demanda un desafío para el Derecho y en especial para los sistemas jurídicos penales, que deben concebir la necesidad de ciertos niveles mínimos de coordinación, que permitan un combate eficaz de este tipo de actividad delictiva*"[167]

Uno de los autores más importantes en el tema de ciberdelincuencia es Manuel Castells, tiene múltiples libros que tratan sobre la era digital y todos los aspectos relacionados a ella, este autor expresó que la definición de la trasgresión dependía, naturalmente, de los sistemas legales y políticos de cada jurisdicción, lo que es un delito en Singapur no necesariamente lo es en España y los delincuentes se aprovechan de esto, este es uno de los puntos donde se presentan dificultades[168], de ahí la importancia de una regulación adecuada y de cooperación internacional principalmente.

La Ley 800 de 2003 es la ley que introduce al sistema jurídico interno la "*Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional" y el "Protocolo para Prevenir, Reprimir y sancionar la Trata de Personas, especialmente Mujeres y Niños, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional*". Esta convención trata, como lo dice su nombre, sobre la delincuencia organizada trasnacional, principalmente es un esfuerzo para que los países implementen ciertas normas y directrices generales en sus ordenamientos jurídicos, lastimosamente casi todos sus preceptos son tareas pendientes para los estados parte. Pero en su artículo 3, numeral 2, define los delitos transnacionales para

[167] Op cit.,TEMPERINI M. G. I. p.1.
[168] Ibid, p.2.

efectos de esa ley, lo que da una luz para entender mejor este concepto. Un delito se entiende como trasnacional si:

"*a) Se comete en más de un Estado;*
b) Se comete dentro de un solo Estado pero una parte sustancial de su preparación, planificación, dirección o control se realiza en otro Estado;
c) Se comete dentro de un solo Estado pero entraña la participación de un grupo delictivo organizado que realiza actividades delictivas en más de un Estado; o
d) Se comete en un solo Estado pero tiene efectos sustanciales en otro Estado"

El Código de Procedimiento Penal establece que será objeto de la jurisdicción penal ordinaria, la persecución y el juzgamiento de los delitos cometidos en el territorio nacional y de aquellos cometidos en el extranjero en los casos que determinen los Tratados Internacionales suscritos y ratificados por Colombia y la legislación interna. El Código Penal por su parte dice que *"la ley penal colombiana se aplicará a toda persona que la infrinja en el territorio nacional, salvo las excepciones consagradas en el derecho internacional.*

La conducta punible se considera realizada:
1. En el lugar donde se desarrolló total o parcialmente la acción.
2. En el lugar donde debió realizarse la acción omitida.
3. En el lugar donde se produjo o debió producirse el resultado".

Estos últimos numerales son de suma importancia pues definen que hay diferentes criterios para establecer el lugar donde se entiende realizada la conducta punible, es decir, no se necesita que se haya desarrollado totalmente o aún desarrollado en Colombia para que se entienda realizada aquí, pues puede ser realizada en este país de forma parcial o que su resultado se produjera o debiera producirse en este país o aún que aquí se hubiera debido realizar la

acción omitida, aunque los ataques cibernéticos generalmente son por acción y no por omisión.

Relacionado con el artículo 15 y el 16 de este mismo Código. El 15 establece que esta ley penal, también se aplicará a la persona que cometa un delito a bordo de una nave o aeronave del Estado o explotada por este, cuando este fuera del territorio nacional, salvo las excepciones consagradas en los tratados o convenios internacionales ratificados por Colombia; pero más relevante es el 16 pues habla de la extraterritorialidad, expresando que la ley penal colombiana se aplicará: 1. A la persona que cometa en el extranjero delito contra la existencia y seguridad del Estado, contra el régimen constitucional, contra el orden económico social excepto la conducta definida en el artículo 323 (lavado de activos), contra la administración pública, o falsifique moneda nacional o incurra en el delito de financiación de terrorismo y administración de recursos relacionados con actividades terroristas, con independencia de una condena o absolución en el exterior, a una pena menor que la prevista en la ley colombiana, pero teniendo como parte cumplida de la pena el tiempo que hubiere estado privada de su libertad allá. 2. A la persona que estando al servicio del Estado colombiano, con inmunidad reconocida por el derecho internacional, cometa delito en el extranjero. 3. A la persona que estando al servicio del Estado colombiano, sin inmunidad reconocida por el derecho internacional, cometa en el extranjero un delito distinto de los mencionados en el numeral 1º, si no fue juzgada ya en el exterior. 4. Al nacional que se encuentre en Colombia después de haber cometido un delito en territorio extranjero (fuera de los casos previstos en los numerales anteriores), cuando la ley penal colombiana lo reprima con pena privativa de la libertad cuyo mínimo no sea inferior a dos años y sin haber sido juzgado en el exterior[169]. 5. Al extranjero que se encuentre en Colombia después de haber cometido en el exterior un delito en perjuicio del

[169]En caso de tratarse de una pena inferior, no se procederá sino por querella de parte o petición del Procurador General de la Nación.

Estado o de un nacional colombiano (fuera de los casos previstos en los numerales 1, 2 y 3), que la ley colombiana reprima con pena privativa de la libertad cuyo mínimo no sea inferior a dos años y no hubiere sido juzgado en el exterior[170]. Y por último: 6. Al extranjero que haya cometido en el exterior un delito en perjuicio de extranjero, siempre que se reúnan estas condiciones: a) Que se halle en territorio colombiano; b) Que el delito tenga señalada en Colombia pena privativa de la libertad cuyo mínimo no sea inferior a tres años; c) Que no se trate de un delito político, y d) Que solicitada la extradición, no hubiere sido concedida por el gobierno colombiano (cuando la extradición no fuere aceptada habrá lugar a proceso penal).

A su vez se advierte que en el caso a que se refiere el presente numeral no se procederá sino mediante querella o petición del Procurador General de la Nación y siempre que no hubiera sido juzgado en el exterior.

De estas normas se extrae entonces, que los delitos informáticos tiene penas de prisión de más de dos años, por lo que podrían ser objeto de aplicación de este artículo; que es posible, siempre que se reúnan las condiciones, condenar en Colombia a extranjeros que cometieran delitos en contra de los nacionales colombianos o del Estado, lastimosamente se requiere que se encuentre en Colombia, situación que es difícil que se dé, salvo en el caso del numeral 1 que no se requiere su estancia en este país. Para el tema de estudio este precepto es el de mayor importancia y aplicación.

Por otro lado también se le aplica la ley colombiana a los nacionales que cometan delitos en el extranjero, siempre que se hallen en Colombia y cumplan con los demás requisitos. Más sorprendente todavía, a los extranjeros que cometan delitos contra extranjeros, pero además de las condiciones que se deben cumplir,

[170] *"En este caso sólo se procederá por querella de parte o petición del Procurador General de la Nación".*

el hecho de que se exija que el Procurador pida que se juzgue este es complicado pues tendría que tener una gran trascendencia para que este funcionario lo hiciera.

Las personas que estén al servicio del Estado y que cometan este tipo de infracciones también deberán ser sancionadas, las consecuencias que se les aplicarán serán más gravosas que las de los nacionales o extranjeros que no estén al servicio del Estado colombiano pues no se requiere que se encuentren en Colombia para que se les aplique la ley de este país y no tiene que ser un delito en perjuicio de alguien específico, sino simplemente que cometa un delito.

Se encuentra entonces que Colombia consagra en su Código Penal tratamiento para delitos que traspasen fronteras, tanto en su comprensión de cuando se entiende realizada la conducta punible, como de su aplicación de ley penal colombiana incluso a personas que no son colombianas, ni cometieron delitos en Colombia, ni con perjuicio para colombianos.

Por otra parte, relacionado a esto, el mismo código consagra que la sentencia absolutoria o condenatoria pronunciada en el extranjero tendrá valor de cosa juzgada para todos los efectos legales, salvo respecto de los delitos señalados en los artículos 15 y 16, numerales 1 y 2, que se acaban de analizar.

"*La pena o parte de ella que el condenado hubiere cumplido en virtud de tales sentencias se descontará de la que se impusiere de acuerdo con la ley colombiana, si ambas son de igual naturaleza y si no, se harán las conversiones pertinentes, comparando las legislaciones correspondientes y observando los postulados orientadores de la tasación de la pena contemplados en este código".*
A su vez las sentencias extranjeras (contra extranjeros o nacionales colombianos) podrán ejecutarse en Colombia a petición formal de las respectivas autoridades

extranjeras, formulada por la vía diplomática, siempre que se cumpla con ciertos requisitos[171].

En conclusión, la legislación colombiana se ha anticipado a los delitos informáticos y transnacionales que se pudieran dar, fundamental en cuanto al manejo de información digital, incorporando al ordenamiento un tratamiento jurídico para estos, uno razonable y en general completo para las necesidades que se pueden presentar. Lo que se dificulta actualmente es identificar al autor del delito y se deben encaminar todos los esfuerzos a evitar que haya impunidad, sobre todo cuando la Fiscalía General de la Nación puede hacer parte de una comisión internacional e interinstitucional destinada a colaborar en la indagación o investigación de delitos de revisten de una dimensión internacional. Finalmente, es relevante decir que no se requiere para la responsabilidad penal, a diferencia de la civil, que haya un daño, solo la comisión del delito.

[171]1. Que no se oponga a los Tratados Internacionales suscritos por Colombia, o a la Constitución Política o a las leyes.2. Que la sentencia se encuentre en firme de conformidad con las disposiciones del país extranjero.3. Que en Colombia no se haya formulado acusación, ni sentencia ejecutoriada de los jueces nacionales, sobre los mismos hechos, salvo lo previsto en el numeral 1 del artículo 16 del Código Penal.4. Que a falta de tratados públicos, el Estado requirente ofrezca reciprocidad en casos análogos.

4. CONCLUSIONES

1. La era digital se está viviendo plenamente en el siglo XXI, logrando abarcar varias esferas de las personas naturales y jurídicas, siendo hoy en día el Internet un medio de comunicación, negociación, comercialización, entre muchos más; una herramienta en la cual se recolecta información de todo tipo, dentro de las cuales se encuentra información personal y crediticia. Debido a la información que se recolecta en esta herramienta tecnológica de gran alcance para la población y empresas, es un gran foco de atracción para los delincuentes informáticos materializando el riesgo cibernético de robo de información personal y crediticia tanto de personas naturales como jurídicas, generando la posibilidad de perjudicar a los titulares de la información robada.

2. El trato de los casos de ciberataque en países como Estados Unidos o Inglaterra es disímil, de lo cual se puede interpretar la necesidad de una regulación apropiada para tratar este tema en ambos. Sin embargo, la semejanza en ambas legislaciones es la intención de sancionar severamente este tipo de incidentes, buscando que las empresas que recolecten información personal o crediticia tengan la obligación de tener una seguridad apropiada para que esta información no sea adulterada, usada, robada, manipulada, entre otros, por terceros no autorizados por el titular de la información.

Respecto a Estados Unidos, debido a su sistema de Gobierno federal, la decisión de los Tribunales es desigual y algunas veces fundamentada en el ordenamiento jurídico federal y otra en legislación estatal, presentado disímiles tratamientos a los casos relacionados con ataques cibernéticos, y aun fundamentados en la misma norma se presentan interpretaciones opuestas de la misma. Por su lado, la legislación británica permite a las entidades administrativas sancionar este tipo de conductas y hasta el momento ha sido el trato que se le ha dado a estos casos en su mayoría.

El mayor aporte que puede dar la jurisprudencia extranjera es que en Colombia debería existir un tiempo limite establecido para que aquellos que tengan acceso autorizado a la información personal dejen de tenerlo.

3. La responsabilidad que pueda surgir por un ataque cibernético se enmarca en los regímenes de responsabilidad extracontractual, contractual y responsabilidad de los profesionales, siendo el tema de mayor relevancia el daño/perjuicio generado por la vulneración de datos personales. Para que se configure la responsabilidad civil se debe cumplir con todos los elementos necesarios que esta exige para que surja dicha responsabilidad, hecho imputable, daño y nexo causal. En el caso de responsabilidad civil por afectación de información personal o crediticia del titular de la información no existe jurisprudencia colombiana concreta que se pueda citar en aras de solicitar la indemnización de perjuicios, lo cual hace necesario un desarrollo legislativo y jurisprudencial que direccione al juez a la toma de la decisiones judiciales ajustadas a derecho, en las cuales no dependa de la línea jurisprudencial que acoja el juez para identificar los daños y perjuicios que se presenten en el caso concreto.

4. Otros elementos que son importantes a tener en cuenta respecto a la responsabilidad civil que se pueda desprender de un ataque cibernético son la responsabilidad profesional y el beneficio que le reporte a una de las partes la celebración de un contrato. Los requisitos de la responsabilidad pueden atenuarse o hacerse más exigentes de acuerdo a la persona que cometa la culpa y a las características de la relación contractual, si es que se tiene una. No se deberá tener, en principio, la misma diligencia respecto a la seguridad que prestan las empresas que ofrecen un servicio gratuito, a aquellas que cobran su servicio y así debe ser, no es el mismo beneficio el recibido por cada una de parte del suscriptor; ni mucho menos debe la misma diligencia una parte contractual experta a un ciudadano del común. Esto tiene sentido en cuanto no se deben desconocer

ciertos elementos, en cada caso concreto, que cambien el panorama jurídico y den equilibrio y coherencia al sistema.

5. La Corte Suprema de Justicia ha establecido que la afectación a un bien jurídico de especial protección constitucional, como lo son los derechos fundamentales a la dignidad, la honra y el buen nombre, en los que no se materializa físicamente un daño, deben ser indemnizados, lo cual ha generado confusión por la doble característica de daño y perjuicio, frente a este aspecto es necesario que la Corte se pronuncie otorgando claridad al tema tanto para los titulares de los derechos como para el juez destinado a fallar el caso. La decisión judicial que tomará el juez deber ser razonable en cada caso y se debe determinar si la medida de reparación es equitativa, suficiente, necesaria y adecuada para consolar a la víctima, por la pérdida de un bien inestimable en dinero, para reivindicar su derecho fundamental y para reparar el agravio o la ofensa infligida a su dignidad.

6. Si bien la normatividad colombiana en relación al derecho a la intimidad y al buen nombre ha sido muy ambiciosa a la hora de establecer el marco general de la protección del tratamiento de datos personales, esta regulación generará problemas al momento de su cumplimiento por parte de los Responsables y Encargados del tratamiento de datos personales, debido a la amplia definición de dato personal, abarcando todos los aspectos íntimos de las personas sin tener en cuenta la sociedad actual.

Existe legalmente una obligación de asegurar la información personal de la que se disponga.

7. El Estatuto del Consumidor consagra una normatividad de protección de datos personales en el marco del comercio electrónico, en el que le impone a los proveedores obligaciones de resultado respecto a la seguridad de la información del consumidor.

8. Los delitos informáticos constituyen una nueva forma de crimen trasnacional y su combate requiere de una eficaz cooperación internacional concertada. Sin embargo, el sistema jurídico colombiano consagra el tratamiento correspondiente para delitos que traspasen fronteras, tanto en su comprensión de cuando se entiende realizada la conducta punible, como de su aplicación de ley penal colombiana incluso a personas que no son colombianas, ni cometieron delitos en Colombia, ni con perjuicio para colombianos.

9. Debido al gran aumento de los delitos informáticos transnacionales, se hace necesario una regulación internacional al respecto, la cual pretenda efectivamente la disminución de los delitos informáticos transnacionales, y en la cual no sea posible que los ciberdelincuentes se acentúen en un lugar en el cual su conducta dañosa sea impune. A pesar de que en la actualidad se ha realizado el intento de regular los delitos transnacionales por medio del Convenio de Budapest de 2001, este aún no ha sido ratificado por todos sus países miembros, dejando por inconcluso su objetivo y dejando abierto un tema de gran auge en la actualidad y que requiere con urgencia su atención por parte de organismos internacionales.

A pesar de que en Colombia se ha tratado de avanzar al ritmo de la era digitial este esfuerzo no ha sido suficiente para estar a la vanguardia en la regulación de ciberseguridad, por lo cual se hace necesario que el desarrollo en este aspecto no sea meramente legislativo, a través de mecanismos nacionales e internacionales, sino que se presenta la necesidad de que existan entidades que estén dirigidas exclusivamente a generar estrategias a favor de la ciberseguridad, crear campañas que hagan más consciente a la sociedad colombiana de los riesgos digitales a los que se exponen cada vez que utilizan Internet, una entidad que esté dirigida a crear politicas de ciberseguridad actualizadas a las circunstancias que se estén presentando.

5. BIBLIOGRAFÍA

ABAL, R. Z. Estructuras de la comunicación y la cultura: Políticas para la era digital. Editorial Gedisa. 2011. p. 25.

AGHAEI, S., NEMATBAKHSH, M. A., &FARSANI, H. K. Evolution of the world wide web: from Web 1.0 to Web 4.0. International Journal of Web & Semantic Technology, 2012. vol. 3,1, p.1-10.

BALLESTEROS, J.S. Instituciones de responsabilidad civil. Tomo 3. vol. 21). Pontificia Universidad Javeriana. 1996). p.13.

BANCO MUNDIAL. Usuarios del internet (por cada 100 personas). Recuperado de: http://datos.bancomundial.org/indicador/IT.NET.USER.P2

BIANCHINI, A. Conceptos y definiciones de hipertexto. Reporte Técnico Interno. Departamento de Computación y Tecnología de la Información, Universidad Simón Bolívar. Caracas. 1999. .pág 2. Disponible en: http://ldc. usb. ve/~ abianc/hipertexto. pdf.

BLACK, J. Developments in Data Security Breach Liability. Bus. Law. 2013. Vol. *69*, p. 99-206.

CASTELLS, M. La era de la información: economía, sociedad y cultura, Vol. 3. siglo XXI. 2004. p. 25.

CHAVEZ URREA, Julio César. Transmission Contorl Protocol (TCP) y el Internet Protocol (IP). Es un protocolo DARPA que proporciona transmisión fiable de paquetes de datos sobre redes. Recuperado de:http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml#ixzz3v62eUBd5.ELGUEZ

COLOMBIA. Decreto 1400 de 1970 Artículo 177 (agosto 6). Por los cuales se expide el Código de Procedimiento Civil.
Diario Oficial No. 33.150 de 21 de septiembre de 1970. <Código derogado por la Ley 1564 de 2012 en los términos establecidos en el artículo 626>

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1266 (31, diciembre, 2008). por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario oficial, Bogotá, 2008.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1581 de 2012. Artículo 3. (octubre, 7, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá: Diario Oficial 48587 de octubre 18 de 2012.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 527 de 1999. Artículo 2 (agosto, 18,1999). por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Diario Oficial 43.673. Bogotá.

COLOMBIA. CORTE CONSTITUCIONAL. Sentencia C-1008 de 2010. Magistrado Ponente: Luis Ernesto Vargas Silva.

COLOMBIA. CORTE CONSTITUCIONAL. Sentencia C-1011 de 2008. Magistrado Ponente: Jaime Córdoba Triviño.

COLOMBIA. CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN CIVIL. Magistrado Ponente: César Julio Valencia Copete. Bogotá D.C., trece (13) de mayo de dos mil ocho (2008). Ref: Exp. 11001-3103-006-1997-09327-01.

COMISIÓN AL CONSEJO Y AL PARLAMENTO EUROPEO .Comunicado de 14 de diciembre de 2001.

CORTE DISTRITAL DE MAINE. Hannaford Brothers Co. Customer Data Security Breach.Case 2:08-MD-1954-DBH. 2013. Disponible en: http://www.med. uscourts.gov/Opinions/ Hornby/MDL/MDL1954_2013_03_20_ORDER11.pdf

CORTE DISTRITAL DEL NORTE DE CALIFORNIA.Szpyrka vs. LinkedInCorporation. Case5:12-cv-03088-EJD. 2012. Disponible en http://recruitingdaily.com/wp-content/uploads/sites/6/2015/02/Szpyrka-v-Linkedin-Complaint.pdf

CORTE SUPREMA DE JUSTICIA**.** SALA DE CASACIÓN CIVIL**.** Magistrado Ponente: Ariel Salazar Ramírez. Radicación: 11001310300320030066001. Bogotá D. C., cinco (5) de agosto de dos mil catorce (2014).

GIL, S. A. T., & KIM, H. S. L. (2014). La evolución de la telecomunicación hacia una sociedad conectada. En: INCEPTUM Revista de Investigación en Ciencias de la Administración, vol.*9 No.*16, p.27-48.

HOCSMAN, Simón Heriberto. Negocios en Internet. Editorial Astrea. 2003. p. 224.

INTERNET WORLD STATS. *World internet usage and population statistics* november 30, 2015 – update. Recuperado de : http://internetworldstats.com/stats.htm

LEINER, B. M., CERF, V. G., CLARK, D. D., KAHN, R. E., KLEINROCK, L., LYNCH, D. C.& WOLFF, S. Una breve historia de internet. Primera y segunda parte, 1999. p. 1.

MARTIN, P. E. Inseguridad Cibernética en América Latina: Líneas de Reflexión para la evaluación de riesgos, 2015. p. 6.

McENENEY, AND KARLF. KAUFMANN. "*Privacy & Data Security Law Journal".*October 2009.

MELIÁN, J. M. M. Riesgos cibernéticos. Cuadernos de estrategia, 2003. No.120, p.131.

MÚRTULA LAFUENTE, Virginia. Causalidad alternativa e indeterminación del causante del daño en la responsabilidad civil. Facultad de Derecho Universitatd'Alacant. Barcelona, Abril de 2006. p. 4.

ORTIZ, J. M. D. G. El seguro de responsabilidad. Universidad del Rosario. 2006. p. 65.

PEÑA VALENZUELA, Daniel y BAZZANI MONTOYA, Juan David. Aspectos legales de la computación en la nube. Universidad Externado de Colombia. 2012..p.15.

RINCÓN CÁRDENAS, Erick. Derecho del Comercio Electrónico y de Internet. 2 ed. 2015. p. 11.

TAMAYO JARAMILLO, J. Tratado de Responsabilidad Civil. Tomo I y II. Legis Editores. 2009.

TELEFÓNICA, F. La Sociedad de la Información en España 2013: siE *13*. Fundación Telefónica.

TEMPERINI, Marcelo Gabriel Ignacio. Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte.

VILCHEZ, Lorenzo. La construcción social del virus informátic*o.* En: Revista Signo y Pensamiento, Universidad Javeriana. 2000

YZQUIERDO TOLSADA, M., Sistema de Responsabilidad Civil Contractual y Extracontractual. Ed. Dykinson. Madrid, 2001.