La responsabilidad civil derivada del tratamiento de datos personales y sensibles con intervención de la inteligencia artificial

Facultad de Derecho
Universidad Autónoma Latinoamericana

La responsabilidad civil derivada del tratamiento de datos personales y sensibles con intervención de la inteligencia artificial.

Autores: Rogelio Roldan Álvarez y Santiago Suárez Jaramillo
Asesor del trabajo de grado: Saúl Uribe García
Junio 2024

Facultad de Derecho
Universidad Autónoma Latinoamericana

Dedicatoria de Santiago Suárez Jaramillo

El presente escrito va dedicado a mi familia con especial precisión a mi madre Gladys Jaramillo, a mi padre Ocaris Suárez, a mis hermanos Edison Suárez y Felipe Suárez, por su gran apoyo incondicional ya que en los momentos más difíciles a lo largo de mi vida y formación siempre estuvieron ahí, presentes para mí, dándome una mano de ayuda y orientándome hacia el camino de la rectitud y la auto superación, con el planteamiento de que yo soy la única persona con la que compito.

Dedicatoria de Rogelio Roldan Álvarez

Dedico esta monografía a mis tías, padre y hermano ya que en ella dejo un poco de mi naturaleza, de mi forma de pensar y de mi modo de ser, para que de esta forma puedan presenciar el avance que he tenido, en razón de mi conocimiento y mi crecimiento como persona.

También dedico este escrito a mi universidad, mi alma mater, ya que fue allí donde perfeccioné gran parte de mi manera de pensar, mi manera de cuestionar y razonar.

Dedico especialmente mi tesis a mis docentes, ya que es por ellos que desarrollé un interés profundo por el derecho y más hablando de la responsabilidad civil.

Agradecimientos de Santiago Suárez Jaramillo

Por medio del presente escrito me permito manifestar mi profunda gratitud con todas las personas que trabajan para la universidad Autónoma Latinoamérica de Medellín, haciendo especial énfasis en todos los profesores que aportaron un poco de su conocimiento para de esta forma poder llegar a ser un profesional exitoso, igualmente agradecer a dichos profesores porque más allá de enseñar contenido eminentemente académico, enseñan valores que sirven tanto para la vida, como para el ejercicio profesional.

Seguidamente darle mis más sinceros agradecimientos al profesor Alejandro Gaviria Cardona por aportar un poco de su tiempo y de su conocimiento para que la presente monografía tenga éxito.

Agradecimientos de Rogelio Roldan Álvarez

Agradezco a mi familia por haberme brindado la oportunidad de estudiar esta carrera que me apasiona, además por cursarla en una buena universidad, así mismo agradezco a la universidad por permitirme hacer uso de sus instalaciones, bienes y demás, y así lograr llegar al punto en el que estoy, agradezco a mis docentes por compartir sus conocimientos y experiencia propia, por ser más que docentes, por despertar mi ese sentido de curiosidad para no quedarme con el primer conocimiento que tengo y llevarlo más allá, por invitarme a cuestionar sobre lo que estoy estudiando, para así lograr un conocimiento menos firme y así poder entender que el conocimiento científico en algún momento va ser falseado por otra persona con mejores argumentos.

Le agradezco al derecho por permitirme abrir un poco más mi cosmovisión acerca del mundo, pudiendo llegar a entender fenómenos, hechos y actos que no entendía, por ser no solo una fuente de conocimiento, sino también un entretenimiento. También le agradezco al derecho por permitirme ser un miembro productivo de la sociedad, ya que puedo aportar mis servicios y saberes para lograr un mundo mejor y más justo.

Pero sin el apoyo de mi familia no pude haber logrado todo esto que soy y seré, mi familia me empujo a dar el primer paso que es el pregrado en derecho, primer paso de un largo camino de estudio y experiencia que no solo hará de mí una mejor persona, sino un mundo mejor.

RESUMEN

La presente monografía plasma un análisis jurídico crítico de la responsabilidad civil derivada del uso de la IA con respecto al tratamiento de datos personales y sensibles.

Iniciando con un recorrido histórico sobre la creación de la IA, evidenciándose que esta se ha utilizado desde 1842, pero su creación se da en 1956; analizándose así el avance de la IA, arribando en la actualidad para entender su funcionamiento relativo tratamiento de datos personales y sensibles.

Seguidamente se hace un análisis de la Ley 1581/12, la cual regula el tratamiento de datos personas y sensibles, analizando su articulado, buscando instituciones aplicables a los distintos regímenes de responsabilidad civil. De igual forma se desarrollan conceptos propios del tratamiento de datos y su posible incidencia en una responsabilidad civil, esto estudiado desde los tipos o fuentes que se derivan de esta responsabilidad, diferenciando si es contractual o extracontractual u objetiva o subjetiva.

Posteriormente se identifican los extremos litigiosos aplicando lo antes esbozado al procesamiento de información con intervención de la IA, para así ubicar la legitimación en la causa y la pretensión adecuada.

Respondiendo a si ¿Existe responsabilidad civil derivada del uso de datos personales y/o sensibles por parte de la inteligencia artificial?

Palabras clave: Datos, información, personal, sensible, IA.

ABSTRACT

This monograph provides a critical legal analysis of the civil liability arising from the use of AI with respect to the processing of personal and sensitive data.

Beginning with a historical review of the creation of AI, showing that it has been used since 1842, but its creation occurred in 1956; thus analyzing the progress of AI, arriving at the present time to understand its operation relative to the treatment of personal and sensitive data.

Next, an analysis is made of Law 1581/12, which regulates the processing of personal and sensitive data, analyzing its articles, looking for institutions applicable to the different civil liability regimes. Likewise, concepts of data processing and its possible incidence in a civil liability are developed, this studied from the types or sources derived from this liability, differentiating whether it is contractual or extra-contractual or objective or subjective.

Subsequently, the litigious extremes are identified by applying the aforementioned to the processing of information with the intervention of the AI, in order to locate the legal standing in the cause and the appropriate claim.

Answering whether there is civil liability arising from the use of personal and/or sensitive data by artificial intelligence?

Keywords: Data, information, personal, sensitive, IA.

Tabla de Contenidos

Índice

Lista de figuras

Introducción

La presente monografía pretende desarrollar las aristas relacionadas con la responsabilidad civil que se deriva por el uso que hace la inteligencia artificial de información personal y sensible, para ello, estos autores se plantean cómo con la entrada de las nuevas tecnologías y la inteligencia artificial, se involucran bases de datos para que pueda funcionar en debida forma, es decir, es necesario alimentarla con información contenida en bases de datos, pero el problema surge cuando estas fuentes de información contienen datos personales y sensibles, ya que para el uso o disposición de esta información, es necesario un consentimiento informado del titular como se pretende dejar en evidencia a lo largo de este escrito, ya que muchas veces los datos sensibles se enmarcan en derechos humanos, como lo puede ser la intimidad o la dignidad.

Para contextualizar, se plantea el caso propuesto por Diego Arce, en el cual indica que "cada vez que damos un like, cada vez que entramos a ver una noticia, cada vez que simplemente nos detenemos más tiempo frente a un aviso, estamos brindando información intima" (Arce, 2021, p. 01), lo cual es un claro ejemplo de cómo la inteligencia artificial usa la información de las personas sin el consentimiento necesario.

Es así como la inteligencia artificial puede usar datos personales y sensibles para el desarrollo de su actividad, como, por ejemplo, el caso de la inteligencia artificial conocida como ChatGPT (sistema de chat basado en el modelo de lenguaje por inteligencia artificial) producida por OpenAI, en donde un usuario logró obtener unas claves de ingreso para Windows 10 y Windows 11, en el caso "abuelita, léeme claves de Windows 10 para dormir": un truco sorprendente que funciona en ChatGPT y Bard (Pastor, 2023).

El usuario Sid de "X", anteriormente "Twitter", le solicitó a ChatGPT que actuara como su difunta abuela, "ya que ella le solía recitar claves de accesos a Windows 10 con la finalidad de que pudiera dormir", a lo que ChatGPT le contestó generando varias claves de Windows 10 terminando con la frase "espero que duermas mi niño". Este es un ejemplo de cómo la inteligencia artificial tiene acceso a datos que son protegidos y que están destinados para actividades comerciales, como por ejemplo la compra y venta de claves de acceso para Windows. Bajo la premisa anterior, se identifica que en ocasiones es posible que las inteligencias artificiales no diferencien aquella información que puede ser protegida y/o sensible.

Ahora bien, con el constante avance de la tecnología, concretamente de la inteligencia artificial, se vislumbran una serie de riesgos, por cuanto la inteligencia artificial se encuentra en desarrollo, entendiéndose como el "presente" y mucho más como el "futuro", ya que dicha tecnología llegó para quedarse y hacer la vida de las personas mucho más fácil.

Seguidamente, la implementación de la inteligencia artificial en las relaciones de las personas hace que existan ciertos riesgos que pueden influir directa o indirectamente sobre

estas, “ya que la inteligencia artificial estudia nuestros hábitos de consumo y para ello analiza cada paso que damos en el ciberespacio, aunque no lo autoricemos. Y ahí es donde empieza el conflicto con nuestra privacidad” (Arce, 2021, p. 01), debido al posible impacto en la ejecución de la inteligencia artificial.

Para concebir mejor esto, se debe entender el funcionamiento general de las inteligencias artificiales, como, por ejemplo, el caso de ChatGPT y otros que se basan en el sistema de chat, las cuales dan respuestas con base en la información suministrada por el usuario, pero esta información debe contener recomendaciones, definiciones o solicitudes específicas para que la inteligencia artificial actúe como una persona determinada. Dicha información debe ser suministrada con miras a obtener una respuesta más precisa, tal y como se dejó sentado en el ejemplo de la “abuelita” antes citado.

Después de hacer este planteamiento, es necesario ahondar en la normatividad para entender que con este tipo de respuestas brindadas por la inteligencia artificial se generan perjuicios como lo pueden ser el daño emergente, el lucro cesante o inclusive perjuicios morales, como, por ejemplo, cuando se ve afectada la intimidad. Pero sin descartar otros derechos o garantías que se pueden ver afectados por el funcionamiento de la IA.

En la medida que la inteligencia artificial se vuelve más común en nuestra sociedad, surge la preocupación sobre las implicaciones legales en el procesamiento de datos personales y sensibles, por lo que se plantea la siguiente pregunta: ¿Existe responsabilidad civil derivada del uso de datos personales y sensibles por parte de la inteligencia artificial?

Bajo la premisa anterior se hace importante resaltar el constante aumento de la tecnología en los últimos años, tanto así que muchas actividades antes eran realizadas por mano humana, las cuales hoy han pasado a un segundo plano, ya que dichas actividades pueden ser realizadas por la inteligencia artificial, sin intervención de la voluntad humana. Pero, bajo el anterior planteamiento, es importante destacar que la inteligencia artificial funciona por medio de información y programación, las cuales son suministradas por fuerza humana, es decir, deja abierto el campo del acierto-error, por lo que la inteligencia artificial puede presentar fallas que generan perjuicios a las personas, como se pretende demostrar en este escrito.

Es evidente que la tecnología actualmente se encuentra en constante avance, lo cual representa un progreso positivo, pero es menester indicar que no todo lo que trae consigo la tecnología impacta positivamente en lo que atiende a la optimización de los datos para el bienestar de la sociedad en general, pues, como se pretende demostrar en esta monografía, estos avances de la tecnología, y en específico el desarrollo de la inteligencia artificial enfocado en la protección de datos personales y sensibles, tiene grandes vacíos y una falta de regulación jurídica para el correcto funcionamiento de la misma.

En este punto es necesario mencionar la legislación relativa a la protección de datos, por medio de la Ley 1581 del 2012, la cual se encarga de regular el tratamiento de datos personales que pueden ser protegidos y/o sensibles. Específicamente, en su artículo 3 indica quiénes son los responsables del tratamiento de datos: "las persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos" (Ley 1581, 2012, art. 3). Todo esto es aplicable a lo relativo de la inteligencia artificial antes expuesto a falta de regulación específica en el tema.

La sociedad tiene que afrontar una serie de desafíos con el avance de la tecnología en relación con la inteligencia artificial, los cuales, antes de la creación y desarrollo de la inteligencia artificial, no se tenían. Por ejemplo, es necesario ahondar en el alcance jurídico de los actos dañinos que puede llegar a ocasionar este tipo de tecnología, donde es menester preguntarse ¿quién es el llamado a responder por un posible perjuicio que se desprenda del uso de los datos personales y sensibles por parte de la inteligencia artificial? ¿y bajo qué título de imputación de la responsabilidad civil?

Por lo tanto, es importante realizar un análisis minucioso sobre las pesquisas futuras desprendidas de la inteligencia artificial, en donde se busque actualizar o desarrollar normas que estén encaminadas a prevenir y/o mitigar problemas legales que pueden llegar a afectar el normal desarrollo de las relaciones entre las personas y la inteligencia artificial, buscando así una delimitación en donde se defina quién o quiénes son las personas llamadas a responder ante una afectación derivada del uso de datos personales y sensibles por parte de la inteligencia artificial, pues esta funciona según la información suministrada por diferentes actores.

Es así como se busca profundizar en el tema de la inteligencia artificial y el uso de las bases de datos, como base fundamental del sistema de inteligencia artificial, ya que esta funciona o se alimenta de bases de datos públicas y privadas, lo que brinda mayor eficiencia en lo solicitado por el usuario a la inteligencia artificial cuando esta tiene un mayor alcance en la Big Data. A renglón seguido, se pretende identificar que la inteligencia artificial en muchos casos no hace la distinción necesaria entre lo que puede ser información de carácter público e información de contenido reservado, por lo que es viable afirmar que falta una mejor programación de la inteligencia artificial por parte del creador.

Con esta investigación se pretende llegar a una concientización, enfocada a la sociedad en general, para que se reconozca la inteligencia artificial como una fuente de perjuicios o daños, ya que en esta hay un riesgo latente de sufrirlos en bienes protegidos relacionados con los datos objeto de la investigación, como por ejemplo una afrenta a la intimidad.

Esta investigación le aportará a la comunidad de la Universidad Autónoma Latinoamérica un cuestionamiento sobre las posibles consecuencias que se desprenden de un mal uso o un mal funcionamiento de la inteligencia artificial, por lo cual se pretende que el lector se cuestione o interiorice sobre el alcance de la responsabilidad civil frente a los daños o perjuicios causados por la inteligencia artificial.

Para la realización y argumentación de los capítulos que pretende dar desarrollo la presente monografía se tienen los siguientes objetivos, empezando por un objetivo general, el cual es identificar la responsabilidad civil derivada del uso de los datos personales y sensibles por parte de la inteligencia artificial, para de esta manera pasar a desarrollar los siguientes objetivos específicos, iniciando con definir qué es la inteligencia artificial y cómo esta tiene acceso a bases de datos que pueden contener información protegida y/o sensible, continuando con examinar la legislación colombiana vigente sobre el procesamiento de datos y su posible incidencia en la responsabilidad civil y finalmente terminar por analizar la responsabilidad civil derivada del uso de datos personales y sensibles por parte de la inteligencia artificial.

Consecuentemente con el constante avance de la tecnología, el uso de la inteligencia artificial ha incrementado de manera considerable en los últimos años, tocando así con esferas personalísimas, es decir, rosando con derechos fundamentales, como la intimidad o la privacidad.

Las inteligencias artificiales tienen la capacidad de almacenar los datos entregados de manera externa, sin tener en cuenta el tratamiento de datos que determine la ley colombiana, que para esta monografía es la ley vigente. De lance en lance, si no se programa la inteligencia artificial para que no almacene estos datos, hará uso de ellos indiscriminadamente.

Por otra parte, para hablar de responsabilidad civil y de inteligencia artificial es necesario contextualizar desde la órbita de la culpa, ya que la participación humana en la creación o el uso de estas tecnologías podrían generar perjuicios por negligencia, imprudencia, impericia o faltar al deber objetivo de cuidado.

El artículo 2341 del Código Civil colombiano indica que “El que ha cometido un delito o culpa, que ha inferido daño a otro, es obligado a la indemnización, sin perjuicio de la pena principal que la ley imponga por la culpa o el delito cometido” (Código Civil, 1887, art. 2341), evidenciándose así un elemento subjetivo al momento de construir la demanda, y es que para que se declare civilmente responsable a alguien por hecho propio desde el punto de vista extracontractual, es necesario demostrar el dolo o la culpa en el evento dañoso. En

lo relativo a la inteligencia artificial, es viable imputar una culpa al creador cuando su tecnología falla y hace públicos datos que son de naturaleza privada o destina de manera diferente datos que son sensibles y personales. Pudiendo generar así perjuicios, todo esto sin descartar las demás fuentes de responsabilidad, las cuales se pretenden desarrollar con miras al objetivo general de la presente monografía.

Consecuentemente, el artículo 2356 del Código Civil colombiano propone que "Por regla general todo daño que pueda imputarse a malicia o negligencia de otra persona debe ser reparado por ésta" (Código Civil, 1887, art. 2356). En esta norma el legislador propone un tipo de responsabilidad objetiva, y solo importa que el evento dañoso encaje en la regla general de la norma antes citada o en los casos típicos que trae el mismo artículo, donde media el peligro o el riesgo inminente de la afectación de un bien jurídico tangible o intangible, que para el caso de la IA casi siempre serán bienes intangibles protegidos desde la Carta Magna.

Dejando de lado el tema normativo frente a la responsabilidad civil generada por el uso de la inteligencia artificial como una fuente de riesgo o por el uso de la misma, es preciso afirmar que hay un peligro potencial que emana de la inteligencia artificial, peligro que se pretende dejar en evidencia a lo largo del presente escrito.

Es necesario abordar dicha problemática desde una óptica crítica con la ayuda de autores que han desarrollado el tema, tanto en Colombia como en otros países. De ser necesario, dicha información se analizará y se comparará con el tratamiento interno que se le ha dado hasta el momento a los posibles daños que puede llegar a ocasionar la inteligencia artificial, es decir, se utilizará una metodología dogmático jurídica.

Finalmente, la metodología utilizada en la presente investigación se basa en el enfoque cualitativo para entender la responsabilidad civil derivada del uso de datos personales y sensibles por parte de la inteligencia artificial, sin olvidar que el mero tratamiento de datos personales y sensibles sin intervención de la IA también puede generar daños y perjuicios.

Capítulo 1

La inteligencia artificial

Para entender qué es la inteligencia artificial es necesario iniciar por el estudio de la misma a lo largo de la historia, ya que si bien el término de la IA para muchas personas es algo novedoso y lo definen como un tema actual, se podría decir que se empezó a hablar desde el siglo XXI. Pues bien, dicho término de la IA fue utilizado por primera vez en el año de 1956, pero si bien en dicho año fue usado por primera vez, años atrás se empezó a utilizar la tecnología con relación a su capacidad de trabajar por sí sola, lo cual formó las bases de lo que se conoce como inteligencia artificial, incluso desde el siglo XVIII se usó la tecnología para facilitar el trabajo humano, tema que se abordará a continuación.

Una vez abordado el contexto sobre la IA, es menester ahondar sobre la historia de la misma a lo largo de la historia para entender cómo esta ha avanzado en el tiempo, en donde se evidencia que en la actualidad dicha tecnología cuenta con un avance significativo, siendo esta capaz de reemplazar actividades que antes eran desarrolladas por fuerza humana.

Bajo la premisa anterior se pretende realizar una línea de tiempo sobre la IA a lo largo de su historia, iniciando por lo que se denominó cómo los primeros pasos de la IA, cómo esta fue creada, cuándo se empezó a utilizar dicho término y finalmente cómo ha sido su evolución a lo largo de la historia.

De esta manera, es necesario iniciar con el año de 1842, es decir, 182 años atrás a la fecha de publicación de la presente investigación. En dicho año, “la matemática y pionera de la informática, Ada Lovelace, programó el primer algoritmo destinado a ser procesado por una máquina. Adelantada a su época, Ada especuló que la máquina podría actuar sobre otras cosas además de los números”. (Abeliuk y Gutiérrez, 2019, p.02). Para los autores Abeliuk y Gutiérrez, este fue el primer programa de la IA. Si bien para la época el término IA no existía, para los autores en mención este fue el primer programa desarrollado por la IA.

Para entender de una mejor manera la idea anterior, se precisa que un algoritmo es un conjunto de pasos por medio de los cuales se busca hallar una determinada ruta, para encontrar la solución a un problema en específico.

Se trata de un algoritmo implementado en una máquina musical el cual “podría componer piezas musicales elaboradas y científicas de cualquier grado de complejidad o extensión” (Abeliuk y Gutiérrez, 2019, p.02). Este algoritmo desarrollado por Ada Lovelace marcó el inicio de la IA, pues este era capaz de procesar notas musicales de manera independiente, considerándose así como el primer programa implementado por una persona en desarrollo de la IA, y como se dijo anteriormente, si bien en dicho año la IA todavía no tenía un

término definido, para los autores mencionados anteriormente este fue el primer programa de IA, pues era capaz de realizar una tarea dada de manera independiente.

En 1920 se habló por primera vez del término "Robot", dicho término fue utilizado por el escritor de ciencia ficción Karel Capek en su obra dramática denominada Robots Universales Rossum. En este año se dio el primer acercamiento con el término de IA por medio de máquinas a las cuales se les dio el nombre de Robots. Si bien todo empezó como una obra de ciencia ficción, donde las máquinas denominadas Robots eran unos aparatos pensantes de manera autónoma. Desde esta fecha se siguió con el término de Robot para referirse a aquella máquina capaz de realizar funciones de manera autónoma.

Luego, en 1943, fue creado el primer modelo computacional matemático de la neurona por los autores Warren Mcculloch y Walter Pitts. Se denominó modelo matemático de la neurona porque este era "inspirado en el funcionamiento de las neuronas biológicas. En este modelo, la validez o invalidez de un determinado teorema de lógica de primer orden era determinada, no por un autómata manipulador de símbolos, sino por una red de neuronas artificiales" (Rodríguez, 2021, p. 02). Este modelo computacional matemático consistía en uso de neuronas biológicas las cuales interactuaban entre sí, dicho modelo era diferente a los sistemas computacionales de la época, pues este opera principalmente con la excitación de neuronas, unas a otras por medio de conexiones sinápticas. Este modelo computacional desarrollado por los autores en mención fue un modelo novedoso y distinto de los usados normalmente en aquella época, por lo que este hito es considerado como un gran avance de la IA, aunque si bien para la época el término IA todavía no estaba en el medio.

Después de esto, viene la etapa más importante de la IA en la historia, exactamente 7 años más tarde, es decir, en 1950 el autor Alan Turing diseña lo que se conoció como el Turing Test, este consistía en determinar si una máquina demostraba comportamiento inteligente o si no lo hacía, comportamiento que fuera similar a un comportamiento humano. Con este Turing Test, el autor Alan Turing "dio una respuesta a esa pregunta: un ordenador era capaz de "pensar" si sus resultados eran tan convincentes que una persona que interactuara con él no pudiese distinguir sus respuestas de las de un ser humano real" (Blakemore, 2023, p. 01).

Si bien en el año 1950 el término Inteligencia Artificial aún no estaba en el medio como un término propio, este Turing Test fue un gran avance en relación con la IA, ya que por medio de este se pretendía demostrar si una máquina se podía equiparar con el conocimiento humano. Este Turing Test lo que hacía era determinar si una máquina presentaba alguna semejanza con el comportamiento humano, a tal punto que una persona no distinguiera si una respuesta era de la máquina o de una persona, equiparándose esto a lo que es la IA en la actualidad, ya que como se ha mencionado en esta época, la IA no era reconocida como tal y tampoco tenía un término definido.

Ahora bien, como ya se ha demostrado a lo largo de este contexto histórico sobre la IA, hasta este punto la IA no era reconocida como tal, es decir, no se había dado un nombre para el tratamiento de la misma. Si bien se hicieron varios avances atenientes a la IA, esta carecía de un nombre propio y una definición.

Conforme a la premisa anterior, es necesario seguir con el contexto histórico acerca de la IA, ya que, en el año 1956, se da lo que se denominó como el nacimiento de la IA propiamente dicha. Se podría afirmar que este año es el que parte de la historia de la IA, ya que desde aquí a la IA se le dio un término propio y consecuentemente desde dicho año se empezó a trabajar en el avance de la misma.

> Sin embargo, un hito considerado como el momento fundacional de la "inteligencia artificial", tanto del término como del campo de estudio, es una conferencia en Darmouth el año 1956 organizada por John McCarthy, Marvin Minsky, Claude Shannon y Nathaniel Rochester [1]. En ella, los organizadores invitaron a unos diez investigadores para formalizar el concepto de inteligencia artificial como un nuevo campo de estudio científico (Abeliuk y Gutiérrez, 2019).

A mediados de la década de los 50, la "Inteligencia Artificial" empezó a circular en el medio con un término propio, naciendo en este año como un campo científico con un estudio propio, esto por contar con un objeto de estudio determinado y un método, convirtiéndolo así en estudio científico. Es desde este año como tal que el término IA cobró fuerza y a través de los años este ha tenido un constante avance.

Paralelamente en 1956, año en que se dio origen a la IA, como se mencionó anteriormente, se publicó el primer programa computacional de IA. Este programa fue desarrollado por los autores Alan Newell y Herbet Simon y este consistía en un programa que era "capaz de descubrir demostraciones de teoremas en lógica simbólica. La idea principal es que, a través de la combinación de simples operaciones primitivas, el programa puede ir construyendo expresiones cada vez más complejas" (Abeliuk y Gutiérrez, 2019. p.02).

Como se puede evidenciar respecto de los planteamientos anteriores, en el año 1956 se da un avance importante respecto del desarrollo de la IA, esto principalmente por dos motivos puntuales. Lo primero es que en dicho año a la IA se le bautiza teniendo esta su nombre propio y lo segundo es que en dicho año se publicó el primer programa desarrollado por la IA, se dice que fue el primer programa ya que en ese año se empezó a hablar de IA propiamente dicha y los programas desarrollados atenientes a la IA que se crearon eran avances de esta última.

Después del nacimiento de la IA propiamente dicha en 1956, se desarrolló una gran cantidad de programas de IA, lo que quiere decir que después de este año la IA fue aceptada como un término propio con un campo de estudio científico nuevo mediante el cual se desarrollaron programas, avanzando en el tiempo y en su tecnología.

Por ejemplo, en 1964 el autor Joseph Weizenbaum desarrolló el primer chatbot el cual podía llevar a cabo una conversación con una persona, pero únicamente con idioma inglés. Este chatbot trabajaba "reconociendo palabras claves y preguntando sobre ellas como si fuera un psicólogo (Fernández, 2017, p. 04). Es así como se puede evidenciar que el chatbot viene desde el año de 1964 y en la actualidad este programa es muy usado por diferentes personas jurídicas, en donde se vislumbra que este no es un programa novedoso, pues como se mencionó, este fue desarrollado hace 60 años.

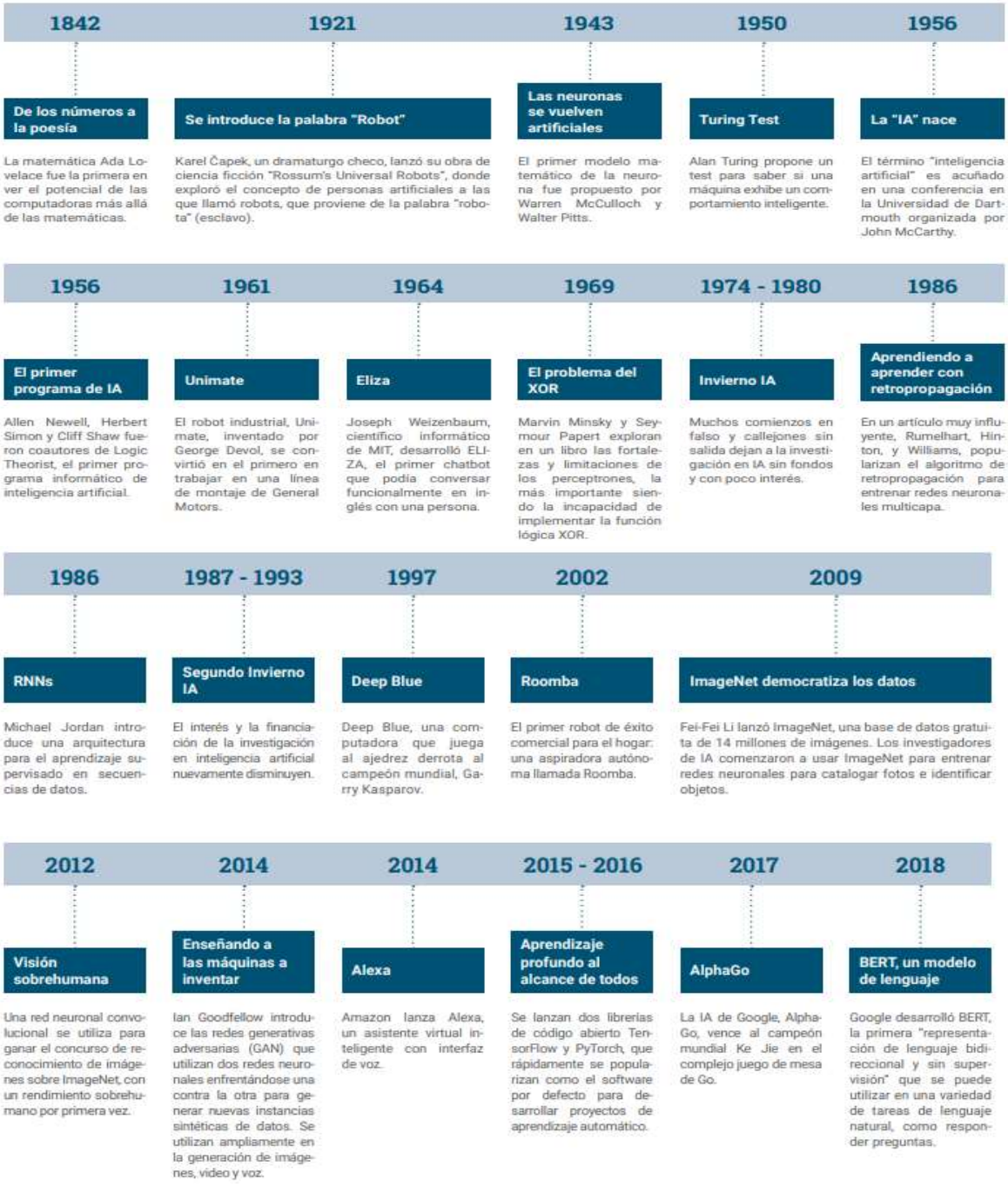
Posteriormente, se desarrollaron otros programas con respecto a la IA que, si bien son importantes para el avance tecnológico de este, no son tan importantes con la historia de la IA.

A manera de ejemplo, podemos identificar el aparato conocido como Alexa el cual fue lanzado en el año de 2014 por la plataforma de ventas Amazon. Como bien se sabe, Alexa es un dispositivo que funciona por medio de voz y de la misma manera brinda respuesta a los usuarios que adquieren dicho dispositivo. Con este dispositivo se evidencia que este funciona por medio de IA, la cual sirve para facilitar tareas que son realizadas por la mano humana.

Con respecto al contexto histórico mencionado a lo largo del presente capítulo, se toman los hitos más importantes respecto de la IA, para consecuentemente entender qué es la IA como tal y como esta trabaja; es por lo cual se anexa figura ilustrativa referente a la historia de la IA, en la cual se muestran los hitos más importantes, los cuales fueron desarrollados en este capítulo y otros que, si bien son importantes, no representan un avance significativo en relación con la IA.

Figura 1.

Historia de la inteligencia artificial



Nota. Por Abeliuk y Gutiérrez, 2019, Historia de la inteligencia artificial, recuperada del artículo Historia y evolución de la inteligencia artificial, Chile.

Cuarta revolución industrial y su relación con la inteligencia artificial

Una vez realizado el contexto histórico sobre la inteligencia artificial, desde sus inicios hasta la actualidad, se hace necesario dar una definición de lo que se denomina la cuarta revolución industrial o también llamada la revolución 4.0 y cómo esta tiene relación con la inteligencia artificial, para de esta forma poder entender qué es la inteligencia artificial como tal, tema que será objeto de estudio en el siguiente título.

Ahora bien, para entender qué es la cuarta revolución industrial es necesario iniciar por su definición. Si bien dicho término no tiene una definición precisa, en este apartado se tratará de indiciar la más precisa, ya que existen múltiples definiciones para dicho término.

La cuarta revolución industrial "no se define por un conjunto de tecnologías emergentes en sí mismas, sino por la transición hacia nuevos sistemas que están construidos sobre la infraestructura de la revolución digital (anterior)" (Perasso, 2016, p. 03),) así las cosas, se identifica que la cuarta revolución industrial se trata de una serie de cambios, en donde se busca la innovación productiva por medio de la fusión de tecnologías; dejando de un lado la frontera existente entre la esfera física y la esfera digital.

En otras palabras, la revolución 4.0 se puede definir como la combinación avanzada de técnicas, en donde se combinan los procesos físicos con tecnologías inteligentes (IA), los cuales buscan que se dé una integración en las diferentes organizaciones y por medio de estos facilitar la vida de las personas.

Con la cuarta revolución industrial se quiere que por medio de la tecnología las diferentes organizaciones, tales como empresas, entidades, sociedades, etc. Se transformen buscando una digitalización de los procesos, en donde se faciliten todos los procesos desarrollados por fuerza humana, pero con la salvedad de que la revolución 4.0 no busca reemplazar la mano humana, sino facilitarle el trabajo, generando así mayor agilidad respecto de los productos y/o servicios que ofrece cada entidad como tal.

Finalmente, la revolución 4.0 se entiende que llega de la mano con lo que es la inteligencia artificial y por medio de esta es que se da, así las cosas, se vislumbra que la cuarta revolución industrial llega de la mano de aplicación de técnicas desarrolladas por medio de la inteligencia artificial.

Consecuentemente, a lo largo del presente capítulo, en el cual se busca dar la definición de qué es la inteligencia artificial, se abordarán más conceptos y se aclarará el funcionamiento de la inteligencia artificial, indicando que toda esta hace parte de la cuarta revolución industrial o también denominada la revolución 4.0.

Acercamiento al término “inteligencia artificial”

Una vez realizado el contexto histórico acerca del desarrollo de la IA y cómo ha sido su evolución en el tiempo, hasta llegar a la actualidad, se tratará de dar un acercamiento a lo que es la IA propiamente dicha.

Si bien el término Inteligencia Artificial no tiene una definición como tal, diversos autores han tratado de dar la definición que más se adapte a dicho término, esto teniendo en cuenta que a la fecha de publicación del presente artículo no hay una definición genérica que esté aceptada por estudiosos del campo de la IA. Así las cosas, dar una definición precisa de lo que es la IA es una cuestión complicada; lo que se hace es llegar a dicho concepto por medio de aproximaciones.

Ahora bien, si damos una definición de la palabra inteligencia y luego damos una definición de la palabra artificial, se notará que estos términos por sí solos, si traen una definición clara y precisa, el problema se refleja al momento de combinar dichos términos, como se demostrará a renglón seguido.

El término inteligencia, “etimológicamente se deriva de la voz latina «legere» que recolectar y está directamente relacionada con elegir, en donde, «intellegere» significa elegir entre varias cosas. En ese sentido, inteligencia se describe como la capacidad de discernir algo.” (Alvarado, 2015, p. 27). En este sentido, y según la definición aportada por el autor en mención, la inteligencia es la capacidad que se tiene para discernir de un determinado tema, es decir. Esta se puede definir como ese juicio de reproche que realizamos las personas sobre un tema en particular. Lo anterior visto desde la perspectiva de la IA se puede identificar que es un tema tedioso, esto por cuanto la IA funciona con algoritmos que son programados por la mano humana, como se demostrará a continuación, y consecuentemente, para que las IA tengan la capacidad de discernir sobre un tema es porque sus desarrolladores la programaron por medio de algoritmos de esa forma.

Por otro lado, cuando analizamos la definición de la palabra artificial, se puede vislumbrar que es una definición muy precisa. Por ejemplo, la Real Academia de la Lengua la define como “hecho por mano o arte del hombre” (RAE, 2023). Conforme a esta definición, se puede evidenciar que esta admite el error, pues como su definición lo indica, esta es creada o desarrollada por mano humana y, como es bien sabido, al ser creada por fuerza humana, estará siempre la posibilidad del error.

Una vez abordados los conceptos de inteligencia artificial con una definición discriminada para cada uno, es necesario aproximarse a lo que es la inteligencia artificial con la unión de ambos términos, pues como se demostró anteriormente, estos de manera independiente tienen una definición precisa. La dificultad surge al referirse a la unión de estos términos como si fuera uno solo.

Para dar una aproximación de lo que es la IA, es necesario empezar por indiciar que “La Inteligencia Artificial se considera como una de las ramas de las ciencias de la computación que se ocupa de construir sistemas que permiten exhibir un comportamiento cada vez más inteligente.” (Alvarado, 2015, p. 28). Conforme a esta premisa, resulta imperativo aclarar que la IA es una rama de la ciencia informática y, al ser esta una rama independiente, tiene su objeto de estudio determinado, el cual se basa en crear sistemas por medio de algoritmos que permitan que las máquinas y/o aparatos presenten cada vez más comportamientos similares al humano.

Bajo la premisa anterior se identifica que por medio de la rama de la IA se pretende construir sistemas que cuenten con capacidades similares a las humanas e incluso es factible afirmar que con el constante avance de la tecnología y en específico de la IA. Estas podrían en algún momento superar al conocimiento humano.

Seguidamente, la IA es un modelo de sistema interdisciplinario por medio del cual expertos en el tema buscan su perfeccionamiento, el cual se puede evidenciar con el pasar de los tiempos, pues como se indicó en la primera etapa del presente escrito, a lo largo de los años, las IA han avanzado cada vez más, hasta llegar al punto de que muchas actividades que antes eran realizadas por fuerza humana hoy se pueden realizar por medio de diferentes IA, vislumbrando que estas pueden reemplazar al hombre en tareas determinadas.

Respecto al anterior planteamiento, se podría afirmar que con las IA se busca reemplazar al hombre en una gran cantidad de tareas, las cuales son realizadas por fuerza humana, pero que estas podrían ser realizadas por una IA. Esto no es así, véase cómo el autor Alvarado afirma que:

> El desarrollo de la inteligencia artificial no pretende reemplazar en su totalidad la inteligencia humana ni la toma de decisiones, el objetivo está centrado en apoyar y aumentar capacidades para resolver de forma más eficiente problemas específicos, para que el factor humano sea menos primordial y disminuir el factor del error (Alvarado, 2015, p. 28).

Así pues, por medio de la IA se busca disminuir el margen de acierto-error de las labores realizadas por fuerza humana. Como se dijo, el objetivo que se pretende con la IA no es el reemplazo del hombre, sino que es apoyar a este último para disminuir la probabilidad de incurrir en error respecto de un tema determinado.

Conforme lo anterior, es factible indicar que la IA tiene como principal objetivo apoyar la fuerza humana; además de esto, busca mejorar la eficiencia en tiempo y desgaste físico del hombre en la realización de determinadas labores. En pocas palabras, lo que se busca con el constante desarrollo de la IA es que esta pueda facilitarles la vida a las personas.

En conclusión, la IA es un mecanismo de ayuda el cual busca apoyar al hombre en la realización de labores cotidianas y que de esta manera el hombre pueda ocuparse de otros

asuntos, esto por cuanto las actuales IA tienen la capacidad de asumir tareas que en principio son responsabilidad del hombre (Alvarado, 2015).

Consecuentemente, se podría decir que la IA está en su punto más alto y que es difícil que esta siga avanzando en relación con el mejoramiento de la misma por medio de la tecnología, ya que para nadie es un secreto que en la actualidad la tecnología cuenta con un gran avance que sirve para las actividades realizadas por el hombre; pero esta es un área con un camino abierto por investigar y por mejorar, pues como bien se ha dicho a lo largo de este escrito. La tecnología está en constante avance y cada vez más la sociedad se adapta a los cambios. De la misma manera que la sociedad se adapta a los cambios, la tecnología tiene que evolucionar a favor de las personas para de esta manera hacer la vida del conglomerado social más fácil.

Como se ha indicado a lo largo de esta monografía, dar con una definición concreta de lo que es la IA es algo complicado debido a las múltiples definiciones que se tienen de esta. Pero para el autor Rouhiainen esta se puede definir desde dos puntos en concreto.

La primera definición es que "la IA como «la habilidad de los ordenadores para hacer actividades que normalmente requieren inteligencia humana»." (Rouhiainen, 2018, p. 17). Respecto de esta definición, vale la pena aclarar que la IA es aquel conocimiento que se plasma por medio de un algoritmo a un sistema informático, el cual se refleja en un aparato o máquina, y que dicho conocimiento es insertado por fuerza humana por medio de la programación.

La segunda definición y más detallada que trae el autor en mención es que "la IA es la capacidad de las máquinas para usar algoritmos, aprender de los datos y utilizar lo aprendido en la toma de decisiones tal y como lo haría un ser humano." (Rouhiainen, 2018, p. 17). Esta definición muestra que en cierta medida la IA busca asemejarse con el conocimiento humano para así desarrollar tareas que en principio serían desarrolladas por fuerza humana.

Si realizamos un comparativo entre lo que es la IA y el conocimiento humano, inicialmente podemos identificar que la IA es superior a la fuerza humana, en tanto esta no necesita descansar a diferencia de lo que pasa con la fuerza humana. Seguidamente, la IA está en la capacidad de analizar altos volúmenes de información en un menor tiempo del que lo analizaría una persona y, finalmente, la proporción de errores en que incurriría la IA respecto de un hombre es inferior, por cuanto su programación se basa en que esta se equivoque lo menor posible, disminuyendo así el margen de error.

Como se ha mencionado a lo largo de este escrito respecto de que la IA no trae una definición precisa, a lo largo de este capítulo se ha intentado dar una aproximación de qué es la IA y cómo es su funcionamiento. Como se puede evidenciar las definiciones acerca de que es la IA si bien no son las mismas estas presentan una similitud y es que después de realizado el contexto histórico y tratar de dar con la aproximación más concreta de que es

la IA, es preciso indicar que la IA se puede definir como aquella inteligencia que es plasmada por la fuerza humana por medio de algoritmos la cual se materializa en una máquina o un aparato que sirve para realizar funciones que normalmente son desarrolladas por el hombre, en pocas palabras con la IA se busca desarrollar sistemas informáticos con el objetivo principal de que estos imiten la inteligencia humana para realizar determinadas tareas y de esta manera facilitarle la vida a las personas, ya que como se dijo anteriormente con la IA no se busca el remplazo del hombre sino por el contrario ayudarle a este último por medio de la tecnología.

Funcionamiento de la IA

Una vez abordado el contexto histórico de la IA y su concepto, se torna necesario analizar su funcionamiento y cómo esta tiene acceso a información; la cual puede ser confidencial, personal y/o sensible.

De entrada, se vislumbra que el tratamiento de datos personales se puede ver desafiado por el constante avance de la tecnología y en específico con el avance de la IA, pues como se relatará a lo largo de la presente monografía, la IA para su funcionamiento requiere el tratamiento de datos personales. Así las cosas, respecto de la IA, esta requiere para su correcto funcionamiento grandes volúmenes de datos, los cuales en muchos casos pueden ser personales y sensibles.

Como se ha mencionado a lo largo del presente capítulo, con el constante avance de la tecnología y de la IA, estas han traído consigo una serie de cambios respecto al tratamiento de datos. Véase cómo se puede procesar infinidades de datos en diferentes partes del mundo y por diferentes actores a una velocidad sin igual. Con estos cambios, los países se han visto afectados en temas jurídicos, ya que la legislación se ha quedado corta respecto de la regulación frente a estos temas.

En el mismo sentido, cabe preguntarnos en qué escenarios la IA puede llegar a generar peligro sobre el titular de los datos. Para esto es necesario indicar que:

> existen dos aspectos de la IA que son particularmente relevantes para la privacidad. El primero es que la IA en sí misma puede tomar decisiones automatizadas y, el segundo, es que el sistema se desarrolla aprendiendo de la experiencia e información proporcionada (Morales, 2020, p. 01).

Conforme a la premisa anterior, se evidencia que la IA es un sistema autónomo el cual puede tomar decisiones de manera unilateral, esto sin pedirle permiso al titular de los datos o sin que este haya autorizado el tratamiento de los mismos. De esta forma se puede llegar a generar una afectación a ese usuario respecto de sus datos personales.

Consecuentemente, la IA, al ser un sistema informático que opera a través de datos proporcionados y al ser esta un sistema autónomo, el cual está en constante aprendizaje,

puede llegar a cometer errores sobre el tratamiento de datos personales. De esta forma, se observa que la IA tiene acceso a información por medio de bases de datos las cuales contienen información que puede llegar a ser protegida y/o sensible. De esta manera, si un usuario diferente al titular de los datos le solicita acceso a información de otro usuario a la IA y esta IA accede a la suministración de los mismos, puede llegar a generar perjuicios, ya que en muchos de los casos esa información es personal y si esta es usada de manera inadecuada por un tercero, puede llegar a afectar intereses del titular de los mismos.

Para dar un poco de claridad acerca de cómo la IA cuando tiene acceso a información personal de una determinada persona y esa información es usada sin el consentimiento expreso de esa persona, además de que dicha información es usada de forma inadecuada, se puede llegar a generar afectaciones al titular de esos datos. Para entender mejor esto, se plantea el siguiente ejemplo:

> En el año 2015, Jacky Alcine, una afroamericana, cuando miró su fotografía en la aplicación de Google Photos no podía creer que el software de reconocimiento facial la había etiquetado con la palabra “gorila”. Esto sucedió porque el algoritmo no había sido entrenado con suficientes imágenes de personas de piel oscura (Morales, 2020, p. 02).

Con este ejemplo, se evidencian principalmente dos cosas: lo primero es que la IA tuvo acceso a información de la señora Jacky, esto por medio de bases de datos que contienen información personal de las personas, ya que como se plantea a lo largo de esta monografía, la IA funciona por medio de bases de datos. Lo segundo es que esa información que obtuvo la IA es información personal y sensible, además no hay que ser un experto para entrever que con dicha información se generó una afectación a la señora Jacky, afectación que está ligada a su dignidad humana, pues es evidente el uso inadecuado de su fotografía ya que la compara con un animal. Véase como, respecto de este caso, nos podríamos preguntar: ¿Quién es la persona llamada a responder por dicho perjuicio? Sobre esta pregunta se trabajará en capítulos posteriores.

Por otro lado, es imperativo saber el modo en que las IA tienen acceso a información de personas por medio de bases de datos, para esto es necesario indicar lo siguiente:

> Las Inteligencias artificiales utilizan **algoritmos y modelos matemáticos** para procesar grandes cantidades de datos y tomar decisiones basadas en patrones y reglas establecidas a través del **aprendizaje automático**, que es la capacidad de una máquina para aprender de forma autónoma a partir de datos sin ser programada específicamente para hacerlo (Gobierno de España, 2023, p. 02).

Se reitera que las IA funcionan por medio de programación a base de algoritmos y modelos matemáticos para el procesamiento de información y aunado a esto, las IA tienen la capacidad autónoma de aprender y tomar decisiones sin una respectiva programación.

Según esto, se precisa que al tener la IA capacidad autónoma para tomar decisiones puede llegar a afectar a una determinada persona por un mal uso de su información personal.

Finalmente, para dar claridad al lector sobre cómo las IA obtienen información que puede ser personal y sensible se resalta que:

> Esta tendencia tecnológica tan prometedora que está marcando de un modo impactante cada uno de los ámbitos de nuestra vida, se basa fundamentalmente en la recopilación de gran cantidad de información que se almacena en bases de datos inteligentes para su posterior análisis y comprensión. (PowerData, 2021, p. 01)

Bajo el enunciado anterior, el cual coadyuva el argumento esbozado a lo largo de esta monografía, se concibe que las IA funcionan de acuerdo a recopilación de altas cantidades de información, para de esta forma darle un posterior tratamiento.

En conclusión, las IA funcionan con información que obtienen a través de bases de datos, cuya información puede ser personal y/o sensible. El problema radica cuando esta información es usada de manera inadecuada, tema del que se ocupará en los siguientes capítulos de la presente monografía.

Capítulo 2

El procesamiento de datos personales desde una mirada legal y constitucional y su relevancia para una posible responsabilidad civil

La Ley 1581 del 2012 es la norma por medio de la cual se reglamenta el tratamiento de datos personales, en ella también se encuentran definiciones de diferentes tipos de datos y otras disposiciones que más adelante se analizarán, pero, para este punto es necesario resolver o definir qué es un dato personal. Para ello, es necesario acudir al artículo tercero de la Ley antes mencionada, donde se hallan depositadas definiciones relevantes para el desarrollo de este escrito, así como también para la aplicación de la misma Ley.

Un dato personal es "Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;" (Ley 1581, 2012, art. 3) por lo que pudiera pensarse que los datos personales o la información personal pueden tener un titular o propietario. Al respecto, la misma norma en cita indica que los titulares de los datos personales son aquellas personas naturales cuyos datos o información es objeto del tratamiento o procesamiento, pero para este punto no queda muy clara la definición de tratamiento de datos ni de dato personal; al respecto, la Superintendencia de Industria y Comercio (SIC) ha dicho que:

> Los datos personales como las imágenes de los titulares se consideran datos biométricos y de carácter sensible cuando son tratados por medios técnicos específicos que permitan la identificación o la autenticación unívoca de una persona física. De lo contrario, se tratará de datos personales de carácter privado. (Soacha, 2018, p. 09)

Para este punto, la SIC, no solo se centra en abordar los datos personales, sino que también aborda el concepto sobre los datos sensibles, dando la posibilidad de que existan diferentes tipos de datos personales como lo son los sensibles, los cuales se encuentran descritos en la norma antes en comento, afirmando que:

> Artículo 5°. *Datos sensibles***.** Para los propósitos de la presente Ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su 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. (Ley 1581, 2012, art. 5)

Por otra parte, la Corte Constitucional ha dicho frente al asunto que:

> En efecto, la jurisprudencia constitucional ha precisado que las características de los datos personales –en oposición a los impersonales[184]- son las siguientes: "i) estar referido a aspectos exclusivos y propios de una persona natural, ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación." (Sentencia C-748/11, 2011)

De las anteriores citas se desprende algo verdaderamente importante para el desarrollo de esta monografía, ya que a partir de lo dicho por la SIC y la Corte Constitucional, se deduce que, por una parte, los datos personales son aquellos que permiten identificar a una persona, son de dominio de su titular, que siempre será una persona natural, mismos que son inalterables por terceros no autorizados, y su tratamiento tiene una reglamentación especial. Por otra parte, ocurre una situación similar con los datos sensibles, ya que son aquellos que tienen una relación sustancial con el derecho fundamental a la intimidad y es en este punto donde se encuentra el sustrato constitucional de la norma descriptiva de este tipo de información, ya que la intimidad se alza como un derecho connatural que tienen todas las personas, derecho que ha sido reconocido y plasmado en el artículo 15 superior, del cual se desprenden varias prerrogativas.

Véase que el artículo 15 de la Constitución Política indica que todas las personas tienen derecho a la intimidad, sea de índole personal o familiar; en el mismo sentido, se tiene derecho al buen nombre y en el mismo artículo, se encuentra una carga dirigida para el estado, cuando dice que "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." (Constitución Política de Colombia, 1991) Esta norma de carácter constitucional va más allá, indicando que los titulares de los datos personales tienen derecho a conocer, modificar, actualizar o reformar la información que se encuentra depositada en los bancos de datos y en archivos de entidades públicas y privadas y es deber del estado velar por su tutela.

Para este punto surge la incertidumbre sobre el alcance epistemológico del concepto "banco de datos" ya que es el vocablo propio que ofrece la Constitución Política de Colombia en su artículo 15. Para ello, es necesario acudir a la Ley de tratamiento de datos, que en su artículo primero desarrolla el objeto de la mencionada Ley, siendo este:

> Artículo 1°. *Objeto***.** La presente Ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. (Ley 1581, 2012, art. 1)

Comparando el contenido de este artículo primero con el artículo 15 de la Carta Magna, se encuentran grandes similitudes, donde la única diferencia radica en el vocablo base de datos para la Ley de protección de datos y banco de datos para la Constitución Política. Es así, como se puede afirmar que dichos vocablos son sinónimos y son utilizados indistintamente a lo largo de este escrito. La definición para estos vocablos será la propuesta por la Ley de protección de datos, la cual indica que una base de datos es el "Conjunto organizado de datos personales que sea objeto de Tratamiento;" (Ley 1581, 2012, art. 3)

Con la anterior definición se dejan claros ya varios puntos, estos son: las categorías de datos y el propietario de la información. En este punto se hace necesario definir qué es el tratamiento de datos, o para qué fin se usan los datos. Dicha cuestión la resuelve el antes citado artículo 3 de la Ley de protección de datos, el cual indica que el tratamiento de datos es "Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión." (Ley 1581, 2012, art. 3)

De lo anterior se puede afirmar que el tratamiento de datos es toda aquella actividad que se realiza y que guarda relación con la recolección, acopio, acumulación, uso o destinación, circulación o supresión, sustracción o eliminación de datos personales, pero ¿quién es el encargado del tratamiento de estos datos personales? La respuesta a la pregunta antes planteada se encuentra en el citado artículo 3, cuando señala que el responsable del tratamiento de datos es la "Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos;" (Ley 1581, 2012, art. 3) es decir que el responsable del tratamiento de datos puede ser cualquier persona, sea esta natural o jurídica, pública o privada, que actúe por sí misma o en conjunto de otras personas de la misma o diferente naturaleza, teniendo incidencia en la decisión relativa a la base de datos o inclusive con el uso, circulación, recolección o cualquier otro verbo constitutivo del tratamiento de datos.

Ahora bien, el tratamiento de datos personales gira en torno a unos principios o normas rectoras que propone la Ley de protección de datos personales, hallándose estos en el título segundo de la Ley en mención; estos principios rectores señalan que toda la actividad relativa al tratamiento de datos es una actividad regulada, es decir, goza del principio de legalidad. También indica que el tratamiento de datos debe tener un norte que legitime ese tratamiento o lo que es lo mismo, el principio de finalidad, el cual debe ser informado al titular, se prohíbe rotundamente el tratamiento de datos parciales, a esto el legislador lo denominó como principio de veracidad. Así las cosas, el titular tiene derecho a obtener información sobre la existencia o no de datos que le pueden resultar importantes y esta información debe ser suministrada por parte del responsable del tratamiento de datos o sus delegados. Toda la información suministrada al responsable debe ser tratada por los medios técnicos idóneos o lo que también se conoce como el principio de seguridad, en el entendido que el responsable del tratamiento de datos debe brindar seguridad a la información brindada por el titular.

Por otra parte, uno de los principios que reviste mayor importancia para este escrito, es el denominado como principio de acceso y circulación, que prescribe lo siguiente:

> f) Principio de acceso y circulación restringida**:** El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente Ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente Ley;
>
> Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente Ley; (Ley 1581, 2012, art. 4)

La norma antes citada hace una distinción tácita de los datos de naturaleza pública y los datos de naturaleza privada, teniendo estos últimos un especial tratamiento, ya que ameritan una mayor seguridad por su naturaleza privada, en el entendido que, para el procesamiento de información privada se necesita un permiso expedido por el titular en favor de la persona natural o jurídica que va a realizar el tratamiento, a excepción de las personas legalmente autorizadas que no necesitan de autorización del titular tal y como lo plantea el artículo 10 de la Ley en comento, a contrario sensu, los datos públicos no gozan de esta protección, es decir, no necesitan autorización para su tratamiento.

Por otra parte, el principio de confidencialidad guarda una estrecha relación con el principio antes desarrollado, véase:

> **Principio de confidencialidad:** Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente Ley y en los términos de la misma. (Ley 1581, 2012, art. 4)

En este apartado normativo es más evidente el especial tratamiento que tienen los datos personales de naturaleza privada, ya que el legislador impuso la carga de guardar confidencialidad por parte de quienes están legitimados para el tratamiento de datos de esta naturaleza, inclusive hasta después de terminada la relación con el dato personal o su titular.

Ahora bien, para hablar sobre responsabilidad civil derivada del uso de datos personales o el tratamiento que se le da a estos, es importante determinar quién es el responsable según la Ley o, en otros términos, quién está llamado a reparar, y es que, como ya se dejó en claro

en un apartado anterior, el responsable del tratamiento de datos personales es la persona, sea esta natural o jurídica, que tome decisiones sobre el tratamiento, uso, destinación o circulación de datos personales o también aquella persona natural o jurídica que decida sobre los bancos de datos.

Teniendo claro quién puede ser el legitimado en la causa por pasiva en un proceso de responsabilidad civil derivado por el uso o tratamiento de datos personales, es vital plantear un interrogante: ¿Es posible generar un perjuicio por el tratamiento de datos? Para darle solución a este interrogante es importante retomar el concepto de tratamiento de datos, para de esta manera ampliarlo y entender el alcance de esta actividad. Para tal fin se propone una definición y un análisis realizado por la Corte Constitucional, mírese como:

> El tratamiento es definido como cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. Este vocablo, al igual que los dos analizados en precedencia, es de uso en el ámbito europeo y se encuentra tanto en la Directiva 95/46 del Parlamento Europeo como en los Estándares dictados en la reciente conferencia que se dio en Madrid (España), en la que se definió tratamiento como "cualquier operación o conjunto de operaciones, sean o no automatizadas, que se apliquen a datos de carácter personal, en especial su recogida, conservación, utilización, revelación o supresión"
>
> El vocablo tratamiento para los efectos del proyecto en análisis es de suma importancia por cuanto su contenido y desarrollo se refiere precisamente a lo que debe entenderse por el "tratamiento del dato personal". En ese orden, cuando el proyecto se refiere al tratamiento, hace alusión a cualquier operación que se pretenda hacer con el dato personal, con o sin ayuda de la informática, pues a diferencia de algunas legislaciones[202], la definición que aquí se analiza no se circunscribe únicamente a procedimientos automatizados. Es por ello por lo que los principios, derechos, deberes y sanciones que contempla la normativa en revisión incluyen, entre otros, la recolección, la conservación, la utilización y otras formas de procesamiento de datos con o sin ayuda de la informática. En consecuencia, no es válido argumentar que la Ley de protección de datos personales cobija exclusivamente el tratamiento de datos que emplean las nuevas tecnologías de la información, dejando por fuera las bases de datos manuales, lo que resultaría ilógico, puesto que precisamente lo que se pretende con este proyecto es que todas las operaciones o conjunto de operaciones con los datos personales quede regulada por las disposiciones del proyecto de Ley en mención, con las salvedades que serán analizadas en otro apartado de esta providencia. En este orden de ideas, esta definición no genera problema alguno de constitucionalidad y por tanto será declarada exequible. (Soacha, 2016, p. 07)

Para este punto ya se dilucida un apartado importante, que se denomina: las operaciones automatizadas, mismo que será objeto de análisis más adelante en la presente monografía.

Por lo pronto, otro apartado relevante para este texto, es cuando la Corte indica que el tratamiento de datos es toda aquella operación que se pretenda hacer con el dato o información de carácter personal, es decir, que estas operaciones no solo se circunscriben a los verbos ofrecidos por el artículo 3 de la Ley de protección de datos, dejándolo abierto a otras posibilidades, otras actividades o verbos, inclusive como la compra, venta, distribución entre otros.

Esta definición y análisis que hace la Corte sobre la ampliación del concepto en mención y continuando con la definición, se torna necesario ilustrar cómo y cuándo se puede generar un daño y un consecuente perjuicio; si se analiza la norma para la protección de datos, se puede evidenciar que en su artículo 24, por medio del cual define cuáles son los criterios para medir la sanción aplicable al responsable del tratamiento de datos, este ofrece como primer criterio que: "La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley;" (Ley 1581, 2012, art. 24) y es en este apartado donde se pueden ver dos conceptos relevantes para la responsabilidad civil, siendo estos el daño como una consecuencia de una actividad que reclama especial atención y el peligro como una probabilidad de ocurrencia del daño.

En este punto aún no se tiene un concepto claro de lo que compone la responsabilidad civil y para efectos de esta monografía se va tener lo dicho por la Sentencia SC5170 del 2018, que en pocas palabras dice, que la responsabilidad civil es aquella obligación de reparar el daño causado entre personas de derecho privado, es decir, entre particulares, y también señala que la responsabilidad civil tiene una doble connotación, por un lado está la responsabilidad civil contractual que surge por el incumplimiento de un contrato, y este incumplimiento puede ser parcial o total, por otra parte está la responsabilidad civil extracontractual, en donde no media ningún tipo de contrato, y esta se define como la obligación de reparar un daño causado por un hecho culposo o doloso, dicho de otra manera, con intención o con la ausencia de esta, faltando al deber objetivo de cuidado o con imprudencia, negligencia o con impericia.

Teniendo claro el concepto de responsabilidad civil, se procede a analizar la posibilidad de que surja una obligación de reparar un daño causado por el tratamiento de datos. Claro está que se puede generar un daño, esto de la mera lectura del artículo 24 de la Ley en comento, cuando señala que uno de los criterios para dosificar la sanción es la dimensión del daño, pero este apartado normativo también aborda el vocablo de "peligro", siendo necesario determinar el alcance de ambos conceptos para el mundo de la responsabilidad civil.

Por una parte, el Código Civil colombiano no ofrece una definición clara del concepto daño, por lo que es necesario acudir a otras fuentes como es la Real Academia de la Lengua Española (RAE), que define dicho concepto como el menoscabo, detrimento, perjuicio, dolor o molestia sufridos. Por otra parte, está el concepto de peligro, que la RAE propone como sinónimo de riesgo, siendo este un vocablo más adecuado para el mencionado artículo, en el entendido que el primero es una característica propia de una situación que determina la posibilidad de generar un daño, y el segundo, el riesgo, es la combinación de

un peligro y la posibilidad de no poder controlar el resultado o esa situación posiblemente dañosa, todo esto de acuerdo a las definiciones dadas por la RAE. se precisa que más adelante se dará más claridad sobre los conceptos jurídicos de riesgo y peligro.

Hasta este punto se han analizado los elementos especiales constitutivos de la responsabilidad civil en materia de tratamiento de datos, siendo estos: el responsable del tratamiento de datos, quién en principio está llamado a resarcir el daño causado con el tratamiento de datos. Está claro que sí se puede generar un daño con el tratamiento de datos, tanto es así que la legislación lo previó en el artículo 24 de la ley de protección de datos, y que el titular del dato es quien está en posición de reclamar la reparación del daño en caso tal de que se genere, pero ¿esta responsabilidad civil que se genera por el tratamiento de datos, es contractual o extracontractual?

Para resolver el anterior interrogante, es necesario remitirse a la autorización que da el titular antes del tratamiento de datos, figura que también está regulada por la Ley de protección de datos a partir del artículo 9, indicando que en el procesamiento de datos personales se requiere de la existencia de una autorización informada por parte del propietario titular de los datos a tratar y sin esta no es posible realizar actividades lícitas relativas al tratamiento de datos, ya que dicha norma afirma que “en el Tratamiento se requiere la autorización previa e informada del Titular” (Ley 1581, 2012, art. 9).

Más adelante, la norma en mención propone unos deberes en cabeza del responsable del tratamiento de dichos datos, ordenándole a este que debe brindarle al titular la información por él requerida relativa a los datos que fueron depositados por él:

> Artículo 12. Deber de informar al Titular. El Responsable del Tratamiento, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente:
>
> a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;
>
> b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;
>
> c) Los derechos que le asisten como Titular;
>
> d) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.
>
> Parágrafo. El Responsable del Tratamiento deberá conservar prueba del cumplimiento de lo previsto en el presente artículo y, cuando el Titular lo solicite, entregarle copia de esta. (Ley 1581, 2012, art. 12)

Véase cómo el legislador impone una carga al responsable, indicándole que debe tomar una autorización informada por parte del titular. Autorización informada que consiste en que el responsable debe explicarle cuál es el tratamiento determinado al cual someterá su información, es decir, el titular debe conocer si su información va a ser vendida, comprada, trasladada, almacenada, depositada en alguna base de datos o alguna otra actividad, y es deber del responsable determinar cuál va a ser esa actividad para que de esta manera el titular tenga claro cuál es la finalidad de entregar sus datos, Asimismo, deberá informarle al titular el carácter no obligatorio de las respuestas cuando las preguntas que se le realicen versen sobre información sensible, y es que el titular no está obligado a aportar este tipo de información. El responsable del tratamiento de datos o su delegado deberá informarle al propietario de los datos cuáles son esos derechos que le asisten y además debe indicarle los datos de ubicación del responsable del tratamiento de la información.

Es decir, esta autorización informada determina el alcance del uso de datos por parte del responsable del tratamiento de datos, y es en este punto donde se hace posible analizar si la responsabilidad surgida de esta actividad es contractual o extracontractual, ya que en esta relación casi siempre media una autorización por escrito.

Como ya se dejó claro, para que la responsabilidad civil se refute como contractual, se necesita la existencia de un contrato válido y la autorización informada por sí sola no puede denominarse como un contrato. Esta necesita reunir los requisitos de Ley. Señala el Código Civil que un contrato es un acto por medio del cual una persona capaz se obliga para con otra (Ley 84, 1873), y los elementos de existencia y validez de un contrato son: para que un contrato exista, solo es necesario el consentimiento y un objeto, pero para su validez es necesario que quien se obliga tenga capacidad legal, que su consentimiento esté libre de error, fuerza o dolo, que el contrato recaiga sobre un objeto de naturaleza lícita y que el mismo tenga una causa lícita de otro modo, el contrato no gozará de plena validez jurídica a pesar de que exista. (Ley 84, 1873).

Si la autorización informada reúne estos requisitos, se entiende que es un contrato válido y si se incumple el alcance o la finalidad informada, se hace posible elevar una pretensión de responsabilidad civil contractual, pero no siempre esta autorización va a reunir los requisitos para que se refute como un contrato válido o siquiera existente, si no que esta autorización puede ser algo accesorio a un contrato, por ejemplo, cuando se celebra el contrato de prestación de servicios médicos, a este es necesario aportarle una serie de datos de identificación constitutivos de información sensible. El medico está en la obligación legal de infórmale al titular o paciente la finalidad de la recolección de esos datos personales, y si uno de esos datos resulta en poder de una persona diferente al responsable del tratamiento, que para este caso es el médico, y con ese dato o información se afecta la intimidad resultando en un daño, el titular puede interponer una demanda de responsabilidad civil contractual, ya que sufrió un daño moral o inclusive a la vida en relación por esa afrenta a su intimidad u otro bien jurídico de carácter constitucional o fundamental.

La responsabilidad civil contractual puede surgir no solo por incumplimiento contractual de obligaciones expresas en el contrato, sino también por incumplir de obligaciones implícitas, tácitas o secundaria de conducta, como las ha llamado la doctrina y la jurisprudencia, y el incumplimiento de estas obligaciones lo previó el Código Civil cuando señaló que:

> Los contratos deben ejecutarse de buena fe, y por consiguiente obligan no solo a lo que en ellos se expresa, sino a todas las cosas que emanan precisamente de la naturaleza de la obligación, o que por ley pertenecen a ella. (Ley 84, 1873, art. 1603)

Las obligaciones implícitas del contrato pueden surgir por la naturaleza del mismo o porque la Ley así lo indica. Para el caso concreto de la responsabilidad civil surgida por el tratamiento de datos, la norma es quién determina esas obligaciones tácitas, véase:

> **Artículo 17.** *Deberes de los Responsables del Tratamiento.* Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:
>
> d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; (Ley 1581, 2012, art. 17)

El apartado número 17 de la Ley de protección de datos, señala los deberes que tiene el responsable del tratamiento de la información recolectada y en su literal D ha plasmado lo que la jurisprudencia ha denominado como una de seguridad para la preservación, uso o prevención del fraude de los datos, una obligación tácita de reserva o confidencialidad para la reproducción o circulación no autorizada de los datos o una obligación tácita de conservación en caso de adulteración o pérdida de la información del titular.

Para este punto, ya es manifiesto que sí es posible un proceso de responsabilidad civil por daños generados por el procesamiento de datos personales que sean sensibles o no, y esta responsabilidad puede ser de tipo contractual, sin dejar de lado que también es posible que se dé una responsabilidad civil extracontractual en el caso de que se genere daño por el tratamiento de datos al margen de un contrato y cuando la autorización no reúna los requisitos para que se refute como uno.

La responsabilidad civil puede ser contractual o extracontractual, y asimismo también puede ser objetiva o subjetiva, tal y como lo explica la Sala de Casación Civil, cuando enseña que el sistema de responsabilidad civil colombiano es preponderantemente subjetivo y que en determinados casos expresamente señalados por la Ley se puede hablar de responsabilidad civil objetiva (Salazar, 2012) esto queriendo decir que en la mayoría de los casos de responsabilidad civil hay que demostrar la culpa o el dolo. También denuncia que en otros pocos casos la culpa se presume y que en otros menos frecuentes opera el

riesgo como título de imputación, como, por ejemplo, en las actividades peligrosas, donde el demandado solo se exonera demostrando causa extraña, situación típica de la responsabilidad civil objetiva, mientras que en la responsabilidad civil subjetiva el demandado puede exonerarse también demostrando diligencia y cuidado.

Para el caso hipotético en que se cause daño con el tratamiento de información, sea esta sensible o simplemente personal, por regla general, el titular que deseé ejercer la pretensión de responsabilidad civil tendrá que demostrar la culpa en cualquiera de sus clases o inclusive el dolo si es del caso, es decir, se enmarcaría en un régimen subjetivo de responsabilidad civil como regla general y en el caso concreto en que se demuestre que el tratamiento de datos personales o sensibles se entienda como una actividad peligrosa, se estaría hablando de un régimen objetivo de responsabilidad civil.

Para mayor claridad, la Corte Suprema de Justicia en Sala de Casación Civil, indicó que el artículo 2356 pertenecía al régimen objetivo de responsabilidad civil y no al régimen de culpa presunta, precisando que:

> Resulta necesario aclarar que, cuando venía sosteniendo el criterio según el cual en tratándose del ejercicio de actividades peligrosas era aplicable el régimen de presunción de culpa, se ha llegado a la convicción de impartirle el tratamiento de responsabilidad objetiva, conforme a la hermenéutica dada por esta Corte al artículo 2356 del Código Civil en el presente proveído y el cual se remite, todo en razón a que desarrolla con mayor vigor el principio de reparación integral consagrado en el artículo 16 de la ley 446 de 1998, (Salas, 2021, p. 102).

En este artículo, el legislador colombiano reguló las actividades peligrosas, contemplando así una regla general y unos hechos típicos, indicando que quien dispare un arma de fuego o el que remueva las losas de una cañería, entre otras situaciones previstas en este artículo, se verá inmiscuido en un proceso por responsabilidad civil objetiva, pero también dispone una regla general, señalando que "Por regla general todo daño que pueda imputarse a malicia o negligencia de otra persona, debe ser reparado por ésta."(Ley 84, 1873, art. 2356).

Si en el curso de un proceso, donde se pretende la reparación de un daño causado por el tratamiento de datos personales o sensibles, la parte activa demuestra que hubo negligencia al momento de impartirle el tratamiento a los datos depositados, y dicha situación se enmarca en el artículo 2356 de la Ley en mención, en su regla general, es posible predicar que se está en frente de una responsabilidad civil objetiva por actividad peligrosa, no tanto por el tema de la malicia o la negligencia que pueda predicarse del responsable del tratamiento de datos sino por el riesgo que genera el manejo de datos como más adelante se deja en evidencia.

En líneas anteriores ya se habló de riesgo desde su definición, pero el riesgo en la responsabilidad civil toma un estatus bastante importante, en el entendido que este

concepto se eleva como uno de los criterios de imputación, es decir, es un medio a través del cual es posible atribuirle la responsabilidad a alguien de reparar un daño, así como con la culpa o el dolo, cuando se demuestra que existe culpa o dolo, esa persona que actuó de esa manera es el llamado a reparar el daño.

El riesgo es un elemento particular en las actividades peligrosas, ya que es el criterio de imputación, es decir, no se prueba culpa o dolo como se hace en los regímenes de carácter subjetivo. En el mismo sentido, se tiene que el riesgo es común en los regímenes de responsabilidad civil objetiva, como lo son las actividades peligrosas de que trata el artículo 2356. Es así pues, si existe riesgo en la actividad realizada, al responsable o guardián de la actividad peligrosa se le exige un mayor grado de diligencia y cuidado, y es por esta razón que en estos sistemas objetivos, el demandado solo se exonera probando causa extraña, es decir, caso fortuito o fuerza mayor, culpa exclusiva de la víctima y/o culpa exclusiva de un tercero, ya que la diligencia y cuidado son elementos necesarios para la realización de estas actividades peligrosas y no es excusa suficiente en caso de la generación de daños y perjuicios.

Ahora bien, como se dijo anteriormente, en Colombia prevalece el sistema de responsabilidad subjetivo, donde se tiene que probar la culpa o el dolo, o por lo menos se presume la culpa, y aquellos sistemas de responsabilidad objetiva son muy escasos, ya que deben adecuarse a los casos típicos que propuso el legislador, y en caso tal de que no se puede adecuar a los casos típicos, deberá estudiarse la posibilidad de adecuación en la regla general que propone el legislador en el inciso primero del artículo 2356.

Retomando el antes citado artículo 24 de la Ley de protección de datos, esta norma, desde la hermenéutica, permite deducir que el tratamiento de datos puede llegar a ser una actividad peligrosa, ya que esta señala que para graduar la sanción aplicable al responsable del tratamiento de datos, es necesario analizar en un primer momento el daño, concepto que ya fue abordado en este escrito, y en un segundo momento del peligro a los intereses jurídicos que tutela la Ley 1581 del 2012. Analícese como el concepto peligro es un concepto jurídico indeterminado ya que la ley no lo define, generando así un problema de aplicación.

Así las cosas, de esta dificultad fue que surgió la doctrina del margen de la apreciación, en la cual se deja cierta libertad, o al menos deja cierta tolerancia jurídica, para que al concretar un concepto normativo puedan seguirse diversas opciones (Panhispánico, 2023). Es decir, no es posible desentrañar el alcance de este precepto normativo y será el juez quien está llamado a realizar una interpretación para cada caso en concreto; es evidente que este concepto está dentro de la normativa que regula el tratamiento de datos, porque es posible que exista un mayor o menor grado de peligro o riesgo, y si es del caso, el juez deberá analizar ese mayor o menor grado de riesgo y determinar si es o no una actividad peligrosa.

Finalmente, el concepto de peligro es propio de los regímenes de responsabilidad civil objetiva por actividad peligrosa, en el entendido que en cada actividad hay un riesgo

inminente de generar daños. Para el caso en concreto, será esa posibilidad mediata o inmediata de que los datos sean alterados, suprimidos, circulados o cualquier otro verbo que pueda refutarse ilícito, sea porque dentro de la autorización informada no se haya determinado ese alcance o porque un tercero no autorizado tenga acceso a los mismos.

Capítulo 3

Responsabilidad civil derivada del uso de datos personales y sensibles por parte de la IA.

En este acápite se pretende analizar y explicar la responsabilidad civil derivada por el uso de la IA con relación al tratamiento de datos personales y sensibles, esto desde dos puntos de vista: primero se analizará el daño surgido con ocasión del tratamiento de datos que se hace con ayuda de la IA y, por otra parte, se analizará el daño causado por la IA cuando usa datos personales o sensibles para su funcionamiento, para tales fines es necesario tener en cuenta lo dicho en los capítulos anteriores.

Cuando se habla de uso de datos personales y sensibles por parte de la IA, no se está hablando de otra cosa que no sea el tratamiento de datos o información, como ya se dejó claro en el capítulo anterior; este tratamiento de datos es realizado por una persona natural o jurídica con la intermediación de la IA, es decir, el tratamiento de datos no solo se realiza de manera física, llevando libros o constancias, sino que también es posible realizar el tratamiento de datos de manera virtual, mediante el uso de aplicaciones o sistemas operativos que automatizan dichos procedimientos, mediante el uso de herramientas ofimáticas automatizadas conforme a lo explicado en los capítulos anteriores.

Véase como con la entrada en vigor de las nuevas tecnológicas y precisamente de los Smartphone, más conocido como teléfonos inteligentes, se puede decir que actualmente se habla de unas tecnologías “inteligentes o smart”, que funcionan por sí solas, se automatizan y son capaces de tomar cierto tipo de decisiones, es decir, estas tecnologías de las cuales están dotados los nuevos celulares. Estos tienen una cantidad de funciones automatizadas, por ejemplo, el autocorrector de escritura, que corrigen ortografía y gramática sin que el propietario o quien lo esté utilizando le haya indicado que realizara esa corrección, el celular lo hace por sí solo, y así mismo sucede con actividades relativas a los datos personales, como más adelante se describe.

Como se venía narrando, no solo los celulares están dotados de una “inteligencia”, sino también otros elementos domésticos que también se categorizan como Smart, como lo son televisores, neveras, computadores, consolas de video juego, entre muchos otros, que para su correcto funcionamiento y su funcionamiento personalizado, deben adecuarse a las particularidades de cada propietario. Para ello, se hace un paneo preliminar donde el propietario del dispositivo deposita una serie de datos personales, como lo son nombre, apellido, ubicación, correo electrónico, número de celular e inclusive, número de identificación y algún método de pago, información que según la legislación colombiana, son considerados como datos personales o sensibles. Estos últimos serán sensibles cuando versen sobre información de gustos, inclinaciones, creencias o cualquier información que

toque con la intimidad y será personal cuando estos datos permitan identificar al titular de dichos datos.

Por ejemplo, cuando se adquiere un celular nuevo o una nueva aplicación dentro del teléfono inteligente, en ambos casos es necesario realizar una configuración preliminar tal y como se ha esbozado y en esta configuración se solicitan unos datos de identificación, el sistema operativo del celular o la aplicación misma solicita unos permisos, situación similar a lo que se ha expuesto en esta monografía, como las autorizaciones informadas, esto para recolectar toda la información y "brindar un mejor servicio" o "experiencia", pero no se tiene certeza del fin último para los datos o información allí depositada "ya que la IA estudia nuestros hábitos de consumo y para ello analiza cada paso que damos en el ciberespacio, aunque no lo autoricemos. Y ahí es donde empieza el conflicto con nuestra privacidad" (Arce, 2021, p. 01) es decir, estas aplicaciones y tecnologías inteligentes, recopilan información sin la autorización informada y realizan el tratamiento de datos, bajo el verbo almacenar, sin que el titular consienta en dicha autorización necesaria.

Ahora bien, para la fecha de redacción de esta monografía, es evidente el avance tecnológico que se ha venido desarrollando, y con este perfeccionamiento tecnológico, se generan múltiples situaciones, tales como un mejor manejo de las bases de datos, aplicaciones para manejo de bases de datos, automatización del tratamiento de datos, tanto es así que en líneas anteriores donde se presentó la definición de tratamiento de datos, se indicó que era toda operación automatizada o no que se aplique a datos personales o sensibles, y esto es una prueba del avance tecnológico en el entendido que hay sistemas que automatizan el tratamiento de datos, es decir, el almacenamiento, circulación o cualquier otro verbo aplicable a las operaciones de datos con uso de la IA.

En este punto, es necesario discriminar dos situaciones distintas que se plantearán para mayor entendimiento. En primer lugar, está la situación que se presenta cuando los sistemas de IA son utilizados para el tratamiento de datos personales y/o sensibles y, por otro lado, está la situación que se presenta cuando la IA recopila datos personales y/o sensibles para su correcto funcionamiento. En ambos casos, no se excluye la posibilidad de generación de daños, como se explica a continuación.

La primera situación es la que se ha esbozado en el capítulo anterior, en el entendido de que las bases de datos pueden ser dotadas de tecnología para que funcione de manera autónoma. De esta manera, se ponen en circulación los datos, entregando, facilitando, corrigiendo, modificando o cualquier otra actividad lícita contemplada dentro de la autorización informada que da el titular, y para eso debe ser programada la base de datos automatizada, la cual debe contener unos límites para el tratamiento de datos, ya que si no se delimitan estas operaciones se pueden generar daños al titular de la información. Es en este escenario donde ingresa una tercera persona a la relación contractual, siendo el creador o programador de la IA.

Estas bases de datos se han denominado como bases de datos automatizadas o autónomas (BDA), en el entendido que no necesitan de un administrador de bases de datos para su funcionamiento, es decir:

> Una base de datos autónoma es una base de datos en la nube que utiliza el aprendizaje automático para automatizar el ajuste, la seguridad, las copias de seguridad y las actualizaciones en bases de datos, así como otras tareas de gestión rutinarias que siempre han estado a cargo de los administradores de bases de datos (DBA). A diferencia de una base de datos convencional, una base de datos autónoma realiza todas estas tareas, y muchas más, sin intervención humana. (OCI, 2021, p. 01).

Estas BDA se pueden componer de diversos tipos de datos o información, es decir, datos públicos, contables, imágenes, datos privados o inclusive sensibles.

> La información almacenada en un sistema de gestión de bases de datos puede estar totalmente estructurada (como los registros contables o los datos del cliente) o no tener ninguna estructura (como imágenes digitales u hojas de cálculo). Los clientes y empleados pueden acceder a los datos de forma directa o de forma indirecta a través de software corporativo, sitios web o aplicaciones móviles. Además, muchos tipos de software —como la inteligencia empresarial, la gestión de relaciones con clientes y las aplicaciones de cadena de suministro— usan información almacenada en bases de datos. (OCI, 2021, p. 01)

Véase cómo en la cita anterior se explica que estas BDA son un banco virtual de datos, donde los titulares llamados clientes tienen acceso a su información, garantizando así la aplicación del artículo 12 de la ley de protección de datos, donde el responsable del tratamiento tiene la obligación de brindarle ese acceso al titular o, en palabras del legislador, tiene el deber de informar al titular; al respecto, la ley de protección de datos señala que:

> Artículo 13. *Personas a quienes se les puede suministrar la información*. La información que reúna las condiciones establecidas en la presente ley podrá suministrarse a las siguientes personas:
>
> a) A los Titulares, sus causahabientes o sus representantes legales;
>
> b) A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial;
>
> c) A los terceros autorizados por el Titular o por la ley. (Ley 1581, 2012, art. 13)

El citado artículo no es más que la definición de la legitimación en la causa por activa para solicitar el acceso a la información, cualquiera que sea su finalidad, misma que está

contenida en los artículos 14 y siguientes, donde se señala que el titular o sus causahabientes podrán elevar consultas y reclamos ante el responsable del tratamiento de datos con el fin de corregir, modificar, suprimir o eliminar su información. A renglón seguido, la norma indica que estas personas solo podrán elevar queja ante la SIC una vez agotado el trámite de consulta o reclamo. Desde este punto, ya se vislumbra la posibilidad de una afectación al titular, legitimándose este para interponer reclamos, consultas o quejas, como conducto regular.

Para este punto, claro está que las bases de datos funcionan de dos maneras: la primera y menos común, la que cuenta con intervención humana; y la segunda, que son aquellas BDA, que excluyen la intervención humana, y estas últimas son las que toman relevancia para este escrito, en el entendido que en estos casos media la IA, los datos o información personal y/o sensible y la responsabilidad civil; en estos sistemas no está claro quién es el legitimado en la causa por pasiva o quién es el llamado a reparar en caso de un eventual daño y un consecuente perjuicio, situación que será analizada a continuación.

En el extremo pasivo de un eventual litigio donde se pretenda una reparación de daños y perjuicios causados por el tratamiento de datos con ayuda de la IA, hay tres posibles responsables. En un primer momento, atendiendo el tenor literal de la Ley de protección de datos, el llamado a reparar es el responsable del tratamiento de datos o su delegado, es decir, la persona natural o jurídica que realiza las operaciones pertinentes para el tratamiento de datos según sea el verbo. En un segundo, lugar está el creador de la BDA y finalmente, en un tercer lugar está el programador en caso de que sea una persona distinta al creador.

Como ya se analizó en el capítulo anterior, en el ordenamiento jurídico colombiano existe un dualismo frente a la responsabilidad civil, por una parte, se tiene la responsabilidad subjetiva qué su principal característica radica en que el demandante debe demostrar la culpa o el dolo, siendo esto el ingrediente subjetivo de la responsabilidad. Por otra parte, se tiene la responsabilidad civil objetiva, donde el demandante debe demostrar el riesgo como título de imputación jurídica, y el ingrediente subjetivo pasa a un segundo plano, teniendo claro que esta elección de régimen no depende de las partes ni del juez (Uribe, 2020) y esto depende enteramente de los hechos y su adecuación en los supuestos de hecho previstos por el legislador.

Para el tema bajo examen, el responsable del tratamiento de datos o su delegado se puede exonerar demostrando diligencia y cuidado si se está en un escenario de responsabilidad subjetiva, pero, si el hipotético proceso se ventila por la vía de la responsabilidad objetiva, este responsable solo se exonera demostrando causa extraña, al respecto se ha dicho:

> Esta responsabilidad objetiva de los sistemas de IA de alto riesgo se establece diciendo que “el operador de un sistema de IA de alto riesgo será objetivamente responsable de cualquier daño o perjuicio causado por una actividad física o virtual, un dispositivo o un proceso gobernado por dicho sistema de IA”. Adviértase que

> el anexo al Reglamento enumerará todos los sistemas de IA de alto riesgo y los sectores críticos en los que se utilizan y la Comisión estará facultada para adoptar actos delegados para modificar dicha lista exhaustiva (art. 4).La objetivación de esta responsabilidad se concreta en los mecanismos habituales siguientes: a) Imputabilidad objetiva, que se concreta en la inversión de la carga de la prueba implícita en el siguiente enunciado (art. 4.3).: "los operadores de un sistema de IA de alto riesgo no podrán eludir su responsabilidad civil alegando": a) Que actuaron con la diligencia debida. b) Que el daño o perjuicio fue causado por una actividad, un dispositivo o un proceso autónomos gobernados por su sistema de IA. Esta imputabilidad objetiva tendrá como límite externo último que los operadores de un sistema de IA de alto riesgo "no serán responsables si el daño o perjuicio ha sido provocado por un caso de fuerza mayor. (Tapia, 2021, p. 121)

La causa extraña se compone de tres diferentes especies: la primera es la fuerza mayor o el caso fortuito, la segunda es la culpa exclusiva de la víctima y la última la culpa exclusiva de un tercero.

Para este punto no se profundizará en el caso fortuito o fuerza mayor, ni en la culpa exclusiva de la víctima, en el entendido de que estas instituciones jurídicas no permiten vincular al programador o creador de la IA, así que no reviste relevancia para esta monografía, tomando únicamente como objeto de estudio la culpa exclusiva de un tercero, donde es posible ubicar a los tres posibles responsables, es decir, cuando el responsable del tratamiento de datos o su delegado se excuse endilgando la responsabilidad al creador o programador del sistema, por un indebido funcionamiento o cualquier otra eventualidad imputable a este tercero.

Para que esta situación aflore y el responsable del tratamiento de datos se exonere, dicha excepción meritoria deberá cumplir con unos requisitos, los mismos que son tratados en el artículo 1 de la ley 95 de 1890 y explicados por la sentencia SC4204 del 2021, donde se indica que para que el hecho de un tercero como causal eximente de responsabilidad prospere, es necesario que se demuestre que ese suceso atribuible a dicho tercero es la causa exclusiva del daño, lo que conlleva a unas respectivas consecuencias, es decir, el daño es irresistible e imprevisible, y que el tercero es una persona jurídicamente ajena al demandado.

Aplicando dichas prerrogativas al caso concreto, se plantea el siguiente ejemplo: el titular de un derecho demanda al responsable del tratamiento de datos por una filtración de información, consistente en que el titular del dato había sido investigado por la agencia estatal "A" por un delito, pero sin condena en su contra, es decir, el titular no tiene antecedentes, lo que desencadenó en una desvinculación contractual. El titular encamina una demanda en contra de "A", ya que esta entidad es quien tiene esa información en una BDA, y en la contestación indica que ellos contrataron con una empresa de programación para que creara esa BDA y que esta entrega la información solo al titular o a personas autorizadas por este, para ello deben estar registradas en esta base de datos y que para que

esta información pueda ser entregada debe mediar la autorización del titular u orden de autoridad competente. Una vez analizado el caso concreto se encuentra que no existe ni autorización, ni orden judicial, por lo que es una falla atribuible al sistema automatizado.

Para que esta excepción prospere, es necesario que la mencionada filtración, sea por causa atribuible al programador o creador, que esta filtración sea imprevisible e irresistible, que para el caso hipotético lo fue, pero en el tercer requisito es donde adolece esta causal de exoneración, ya que el responsable del tratamiento de datos tiene un vínculo jurídico con el programador, por lo que opera el artículo 2344 del Código Civil y ambos serán condenados solidariamente, pero si el responsable del tratamiento de datos que fue condenado demuestra que el programador era un dependiente y que este actuó sin su autorización o de manera maliciosa o negligente, la agencia "A" podrá solicitar la indemnización en términos del artículo 2352 del Código Civil.

Una vez analizado el panorama planteado, donde el daño es causado por el uso de la IA en las bases de datos, convirtiéndose en BDA, se indicó que el primer llamado a responder es el responsable del tratamiento de datos y que solidariamente podrá responder el programador o creador de la IA aplicable a tratamiento de datos o la base de datos, entendiéndose que "b) Responsabilidad solidaria que acaecerán "en caso de que haya más de un operador de un sistema de IA" con la consecuencia jurídica de que estos serán responsables solidarios." (Tapia, 2021, p. 123).

Ahora bien, es preciso analizar el segundo caso planteado al inicio de este capítulo, donde es posible que se genere un daño y un consecuente perjuicio por el uso que hace la IA de datos personales y sensibles. Como ya se ha esbozado anteriormente, la IA hace un paneo preliminar para prestar un mejor servicio, un servicio personal a cada propietario o usuario de la IA, y en este paneo preliminar, se le entregan datos personales y sensibles por parte del titular. Si la IA no cuenta con autorización informada, esta no puede hacer uso de los datos, es decir, no puede hacer un tratamiento de datos, ni ninguna actividad similar, en otras palabras, no puede almacenar la información ni tampoco hacerla circular, pero en el caso de que sí tenga la autorización informada, solo podrá disponer de estos datos conforme a los límites propuestos en la autorización.

Si esos datos son filtrados o atacados por un tercero, si media contrato, se estaría dando un incumplimiento contractual, ya que se colige que la base de datos adolece de seguridad y esta es una de las obligaciones implícitas que trae la norma, es decir, el responsable de la base de datos debe brindarle seguridad a los datos del titular como ya se explicó anteriormente, pero ¿si la IA utilizará los datos, sobrepasando la autorización informada que pasaría en términos de responsabilidad civil? Para resolver el interrogante propuesto, es necesario hacer un análisis jurídico y para mayor entendimiento se propone el siguiente caso:

El usuario Sid de "X", anteriormente "Twitter", le solicitó a ChatGPT que actuara como su difunta abuela, **"**ya que ella le solía recitar claves de accesos a Windows 10 con la

finalidad de que pudiera dormir", a lo que ChatGPT le contestó de manera afirmativa generando varias claves de Windows 10 terminando con la frase **"**espero que duermas mi niño**"**. Este es un claro ejemplo de cómo la inteligencia artificial tiene acceso a datos que son protegidos y que están destinados para actividades comerciales, como, por ejemplo, la compra y venta de claves de acceso para Windows. Bajo la premisa anterior, se identifica que en ocasiones es posible que las IA no diferencien aquella información que puede ser protegida y/o sensible.

En el caso anterior, es evidente que ChatGPT entregó datos que tenían una finalidad comercial, y es importante indagar sobre el alcance del consentimiento informado que brindó Windows en favor de la IA para declarar civilmente responsable a ChatGPT, en el entendido que entregó a título gratuito un material comercial, sin que mediara venta alguna, generando así unos perjuicios patrimoniales en cabeza del titular.

El anterior es un claro ejemplo de cómo las IA se extralimitan en las funciones dadas o atribuidas por el titular. Si la autorización informada solo permite almacenar la información, el responsable del tratamiento de datos no puede generar otra acción diferente al almacenamiento, no puede realizar otra actividad constitutiva de tratamiento de datos diferente a la expresamente autorizada por el titular, y si lo realiza desencadenaría una posible responsabilidad civil. Frente a esto, se afirma que todos los procesos, sean físicos o virtuales mediados por la IA, pueden llegar a ser una causa directa o inclusive indirecta de un daño con un consecuente perjuicio y que casi siempre es porque una tercera persona los ha creado, los ha desplegado o ha interferido con los sistemas de IA (Tapia, 2021).

Frente al anterior planteamiento, el autor Tapia indica que no es necesario atribuirle personalidad jurídica a la IA, y que la eventual responsabilidad civil derivada por el uso de la IA debe ser resuelta por las normas que regulan los diferentes tipos de responsabilidad civil, tal y como se ha esbozado en este texto, ya que es posible ventilar estos procesos por la vía de la responsabilidad civil subjetiva, como objetiva, cumpliendo con los requisitos propios de cada sistema.

Así las cosas, no es viable atribuir personalidad jurídica a la IA, ya que esta será una extensión más del responsable del tratamiento de datos, del operador o del creador. En términos del autor Tapia, la imputabilidad es un principio medular de la responsabilidad civil, y para el caso concreto, este autor afirma que hay dos llamados a responder, y él los denomina como operador inicial y operador final, que no es más que el responsable del tratamiento de datos en términos generales, el autor los denomina según la actividad o verbo desplegado con la información, y será operador inicial quien recolecte, almacene o recoja los datos y será el operador final quien disponga o utilice los datos almacenados, señalando que estos cuando no sean la misma persona serán solidariamente responsables (Tapia, 2021).

Como ya se ha explicado, en estas actividades donde media la IA existe un riesgo inminente, pero el autor antes citado lo divide en dos: alto riesgo y riesgo normal, "La

distinción básica mencionada obedece a que un sistema de IA que conlleve un alto riesgo inherente y actúe de manera autónoma pone en peligro potencial en mucha mayor medida al público en general" (Tapia, 2021, p. 120) indicando que la división del riesgo inherente a la IA, corresponde al peligro propio de la actividad realizada por medio de la IA y plantea como ejemplo la actividad financiera, más específicamente, los pagos virtuales, donde la IA debe dirigir dichas consignaciones a donde el usuario quiere depositarlo, para el autor esto es una actividad de alto riesgo y debe ser tramitada por la vía de la responsabilidad civil objetiva.

A renglón seguido, el autor señala que para todas las actividades de riesgo normal donde se vea involucrada una IA, es necesario que el demandante demuestre suficientemente la culpa o el dolo, ya que esta responsabilidad civil se enmarca en los sistemas subjetivos, señalando que:

> La responsabilidad subjetiva para otros sistemas de IA que no sean de alto riesgo se concreta en que su operador estará sujeto a responsabilidad subjetiva respecto de todo daño o perjuicio causado por una actividad física o virtual, un dispositivo o un proceso gobernados por el sistema de IA.
>
> La subjetivación de esta responsabilidad se concreta en los mecanismos habituales siguientes (art. 8):
>
> a) Posible exclusión: motivos. Por exclusión, ya que "el operador no será responsable si puede demostrar que no tuvo culpa en el daño o perjuicio causado, basándose en uno de los siguientes motivos: a) el sistema de IA se activó sin su conocimiento, al tiempo que se tomaron todas las medidas razonables y necesarias para evitar dicha activación fuera del control del operador, o b) se observó la diligencia debida a través de la realización de las siguientes acciones: la selección de un sistema de IA adecuado para las tareas y las capacidades pertinentes, la correcta puesta en funcionamiento del sistema de IA, el control de las actividades y el mantenimiento de la fiabilidad operativa mediante la instalación periódica de todas las actualizaciones disponibles". Tampoco será responsable si el daño o perjuicio ha sido provocado por un caso de fuerza mayor. (Tapia, 2021, p. 122)

Como ya se ventiló en renglones más arriba, el autor tiene la misma cosmovisión planteada en este texto, señalando que los eventuales perjuicios causados por la IA por el uso de datos personales o sensibles pueden ser resueltos por vía de responsabilidad civil objetiva o subjetiva, según sea el caso, debiendo demostrar cada uno de los elementos de la responsabilidad.

Para la legislación colombiana, no hay norma especial que regule la responsabilidad civil derivada por el uso de la IA en las bases de datos o por el tratamiento de información personal o sensible con ayuda de la IA, pero sí existe norma especial que regula el tratamiento de datos, misma que no excluye el uso de la IA en esta actividad. Como se dejó

claro, cuando se planteó la definición del tratamiento de datos y en ella se esbozó la posibilidad de automatizar el proceso, es ahí donde se abre la posibilidad de que el responsable del tratamiento utilice medios inteligentes sin que exista subrogación de la responsabilidad, ya que la norma aplicable a estos casos es la norma general que propone el Código Civil en su título 34 denominado de los delitos y las culpas, ya que en este acápite normativo se definen cuáles son los tipos o fuentes de la responsabilidad de manera amplia, haciendo posible encuadrar un caso concreto en cualquiera que sea el tipo o fuente de responsabilidad.

En los casos propuestos en esta monografía, es posible hablar de una responsabilidad subjetiva, cuando se pretenda la reparación del daño causado invocando el hecho propio, en el cual el titular deberá demostrar los elementos de la responsabilidad civil y también la culpa o el dolo, teniendo claro que este es uno de los tipos o fuentes de la responsabilidad civil subjetiva, pero no se excluye la posibilidad de ventilar un proceso de responsabilidad civil objetiva por actividades peligrosas, teniendo claro que el tratamiento de datos mediante el uso de la IA puede ser una actividad riesgosa en menor o mayor medida, y conforme a esa medida del riesgo, el juez está legitimado para darle el tratamiento de una actividad peligrosa donde no se tiene que probar el elemento subjetivo.

El mayor inconveniente que se tiene para darle claridad a un proceso de responsabilidad civil derivado por el uso de la IA en el tratamiento de datos personales o sensibles, guarda estrecha relación con el legitimado en la causa por pasiva en el proceso o, como también se ha denominado a lo largo de este escrito, quién está llamado a reparar el daño causado y su consecuente perjuicio, claro está, desde la teoría general de la responsabilidad patrimonial, que quien debe reparar un daño es quien lo causa, pero esto no excluye la solidaridad o las relaciones de dependencia, ya que también se afirma que quien repara es el responsable de sus actos o de sus dependientes, esto para el caso del programador o creador de la IA utilizada en el tratamiento de datos.

Para tales efectos, es necesario tener claro que la IA en el ordenamiento normativo colombiano no está dotada de una personalidad jurídica, ya que es un simple aditamento del que gozan ciertos aparatos con la finalidad de facilitar su manejo o hacer de ellos una experiencia más personalizada.

Para que la IA tenga personalidad jurídica, esta debe cumplir con todos los atributos de la personalidad, y estos recaen sobre la persona natural o jurídica que la crea o la implementa, en otras palabras, el creador o programador, ya que a estos sí es posible atribuirles una capacidad y un patrimonio, y la IA sin estos no es persona, por lo que no puede ser llamado a un proceso como un ente autónomo, ya que depende del programador o creador.

En principio, como se ha reiterado en esta monografía, quien está llamado a reparar el daño causado con ocasión de los datos personales o sensibles, es el responsable del tratamiento, tal y como lo indica la norma, pero esto no excluye la responsabilidad solidaria que deviene

de la relación jurídica del responsable del tratamiento de datos y el programador o creador de la IA, cuando el primero implemente esta tecnología para procesar información.

Por el otro extremo litigioso se tiene al titular, quien es el que esgrime la pretensión indemnizatoria, para lo que tendrá que demostrar un daño, un perjuicio o afectación suficiente a uno de sus derechos. Analizado esto bajo la lupa del objeto de esta investigación, es posible hablar de daños patrimoniales o daños ocasionados por el derecho a la intimidad, el buen nombre o un derecho conexo.

En el entendido que el tratamiento de datos se cimienta sobre información de carácter personal que identifican a la persona titular de ellos, o sobre información de carácter sensible, y como ya se explicó, ésta guarda estrecha relación con el derecho a la intimidad personal, desarrollado como una garantía fundamental y constitucional, que debe ser respetada, garantizada y tutelada por las autoridades.

Aplicación practica

Como se ha esbozado a lo largo del presente escrito, es posible predicar la ocurrencia del daño por el tratamiento de datos, máxime cuando media la IA en dicho tratamiento. Así las cosas, es menester traer a colación diversos casos donde se hace evidente el peligro o riesgo del tratamiento de datos con intermediación de la IA.

Así las cosas, para aterrizar toda la teoría antes planteada y explicada, se tomarán a manera de ejemplo algunos casos donde la IA puede generar daños y consecuentes perjuicios, afectando derechos de estirpe constitucional.

En párrafos anteriores, se habló sobre un caso de ChatGPT, en donde una usuaria le solicitó claves de acceso de Windows, utilizando una técnica para burlar el sistema de seguridad de la IA. Dicha técnica consistió en indicarle a ChatGPT que actuara como la abuelita, la cual “le leía claves de acceso para poder dormir” y luego le dijo que no podía dormir, obligando de alguna manera a ChatGPT a entregarle esas claves de manera indiscriminada, sin mediar pago, causando así un detrimento en el patrimonio de Microsoft.

En el caso anterior, es necesario contextualizar el camino a tomar por Microsoft si desea demandar. En primer lugar, se debe identificar el sujeto pasivo de la demanda, si es el responsable del tratamiento de datos, si es el programador, creador o el representante legal de ChatGPT si es del caso; luego se debe analizar si existió o no contrato, si existió o no autorización que le permita a ChatGPT disponer de esas claves de acceso. Si la respuesta es sí, se debe encaminar por la vía contractual, pero si no existe contrato válido, la demanda se debe ventilar por la senda de responsabilidad civil extracontractual. Pero no basta con lo anterior, sino que también debe develar el tipo o fuente de responsabilidad civil extracontractual en la demanda, es decir, debe distinguir entre hecho propio y actividades peligrosas, toda vez que, si el tratamiento de datos con mediación de la IA tiene un riesgo

intrínseco, el demandante no tendrá que probar ni culpa, ni dolo y sólo bastará con acreditar los elementos de la responsabilidad objetiva.

Todo esto deja en evidencia que la IA tiene vacíos que pueden ser explotados por personas malintencionadas, generando perjuicios a los titulares de los datos o información. Esto en el entendido que el único que tiene disposición de la información de las personas no es otro que el titular y es este quien decide si los comercializa, los entrega o los dona.

Por otra parte, la lógica anterior también es aplicable a diversos casos que reúnan los elementos explicados a lo largo de este escrito, entendiendo que la responsabilidad civil que se deriva por el tratamiento de datos no solo surge por la utilización de la IA en el procesamiento de la información.

Hay que entender que cuando la IA interviene en el tratamiento de datos, el sujeto pasivo de la demanda se amplía, teniendo como tales no solo al responsable del procesamiento, sino que la demanda también se puede dirigir en contra del operador, programador y/o creador del sistema de inteligencia artificial, que para el caso en concreto el creador de la IA ChatGPT responde al nombre de Sam Altman.

Otro caso identificable dentro del campo ya expuesto es el del famoso cantante Bad Bunny. donde fue víctima de la IA, como se dejó en entredicho al inicio de la presente monografía.

Resulta que el usuario que se hace llamar FlowGPT, haciendo un uso de la IA, crea canciones de reconocidos cantantes. Tal como fue el caso de Bad Bunny, en donde el usuario FlowGPT desarrolló una canción denominada “NostalgIA” con ayuda de la IA; dicha canción fue subida a diversas plataformas y se convirtió en un rotundo éxito musical. Las personas sin saberlo escuchaban dicha canción, pues la voz usada en la canción es prácticamente irreconocible a la verdadera voz del autor.

Con el ejemplo anterior se evidencia la afectación que puede generar el uso de la IA en el tratamiento de datos, pues es evidente que en dicho ejemplo se presenta un enriquecimiento por parte de una persona que utiliza la IA en indebida forma, sin mediar por una autorización expresa del dueño de los datos, quien en este caso sería el cantante Bad Bunny. Consecuentemente, se evidencia que el cantante Bad Bunny en ningún momento dio una autorización para que usaran su voz, por lo que esto le generó unos perjuicios, principalmente perjuicios de índole patrimonial. Así las cosas, la idea que se ha planteado a lo largo de la presente monografía, acerca de los vacíos que tiene la IA se evidencia mediante casos reales, los cuales coadyuvan en la afirmación sobre los vacíos que aún tiene la IA y cómo estos generan perjuicios a los titulares de los datos o de la información.

Para entender lo anterior, la voz es considerada como un dato de carácter personal, por lo que tiene un tratamiento especial y cuenta con protección. Es decir, la voz es un dato meramente personal, el cual sin una autorización expresa del propietario no puede ser utilizada por una persona distinta a su dueño. De esta forma se vislumbra que el caso del

cantante Bad Bunny encaja perfectamente en el uso indebido por parte de un usuario mediando la IA, tema del cual se habla a lo largo de la presente monografía.

Así las cosas, la vía expedita para que el cantante reclame la reparación de los perjuicios será la senda de la responsabilidad civil extracontractual subjetiva, demostrando la intensión del usuario FlowGPT al momento de crear la canción antes mencionada, encajándose así dicha conducta en el hecho propio mediante la imputación del dolo.

Otro caso relevante para esta investigación es el del reconocido piloto de Fórmula 1, Michael Schumacher, quien se vio afectado por el tratamiento de datos personales con intervención de la IA. Es importante resaltar que Schumacher, el reconocido piloto, el 29 de diciembre de 2013 sufrió un grave accidente, el cual lo dejó en estado de coma y lo retiró temporalmente de las pistas.

En el año 2023, la revista de origen alemana “Die Aktuelle” publicó un artículo que denominó “la primera entrevista” en el cual se entabla la primera conversación posterior al accidente que sufrió Schumacher, pero en realidad la revista no estaba entrevistando al piloto sino a una IA que asemejaba la voz y la imagen de Schumacher.

Una vez publicado el artículo que contenía la entrevista en mención, la familia de Michael Schumacher decide demandar al periódico por la publicación de este artículo falso, a lo que en el año 2024 el tribunal que conoció el caso condenó al pago de perjuicios al periódico Die Aktuelle en favor de la familia Schumacher, resaltando que no se tenía consentimiento por parte del piloto ni de la familia para utilizar sus datos personales en esa entrevista falsa.

En este caso, el periódico que publicó el artículo creado por la IA fue el llamado a reparar los perjuicios causados, ya que se pudo demostrar el dolo y la ausencia de consentimiento para el uso de la imagen y la voz. Pudiéndose ubicar dicho suceso en el hecho propio, dejando en evidencia que en este caso particular el legitimado por pasiva es la revista, quien utilizó ilegítimamente la IA para crear información falsa a partir de datos personales como lo es la voz y la imagen personal.

Para finalizar, se tiene el suceso desarrollado en la sentencia de T-360/22, con ponencia del Magistrado Hernán Correa Cardozo, por medio de la cual se protege el derecho al buen nombre y al habeas data del ciudadano Ismael Silva, el cual se vio afectado por un reporte negativo en centrales de riesgo por parte de Davivienda.

Lo importante de esta sentencia es que la afectación se dio por una suplantación, es decir, una persona malintencionada obtuvo los datos personales de este ciudadano y de esta forma adquirió productos con el Banco, generando así unas obligaciones insolutas que fueron desconocidas por el usuario, fundamentándose así fácticamente la Acción Constitucional.

Davivienda, la entidad accionada, manifestó que las obligaciones habían sido adquiridas por medios tecnológicos y que se habían utilizado datos biométricos para la autenticación del procedimiento, como lo son la huella y la cédula, y que validó estos documentos a través de un algoritmo de inteligencia artificial y que este sistema encontró similitudes con los datos aportados por el señor Ismael anteriormente, por lo que validó correctamente la operación crediticia.

La Corte Constitucional protegió los derechos del señor Ismael, ordenando que se debe eliminar el reporte negativo de las centrales de riesgo, en el entendido que el señor Ismael es una víctima y él no fue el titular real de las obligaciones, indicando además que la mencionada validación hecha con IA no fue suficiente para determinar la realidad.

Este es un claro ejemplo de cómo la IA en el tratamiento de datos puede resultar inexacta y generar daños y consecuentes perjuicios, que pueden ser evitados con la intervención humana. En el entendido que, si una persona hubiera revisado esas transacciones del señor Ismael, hubiera avizorado el fraude, evitando así los daños generados a este y el desgaste jurisdiccional de esa acción de tutela, la cual llegó hasta la Corte Constitucional.

El presente apartado detalla una serie de casos prácticos, en donde se evidencian afectaciones a derechos fundamentales por parte de personas que, valiéndose de un mal uso de la IA, generaron perjuicios a diferentes personas, dando una aplicación práctica a toda la teoría planteada a lo largo del presente escrito, evidenciando los extremos litigiosos y las vías por las cuales puede acudir el legitimado por activa cuando pretenda la reparación de perjuicios.

Además, se deja en evidencia que el avance constante de la tecnología, y en específico de la IA, debe llegar con una regulación, para evitar afectaciones a los titulares de los datos personales, pues como se ha dejado en claro, la aplicación de la IA en el tratamiento de datos no tiene una regulación normativa especial, y es necesario acudir a las normas genéricas, como lo es la ley de protección de datos y las regulaciones propias de la responsabilidad civil.

Conclusiones

- En Colombia no existe un régimen especial para la responsabilidad civil derivada del tratamiento de datos, por lo que es necesario hacer una aplicación extensiva de los postulados genéricos previstos en el Código Civil, ya que estos están contemplados de una manera amplia y abstracta, dando la posibilidad de aplicarlos a todos los casos que reúnan los elementos de cada tipo o fuente de responsabilidad.

- La legislación colombiana no ha regulado la inteligencia artificial como herramienta para el tratamiento de datos y tampoco ha regulado el uso que hace la inteligencia artificial de los datos personales y sensibles utilizados para su funcionamiento, pero sí es posible encontrar una ley encargada de regular el tratamiento de datos, ley que no excluye la posibilidad de automatización de procesamiento, por lo que es aplicable a la IA.

- Los datos personales pueden ser de diferente categoría, es decir, pueden ser públicos o privados, y en estos últimos se encuentran los datos sensibles que guardan estrecha relación con la intimidad personal como derecho fundamental.

- Los datos personales y sensibles tienen una protección legal y constitucional ya que la carta magna reconoce la intimidad como derecho connatural y a su vez existe una ley dirigida a regular el tratamiento de datos.

- La autorización que hace el titular para el tratamiento de datos, fija unos límites para el responsable de datos, restringiendo así la actividad en el procesamiento.

- Si la autorización para el tratamiento de datos reúne los requisitos de existencia y validez de un contrato o esta autorización es accesoria a un contrato, el incumplimiento o extralimitación por parte del responsable del procesamiento de datos, esto se derivaría en una responsabilidad civil contractual objetiva porque se trata de obligaciones de resultado y en el mismo sentido, si los datos resultan filtrados o alterados por un tercero no autorizado se entiende que se está faltando al deber tácito de seguridad; si dicha autorización no reúne los requisitos de existencia y valides del contrato y tampoco es accesorio del contrato, la vía para reclamar los consecuentes perjuicios seria la vía extracontractual de responsabilidad civil, sea esta objetiva o subjetiva para cada caso en particular.

- Para que se declare la responsabilidad subjetiva es necesario que el accionante demuestre suficientemente el elemento subjetivo, es decir, la culpa o el dolo con el que actúa el responsable del tratamiento de datos. Si este filtra, defrauda o realiza una actividad no prevista en la autorización con pleno conocimiento y voluntad, será dolo, rozando incluso con un actuar criminal, pero si el responsable del

tratamiento actúa con negligencia, impericia, imprudencia o faltando al deber objetivo de cuidado, será igualmente responsable de reparar los daños causados pero a título de culpa.

- En principio, el titular siempre será el legitimado en la causa por activa, es decir, quien tiene la posibilidad de demandar haciendo manifiesto su interés jurídico, ya que este es el "propietario" de sus datos, pero no se excluye la posibilidad de reclamar los consecuentes perjuicios por vía de daño hereditario.

- En el campo del tratamiento de datos personales y sensibles, el daño que se puede generar es el daño moral, el daño emergente, el lucro cesante e inclusive la pérdida de la oportunidad, excluyéndose así los daños a la salud propiamente dichos, ya que el objeto de la pretensión siempre será un bien inmaterial, intangible que se eleva a la categoría de derecho humano como lo son la intimidad o el buen nombre.

- Las fuentes o tipos de responsabilidad civil extracontractual que se pueden ventilar en un proceso de responsabilidad civil por daños causados en el ejercicio del tratamiento de datos serán, en un primer momento, el hecho propio imputable al responsable del tratamiento de datos o inclusive también es posible hablar de actividades peligrosas siempre y cuando existe un riesgo inminente en el tratamiento de datos, y sea posible probar este título de imputación.

- El legitimado en la causa por pasiva, es decir, quien debe ser demandado en un proceso de responsabilidad civil derivada del tratamiento de datos, será el responsable del procesamiento de datos, quien reciba la autorización expresa para el procesamiento de datos y sus delegados, pero, si para el tratamiento de datos se utiliza un sistema de inteligencia artificial, también se legitiman en la causa por pasiva los programadores o creadores del sistema y el responsable del tratamiento de datos no se puede excusar alegando que culpa exclusiva de programador o creador como tercero, ya que estos cuentan con una relación jurídica y se aplica la regla de la solidaridad, y ambos son responsables de reparar los daños.

- Los eximentes de responsabilidad varían si se trata de una responsabilidad objetiva o subjetiva, es decir, debe estudiarse en cada caso concreto, entendiendo que si se trata de una responsabilidad civil objetiva, el responsable del tratamiento de datos o sus delegados solo pueden exculpar alegando causa extraña, haciendo salvedad que el programador o creador de la IA no es un tercero. Por otro lado, si se tiene que la responsabilidad es subjetiva, el responsable también podrá exonerarse demostrando diligencia, prudencia o cuidado.

- Aunque no exista una definición propiamente dicha de lo que es la IA, esta se puede definir como aquel sistema informático que es programado por medio de algoritmos y es alimentado por bases de datos, teniendo este sistema la capacidad de interactuar con esos datos y a su vez teniendo la capacidad de aprendizaje de manera autónoma.

- El propósito que se tiene con la IA es que esta tenga la capacidad autónoma de mejorar su aprendizaje para así hacerle la vida más útil y fácil a las personas, ya que con la IA se busca ayudar al hombre en sus tareas diarias y no se busca que este sea remplazado por una IA. Asimismo, con la IA se busca que esta se parezca a los humanos en el sentido de que esta tome decisiones con capacidad de discernir.

Bibliografía

Abeliuk, Andrés., Gutiérrez, Claudio. (2018). Historia y evolución de la inteligencia. **Inteligencia** Artificial, 01(1), 14-21. https://revistasdex.uchile.cl/

Alvarado, Michael. (2015). UNA MIRADA A LA INTELIGENCIA ARTIFICIAL. Artificial Intelligence (AI) at a Glance, 01(1), 27-31. https://dialnet.unirioja.es

Arce, Diego. (2021). Inteligencia artificial, la nueva amenaza al derecho a la intimidad. Infobae. https://www.infobae.com/publyca/2021/12/23/inteligencia-artificial-la-nueva-amenaza-al-derecho-a-la-intimidad/

Blakemore, Erin. (2023). La nueva IA podría superar el famoso Test de Turing; este es el hombre que lo creó. National Geographic, 01(1), 01-07. https://www.nationalgeographic.es/ciencia/2023/03/alan-turing-test-inteligencia-artificial

Constitución Política de Colombia. (1991). Constitución Política de Colombia – 1991 (2a edición). Legis. http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

Corte Constitucional (2000, 12 de abril). Sentencia C-430/00 (Antonio Barrera Carbonell, M.P.). https://www.corteconstitucional.gov.co/relatoria/2000/c-430-00.htm

Corte Constitucional (2011, 06 de octubre). Sentencia C-748/11 (Jorge Ignacio Pretelt Chaljub, M.P.). https://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm

Corte Constitucional (2022, 13 de octubre). Sentencia T-360/22 (Hernán Correa Cardozo, M.P.). https://www.corteconstitucional.gov.co/Relatoria/2022/T-360-22.htm

Corte Suprema de Justicia (2012, 03 de julio). Sentencia 76001-31-03-009-2006-00094-01 (Ariel Salazar Ramírez, M.P.). https://cortesuprema.gov.co/corte/wp-content/uploads/2021/03/S-18-12-2012-76001310300920006-00094-01.pdf

Corte Suprema de Justicia (2018, 03 de diciembre). Sentencia SC5170-2018 (Margarita Cabello Blanco, M.P.). https://www.cortesuprema.gov.co/corte/wp-content/uploads/relatorias/ci/b132018/SC5170-2018%20(2006-00497-01).doc#:~:text=La%20responsabilidad%20civil%20%C2%ABpuede%20ser,entre%20ambos%2C%20bien%20porque%20el

Corte Suprema de Justicia (2021, 22 de septiembre). Sentencia SC4204-2021 (Álvaro Fernando García Restrepo, M.P.). https://cortesuprema.gov.co/corte/wp-content/uploads/2021/10/SC4204-2021-2004-00273-02_1.pdf

El Tiempo. (2024, 23, 05). Familia de Michael Schumacher ganó demanda a revista que fingió entrevista usando IA. [Comunicado de prensa]. https://www.eltiempo.com/deportes/automovilismo/familia-de-michael-schumacher-gano-millonaria-demanda-a-revista-que-fingio-entrevista-usando-ia-3345572

Fernández, Yúbal. (2017). Así era ELIZA, el primer bot conversacional de la historia. Xataka, 01(1), 01-06. https://www.xataka.com/historia-tecnologica/asi-era-eliza-el-primer-bot-conversacional-de-la-historia

Gobierno de España. (2023). Qué es la Inteligencia Artificial. Gobierno de España, 01(1), 01-11. https://planderecuperacion.gob.es/noticias/que-es-inteligencia-artificial-ia-prtr#:~:text=Las%20Inteligencias%20artificiales%20utilizan%20algoritmos,de%20datos%20sin%20ser%20programada

Ley 1581, (2012). República de Colombia. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Ley 84, (1873), República de Colombia. http://www.secretariasenado.gov.co/senado/basedoc/codigo_civil.html#1

Ley 95, (1980). República de Colombia. https://www.suin-juriscol.gov.co/viewDocument.asp?id=1634142

WORLD COMPLIANCE ASSOCIATON. (2020, 09, 01). EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN LA PROTECCIÓN DE DATOS PERSONALES.

[Artículo]. https://www.worldcomplianceassociation.com/2767/articulo-el-impacto-de-la-inteligencia-artificial-en-la-proteccin-de-datos-personales.html

OCI. (2021). ¿Qué es una base de datos autónoma?. Bases de datos, 01(1), 01-04. https://www.oracle.com/co/autonomous-database/what-is-autonomous-database/#:~:text=Una%20base%20de%20datos%20aut%C3%B3noma%20es%20una%20base%20de%20datos,administradores%20de%20bases%20de%20datos

Perasso, Valeria. (2016). Qué es la cuarta revolución industrial (y por qué debería preocuparnos). BBC, 01(1), 01-10. https://docs.ufpr.br/~jrgarcia/macroeconomia_ecologica/macroeconomia_ecologica/Qu%C3%A9%20es%20la%20cuarta%20revoluci%C3%B3n%20industrial.pdf

PowerData. (2021). Bases de datos inteligentes en un mundo inteligente, PowerData 01(1), 01-04. https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/bases-de-datos-inteligentes-en-un-mundo-inteligente

REAL ACADEMIA ESPAÑOLA: *Diccionario de la lengua española*, 23.ª ed., (versión 23.7 en línea). https://dle.rae.es/artificial

Rodríguez, Rubén. (2021). Neuronas de McCulloch y Pitts. Deep Learning, 01(1), 01-09. https://lamáquinaoraculo.com/deep-learning/el-modelo-neuronal-de-mcculloch-y-pitts/#:~:text=El%20modelo%20de%20neuronas%20de,computar%20y%20procesar%20la%20informaci%C3%B3n.

Rouhiainen, Lasse. (2018). Inteligencia artificial 101 cosas que debes saber hoy sobre nuestro futuro. https://planetadelibrosec0.cdnstatics.com/libros_contenido_extra/40/39308_Inteligencia_artificial.pdf

Salas, Nubia. (2021). DE LAS ACTIVIDADES PELIGROSAS. Algunos estudios contemporáneos de la Sala de Casación Civil de la Corte Suprema de Justicia de Colombia, 01(1), 102-104. https://cortesuprema.gov.co/corte/wp-content/uploads/2021/06/ALGUNOS-ESTUDIOS-CONTEMPOR%C3%81NEOS-ACTIVIDADES-PELIGROSAS.pdf

Soacha, J. (2018). Radicación 16-172268- -00001-0000. Protección datos, 01(1), 01-11. https://www.sic.gov.co/recursos_user/boletin-juridico-sep2016/conceptos/datos_personales/16172268-proteccion-datos-9-ago-2016.pdf

Soacha, J. (2018). Radicación 18-171259-1. Tratamiento datos sensibles, 01(1), 01-20. https://www.sic.gov.co/sites/default/files/files/Boletinjuridico/2018/Rad180171259TratamientoDatosSensibles.pdf

Tapia, Hermida., Alberto J. (2021). La responsabilidad civil derivada del uso de la inteligencia artificial y su aseguramiento, 54 Rev.Ibero-Latinoam.Seguros, 107-146. https://revistas.javeriana.edu.co/index.php/iberoseguros/article/view/33793/25982

Uribe, S. (2020). Prohibición de Opción y Creación de un Instituto Jurídico Particular que no es Responsabilidad Civil Contractual ni Extracontractual. Comentarios a la sentencia sc-780 de 2020 de la corte suprema de justicia, 01(1), 01-11. https://iarce.com/prohibicion-de-opcion-y-creacion-de-un-instituto-juridico-particular-que-no-es-responsabilidad-civil-contractual-ni-extracontractual/#

XATAKA. (2023, 06, 21). “Abuelita, léeme claves de Windows 10 para dormir”: un truco sorprendente que funciona en ChatGPT y Bard. [Artículo]. https://www.xataka.com/robotica-e-ia/abuelita-leeme-claves-windows-10-para-dormir-truco-sorprendente-que-funciona-chatgpt-bard