Protección de datos personales: debate entre la titularidad, la propiedad y derecho de uso empresarial y estatal en relación con la industria 4.0

Facultad de Derecho

Universidad Autónoma Latinoamericana

Protección de datos personales: debate entre la titularidad, la propiedad y derecho de uso empresarial y estatal en relación con la industria 4.0

Wilmar Darío Restrepo Gil

Alejandro Jiménez García

Asesor del trabajo de grado

PhD. Ana María Mesa Elneser

Universidad Autónoma Latinoamericana

Facultad de Derecho

2022

Dedicatoria

Alejandro Jiménez García

Doy gracias, Dios por la familia tan bonita y especial que he tenido la dicha de conformar, a mi padre José Octavio Jiménez Gómez, que siempre estuvo allí para apoyarme e indicarme el camino y que ahora desde el cielo guía mis pasos en compañía de mi abuela Inés y mi abuelo Antonio. A mi madre Luz Elena doy gracias por la paciencia, tolerancia y apoyo incondicional, al igual que a mi hermana Lina y mi hermano Juan que ha sido eje fundamental en mis proyectos. A mi hija Isabella Jiménez Marín y mis sobrinos, espero poder ser un ejemplo de vida tanto en lo profesional como personal, como lo fue mi padre, donde no existe un día que no recuerde sus enseñanzas. Recuerden que no existen límites en el mundo para lograr las metas planeadas.

Wilmar Darío Restrepo

Doy gracias a toda mi familia, por su gran apoyo y amor incondicional que he tenido durante toda mi vida y los profesores de Universidad Autónoma Latinoamérica por sus enseñanzas y gratas experiencias que me han trasmitido en el desarrollo del presente trabajo.

Agradecimientos

Este trabajo ha sido fruto de la perseverancia, disciplina, esfuerzo, dedicación, trabajo en equipo y actitud, para convertirnos día a día en mejores seres humanos, que puedan aportar un grano de arena en la sociedad y contribuyan a una transformación de forma positiva. Queremos agradecer de manera muy especial a nuestra profesora y asesora Ana María Mesa Elneser, Abogada Titulada y Doctora en Derecho Procesal contemporáneo de la Universidad de Medellín, Investigadora y Experta en Derecho Informático, Especialista en Docencia e Investigación, Docente de la Universidad Autónoma Latinoamericana; gracias por su dedicación, compromiso y esfuerzo en las asesorías.

RESUMEN

En era de la industria 4.0, su principal materia prima son los datos, es la base primigenia de la inteligencia artificial llevando al hombre hacer lo impensable, lo antes era solo un sueño surrealista hoy es una realidad, estos poderosos algoritmos están evolucionado de tal manera que gracias al procesamiento de datos de todas las personas que se encuentran hiperconectadas alimentado poderosos servidores cuánticos que realizan un sin número de ecuaciones en milésimas segundo y aprenden de manera autónoma y permanente , evolucionado el cada rama conocimiento de la humanidad.
Las normatividad existente en el tratamiento de datos personales, debe entenderse desde las regulaciones e internacionales, que buscan la protección de los derechos fundamentales como garantía de los estados democráticos y donde han permitido a sus ciudadanos, empresas e instituciones en la construcción de mecanismos para garantizar esos derechos, desde diferentes visiones multidisciplinares que permiten identificar problemáticas y que a través del debate permitan una sociedad más justa como es el caso de la Inteligencia Artificial. La legislación Colombia en tema de protección de datos personales, ha sido producto de la necesidad y la exigencia de las organizaciones internacionales, que han logrado de forma general una protección general en cuanto al tratamiento por parte del responsable o encargado, pero que se quedan corto para poder regular la industria 4.0.

Palabras clave: hiperconectado, datos, responsable, encargado, tratamiento, industria 4.0, computación quántica, algoritmo, inteligencia artificial.

ABSTRACT

In the time of the industry 4.0, its main raw material is data, it is the original basis of artificial intelligence, leading man to do the unthinkable, before it was just a surreal dream, today it is a reality, these powerful algorithms are evolving in such a way that so that thanks to the data processing of all the people who are hyperconnected sources, powerful quantum servers that perform countless equations in thousandths of a second and learn autonomously and permanently, each branch of knowledge of humanity has evolved.
The existing norms in the processing of personal data must be understood from the international and regulations, which seek the protection of fundamental rights as a guarantee of democratic states and where they have allowed their citizens, companies and institutions in the construction of mechanisms to guarantee those rights, from different multidisciplinary visions that allow identifying problems and that through debate allow a fairer society as is the case of Artificial Intelligence. Colombian legislation on the subject of personal data protection has been the product of the need and demand of international organizations, which have generally achieved general protection in terms of treatment by the person in charge or person in charge, but which fall short, in order to regulate the industry 4.0.

Keywords: hyperconnected, data, controller, manager, treatment, industry 4.0, quantum computing, algorithm, artificial intelligence.

Tabla de contenido

Introducción

Cada día el mundo digital mueve sus economías por medio de herramientas tecnológicas a través de dispositivos electrónicos o inteligentes, que permiten almacenar y capturar masivamente las transacciones de datos realizadas por sus usuarios, la sociedad actual cambia rápidamente por el uso nuevas tecnologías, que trae consigo nuevos desafíos en materia de protección de derechos fundamentales que se vulneran a través del uso información sensible de las personas.

La evolución de la industria de los datos ha traído una nueva revolución basado el mundo del algoritmo, que parte del dato indexado para el proceso de analítica, permitiendo entender de mejor forma el comportamiento de los individuos, brindando servicios eficientes y efectivos que poco a poco han transformado la vida de las personas, cambiando las formas de relacionarse, así como la forma de hacer negocios y la forma de gestionar la información. Este cambio trae consigo un sin número de riesgos y amenazas que pueden influir en la capacidad que tienen los individuos de autodeterminarse, donde deben respetarse las políticas y normativas referentes a la protección de los datos personales para que estos sean usados con consentimiento previo y no existan extralimitaciones en el tratamiento de los mismos.

Las empresas, personas o instituciones que gestionar la información, que tengan el rol de responsables o encargados, que deberán informar de manera clara, precisa y expresa, el tratamiento que le darán a la información y sus fines, donde el titular o propietario de la información una vez leído negará o dará de su autorización de forma consciente y voluntaria al tratamiento de sus datos, respetando la expectativa razonable de intimidad que tiene las personas

De acuerdo a lo anterior, es importante que cada sitio web o cada App indique cuál es su política de tratamiento de datos personales, para que los usuarios puedan tener claro el alcance del tratamiento que realizarán estas empresas con la información suministrada y que luego de leer,

puedan decidir si acepta los términos. Uno de los inconvenientes que existe, es la dificultad para que las personas lean y entiendan las políticas de tratamiento de datos personales, pues es el lenguaje en el cual está escrito es algo técnico y extenso, por lo cual se hace necesario conocer un poco de los temas y dedicar varios minutos antes de aceptar las condiciones, que por lo general las personas aceptan sin leer el documento, tan solo para obtener la funcionalidad o beneficio del programa.

El presente documento monográfico hace un análisis detallado desde el punto de vista socio jurídico de la protección de datos personales, titularidad y uso con relación a la industria 4.0, así mismo se realizará un análisis detallado del marco del marco legal e internacional, el presente estudio se realizará mediante el uso de técnicas cualitativas donde se busca analizar el impacto social y jurídico del tema de estudio. La normatividad y regulaciones internacionales, permiten la creación de políticas protección de datos personales que logren pasar de una concepción abstracta y general, a una concepción más puntual, que hacen posible la definición con mayor claridad del marco de aplicación. El uso de dispositivos inteligentes y aplicaciones de uso diario impactan en la forma de vida de las personas, producto de la evolución del Internet de las Cosas y los sistemas de inteligencia Artificial implementados para ser utilizados como estrategias corporativas para maximizar la rentabilidad de los negocios negocios, vulnerando derechos fundamentales.

Para lograr el resultado de un análisis de las regulación referentes a la protección de los datos personales de los titulares frente al uso empresarial, donde pueden existir vulneraciones a los derechos fundamentales, fue posible al **plantearse la siguiente la pregunta investigativa** *¿Cuáles son los criterios legales constitucionales y tecnológicos para establecer los límites entre el uso , la titularidad y la propiedad del dato en la industria 4.0?*, obteniendo como resultado la

necesidad de la implementación de nuevas políticas públicas, que definan, prohíban y delimiten el uso de los datos personales en Colombia, que permitan la innovación y desarrollo de forma ética, que vaya a la vanguardia de las nuevas tecnologías.

Para materializar el logro del desarrollo de esta investigación, fue necesario plantearse como **objetivo general** *"Establecer los criterios legales, constitucionales y tecnológicos que permitan identificar los límites entre el uso, la titularidad y propiedad del dato en la industria 4.0"*, resultados que se vieron se exponen en tres capitules, lo dos iniciales de los aspectos normativos internacionales y nacionales, y el ultimo donde se realiza una reflexión de las problemáticas actuales que han sucedido de manera real, que evidencia las falencias en el ordenamiento jurídico.

Por ello fue necesario entender la evolución de una sociedad digitalizada, que transforma radicalmente los entornos sociales, laborales y personales de todos los seres humanos, quienes demandan grandes cambios y generan nuevas necesidades, nacen nuevas ramas y disciplina del conocimiento, hacen que lo imposible sea posible, que lo impensable se haga realidad y que los mayores temores se conviertan en un riesgo más latente. Hoy en día la solución a diferentes problemas los encontramos en complejos algoritmos, basados en inteligencia artificial y desarrollo de nuevas áreas de conocimiento, implantadas, desarrolladas e impulsadas en la era de la industria 4.0, a través de la big data, que es alimentada de manera insaciable por los datos personales que son indexados, utilizados y analizados para generar nuevos productos, necesidades y evolucionar , buscan que las personas dependa más de ellos, se conviva y se utilicen en cada aspecto de la vidas de cada persona, realizan perfilamiento, clasifican y personalizan la publicidad e información, a las cuales tiene acceso, manipulando las necesidades, conductas y hacen que se dependa de estas grandes empresas de tecnología.

Surge entonces la necesidad de profundizar en las diferentes organizaciones en el mundo que regulan la protección de los datos personales, de la cual se puedan extraer para el cumplimiento del **primer objetivo específico** "*1. Presentar las normas y reglas de la OCDE, OEA, RIPD y de la RGPD en el tratamiento de datos personales y su relación con la industria 4.0".*

En últimos los veinte años, Colombia ha evolucionado en la protección de los datos personales, pero no ha alcanzado a dimensionar y regular las nuevas conductas, tendencias, políticas, sociales y económicas, en materia digital, el plan ha sido acogerse normas internaciones, que establecen parámetros éticos en el uso para la protección de datos personales, quedando pendiente temas como la inteligencia artificial, desarrollo de algoritmos de analítica de datos, algoritmos cuánticos, machine learnig que afecten los derechos fundamentales los ciudadanos y su libertad para decidir.

El sistema normativos y constitucional que regula la protección de los datos personales en Colombia, específicamente el derecho de habeas data, derecho a intimidad, el derecho a la autodeterminación informática, libre desarrollo de la personalidad, los principios rectores de la protección de datos, los tratados internacionales y demás normativas, se requieren analizar para poder entender los pasos que debe seguir el país, para proteger y garantizar los derechos de sus habitantes, que debido a los avances de la industria 4.0 deben tener limitantes y prohibiciones desde una postura de un estado democrático.

De ahí tomó fuerza la investigación de las normativas y directivas aplicadas por la Super intendencia de Industria y Comercio, en la protección de datos personales, que permitan sentar las bases del **segundo objetivo específico** "2. Presentar el marco normativo en Colombia de protección de datos personales y su relación con la industria 4.0".

La recolección de datos sensibles de manera masiva se realiza a través de dispositivos inteligentes hiperconectados instalados en los vehículos, casas, oficinas y empresas, relojes inteligentes, asistentes virtuales, dispositivos médicos entre otros, que tienen la capacidad de intercomunicarse entre ellos e intercambiar los datos que se almacenan en servidores cuánticos, procesando los datos e indexándolos, ejecutado complejas operaciones algoritmias que permiten identificar y perfilar a sus usuarios a través de la data mediante el uso de data points o puntos de almacenamiento de datos, cookies y sistemas identificación de patrones morfológicos y faciales, obteniendo la identificación digital única de cada persona. Lo anteriormente mencionado debe entenderse desde los casos reales, del uso de dispositivos en las actividades cotidianas con grandes beneficios y costos bajos, es allí donde surge el **tercer objetivo específico** *"3. Plantear los efectos de la captura y tratamiento de los datos personales con el apoyo de la industria 4.0, que supongan un desafío para la defensa de los derechos fundamentales y legales, a través de dispositivos inteligentes, aplicaciones de uso diario, reconocimiento facial y Biomarketing".*

.

Capítulo 1

Los tratados internacionales y normativas en relación con la protección de los datos personales

Los tratados internacionales han permitido poner fin a los diferentes conflictos que ha tenido la humanidad, donde la soberanía es definida por el poder absoluto y exclusivo sobre espacio y población, según el filósofo francés Jean Bodin. Este resalta el principio de no intervención entre los países, y de allí nacen los tratados que son acuerdos de voluntades para crear, modificar o extinguir derechos u obligaciones que dependen del caso particular, posteriormente Hugo Grotius (Padre del Derecho Internacional), logro incorporar el derecho de gentes, donde se permitió a los extranjeros participar en las instituciones del derecho romano.

El tratado de Paz de Westfalia en 1648 pone fin a una guerra que llevaba 30 años en el cual se definieron un conjunto de normas que permitieron establecer las bases del principio de soberanía. La revolución francesa en el año 1789 permitió poner fin al feudalismo y al absolutismo, donde la burguesía era en ocasiones acompañada por las masas populares, permitiendo sentar las bases de la democracia moderna y la soberanía popular. Es en el año de 1789 nace la Declaración de los derechos del hombre y del ciudadano, influido por la doctrina de los derechos naturales, que se refieren a que los derechos del hombre son universales sin excepciones. Luego vino el golpe de Estado en 1799 por parte Napoleón Bonaparte e inicio con las cruzadas por la adquisición de territorios, en 1802 fue proclamado emperador hasta 1815, año en el cual fue derrotado en la batalla de Waterloo y se vio obligado a firmar el tratado de Paris el 20 de noviembre de 1815.

El pacto de Briand Kellogg 1928, fue un tratado firmado por 15 estados, en el cual se comprometieron a no usar la guerra como mecanismo para la solución de controversias internacionales. La segunda guerra mundial surge en el año 1939 cuando Hitler decide invadir a Polonia,

continuando con el control de Noruega, Dinamarca, Países Bajos, Bélgica y Francia. Luego el 1 de enero de 1942 cuarenta y cinco estados declaran la guerra y es en 1945 donde finaliza la guerra.

Después de la Segunda Guerra Mundial nace la Organización de Naciones Unidas (ONU), para la institucionalizar el mantenimiento de la paz, la seguridad internacional, fomento de relaciones de amistad, respeto al principio de igualdad, libre determinación de los pueblos y cooperación internacional con la Carta de las Naciones Unidas que fue firmada en San Francisco en 1945 y que entró en vigor el mismo año, y es así como el 10 de diciembre de 1948 fue adoptada la Declaración Universal de Derechos Humanos por la Asamblea General de la ONU.

En abril de 1948 nace la Organización de Estados Americanos (OEA) con el objeto de ser un foro político para la toma de decisiones de integración y de dialogo, para consolidar la democracia y promover los derechos humanos para apoyar el desarrollo social y crecimiento sostenible en América. La Comisión Interamericana de Derechos humanos (CIDH) es un órgano de la OEA, creado en 1959 para promover la observancia y defensa de los derechos humanos y como ente consultivo que tiene su sede en Washington D.C. La Corte Interamericana de Derechos Humanos es un órgano judicial autónomo de la OEA que fue creado en 1979, con sede en Costa Rica, y su función es la protección de los derechos humanos, aplicando e interpretando la Convención Americana, sancionando a los diferentes Estados que hacen parte de la organización por violaciones a los derechos humanos, supervisando que las sentencias se cumplan y brindando medidas de protección a las personas o sus familiares que han sufrido algún tipo de daño o perdida donde el estado implicado ha tenido responsabilidad por acción o por omisión.

El consejo permanente de la OEA ha trabajado en la protección de los individuos a través de la Comisión de Asuntos Jurídicos y Políticos (CJI), estableciendo los principios y recomendaciones que deben seguir las sociedades democráticas de los Estados miembros, en relación con

las políticas definidas de acuerdo a diferentes estudios realizados por la CJI, que han permitido establecer directrices para la protección de datos personales que eviten o reduzcan violaciones o vulneración de derechos, que afecten de forma negativa a los individuos y la sociedad (Consejo Permanente de la OEA, 2011).

El Comité Jurídico Interamericano (CJI), desde 1996 ha venido trabajando en la protección de datos de personales con los Estados miembros, para que estos diseñen, ejecuten y evalúen políticas sobre acceso a la información pública, consideren la aplicación e implementación de la Ley Modelo Interamericana sobre Acceso a la Información Pública contenida en la resolución AG/RES. 2607 (XL-O/10) y su Guía de Implementación AG/RES. 2727 (XLII-O/12). Con el fin de promover las mejores prácticas con relación al dato personal, que no restrinjan los avances e innovación tecnológica que ocurren día a día, pero que delimiten un marco de acción para mitigar y controlar el manejo de la información, que es un insumo fundamental en la era actual.

El Convenio del Consejo de Europa para la protección de datos personales define los datos personales como "Toda información relacionada con una persona identificada o identificable", donde se consagran los principios y los estándares para los miembros de la Unión Europea y que reconoce una vez más el derecho de los particulares a la privacidad.

En los Estados Unidos el derecho a la privacidad protege únicamente contra la intrusión del gobierno federal, en los asuntos referentes al derecho privado, cada empresa o persona puede realizar el tratamiento de datos personales siempre que las conductas desplegadas por el responsable no tipifiquen un delito o causen un daño al titular de la información, algunos estados de la federación cuentan con normativas que deben seguir las empresas privadas o particulares en lo referente al tema en mención.

En Canadá la privacidad es protegida en la Carta de Derechos y Libertades que forma parte de la Constitución y donde está reconocido el derecho a oponerse a un registro o incautación de los datos privados personales por parte del Gobierno siempre y cuando se encuentre justificación, debidamente motivada. Las empresas o personas naturales que realicen algún tipo de tratamiento de datos personales deben asegurarse de que la protección a la información es adecuada, las políticas son trasparentes, exista la posibilidad de denunciar el incumplimiento, limitar su uso, tiempo de conservación, contar con el consentimiento valido e informado, cumplir con los fines, permitir la corrección y suspensión de acuerdo a las políticas definidas por la OCDE.

En el año 2013 Colombia inicio su proceso de adhesión a La Organización para la Cooperación y el Desarrollo Económicos (OCDE), en el año 2018 fue invitada a ser parte; luego de haber realizado una serie de reformas estructurales en políticas públicas, de comercio, temas ambientales, fiscales, laborales, financieros, educativos , salud y agricultura entre algunos de los requeridos para completar los procedimientos indicados por la organización, convirtiéndose en el miembro 37 el 28 de abril de 2020.

La OCDE tiene sus objetivos estipulados en la convención artículo 1, define la promoción de políticas que permitan una sana expansión de sus economías, el empleo y el nivel de vida en los países miembros, buscando estabilidad económica permitiendo el crecimiento del comercio sobre una base multilateral donde no exista discriminación de acuerdo con la normatividad internacional. Adicionalmente, en su artículo 2, deben cumplir con los compromisos enunciados como la utilización eficiente de los recursos tanto técnicos, científicos, investigativos y educativos, donde se desarrollarán políticas para lograr el crecimiento económico, estabilidad financiera que permitan reducir los riesgos que puedan afectar sus economías (Convención de la OCDE, 1960).

Colombia es un país que busca afianzar las relaciones internacionales con los demás países, a través de la firma de diferentes tratados que le permite incluir en su ordenamiento jurídico esas nuevas normativas, que para el caso particular van de la mano con los avances tecnológicos que requieren políticas que permitan un control, para brindar derechos y obligaciones, garantizando el debido proceso consagrados en la carta política.

El artículo 230 de la Constitución Política de Colombia es claro al recalcar que si no hay una norma que pueda suplir un vacío normativo, el juez podrá analizar la problemática de acuerdo a la doctrina existente, esto quiere decir que podría consultar en diferentes fuentes nacionales e internaciones que aborden el tema para entenderlo y aplicar una decisión justa como criterio auxiliar para dar sentencia.

Con el pasar del tiempo, el legislador ha venido construyendo un sistema híbrido de protección de datos personales y ha suscrito una serie de tratados, convenios internacionales en materia referente a la protección, acceso y uso de datos personales, buscando cubrir los vacíos normativos y mejores prácticas en el mundo referente a esta materia. Las diferentes normativas y políticas existentes del tratamiento de datos personales han sido el fruto de reuniones, debates y foros de la Red Iberoamericana de Protección de Datos Personales (en adelante RIPD), cuenta con miembros, observadores e invitados de las diferentes entidades públicas del entorno iberoamericano que su actividad esté relacionada con la protección de datos personales.

La RIPD fue creada en 2003 como mecanismo de integración y cooperación entre las autoridades de cada país, la cual está integrada por 34 organizaciones de ellas 16 son autoridades de protección de datos personales y donde el 7 de diciembre de 2020 fue elegido el presidente entre uno de los miembros en sesión cerrada por votación, ganando por mayoría simple la Superinten-

dencia de Industria y Comercio de Colombia, por un periodo de 2 años. En Colombia las 2 entidades que hacen parte del RIPD son la Superintendencia anteriormente mencionada como miembro y la Procuraduría General de la Nación como observador en su Delegatura para la Defensa del Patrimonio Público, la Transparencia y la Integridad.

Desprendiendo de ellos, encontramos el tratado de Budapest, este acuerdo permite crear un acuerdo internacional de cooperación para combatir el crimen organizado, específicamente delitos informáticos permitiendo la generación deg directrices para que los legisladores que se vinculan a estos tratados, estableciendo una legislación penal y procedimientos para combatir los delitos informáticos y la protección de los datos personales Colombia ratificó este tratado mediante Ley 1928 del 2008.

El tratado de Budapest es también conocido como el tratado de la ciberdelincuencia que busca vincular a los países suscritos a establecer herramientas legales en materia penal para perseguir los delitos cometidos por medios informáticos.

EL 12 de julio del 2002, la Unión Europea aprobó la directiva 2002/58/CE con el fin de dar tratamiento a los datos personales y la protección a la intimidad en el sector de las comunicaciones electrónicas, que es conocido como la Directiva ePrivacy, modificada en el año 2009, la cual busca mejorar la gestión de las cookies y el seguimiento online, prohibiendo el almacenamiento de automático de cookies, definiendo al propietario de la web como el legalmente responsable frente a las autoridades.

Las cookies es la información que se almacena de un usuario en un sitio web, que permite mejorar la experiencia de este en el sitio en el cual se navega y donde terceros incluyen sus cookies para realizar tácticas de marketing o monitoreo de una red social del comportamiento del usuario. La Directiva ePrivacy define que no se puede establecer ninguna cookie sin la aprobación del

consentimiento previo, solo se podrán las disponer de las funciones básicas de la web. Esta directiva permite hacer páginas web más seguras con los datos, deben permitir el acceso a la información de forma anónima y que siempre se informe cual es el propósito que permita dar confiabilidad y seguridad al navegar en el sitio. La anterior directiva fue adoptada por cada país miembro de la Unión de propia en sus ordenamientos jurídicos (Parlamento Europeo, 2002).

El Reglamento General de Protección de Datos (en adelante RGPD), que fue expedido por la Unión Europea el 27 de abril de 2016, busca generar trasparencia a los usuarios que navegan en la web, brindando derechos para exigir el acceso a la información almacenada, rectificación, suspensión y derecho al olvido (artículo 17). Esta normativa se integra de forma automática a todos los países miembros de la Unión y entró en vigor a partir del 25 de mayo de 2018. Este reglamento define la licitud del tratamiento (artículo 6), donde debe cumplir una de las siguientes condiciones:

- Interesado de su consentimiento
- Necesario para la ejecución de un contrato
- Necesario para el cumplimiento de una obligación
- Necesario para proteger intereses vitales
- Necesario para el cumplimiento de una misión de interés público.
- Necesario para satisfacer intereses legítimos (Reglamento (Ue) 2016/679 Del Parlamento Europeo, 2018, p. 7).

El RGPD define que para los menores de edad es lícito su consentimiento, si es mayor a 16 años, de lo contrario la autorización la debe dar el titular de la patria potestad que podrá ser verificable, en algunos Estados puede varias la edad, pero no puede ser inferior a 13 años. Esta

reglamentación prohíbe el tratamiento de datos que revelen el origen étnico, racial, político, sindical, religioso, genético, filosófico, sexual y biométrico que permitan la identificación de una persona, así como cualquier tipo de perfilamiento que pueda convertirse en algún tipo de discriminación. La transparencia es un principio que inicia con la autorización, se debe informar por medio de un lenguaje claro y sencillo que sea entendible por el usuario y que permita entender al interesado que en cualquier momento posterior podrá ejercer sus derechos, por medio de una solicitud y si transcurrido un mes una vez radicada su solicitud, podrá presentar la reclamación frente a las autoridades de control de su país. Existen algunas limitaciones definidas en el artículo 23, para preservar en forma necesaria la sociedad democrática, como son la seguridad del Estado, la defensa, la seguridad pública, prevención, plazos de conservación, protección del interesado, ejecución de demandas civiles y la función de supervisión entre otras.

Encontramos la protección de datos desde el diseño y por defecto (artículo 25), que busca que desde el diseño de la aplicación se implemente la protección de los datos personales a través del uso de certificados digitales que permitan garantizar la fiabilidad del sitio y de la App, lo cual incluye el componente de cifrado (artículo 32) de la información, componente fundamental que garantiza la confiabilidad, integridad y disponibilidad de la información[1]. La configuración por defecto o predeterminada desde el comienzo de su utilización, pretende brindar seguridad en el uso de aplicaciones, que el usuario debe ir habilitando de acuerdo a sus necesidades y sus preferencias. El registro de actividades en el tratamiento cobra relevancia debido a que el encargado debe llevar un control de bitácora de las actividades realizadas con los datos y sus fines, los que podrán ser auditados y revisados por el ente de control. La Comisión y las autoridades son los

[1] Integridad, Confiabilidad y Disponibilidad pilares de la seguridad en la información.

obligados a la elaboración de los códigos de conducta en lo que respecta al tratamiento leal y transparente, en los contextos específicos de acuerdo con el artículo 40 del reglamento. La imposición de sanciones administrativas está definida en el artículo 83, que se puede presentar a causa de un incumplimiento o negligencia que pueden ir hasta los 20 millones de euros o el 4% del volumen máximo anual del negocio.

1.1.La Unión Europea y su regulación de la IA en el reconocimiento facial

El 25 de abril de 2018, la Unión Europea estableció una Comisión encargada de generar una estrategia para abordar los temas referentes a la IA aplicable a todos los países miembros, con el objeto de armonizar sus relaciones y unificar los planes acción para superar los obstáculos que puedan presentarse en la adopción de estas tecnologías.

La comisión se acogió a siete requisitos esenciales para la IA:

- Acción y supervisión humanas;
- Solidez técnica y seguridad;
- Gestión de la privacidad y de los datos;
- Transparencia;
- Diversidad, no discriminación y equidad;
- Bienestar social y medioambiental;
- Rendición de cuentas. (Libro Blanco - Comisión Europea, 2020, pp. 12-13)

Luego de acogerse a los siete requisitos mencionados, la Comisión el 19 de febrero público el “Libro Blanco sobre la Inteligencia Artificial” que tocaba los temas de la inteligencia artificial, desde la visión de los expertos, que buscaba crear un espacio para que las organizaciones, empresas

y particulares realizaran observaciones para la creación de un marco regulatorio, el cual estuvo disponible en sitio web de la Unión hasta el día 14 de junio de 2020, contando con la participación de 1250 interesados de todos los países miembros de la Unión. El Libro Blanco comprende 450 documentos y posiciones referentes a la protección de datos, que permitió la definición de políticas para la IA, que garantizaran un desarrollo seguro, siempre pensando en la protección y defensa de los derechos fundamentales y que brinden confianza a los usuarios del sistema.

La Inteligencia Artificial buscar mejorar las condiciones de vida de las personas en lo social, a través de diferentes implementaciones en el sector salud, ambiental, económico, de entretenimiento y agrícola, potenciando grandes beneficios, pero que dan lugar a la creación de riesgos que podrían considerarse de alto impacto para la sociedad y por los cuales se han definido prohibiciones a su implementación debido a que vulneran los derechos fundamentales de las personas. El enfoque de la regulación es de carácter normativo horizontal, equilibrado y proporcionado, que define los requisitos mínimos y los planes de gestión que permitan permanecer en el tiempo. Los sistemas de IA definidos como de alto riesgo, deben cumplir con los requisitos estipulados en el reglamento, obligatoriamente pasar por un sistema de pruebas de funcionamiento, gestión de riesgos, gestión de incidentes, documentación y verificación humana durante su operación, con verificaciones periódicas de cumplimiento con las respectivas actualizaciones al mismo sistema, que busca garantizar la seguridad general del producto final que se va nutriendo de nueva información que inferirá es sus reglas de decisión y que el resultado final pueda ser inesperado.

Algunos sistemas de IA son considerados como de alto riesgo, debido que pueden vulnerar los derechos de la dignidad humana, privacidad, libertad, derecho a la defensa, debido proceso y de reunión, generando afectaciones sociales individuales o colectivas. Adicionalmente, los sistemas de IA vulneraban los derechos del consumidor, al no existir un mecanismo definido frente a

las reclamaciones de usuarios y al entrar en el ámbito probatorio, no era posible obtener la prueba que se requería demostrar en el fallo del sistema, como causa del daño sufrido, que debido a su concepción compleja y a la falta de normativas o regulaciones que exigieran al proveedor o fabricante del sistema, brindar herramientas para que las autoridades vigilantes o de control lograran obtener los datos a través de una API (Interface de Programación de Aplicaciones), que permitan identificar que sucedió y que de acuerdo a estas, permitieran tomar medidas que obliguen a la corrección y en casos excepcionales suspensión y multas que pueden ir hasta los 30 millones de euros o el 6% del valor de la compañía dependiendo del caso particular.

Los sistemas de IA en la Unión Europea deben contar con el Certificación de Evaluación (CE) para operar en los territorios de los estados miembros, donde previamente debieron cumplir con los requisitos exigidos en el reglamento, como son la entrega del código fuente y pruebas de funcionamiento en el laboratorio designado por organización, siempre garantizando la protección de los conocimientos técnicos, los secretos comerciales y la propiedad intelectual. Una vez se implemente el sistema de IA, este deberá cumplir con las obligaciones estipuladas en el reglamento, como son la gestión de incidentes, la corrección de errores, la revisión periódica por parte de las autoridades, manteniendo actualizada la documentación del sistema en caso de ser requerido por las autoridades encargadas, con lo cual se logrará cumplir con el principio de transparencia en todo el ciclo de funcionamiento del IA. La gestión de la ciberseguridad es fundamental para que las funcionalidades de los sistemas de IA no se vean afectados por personas maliciosas que exploten las vulnerabilidades que puedan alterar el funcionamiento.

Los sistemas de IA que sean de bajo riesgo o medio no requieren pasar por el proceso de certificación, pero la certificación es garantía para los miembros de confiabilidad y seguridad en

su operación, es por esta razón que, si un sistema de IA de riesgo bajo es certificado, sus usuarios tendrán mayor confianza y podrá operar fácilmente en los Estados miembros de la Unión.

En el Título II del RGPD, estable una lista de sistemas de IA prohibidas como riesgo inaceptable, por ser contrario a los valores de la Unión Europea, debido a que violan los derechos fundamentales, puesto pueden realizar algún tipo de manipulación como son los mensajes subliminales imperceptibles para el ser humano que trascienden en la conciencia de las persona o grupos vulnerables y que pueden alterar de forma significativa el comportamiento y el libre albedrio. Adicionalmente existe prohibición a que las autoridades, realicen algún tipo de perfilamiento o calificación social o emocional o categorizar las personas por raza, género o edad que pueda violentar los derechos fundamentales. Los sistemas de IA utilizados en la industria militar quedan excluido del ámbito de aplicación del reglamento.

La utilización de IA para la identificación biométrica de forma remota en tiempo real está prohibida a menos que exista una autorización de la autoridad judicial o administrativa independiente del Estado miembro, la cual deberá ser motivada y que sea estrictamente necesaria para alcanzar uno o varios objetivos. Algunos de los casos en el que están permitidos son:

- La búsqueda selectiva de posibles víctimas concretas de un delito, incluidos menores desaparecidos.
- La prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de un atentado terrorista.
- La detección, la localización, la identificación o el enjuiciamiento de la persona que ha cometido o se sospecha que ha cometido alguno de los delitos.

(Reglamento del parlamento europeo y del consejo, 2021, p. 52)

Capítulo 2

De la protección de datos personales en Colombia

En Colombia las leyes estatutarias son de carácter especial que buscan desarrollar los textos contenidos en la carta política, que permiten regular los derechos, deberes de las personas y de la administración pública, que tienen un rango de superioridad sobre las demás leyes y su estudio es de carácter prioritario, donde el encargado de tramitar los proyectos de ley es el congreso, definido en el artículo 152 de la Constitución Política. Las leyes estatutarias para su aprobación, modificación o derogación requieren de la aprobación en mismo periodo legislativo por la mayoría de absoluta de sus miembros de acuerdo con el artículo 153 Constitución, en la Comisión Primera; compuesta por diecinueve (19) miembros en el Senado y treinta y cinco (35) en la Cámara de Representantes.

La sentencia hito en materia de protección de datos es la Sentencia C-748 del año 2011, la corte constitucional, la Corte Constitucional, hace un profundo análisis de la protección de los datos personales y la protección de derechos fundamentales entre los cuales encontramos el habeas data, cuya base es la expectativa razonable del derecho a la intimidad y la protección integral de los datos de la vida privada y familiar de todos los ciudadanos, que son los titulares de los datos, quienes tienen la capacidad de autodeterminación informática cuya base es que toda persona tiene el derecho de conocer, actualizar y rectificar la información que se halla recogida sobre ellas con previo consentimiento y manifestación de la voluntad, y el Estado debe ser garante proteger las personas, por ello está obligado crear los mecanismos y entidades, que permitan salvaguardar la información recolectada por entidades públicas y privadas que reposa en sus bases de datos. En

Colombia encontramos que la entidad encargada de ejercer vigilancia y control es la Superintendencia de Industria y Comercio que a través de sus diferentes mecanismos aseguran la protección y cumplimiento del tratamiento de datos personales.

Los niños y adolescentes gozan de protección especial por parte del Estado y por lo cual, buscando la protección de sus derechos, se prohíbe de manera expresa cualquier tratamiento de datos, excepto cuando se trate de datos de naturaleza pública siempre cuando se respete el derecho prevalente y no se violente derechos constitucionales.

El derecho al olvido en el tema de habeas data, es un concepto nuevo que refiere a que las personas puedan solicitar la suspensión o supresión de alguna base de las datos de una empresa o entidad que se pueda considerar obsoleta por el transcurso del tiempo o que se desea ser suprimida por que la finalidad del tratamiento no es la acordada en el consentimiento o que autónomamente desee retirar el consentimiento al tratamiento de los datos suministrados, y que pudiera verse afectado en su derecho a la libertad de expresión o en su privacidad.

El derecho al olvido en Colombia no está regulado expresamente, pero los ciudadanos, puedan solicitar a las entidades públicas o privadas, suspender o suprimir cualquier información o datos que reposen en su base de datos que hayan recogido el consentimiento o sin consentimiento de su titular.

En el año 2008 la Corte realizó el proyecto de ley del habas data y manejo de información contenida en las bases de datos, este análisis se dio en la Sentencia C-1011 de 2008, que dio lugar a la Ley 1266 de 2008; esta disposición “regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países” regulando el uso de las datos solamente unos sectores definidos, pero fueron las principales bases jurídicas en la protección de datos personales. Esta ley permitió reconocer a las

personas el derecho a conocer, actualizar y rectificar la información que existente en las bases de datos específicamente en información financiera, crediticia y comercial.

Mediante la Ley1273 del año 2009, “se modifica el Código Penal, se crea un nuevo bien jurídico tutelado, denominado de la protección de información y datos personales” , consagrados del artículo 269A hasta 296J , el legislador en materia penal no podía ser ajeno e impávido, frente a la gravedad de estas conductas y al aumento de denuncias por suplantación, acceso abusivo a sistemas informáticos entre otros, ocasionando daños y perjuicios a personas, empresas y al mismo Estado por la utilización de técnicas indiscriminadas de captura de información y el tratamiento de los mismos.

Para el año 2011, el legislador se vio en la necesidad de dictar unas nuevas disposiciones generales que regulan el habeas data y manejo de información contenida las bases de datos personales, específicamente para las áreas financiera ,crediticia, comercial y servicios provenientes de países terceros, esta ley en un avance importante en la cual se dictan disposiciones y garantizan derechos a las personas de conocer actualizar y ratificar que se halla recogido de ellas, en especial de garantizar derechos constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales.

Mediante el amparo de la constitución encontramos un amplio y profundo análisis de la Corte Constitucional en la protección de los datos personales, tomaremos como base la Sentencia C-748 de año 2011, es el proyecto de la ley habeas data y protección de datos personales, es la sentencia hito en esta materia, hace un análisis jurídico detallado de esta materia, el legislador regula este tema en la Ley 1581 de 2011, se constituye en el marco general de la protección de datos en Colombia. Esta ley hace una análisis profundo y detallado los derechos constitucionales

de referente al tema de datos personales y los derechos de la autodeterminación informática, expectativa razonable de la intimidad, el derecho al olvido, habeas data y protección e interés de los menores y adolescentes, y así mismo, analiza los principios de tratamiento de datos, legalidad, finalidad, libertad de expresión, transparencia y acceso y circulación de datos personales.

Para el año 2014 el legislador regula el derecho acceso a la información pública y la publicidad de la información mediante la Ley 1712 de 2014, en la cual las personas tienen el derecho a conocer la existencia y a acceder de sus datos personales que se encuentren a cargo de las entidades públicas y privadas que cumplan función pública, esta ley fue analizada bajo la Sentencia C-274 de 2013.

El decreto Ley 886 de 2014, reglamenta el artículo 25 de la Ley 1581, el cual norma el registro nacional de bases de datos, esta ley ordena a las empresas a registrar sus bases de datos, control y seguimiento por parte del gobierno a la protección de los datos personales y generar una responsabilidad legal para aquellas personas naturales y jurídicas que son responsables de estos datos personales, respetando los criterio de recolección, uso, tratamiento, procesamiento, intercambio a terceros, transferencias y transmisión de datos personales.

El Decreto 090 del 18 de enero de 2018, Por el cual se modifican los artículos 2.2.2.26.1.2 y 2.2.2.26.3.1 del Decreto 1074 de 2015 - Decreto Único Reglamentario del Sector Comercio, Industria y Turismo., ordena a todas las empresas a registrar sus bases de datos, en registro nacional de las bases personales, que es controlada y gestionada por la Superintendencia de Industria y Comercio. El Decreto Ley 255 de 2022, reglamenta el artículo 27 de la Ley 1581, este decreto reglamenta el sector comercio, industria y turismo, y obliga mediante normas corporativas la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países.

La Corte Constitucional hace un análisis profundo y detallado sobre el principio de la privacidad en la Sentencia C-094 del año 2020, el Estado debe proteger tres esferas de la intimidad de las personas, que son la intimidad personal, intimidad familiar y el buen nombre, así mismo es el responsable de garantizar y respetar estos derechos, pero surgieron varias incógnitas. La primera fue "cómo es posible garantizar la privacidad, donde las personas conviven y usan diariamente dispositivos inteligente y aplicaciones que para su uso sus datos personales de manera masiva" la segunda "cómo regular y controlar la captura de datos personales en atreves de dispositivos inteligentes o cámaras de reconocimiento facial y sistemas biométricos ubicados en espacios públicos, privados o semiprivados los cueles son vigilados e intervenidos por terceras personas.

En el Decreto 1377 de año 2013, emanado por el Ministerio de Comercio Industria y Turismo, quien regula la captura de datos, el límite el datos sensibles y públicos, entiendo que los datos sensibles son todos aquellos que afectan la intimidad de personas, aspectos que lo identifican, en aspectos raciales, étnicos, personales, orientaciones sexuales, políticas, religiosas, sexual, datos biométricos e identificación facial, que identifican las persona a través de diferentes dispositivos inteligentes y aplicaciones en nuestro caso de estudio con fines de marketing y comerciales.

Las empresas buscan fidelizar a las personas con sus productos, mediante agresivas estrategias de mercadeo y estrategia de inteligencia de negocios, que, en redes sociales o Apps o web, es capturada la información y enviada a data points, almacenando en cookies las búsquedas y preferencias de los usuarios. Cada día las personas se habitúan a realizar transacciones comerciales en línea, o sitios de streaming, cada aplicación tiene componentes y modelo de negocio, que busca fidelizar y moldear a sus navegantes hacia ciertos tipos de comportamiento, gustos, sensaciones, emociones y decisiones que generen un tanto adictivo y que se conviertan en una forma de vida para combatir el aburrimiento y desesperación inducido por sus diseñadores, quienes pretenden

generar hábitos en la conducta y modificar la personalidad de los clientes a través de la publicidad personalizada.

El Decreto 338 de del 2022, establece lineamientos para fortalecer el modelo gobernanza y seguridad, delimitando e identificando la infraestructura critica cibernética de la nación, estableciendo protocolos de gestión de riegos y política de respuestas a incidentes cibernéticos que afecten la seguridad digital del estado, obliga a todas las entidades comprometidas en la seguridad digital a generar políticas claras que permitan la protección de la infraestructura digital toma como base diez principios que se relacionan a continuación:

1. Confianza
2. Coordinación
3. Colaboración entre las partes interesadas
4. Cooperación entre ellas
5. Enfoque de la política de gobernó digital
6. Gradualidad
7. Inclusión
8. Proporcionalidad,
9. Salvaguarda de los derechos humanos
10. Uso eficientes de la infraestructura cibernética del país.

(Decreto 338, 2022)

Delimita responsabilidad materia de gobernanza digital, crea el comité se seguridad digital y establece sus funciones, establece grupos, mesas de trabajo y puestos de manado unificado en que permitan el desarrollo de la política de gobernanza digital, así mismos define al identificación

de infraestructura critica, cibernética, servicios esenciales de la nación, así mismo crea y desarrolla el modelo de gestión de incidentes en materia de ciberseguridad (Decreto 338, 2019).

El Decreto 255 del 2022, establece que todas las entidades públicas y privadas, están obligadas a sentar bases de normas corporativas, mecanismos de protección , garantías y códigos de buenas prácticas en materia protección de datos personales, así mismo se debe certificar en cumplimiento de la ley 1581 de 2012, este decreto tiene gran importancia, permite garantizar derechos de las personas obliga a las empresas y corporaciones a certificase en materia de gestión de datos, obligándolo a unificar criterios y mejorar controles internos que permitan garantizar los derechos fundamentales de los ciudadanos (Decreto 255, 2022).

2.1. Constitución Política y Corte Constitucional y el tratamiento de datos personales

La Constitución Política del año 1991 nació no solamente para reformar el Estado y el sistema jurídico, sino como mecanismo para garantizar derechos y libertades que para la época eran limitados (Constitución Política, 1991), que buscaba combatir las diferentes formas de violencia existentes. Esta Constitución reemplazó la de 1886 y trazó la hoja de ruta para que el país logre una sociedad más justa.

El artículo 1 de la Constitución Política garantiza el respeto por la dignidad humana de cada persona que conforman o integran la sociedad, independientemente de la labor o trabajo que desempeñe y donde debe prevalecer el interés general sobre el particular. En el artículo 2 nos habla de los fines del Estado, en el cual se deben garantizar los principios fundamentales incluidos en el título 1 de la misma carta, la cual vela por la convivencia pacífica de sus habitantes, que a través de la existencia de un orden justo, se logrará la armonía del vivir en sociedad, garantizando la protección de su vida, honra, bienes, derechos y libertades que puedan estar expuestos a algún tipo

de daño o afectación psíquica o física que generen menoscabo en la calidad de vida de sus habitantes. El artículo 4, define la supremacía de la norma constitucional frente a cualquier otra ley en caso de algún tipo de conflicto que pueda surgir, donde prima la norma constitucional la cual debe dar aplicación sin excepción alguna.

En el Título Segundo de la Constitución encontramos los derechos, garantías y deberes, donde en el artículo 13 expresa que todas las personas nacen libres e iguales ante la ley, donde no existen privilegios por apellidos, condición social, raza, religión o algún otro tipo característica, donde todos recibirán protección y trato justo por parte de las autoridades, garantizando los mismo derechos, libertades y oportunidades. En el caso de que exista algún tipo de violación, se podrán solicitar acciones ante las autoridades pertinentes para que sea protegido el individuo sin importar su etnia, religión, inclinación sexual o afinidad política, entre otros.

El artículo 15 de la carta política es uno de los pilares para la protección de datos personales, debido a que aborda que el derecho a la intimidad familiar y personal, que puede verse comprometida al ingresar información en un sitio web o App, que puedan ser utilizados para generar algún tipo de tratamiento o procedimiento que genere discriminación o daño, que puedan influir en las decisiones presentes o futuras y que altere la percepción de los navegantes para lograr un objetivo concreto. Tal y como lo menciona el art 15 de la Constitución Política, la recolección de información, tratamiento y circulación deberán respetar la libertades y garantías que brinda la carta magna, por lo tanto las empresas o personas que realizan la captura de información, tratamiento o circulación de información, deben analizar detenidamente si cumplen y respetan las normativas vigentes en su tratamiento, de lo contrario, se podría estar cometiendo una violación que tendrá un tipo de sanción de acuerdo al marco normativo. Las empresas, personas naturales, instituciones públicas o privadas y que realicen algún tipo de tratamiento de datos personales, deben permitir

que las personas conozcan la información que almacenan, incluir nuevos datos, actualizarlos, rectificarlos y por último que se les excluya información de una base de datos.

A partir de lo prescrito en el artículo 16 de la Constitución Política de 1991, donde se define el libre desarrollo de la personalidad:

"Todas las personas tienen derecho al libre desarrollo de su personalidad sin más limitaciones que las que imponen los derechos de los demás y el orden jurídico".

Las personas hoy tiene condicionada su libre desarrollo de la personalidad, a lo que les marque la industria de las App y las redes sociales, a tal punto que cada red social tiene un componente de marketing para posicionarse en el mercado; logrando mayores suscriptores o likes que permitan aumentar sus ventas, siendo esta industria la que define o impone lo que se hace en esa red social, por tanto direcciona a las personas a través de anuncios, noticias, imágenes o videos que influyen en el comportamiento de los usuarios, producto de un algoritmo pensado por equipos multidisciplinarios que estructuraron y definieron reglas, que se implementan en diferentes programas, para lograr un fin económico que genere mayores ingresos a la empresa.

El libre desarrollo de la personalidad permite que cada ser se desarrolle libremente y que tenga libre albedrio, en el cual cada quien pueda tomar sus propias decisiones en su vida sin ningún tipo de preordenamiento, donde se cuenten con entornos familiares, sociales o labores, que permiten tener interacción con el otro y que gracias a la tecnología, se logra tener una comunicación instantánea, sin incurrir en desplazamiento, logrando acceder a información diversa e inimaginable, donde el intercambio de opiniones es fundamental para ejercer el derecho de libertad de expresión prescrito en el artículo 20 de la Constitución y del Capítulo VIII de la Comisión Interamericana De Derechos Humanos (OEA) El Derecho a la Libertad de Pensamiento y Expresión.

En la era de la industria 4.0, para estar hiperconectados y actualizados es necesario hoy en día contar con dispositivos inteligentes, que permiten realizar las labores diarias, dentro de los cuales encontramos: celulares, tabletas, computadores, televisores, neveras, lavadoras, sistemas de entretenimiento, asistentes virtuales y otros dispositivos que integran aplicativos de asistencia virtual basados en IA, como Siri de Apple, o Google ,home mini o Alexa, también en las ciudades encontramos cámaras de vigilancia, que han evolucionado realizando reconocimiento facial, aplicaciones que han sido programadas mediante complejos algoritmos cuánticos, diseñados para habituar al usuario a generar hábitos de comportamiento y conductas en las personas. Afectado sustancialmente el libre desarrollo de personalidad.

Dicho lo anterior, es importante entender al habeas data o el derecho de los datos, es un derecho autónomo, está compuesto por la autodeterminación informática y libertad, donde se hace necesario generar políticas públicas que garanticen, la privacidad e intimidad de las personas, con base a los adelantos tecnológicos que trae la industria 4.0.

El tratamiento de datos debe estar encaminado a generar y asegurar la protección de derechos fundamentales que afecten los datos personales las personas, especialmente la intimidad y privacidad, a recibir información veraz e imparcial que permita libremente y consiente decidir cualquier asunto sin la intervención de terceros, el consentimiento de uso de datos personales debe ser claro y entendible a los titulares los datos así mismo que garantice el derecho a la rectificación de acuerdo con el artículo 20 de la Constitución Política y el artículo 277, numerales 3,4 y 7 y el derecho al olvido.

2.2. Fundamento constitucional de la protección de datos personales

La ley de protección de datos personales desarrolla el marco normativo definido en la Constitución Política, basado en dos principios constitucionales como libertad y la privacidad (artículos 20 y 15 respectivamente). El primer principio, establece que ninguna persona podrá ser censurada, se garantiza la libertad de expresar y difundir sus pensamientos y cualquier tipo de opinión, partiendo de este se desprende el principio de la autodeterminación informática, donde toda persona es libre de manifestar sus pensamientos establecer el ámbito de público y privados de sus datos personales, cualquier tercero de que almacene los datos de las personas deben contar con expreso consentimiento del titular de los datos.

En segundo lugar, encontramos el principio de la privacidad, donde las personas de manera libre y voluntaria deciden quien puede usar su información personal, las cuales de manera voluntaria deciden quien puede tener acceso a su datos sensibles, los responsables del tratamiento deben respetar y guardar la reserva de datos entregados por sus titulares quienes deben conocer ampliamente su propósito y el tiempo de uso, se debe garantizar la protección de la intimidad de las personas y protegerlas de las estrategias malintencionadas que atenten contra la libertad personas, lo anterior genera un desafío con la evolución de la industria 4.0.

2.3. Principios rectores del tratamiento de datos personales

Encontramos los parámetros de la presente norma, desarrollando en ocho principios que fundamentan la protección de los datos pernales: “legalidad, finalidad, libertad, veracidad y calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad” (Ley 1581, 2012).

2.3.1. Principio de legalidad en materia de tratamiento de datos personales

En este principio de legalidad encontramos un número significativo de normas que regulan la jurisprudencia y tratados internacionales en el tratamiento de datos personales, a través de la recolección, tratamiento e indexación de datos personales , los cuales debe ser capturados cumpliendo los parámetros legales y formalidades que establece el legislador

2.3.2. Principio de finalidad

Dentro de sus principales características encontramos que el titular del dato debe ser informado, de cuál va a ser la finalidad de los datos personales a capturar, por ende, ser debe realizar el contrato de trasmisión de datos personales en el acuerdo de voluntades. Se debe informar los alcances del tratamiento de datos personales, especificando la recolección, almacenamiento, uso, circulación y supresión, estableciendo e informado de manera clara, sucinta y detallada de su finalidad, así mismo debe quedar plasmadas las obligaciones del responsable o encargado del tratamiento quien debe garantizar la seguridad y confidencialidad de los datos.

2.3.3. Principio de libertad

Este principio establece que para poder utilizar los datos personales debe contar con la debida autorización legal, que se autorice a terceras personas para la recolección, tratamiento, circulación de datos personales, dicha autorización debe ser libre y consentida por el titular que suministra.

2.3.4. Principio de veracidad y calidad

Este principio base principal radica en que los datos personales deben ser exacta, real, actualizada, confiable e integra que no genere ningún tipo de imparcialidades o sea descontextualizada, inexacta, incorrecta e incoherente, esto afecta el derecho al buen nombre de los titulares de los datos, que cumpla con los estándares calidad internacionales y directrices de la Superintendencia de Industria y Comercio, que regula esta materia.

2.3.5. Principio de transparencia

Este principio obliga al responsable o encargado a salvaguardar los datos, garantizando a los titules de los datos trasparencia en todas las actuaciones que requieran de tratamiento de los datos suministrados, tanto para entidades públicas como privadas, y de requerirse, estar en la disposición de entregar la información solicitada por el titular referente a el mismo.

2.3.6. Principio de acceso y circulación restringida

Este principio indica una restricción, ya que solo las personas autorizadas por los titulares pueden tratar los datos y se debe contar la debida autorización, de acuerdo con lo estipulado en la norma que estableció unos límites legales al acceso y circulación de los datos.

2.3.7. Principio de seguridad

Este principio obliga a todas las entidades tanto públicas como privadas, a adoptar las medidas de seguridad en el tratamiento de los datos personales, de acuerdo con los 3 pilares que son integridad, confidencialidad y disponibilidad que se en cuentan bajo su custodia.

2.3.8. Principio de Confidencialidad

Este principio indica que los datos personales, no se pueden revelar, ni suministrar a terceras personas que no estén definidos en el tratamiento de datos, la ley colombiana tácitamente regula que casos puede ser levando este principio sin que en ello se viole los derechos fundamentales de los titulares de los datos.

La Corte Constitucional en la Sentencia T-114 de 2018, se refiere a la solicitud de videos de sistemas de vigilancia que pueden estar en poder de instituciones públicas, empresas privada o particulares, que buscan brindar seguridad en espacios públicos o de dominio público, la cual puede ser obtenida y ofrecida sin ninguna reserva, también información de carácter semiprivada que cuenta con un grado de mínimo de limitación, que puede ser obtenida por orden de la autoridad administrativa en cumplimiento de sus funciones.

Otro tipo de información es la de carácter privado que puede contener información personal o no, por encontrase en un ámbito privado o de limitaciones al acceso, que sólo podrá ser obtenida y ofrecida por orden de la autoridad judicial en caso de requerirse, por último, encontramos la información reservada o secreta que tiene ver con la protección de los derechos fundamentales como la dignidad, intimidad y libertad que no puede ser obtenida, ni ofrecida por la autoridad judicial, pero podrán existir ponderaciones[2] que surjan en el curso de un proceso y que el juez sea el encargado de valorarlas por su relevancia atendiendo a un tema probatorio donde prime la protección de un derecho fundamental en el cual pueda verse afectado un menor.

---

[2] Código de Procedimiento Penal (Ley 906 de 2002), articulo 23 Cláusulas de exclusión, y artículo 455 Nulidad de la prueba ilícita.

Los dispositivos inteligentes, sistemas video y reconociendo facial utilizados para brindar seguridad a las personas, al momento de realizar algún tipo de transacción de datos personales, deben respetar los principios de la Ley 1581 de 2012 y garantizar el respeto por los derechos fundamentales a la intimidad, privacidad y al buen nombre consagrados en la carta política, donde es indispensable que se informe a los titulares que se encuentra en una zona de video vigilancia ya sea a través de audios o mensajes ubicados en sitios visibles, y también es importante informar que en ese lugar se realiza grabación de audio; de realizarse, como en el caso de entidades bancarias.

La Superintendencia de Industria y Comercio cuenta con una guía[3] para la protección de datos personales en sistemas de video vigilancia, para que las empresas adecuen estos a las disposiciones de protección de datos personales. La Corte ha reconocido que los sistemas de vigilancia son herramientas encaminadas a disuadir, prevenir delitos, faltas e identificar personas que las han cometido, porque las personas al estar en entorno de vigilancia, les resulta más difícil realizar algún acto delictivo.

Las cámaras de vigilancia instaladas en espacio semipúblico o semiprivado donde no es el Estado quien controla la grabación sino un privado, como puede suceder en centros comerciales, unidades residenciales, restaurantes y otros, estos no vulneran ningún derecho al permanecer en su esfera privada a menos que sea divulgada por un tercero.

La Sentencia C-094 de 2020, realiza un control constitucional al artículo 237 de la Ley 1801 de 2016 Código Nacional de Seguridad y Convivencia Ciudadana en el cual expresa:

[3] http://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Guia_Vigilancia_sept16_2016.pdf

"La información, imágenes, y datos de cualquier índole captados y/o almacenados por los sistemas de video o los medios tecnológicos que estén ubicados en el espacio público, o en lugares abiertos al público, serán considerados como públicos y de libre acceso, salvo que se trate de información amparada por reserva legal" (Sentencia C-094, 2020).

La Corte Constitucional declaró exequible condicionadamente este articulo porque deberá ser interpretado de acuerdo con el tipo de espacio (público, semipúblico, semiprivado y privado), tomando los principios de legalidad, finalidad, libertad, trasparencia, acceso, seguridad, confidencialidad y la circulación restringida, que deberán observarse en cada caso particular para no vulnerar el derecho a la privacidad al cual tiene derecho todas las personas. Las posibles violaciones a la protección de datos personales y al derecho a la intimidad y privacidad pueden materializarse al momento en que una persona implemente un sistema de video vigilancia (CCTV) con o sin audio o dispositivos de reconocimiento facial, en el cual se procese la información del video o identificación facial, para perfilamiento y seguimiento, asociado al enlace de esos sistemas con la red de cámaras de la Policía Nacional como mecanismo de vigilancia masiva de los individuos.

El perfilamiento puede realizarse en sistemas de video vigilancia, a través del registro de sucesos diarios realizados de forma manual por una persona en bitácora de control, donde la información relevante del o los sujetos quedara consignada, otra forma es a través de los sistemas de AI, los cuales permiten la identificación de personas de forma automatizada a través las mediciones morfológicas de cada rostro que aparece en el video y que luego es registrado ese identificador o llave única de ese rostro en una base de datos, que permitirá su consulta y clasificación posterior, de acuerdo las necesidades o requerimientos que se deseen aplicar a futuro.

El reconocimiento facial de una persona, genera un id o llave de identificación que puede ser un número o conjunto de caracteres que generan identidad única un rostro, proceso se encuentran regulado por estándares internacionales IEEE de inteligencia artificial, se toma de medidas morfológica del rostro que son digitalizadas establecido una identificación facial, como las mediciones, pueden considerarse datos sensibles de las personas de acuerdo con la Ley 1581 de 2012. Los sistemas de video vigilancia o CCTV deben aplicar la Ley 1581 de 2012 y la guía de la Superintendencia de Industria y Comercio, así como deberán ceñirse a los pronunciamientos de la Corte Constitucional en relación con la protección de datos personales en los diferentes espacios, ámbitos o esferas de la vida privada de las personas que permitan garantizar la privacidad e intimidad.

En la Sentencia T-768 de 2008, la Corte estableció una serie de criterios que se deben realizar al instalar los sistemas de video vigilancia, que son:

- Que el objeto social de la empresa requiere de la medida de seguridad necesaria para proteger sus intereses.
- Que los lugares en los que se instalen las cámaras sean lugares que de forma razonable sean zonas de trabajo, donde el trabajador no ejerza actividad privada como lugares de descanso, baños o vestuarios.
- Que la finalidad tenga una relación directa con la seguridad.
- Que, si existiese otra medida menos invasiva, se implemente.
- Que las personas estén informadas de este tipo de sistema de vigilancia.
- Que los perjuicios causados por la implementación de esta medida sean mínimos.
- Que la medida genere ningún tipo de maltrato o violación a los derechos humanos y del trabajador.

(Sentencia T-768, 2008)

Es de resaltar que actualmente la instalación de cámaras de reconociendo facial no se encuentran reguladas en Colombia.

Capítulo 3

La industria 4.0 e hiperconexión de dispositivos inteligentes

La híper conexión de las personas ya es un hecho, a través de sus dispositivos, celulares, Smartphone, Tablet, computadores personales, relojes inteligentes, equipos control médico, dispositivos instalados en los vehículos, casas, oficinas y empresas, tiene la capacidad de intercomunicarse entre ellos e intercambiar y capturar datos, que son almacenados, usados, procesados indexados a través de la Big data, son llevados ante por poderosos algoritmos basados en inteligencia artificial, permiten identificar hábitos de consumo de las personas, diseñar y crear nuevo productos de acuerdo a las necesidades de las personas y establecer estrategias personalizadas de mercadeo con de captar un mayor número de usuarios, permitiendo identificar cambios y amenazas futuras.

En era de la industria 4.0, su principal materia prima son los datos, es la base primigenia de la inteligencia artificial llevando al hombre hacer lo impensable, lo antes era solo un sueño surrealista hoy es una realidad, estos poderosos algoritmos están evolucionado de tal manera que gracias al procesamiento de datos de todas las personas que se encuentran hiperconectadas alimentado poderosos servidores cuánticos que realizan un sin número de ecuaciones en milésimas segundo y aprenden de manera autónoma y permanente , evolucionado el cada rama conocimiento de la humanidad[4].

Llevando al mundo a la era de la virtualidad, digitalización y automatización de cada una de las actividades productivas y cotidianas de los seres humanos, evolucionado a pasos a giganta-

[4] Autor Wilmar Darío Restrepo Gil

dos, cimentado las bases de conocimiento, fortaleciendo la industria del dato, creando nuevos entornos sociales que se enlazan en una sociedad digital cada día más activa y globalizada, generando costumbres, hábitos, conflictos sociales y nuevos espacios de aprendizaje.

Estamos en sociedad donde su evolución que depende del dato, que habita paralelamente en el mundo virtualidad, que se encuentra interconectada con el espacio físico, su eje principal son sus ciudadanos digitales que se encuentran monitoreados través de dispositivos inteligentes, quienes habitan en ciudades, casas, y trabajan empresas controladas por cámaras de reconocimiento facial, dispositivos biométricos y robots que automatizan las labores cotidianas del hombre, quienes permanentemente generan millones y millones de datos, almacenados en ceros y unos.

Nada es imposible, cada una de las actividades rutinarias que hace el hombre se hacen en menos tiempo, hay menor desgate físico y mental, mejor calidad de vida, pero dependiente totalmente de la tecnología y hasta el punto de no poderse desconectar por la alta dependencia que han generado en la sociedad, vulnerando los derechos fundamentales, especialmente en especial la intimidad, privacidad, libertad, protección de datos personales y la autodeterminación. De manera consentida las empresas accedan a la información más sensible de las personas, acceden a los contactos, fotografías, contraseñas, transacciones bancarias, perfiles de redes sociales, historial de navegación de páginas web, ubicaciones y seguimientos del dispositivo, apertura de cámaras y micrófonos de los dispositivos electrónicos por parte de los responsables o terceros que han sido autorizados o que vulneraron la seguridad.

Los algoritmos controlan la vida de las personas, hacen realidad los sueños, generan barreras con el mundo fisco, se ha perdido el contacto personal con los seres queridos y entornos sociales, las personas se sumergen en redes sociales, la internet profunda y la realidad aumentada, sacrifican lo bello que es interactuar físicamente con los seres queridos, se ha renunciado al

contacto físico y a los entornos sociales, aceptando la soledad y compañía un dispositivo inteligente, sumergiéndose en un mundo de virtualidad y la comodidad de los dispositivos autómatas que hacen un vivir más cómodo, pero con grandes problemas de depresión.

3.1. El tratamiento de datos personales y el Internet de las cosas problemática actual

El libre desarrollo de la personalidad prescrito en el artículo 16, permite que cada ser, se desarrolle libremente y que tenga libre albedrio, en el cual pueda tomar sus propias decisiones, con conciencia, voluntad y sin ningún tipo de coacción, imposición o preordenamiento de su comportamiento. Dicho lo anterior la sociedad globalizada depende hoy en día de los artefactos tecnológicos, que por medio de programas (aplicaciones o Apps), permiten interactuar para hacer la vida más cómoda, conectados a la red de internet, en la cual se pueden gestionar estos artefactos sin estar ubicados en el sitio donde se encuentra el equipo. Cada día aumenta el número equipos electrónicos y eléctricos conectadas a internet, lo que muchos definen como el internet de las cosas, que para entenderlo mejor es una pequeña computadora con memoria, unidad de procesamiento, unidad de almacenamiento, sensores, red wifi y bluethood que van inmersos en bombillas de luz, switches, interruptores, persianas, cafeteras, calefacciones o cualquier tipo de dispositivo que requiera energía puede estar conectado y del cual pueda brindar beneficio o resuelva una problemática. La web 3.0 [5]se refiere a los dispositivos que están conectados a internet, capaces de procesar información de entrada a través de un leguaje natural como órdenes verbales dadas

[5] “La idea de web 3.0, en este contexto, está relacionada a lo que se conoce como web semántica. Los usuarios y los equipos, en este marco, pueden interactuar con la red mediante un lenguaje natural, interpretado por el software” (Definición de web 3.0, 2021)

por el usuario, las cuales son procesadas por un sistema de IA, que realiza las operaciones con rapidez.

Los equipos anteriormente mencionados requieren de una configuración previa para poder utilizarlos, dentro de esta configuración previa se requiere el registro de la persona que lo va utilizar, para que allí asocie y configure todos los dispositivos de ese fabricante y es allí donde debe existir una protección de los datos ingresados y el tipo de tratamiento que se le va a dar a esos datos, puesto que si en algún momento esos datos caen en manos de personas inescrupulosas, podrán generar influir en el comportamiento de las personas, realizando afectaciones leves o severas a la privacidad y al libre desarrollo de la personalidad, como sucedió en el caso de una familia que tenía conectada una cámara IP y un hacker se conectó al sistema[6], logrando conversar con una niña de 8 años de edad. Cualquier persona podría decir que el acceso a las cámaras se debió a la brillantez de hacker o atacante; pero es importante analizar los factores que pueden influir en este tipo de delitos, que van desde el tratamiento de datos personales y el cómo son gestionados, así como la vulnerabilidades que puede tener en el software con el que opera la Cámara y también la forma de trasmisión de la información, que en muchos casos va sin ningún tipo de cifrado, lo que permite que cualquier persona en la red capture las claves de conexión, para luego conectarse[7].

Es importante conocer que muchos de los fabricantes prefieren sacar al mercado un producto a bajo precio que cumple con su funcionalidad, pero que cuenta con vulnerabilidades que el usuario final desconoce y que pueden influir en los comportamientos. La fabricación de los

---

[6] Hackean una cámara 'Ring' en la habitación de una niña - Noticias Telemundo https://www.youtube.com/watch?v=EFkjNNq3l1M

[7] Autor: Alejandro Jiménez García

equipos tecnológicos debería realizarse bajo el sistema de buenas prácticas, el cual realiza gestión de la calidad, los materiales utilizados, que genere responsabilidad social en la contratación del personal y la producción responsable que incorpora la utilización de altos estándares en la integración de hardware y el software, que permita garantizar seguridad en la operación de estos, en un entorno globalizado como es internet y las vulnerabilidades que existen y que han sido mitigadas, para reducir el riesgo de exposición.

El internet de las cosas está permitiendo que las empresas que venden productos puedan tener acceso a las estadísticas en tiempo real en la utilización de los equipos, lo cual podría considerarse como una intromisión a la esfera de privacidad que debe tener cada persona, como es el caso de una persona que sufre de apnea del sueño que hace sus ronquidos sean muy fuertes, y que le indicaron que debía utilizar una máscara con un generador de oxígeno todas las noches. Después de unos días de estarlo utilizando, lo llamaron indicándole que lo estaba utilizando mal porque según la persona que lo contacto de la compañía de seguros, él no había seguido las instrucciones porque el día martes solo lo había utilizado el equipo por 3 horas, el miércoles 4 horas, siendo una clara violación a su privacidad y a los datos personales generados por el equipo[8].

En el mercado existen diferentes dispositivos capaces de medir la información referente a nuestro cuerpo y enviar los datos a través del celular a una base de datos en la nube, un ejemplo de esto es KEGG, este es dispositivo capaz de medir el fertilidad de una mujer en diferentes momentos del día y enviar esos datos a un sistema de almacenamiento, donde serán susceptibles de algún tipo de tratamiento de datos por parte del responsable o encargado de acuerdo a la política de tratamiento de datos que se hubiera aceptado para la utilización, pero es importante resaltar

---

[8] El internet de las cosas - nuestra relación con Internet - DW Documental
https://www.youtube.com/watch?v=iUbR046La68

que si el acuerdo no es aceptado por consiguiente no se podrá utilizar el producto y el usuario no podría obtener los beneficios. La información capturada de cada mujer que adquiera este tipo de dispositivos podría ser vendida y compartida con las farmacéuticas que fabrican estos tipos medicamentos, comprometiendo la información privada e íntima de las mujeres usuarias del dispositivo en vender los medicamentos. El tratamiento de estos datos personales podría resultar muy beneficioso para algunos y para otros sería algo perjudicial, que podría influir en el valor del seguro médico, incrementando o reduciendo su valor y en casos particulares negar el acceso al servicio, imponiendo cuotas desorbitantes.

El internet de las cosas incluye tecnología de Inteligencia Artificial, que permite administrar diferentes equipos enlazados por el internet en hogares, empresas e instituciones, que pueden convertirse en un instrumento para atentar contra tranquilidad psicológica de las personas, por interrumpir violentamente generando sonidos a medianoche, prendiendo y apagando las luches, subiendo las persianas, encendiendo la lavadora que perturben el sueño, causado temor y miedo, afectando tranquilidad. Por lo general una casa inteligente, contiene equipos de diferentes fabricantes, que pueden tener algún tipo de vulnerabilidad que pueda ser explotada por una persona o hacker, que pudo obtener información de un tratamiento de datos personales previo, que pueda ser evidente en las estadísticas o logs de acceso, que sea rastreable por su dirección IP, para que las autoridades inicien la investigación correspondiente para dar con los responsables de esas conductas sancionadas en el código penal Art. 269A al 269J , siempre y cuando no se utilice una VPN para esconder su rastro y sea imposible individualizar a la persona o establecer su ubicación.

3.2. Los algoritmos en aplicaciones diarias

El desarrollo de diferentes aplicaciones de uso diario, ha permitido que las personas se encuentre informadas de los acontecimientos que suceden en el mundo, a través de noticias de los medios de comunicación de amplia circulación dependiendo el país, así como de otros medios alternativos como pueden ser redes sociales o sitios dedicados a informar de una manera particular, donde en unos su objetivo primordial es dar de forma breve la información y donde puede pasar gran cantidad de tiempo interactuando. La piscología social, es el entendimiento del comportamiento de los seres humanos mezclado con la implementación de reglas de comportamiento que van de la mano con los gustos, sensaciones y emociones que han sido implementadas en algoritmos que responden frente a cada situación o comportamiento que ocurre en cada momento de interacción[9].

En la actualidad las personas usan las redes sociales para sentirse conectados con el otro y debido a fácil utilización no es difícil sentirse atrapado viendo videos y videos de personas alrededor del mundo, que venden artículos de vestir, cosméticos, viajes entre otros, información que ha sido programada y puesta allí para cada quien de acuerdo a su perfil, nivel de estudios, edad, genero, gustos y la ciudad de residencia, pero es allí donde se empieza generar una redefinición del ente conectado por la información presentada en la App o programa de acuerdo a los objetivos definidos en el algoritmo[10].

---

[9] Internet de las Cosas DW Documental - https://www.youtube.com/watch?v=iUbR046La68
[10] Autor: Alejandro Jiménez García

3.3. Reconocimiento Facial y Biomarkentig

Hoy en día encontramos una sociedad digital que viene siendo programada y vigilada por la industria de dato, a través de algoritmos cuya finalidad es analizar nuestros hábitos, conductas, gustos entre otros, mediante el uso de data points, cookies o el uso de cámaras de reconocimiento facial muy utilizadas en Colombia en dispositivos de acceso de seguridad en oficinas y conjuntos residenciales, control de espacios públicos y privados, centros comerciales y dispositivos inteligentes (celulares , Tablet, computadores) entre otros.

Cada día es más común habituarnos que nuestros dispositivos de comunicación , son inundados de publicidad personalizada, que surge a partir de la consulta de algún tipo de producto en una página web o cuando se visita una tienda un centro comercial, donde han capturado los datos, ya sea porque los suministro al cajero al momento de realizar la compra o por indexación de bases de datos bancarios o el uso de compras a través de tarjetas crédito, por lo cual han identificado e individualizado a la persona que compro, esta información de las personas se recolectan de forma masiva a través de cámaras de reconocimiento facial, que hacen parte de la información sensible de cada persona, que luego es utilizada para generar publicidad personalizada de acuerdo a un perfilamiento, lo que se llama el Biomarkentig.

El Biomarketing es una tecnología que viene siendo utilizada en países como China, Finlandia y Estados Unidos, en Colombia hay empresas como el grupo éxito y las empresa de apuestas GANA, que han querido implementarlas aun no lo han logrado, debido a que Colombia no existen bases de datos estructuradas de identificación facial, hoy con implantación de la cedula digital en Colombia a través de la registraduría puede hacerse una realidad, ya que las que existen se encuentran almacenadas están en manos de las empresa oficiales y privadas, regular-

mente son utilizadas, para el acceso visitantes a oficinas públicas, control de empleados, residentes, oficinas, conjuntos residenciales y control de espacios públicos en Medellín como el estadio Atanasio Girardot y el Metro de Medellín para temas de seguridad pública. Una vez se estructuren esto será una realidad en nuestro país.

Para entender la evolución Biomarketing y el impacto social, la publicidad personalizada es generada a través cámaras de reconocimiento facial, que analizan e indexan los datos a través algoritmos cuánticos y algoritmos de aprendizaje profundo las personas son clasificadas y perfiladas a través de sus rasgos faciales, por su edad, sexo, raza, gustos, lectura y estudio de expresiones como, aceptación, rabia, tristeza en un determinado producto. Identificados gustos, comportamientos, es enviado atreves de sus dispositivos electrónicos asociados a la persona publicidad personalizada, con el fin de crear la necesidad de compra del producto[11].

La identificación de patrones en el reconocimiento facial a través del análisis las expresiones de las personas, puede determinar qué tipo de producto puede estar requiriendo a través de una publicidad personalizada, enviada al dispositivo móvil en la App, red social, induciendo a la personas a la compra del producto inferido, induciendo a la aceptación de del modelo consumista de moda y costumbre, influyendo de forma psicológica en la personalidad de personas y en la autodeterminación del ser, perdiéndose la capacidad auto determinarse y tomar decisiones de manera consiente.

Los anuncios publicitarios vienen cargados de mensajes que están diseñados, solo para vender producto y generar ganancias a las compañías, basadas en estrategias de engaño y mani-

[11] Autor: Wilmar Darío Restrepo Gil

pulación, invadiendo la privacidad y la capacidad de auto determinarse, que en muchas ocasiones descontextualizan la realidad de la personas, donde no existe la éticas y tampoco controles legales.

Existen grandes beneficios en el Biomarketing, como el poder recibir ofertas de productos a la medida acorde de las necesidades, tener una experiencia personalizada, conectar a las personas con marcas productos que no conocían en el mercado, comprar productos a menor precio y ampliar el catálogo de productos que se ofrecen a los clientes, crear nuevas ideas de emprendimiento entre otros.

Las empresas dedicadas al comercio online en Colombia vienen adelantado campañas publicitarias personalizadas, encontramos cadenas como Falabella, Mercado Libre, Linio, Grupo Éxito, Decatlón, Homecenter entre otros envían a cada uno sus clientes una publicidad híper personalizada con contenido de sus productos[12], una estrategia que va mucho más allá, busca conocer de manera detallada a sus clientes atreves de sus datos ,estableciendo unos patrones de conducta y seguimiento de intereses y gustos a través captura de datos a través de data Points o cookies, permitiéndoles identificar el interés de sus visitantes por determinado producto, seleccionar canales de distribución de manera rápida y efectiva, establecer precios del mercado con referencia a su competencia, fortalecer estrategias la venta por canales de comercio electrónico.

[12] Híper personalización - https://www.puromarketing.com/30/29188/hiper-personalizacion-cual-siguiente-paso-evolucion-customer-engagement

Conclusiones

Colombia ha evolucionado de manera importante en materia de protección de datos personales, con el surgimiento nuevos desarrollos tecnológicos que ha traído cambios trascendentales en las bases la sociedad, generando conflicto de derechos entre los ciudadanos que son dueños de sus propios datos y las empresas de desarrollo tecnológico que buscan sacar beneficios económicos y políticos a costa de sacrificar derechos fundamentes de las personas a cambio de ofrecer beneficio y comodidades.

Es necesario regular el uso de cámaras de reconocimiento facial asociados algoritmos cuánticos y aprendizaje profundo en Colombia, ya esta tecnología va más allá de una expectativa razonable del ámbito privacidad e intimidad y protección de datos sensibles de las personas , al generar un identificación facial con base de cada ciudadano, monitorearlo y realizar seguimiento en espacio públicos y semiprivado e hiperconectarlas con los dispositivos inteligentes que utilizan estas en sus actividades dirías.

Los sistemas de video vigilancia han permitido brindar mayor seguridad en las ciudades y en los espacios privados, semiprivados, semipúblicos y públicos, en los cuales pueden quedar registradas conductas delictivas o que simplemente no se materializan por el solo hecho de saber que están siendo grabadas. Los sistemas de reconocimiento facial son el producto de la evolución de los CCTV y poco a poco toman más relevancia en las sociedades, debido a las capacidades de identificación de las personas que van transitando por los lugares donde están implementados. Las aplicaciones de los sistemas de reconocimiento facial van desde la seguridad en espacio públicos como estadios, estaciones de metro, así como en sitios semiprivados como unidades residenciales o centros comerciales, que son espacios denominados semipúblicos, y no solamente en temas de

seguridad como lo ha venido realizando el gobierno chino para identificar buenos ciudadano de malos ciudadanos con puntuación o crédito sociales[13].

Las implementaciones de reconocimiento facial no solamente van desde el lado gubernamental, las empresas se involucrado en el tema y poco a poco crecen las diferentes aplicaciones de sistemas de reconocimiento facial a través híper personalización en el comercio[14], para perfilar consumidores, hábitos, emociones, necesidades y lograr mayores ventas que permitan lograr una empatía entre el comprador y el almacén. Los almacenes de cadena están implementando reconocimiento facial, como medio para realizar pagos electrónicos, sin la necesidad de tarjeta de crédito y documento de identificación, en algunas universidades, empresas y unidades residenciales se está utilizando este medio como mecanismo de ingreso, pero estas funcionalidades pueden traer consigo algunos errores al momento de reconocer al individuo, puesto que lo puede confundir con otro sujeto con mediciones similares, es el caso de dos hermanos de diferentes edades donde el sujeto número 1 niño puede desbloquear el teléfono iPhone faceid[15] del número 2 y otros casos de similares entre madre e hijo.

Los sistemas de reconocimiento facial con IA, integrados a los CCTV constituyen una injerencia de esta tecnología en la privacidad e intimidad de las personas como medida de control para garantizar derechos y libertades de los gobiernos, que de la misma forma planteo Michael Focaul[16]t en el panóptico donde en una torre se tiene el control a través del poder judicial, político

---

[13] Buenos ciudadanos y malos ciudadanos https://www.youtube.com/watch?v=pZu9N-3yn_M
[14] Híper personalización - https://www.puromarketing.com/30/29188/hiper-personalizacion-cual-siguiente-paso-evolucion-customer-engagement
[15] Hermano desbloquea iPhone faceid de su otro hermano https://www.youtube.com/watch?v=4VdXSOZGoK0
[16] Michael Focault- Filosofo https://es.wikipedia.org/wiki/Michel_Foucault

y económico que en determinado momento pase inadvertido convirtiéndose en una sociedad disciplinaria que controla a los individuos mediante la imposición de vigilancia[17].

Las tecnologías de la industria 4.0 requieren de maduración para que puedan explotar su máximo su potencial, minimizando y controlando errores, que puedan surgir en el proceso, evitando detenciones arbitrarias, como en el caso del ciudadano argentino[18], que fue privado de su libertad durante 6 días. La implementación de pagos a través de reconocimiento facial, pueden ocasionar cobros de compras a personas que no las han realizaron o futuras estafas al engañar a los sistemas de reconocimiento.

En la actualidad no existe una prohibición del uso de reconocimiento facial en sistemas de video para las empresas privadas, pero es aplicable la misma guía de la SIC[19] para CCTV en el tratamiento de datos personales ley 1581 de 2012, el deben cumplir a todas las personas o empresas para el tratamiento de datos personales, pero es importante resaltar que el reconocimiento facial en este tipo de sistemas, implica una extracción de imágenes para el procesamiento IA de forma masiva y automatizada de los rostros de las personas que transitan por el lugar donde están operando y que a la postre requieren de la autorización del titular, donde se indique de manera clara, el objeto, alcance y quienes podrán realizar el tratamiento de datos, debido a que el rostro hace parte de un dato personal y sensible de cada persona y no es un dato anónimo como algunos pueden argumentar.

[17] Autor: Alejandro Jiménez García
[18] Detención ciudadano argentino por 5 días https://www.youtube.com/watch?v=GHDI-VOJgqo
[19] SIC – Superintendencia de Industria y Comercio

Se hace necesario generar mecanismos que permitan informar los ciudadanos de manera permanente, donde se encuentran sus datos sensibles su finalidad y uso de estos, se debe permitir al ciudadano administrar sus datos de manera, consiente, informada y autónoma disponga de ellos, se deben proporcionar medios de consulta que permitan medir en tiempo real uso y ubicación sus datos, borrarlos, modificarlos entre otros sin la intervención de terceras personas, aplicar el derecho al olvido en momento que este los dese , este es un derecho que debe asistir a todos los ciudadanos ya que son los propietarios de estos y no se deben considerarse activos de las empresas.

El estado debe generar y actualizar mecanismos jurídicos e institucionales que permitan garantizar derechos fundamentales en ámbito digital, autodeterminación informática, la intimidad, el derecho al óvido y habeas data, tendientes a proteger a los ciudadanos freten a las nuevas amenazas digitales y regular nuevas conductas digitales , mediante la generación de políticas públicas y adhesión de tratados internacionales, ya que la legislación y jurisprudencia actual quedó corta , para garantizar a su ciudadanos sus derechos en la protección de los datos de los ciudadanos.

La Unión Europea y sus países miembros han desarrollado una serie de regulaciones que busca proteger los derechos fundamentales de las personas y donde los avances tecnológicos imponen la integración de estos sistemas de IA[20] en el ámbito social y cotidiano, que contribuyen al desarrollo de la sociedad más justa e igualitaria, para lo cual es fundamental, reflexionar frente a posibles riesgos que han sido identificados y documentados por la Comisión Europea, para que de la misma forma sean regulados en Colombia, para que no atenten contra el estado social de derecho[21].

---

[20] IA – Inteligencia Artificial
[21] Autor: Alejandro Jiménez García

Bibliografía

Comisión Europea. (19 de Febrero de 2020). Libro Blanco. *Libro Blanco*. Bruselas, Belgica: Comisión Europea. https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf

Comision Europea. (21 de 4 de 2021). Reglamento del parlamento europeo y del consejo - por el que se establecen normas armonizadas P.D.P. *Reglamento del parlamento europeo y del consejo - por el que se establecen normas armonizadas P.D.P.* Bruselas, Belgica. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52021PC0206

Congreso de Colombia. (24 de Marzo de 1992). Ley 3 de 1992. *Ley 3 de 1992*. Bogotá, Cundinamarca, Colombia. http://www.secretariasenado.gov.co/ley-3-de-1992#:~:text=PAR%C3%81GRAFO%202o.,para%20conocer%20de%20materias%20afines.

Congreso De La República. (31 de Diciembre de 2008). Ley Estatutaria 1266 De 2008. *Ley Estatutaria 1266 De 2008*. Bogotá, Cundinamarca, Colombia. http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

Congreso De La República. (5 de Enero de 2009). Ley 1273 De 2009. *Ley 1273 De 2009*. Bogotá, Cundinamarca, Colombia. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso De La República. (17 de Octubre de 2012). Ley Estatutaria 1581 De 2012. *Ley Estatutaria 1581 De 2012*. Bogotá, Cundinamarca, Colombia: Diario Oficial No. 48.587 de 18 de octubre de 2012. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Consejo Permanente De La OEA. (17 de Octubre de 2011). Principios Y Recomendaciones Preliminares Sobre La Protección De Datos. *Principios Y Recomendaciones Preliminares Sobre La Protección De Datos*. Washington DC, ESTADOS UNIDOS: Documento presentado por el Departamento de Derecho Internacional de la Secretaría de Asuntos Jurídicos. https://www.oas.org/es/sla/ddi/docs/CP-CAJP-2921-10_rev1_corr1.pdf

Convención de la OCDE. (14 de Diciembre de 1960). Convención de la OCDE. París, Francia. https://www.oecd.org/acerca/documentos/convenciondelaocde.htm

Corte Constiticional. (31 de Julio de 2008). Sentencia T-768 de 2008. *Sentencia T-768 de 2008*. Bogotá, Cundinamarca, Colombia. https://www.corteconstitucional.gov.co/relatoria/2008/t-768-08.htm

Corte Constitucional. (2 de Abril de 2008). Sentencia C-1011 de 2008. *Sentencia C-1011 de 2008*. Bogotá, Cundinamarca, Colombia. https://www.corteconstitucional.gov.co/relatoria/2008/C-1011-08.htm

Corte Constitucional de Colombia. (2017). Sentencia T-574/ 2017. *Sentencia T-574/ 2017*. Bogotá, Cundinamarca, Colombia: Corte Constitucional de Colombia. https://www.corteconstitucional.gov.co/relatoria/2017/T-574-17.htm#:~:text=T%2D574%2D17%20Corte%20Constitucional%20de%20Colombia&text=La%20Corte%20estima%20que%20el,su%20pronunciamiento%20en%20esta%20oportunidad.

Corte Constitucional de Colombia. (2018). Sentencia T-114/2018. Bogotá, Cundinamarca, Colombia: Corte Constitucional de Colombia. https://www.corteconstitucional.gov.co/relatoria/2018/t-114-18.htm

Corte Constitucional de Colombia. (2020). Sentencia C-094/ 2020. *Sentencia C-094/ 2020*. Bogotá, Cundinamarca, Colombia: Corte Constitucional de Colombia. https://www.corteconstitucional.gov.co/relatoria/2020/C-094-20.htm

El Congreso de Colombia. (17 de Octubre de 2012). Ley Estatutaria 1581 De 2012. *Ley Estatutaria 1581 De 2012*. Bogotá, Cundianamrca, Colombia. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

El Congreso de Colombia. (29 de Julio de 2016). https://www.policia.gov.co/files/codigo-nacional-seguridad-y-convivencia-ciudadana. *Ley 1801 de 2016*. Bogotá, Cundinamarca, Colombia. https://www.policia.gov.co/files/codigo-nacional-seguridad-y-convivencia-ciudadana

El Congreso de la República. (6 de Marzo de 2014). Ley 1712 de 2014. *Ley 1712 de 2014*. Bogotá, Cundinamarca, Colombia. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

El Presidente De La República De Colombia. (27 de Junio de 2013). Decreto 1377 de 2013. *Decreto 1377 de 2013*. Bogotá, Cundinamarca, Colombia. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646#0

El Presidente De La República De Colombia. (13 de Mayo de 2014). Decreto 886 de 2014. *Decreto 886 de 2014*. Bogotá, Cundinamarca, Colombia. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=57338

El Presidente De La República De Colombia. (26 de Mayo de 2015). Decreto 1081 de 2015. *Decreto 1081 de 2015*. Bogotá, Cundinamarca, Colombia. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=73593#0

El Presidente De La República De Colombia. (18 de Enero de 2018). Decreto 090 de 2018. *Decreto 090 de 2018*. Bogotá, Cundinamarca, Colombia. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=85039

El Presidente De La República De Colombia. (4 de Marzo de 2019). Decreto 338 de 2019. *Decreto 338 de 2019*. Bogotá, Cundinamarac, Colombia. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=90730

El Presidente De La República De Colombia. (23 de Febrero de 2022). Decreto 255 de 2022. *Decreto 255 de 2022*. Bogotá, Cundinamarca, Colombia. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=179087

El Presidente De La República De Colombia. (23 de Febrero de 2022). Decreto 255 de 2022. *Decreto 255 de 2022*. Bogotá, Cundinamarca, Colombia. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=179087

Miranda, J. (2018). Tesis Doctoral. *Responsabilidad patrimonial por "wrongful conception","wrongful birth" y "wrongful life"* . Madrid, España: Universidad Complutense de Madrid.

Parlamento Europeo. (12 de Julio de 2022). Directiva 2002/58/CE Del Pamento Europeo y del Consejorla. *Directiva 2002/58/CE Del Pamento Europeo y del Consejorla*. Bruselas, Belgica: Diario Oficial de las Comunidades Europeas.

Pazos, R. (2016). Sentencia Consejo de Estado. Bogota D.C., Colombia.

Rico, L. (2017). Corte Suprema De justicia. *Sentencia SC 12063-2017*. Bogota,D.C., Colombia.

Unión Eurpoea. (25 de Mayo de 2018). Reglamento (Ue) 2016/679 Del Parlamento Europeo. *Reglamento (Ue) 2016/679 Del Parlamento Europeo*. Bruselas: Diario Oficial de la

Unión Europea. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679

Julián Pérez Porto y Ana Gardey. Publicado. (2015). Definición de web 3.0. Buenos Aires, Argentina. https://definicion.de/web-3-0/

Curriculum vitae

Alejandro Jiménez García

Alejandro Jiménez García, nació Medellín el 9 de septiembre de 1976, se graduó como ingeniero de sistemas en el año 2000 en la Universidad EAN de la ciudad de Bogotá, en el año 2002 emprendió su propio negocio de tabulación de encuestas de evaluación docente y análisis de información para U. de los Andes, U. Externado, U. Minuto de Dios, F. Área Andina, U EAN, U. San Buenaventura, U. de la Sabana y U. Iberoamericana. En el año 2015 obtuvo el título de Especialista en Gerencia de Proyectos de la Universidad el Bosque y en el año 2016 obtuvo el título de Especialista en Seguridad Informática de la Universidad Piloto de Colombia.

Desde el año 2004 asesora a la empresa Pinzón Pinzón & Asociados Abogados de la ciudad de Bogotá en el área de tecnología, en el desarrollo y actualización de los sistemas de información Fénix Data.

Wilmar Darío Restrepo Gil

Wilmar Darío Restrepo Gil, Nació Municipio de Concepción Antioquia el 28 de agosto de 1972, se graduó como ingeniero de sistemas en el año 2003 en la Universidad Uniremington Medellín, en el año 2013 obtuvo el título de especialista en Seguridad Informática. En la Universidad San Buenaventura Medellín.

Laboro en la policía Nación de Colombia por 26 años y se pensiono con el grado de subcomisario, se desempeñó como analista operacional y estratégico en la Dirección de Inteligencia y sí mismos fue jefe de Inteligencia del Gaula Medellín, dentro de su labor institución se destacó

por adelantar Operaciones contra el Secuestro y la Extorsión, Grupos de delincuencia Organizada y Operaciones de Táctica urbanas contra la Delincuencia Común