ACTIVIDAD DE APRENDIZAJE 3. Marco Teórico.

ACTIVIDAD 3

Metodología de la Investigación

UNIPANAMERICANA COMPENSAR

GRUPO # 1:

ANDREA RIAÑO PULIDO

DANIEL RICARDO BEJARANO BARBOSA

DIEGO ALEXANDER AGUILAR DIAZ

JONATHAN CASTILLO GRAJALES

RAFAEL ANTONIO CORTES CASTILLO

SEMESTRE VII

MODULO I

FACULTAD DE INGENIERÍA

TECNOLOGÍA EN ANÁLISIS Y DESARROLLO

DE SISTEMAS DE INFORMACIÓN

Mayo de 2020

**Tabla de contenido**

[**Introducción** 3](#_Toc39940460)

[**Marco Teórico** 4](#_Toc39940461)

[**Glosario De Términos Informáticos** 12](#_Toc39940462)

[**Referencias** 13](#_Toc39940463)

# **Introducción**

Esta Actividad de Aprendizaje se desarrolla para construir el Marco Teórico del Problema que se planteó en la primera Actividad, referente a si se debe imponer algún tipo de regulación para el uso de la inteligencia artificial con el fin de proteger la privacidad de los datos de las personas en Colombia.

Con base a lo anterior se realiza investigación de antecedentes válidos para la estructuración del estudio y encaminamiento del análisis del problema planteado.

# **Marco Teórico**

Breve historia de inteligencia artificial Las eras o etapas de la inteligencia artificial. La i.a. tuvo su boom a partir de la conferencia efectuada en el darmouthcollege en 1956 (aquí nace la i.a.).

1.-el inicio (1956-1965) poniéndose principal énfasis en la implementación de juegos en el computador (ajedrez, damas etc.), Así como en la demostración de teoremas.

2.-la etapa obscura (1965-1970) aquí se apoya el entusiasmo por la i.a.

3.-etapa del renacimiento de la i.a. (1970-1975), iniciado en la universidad de stanford con el sistema experto medico mycin (experto en enfermedades infecciosas de la sangre como la meningitis).

4.-etapa de las sociedades. (1975-1980) aquí se identifica la necesidad de trabajar en sociedad con profesionistas en otras áreas del conocimiento(dendral=mycin)

5.-etapa de la comercialización de la i.a. (Zambrano, 2009, pág. 5).

Derecho a la protección de datos personales o autodeterminación de la información

Algunas legislaciones tales como la Data Protection Act de 1998 de Reino Unido, Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal de España, y la Ley Estatutaria 1581 de 2012 de Colombia coinciden en que existen principios que rigen la protección de datos personales:

Consentimiento informado: para la recolección, el almacenamiento, el uso, la modificación o eliminación de los datos personales es indispensable contar con el consentimiento del titular de forma expresa. (2017, Foro revista derecho, foro 9)

Confidencialidad de acceso y circulación restringida: los datos personales siempre son confidenciales, excepto que exista el consentimiento o la autorización judicial para divulgarlos. La autorización judicial se aplica en los casos que exista una lesión, fundamentada en las libertades o derechos de otras personas, que se conoce como principio de lesividad.

Legalidad: el tratamiento de los datos personales estará sujeto a las normas legales.

Al utilizar el mecanismo legal del hábeas data se ejerce el derecho a la información, pero de forma específica, porque es un instrumento que permite a las personas conocer la información propia contenida en bases de datos públicas o privadas con el objetivo de autorizarla, modificarla, rectificarla o eliminarla para de esta forma ejercer el derecho a la protección de datos personales. El objeto del hábeas data es toda la información personal que se encuentre bajo custodia, administración o tenencia del Estado o institución privada, mientras que el objeto del derecho a la información es más amplio, porque es aquel que se encuentre bajo custodia del Estado, al respecto se señala que “se refiere a toda la información en bases de datos públicas significante, cuya definición debe ser amplia, incluyendo toda la que es controlada o archivada en cualquier formato y medio”. (2017, Foro revista derecho, foro 10)

Historia de los drones

En nuestro tiempo, el creciente auge de los drones entre los consumidores ha coincidido con la tecnología que lo ha posibilitado. Nos estamos refiriendo a la tecnología de los smartphones, en virtud de la cual los drones pueden reconocer su posición y la dirección de su movimiento. Los propios teléfonos inteligentes sirven como mandos a distancia para pilotar los drones. Sin embargo, la demanda progresiva por parte de los consumidores finales también ha desempeñado un papel determinante en su éxito. Concretamente, se debe al hecho de que permiten a la llamada generación selfie tomar fotografías espectaculares de sí mismos o de sus hogares desde el aire. Así las cosas, los cuadricópteros se han convertido en los drones más populares debido a su precio económico y menor complejidad. THEILMANN (15) sitúa el auge actual del uso de los drones recreativos en la feria Consumer Electronics de Las Vegas del año 2010, en la que se presentó el Parrot AR 1.0®, dron que puede manejarse mediante una aplicación para iPhone y que permite a los usuarios tomar fotos y vídeos de baja calidad. Sin embargo, fue en 2013 cuando el fabricante chino DJI presentó el dron Phantom®, que muchos autores consideran el precursor de la tecnología moderna de los drones de consumo, que incluía una cámara GoPro de alta calidad y la transmisión de imágenes en directo a través de una aplicación para smartphones. (Barrio, 2018, pág. 44)

Usos actuales

Los drones están siendo aplicados para una creciente variedad de propósitos, en constante ampliación. Su impacto se compara al que los automóviles han tenido en el siglo XX. Como botón de muestra, cabe apuntar que las fuerzas y cuerpos de seguridad los utilizan para el examen forense de las escenas del crimen y en operaciones policiales de alto riesgo. O para la evaluación de daños en catástrofes naturales. También se aplican para la filmación de eventos deportivos y la realización de documentales. Las capacidades de vídeo y fotografía de los drones están siendo aprovechadas en películas, reportajes y obras artísticas. Del mismo modo, se utilizan para el patrullaje de fronteras, la vigilancia del tráfico, el mantenimiento de oleoductos y gasoductos, la limpieza de líneas de alta tensión, la seguridad portuaria, la cartografía del terreno, la detección de construcciones no declaradas o ejecutadas excediendo los contenidos de la licencia urbanística, el rescate en caso de catástrofes o accidentes, la obtención de imágenes a gran altitud, la ayuda humanitaria, la observación e inventario de los recursos del medio ambiente, la observación de la atmósfera, la medición de la humedad del suelo, la vigilancia de cultivos y de explotaciones ganaderas, etc. (Barrio, 2018, pág. 45)

El origen de la IA se basa en construir elementos cuya operatividad se asimilará en diversos campos de acción, uno de ellos dirigidos hacia la fisiología y funcionamiento de las neuronas cerebrales (Gómez, 2016).

La inteligencia artificial es una tecnología que ya se encuentra directamente relacionada con los seres humanos en la actualidad, nos ofrecen muchos beneficios, pero también implican varios interrogantes, los cuales se deben revisar con el fin de identificar que tan invasiva puede llegar a ser en nuestra vida cotidiana.

Teniendo en cuenta que en nuestra vida diaria cada vez está más ligada a la tecnología, podemos afirmar que la inteligencia artificial se vuelve parte de nuestro día a día ya que puede simular nuestras acciones diarias (Martínez, 2019).

Como lo es la inteligencia artificial, supone facilitar el día a día de las personas y para que esta tecnología funcione de manera eficaz, debe alimentarse de los datos los cuales los usuarios proveen.

Un ejemplo de estos nuevos servicios son los motores de recomendaciones automatizados, que no necesitan a un analista que revise los datos y realice estas recomendaciones. Así, Amazon utiliza datos que extrae de sus clientes para hacernos recomendaciones basadas en compras previas de otros clientes. Y la red profesional LinkedIn también nos sugiere personas que podríamos conocer, seleccionando unos pocos focos de datos de entre una cantidad masiva de información sobre sus más de 300 millones de miembros. (Gil, 2016, pág. 16)

Lo que se indica hasta el momento, la inteligencia artificial nos puede ayudar mucho, pero también se deben revisar sus alcances, referente al manejo de estos datos, ya que se evidencia que “… con un solo número de teléfono puede llegar a conseguir acceso a metadatos de 10 millones de personas. Con los metadatos se puede saber mucho de la vida privada de las personas y esto es lo que se utiliza por las agencias de espionaje…” (Prieto, 2018, pág. 35).

El crecimiento del uso de dispositivos móviles a partir del 2012 comienza a marcar un hito en el uso del sistema operativo Android sobre el sistema operativo Microsoft Windows de ordenador, simultáneamente en el mundo, incrementando la presencia de usuarios en la red mundial.

(Muñoz, 2017) afirma: “Este incremento va muy ligado a la demanda sostenida de uso de ciertas aplicaciones de mensajería (WhatsApp, SnapChat, WeChat, etc.) y acceso a redes sociales desde el móvil, que aumentó en un porcentaje similar con respecto al año anterior” (p.2).

Así mismo el aumento en la demanda de las redes sociales es utilizado por dichas compañías para aumentar su análisis en la información de sus usuarios, con el fin de entender mejor a sus clientes y aprender a llegarles de manera más discreta, analizándolos continuamente. Lo cual citó Colle en el libro Algoritmos grandes datos e inteligencia en la red, pues menciona en su análisis sobre el marketing de grandes empresas como Facebook y Google.

Facebook, Twitter, LinkedIn y otros están comenzando a utilizar técnicas de inteligencia artificial para desarrollar su capacidad de aprendizaje “profundo” a partir de los datos que acumulan a través de sus redes, desde las conversaciones hasta el reconocimiento facial de las fotos y la actividad en los juegos. Así, tienen el potencial de ser mucho más personalizados. Y hacen emerger nuevos campos de marketing: la agrupación de audiencia (clustering), el marketing predictivo y el análisis de los sentimientos frente a las marcas. Facebook dispone para ello de un laboratorio de investigación dedicado a la inteligencia artificial (IA); Google adquirió DeepMind, una compañía que agrupa los mejores talentos en IA y crea algoritmos de análisis para el e-comercio; LinkedIn compró Bright, una compañía parecida, que desarrolla algoritmos de selección de trabajos; Pinterest adquirió VisualGraph, que reconoce imágenes. (Colle, 2017, pág. 10)

Este tipo de recolección y estudio de datos ha permitido que las organizaciones puedan ingresar al interior de nuestras mentes y usar dicho conocimiento para sus propios fines.

A principios del mes de julio de 2002, el director del Federal Bureau of Investigation (FBI), John Aschcroft, anunció que el Departamento de Justicia comenzará a introducirse en la vasta cantidad de datos comerciales referentes a los hábitos y preferencias de compra de los consumidores, con el fin de descubrir potenciales terroristas antes de que ejecuten una acción.[4] Algunos expertos aseguran que, con esta información, el FBI unirá todas las bases de datos probablemente mediante el número de la Seguridad Social y permitirá saber si una persona fuma, qué talla y tipo de ropa usa, su registro de arrestos, su salario, las revistas a las que está suscrito, su altura y peso, sus contribuciones a la Iglesia, grupos políticos u organizaciones no gubernamentales, sus enfermedades crónicas (como diabetes o asma), los libros que lee, los productos de supermercado que compra, si tomó clases de vuelo o si tiene cuentas de banco abiertas, entre otros. (Félix, 2002, pág. 4)

Los datos de los usuarios reposan en sistemas de almacenamiento en la nube Y, Cada elemento integrado en esta infraestructura global de comunicaciones plantea riesgos específicos en términos de privacidad y seguridad (Muñoz, 2017). Porque son organizaciones del gobierno y entes privados los que se encargan de procesar y administrar los datos que componen la información de los usuarios.

En este fragmento se dice por ejemplo que para llevar a cabo la implantación de IA “Entre los incentivos para el desarrollo de la misma no debe olvidarse que figura el potencial para incrementar la vigilancia y control sobre consumidores, usuarios y ciudadanos por parte de actores estatales y privados (Weber and Studer 2016 Kshetri 2017; Mollah, Azad y Vasilakos 2017) (como se cita en Muñoz 2017)”.

La causa de esta captación masiva de datos es la disponibilidad de aplicaciones y servicios de No pago que utilizan las empresas desarrolladoras para obtener información o datos para estadística de consumo en estrategias de marketing “ligada al valor estratégico o de mercado que extraen de los datos y estadísticas de uso a gran escala (Truong, Phung, and Dustdar 2012) (como se cita en Muñoz 2017)”.

Los entornos distribuidos podrían ser una solución para llegar a “una expectativa razonable de privacidad (como se cita en Muñoz 2017)”.

Quienes implementen IA deben estar preparados ya que esta traerá nuevas amenazas de seguridad y privacidad, es necesario que estas corporaciones se ganen la confianza de las personas, cumpliendo con todas las normas de seguridad, comprometiéndose con el uso adecuado de los datos.

La desarrollo e implementación de tecnologías de IA debe realizarse con las medidas de control para que no se presenten casos como el siguiente, teniendo en cuenta la protección de datos de los usuarios:

Nos recordaron estas nuevas amenazas en Microsoft cuando lanzamos un bot en Twitter llamado Tay, luego del éxito del bot social equivalente en China, Xiaoice. Tay aprendió de las interacciones en línea con los usuarios para replicar mejor la comunicación humana y los rasgos de personalidad. Sin embargo, dentro de las 24 horas, un ataque coordinado comenzó a alimentar a Tay con retórica intolerante, convirtiéndolo de un bot educado en un vehículo para el discurso de odio. Por supuesto, tuvimos que cerrar el bot de inmediato, eliminar los mensajes ofensivos y emitir una disculpa asumiendo toda la responsabilidad. Este desafortunado episodio nos enseñó una importante lección sobre la vulnerabilidad de la IA a los ataques que influyen en los conjuntos de datos de entrenamiento, especialmente para sistemas con capacidades de aprendizaje automático. Para ayudar a mitigar esta amenaza en el futuro, el equipo desarrolló tecnologías como filtros de contenido avanzados e introdujo supervisores para sistemas de IA que tienen capacidades de aprendizaje automático. Las lecciones aprendidas de Tay y muchas otras experiencias de seguridad basadas en inteligencia artificial también se recopilaron en un documento para ayudar a otras empresas a preparar mejor sus sistemas de inteligencia artificial para estas nuevas amenazas de privacidad y seguridad. (Carmona, 2019)

Teniendo en cuenta los antecedentes “Son los programadores, los usuarios y finalmente los beneficiarios, quienes, por distribución de responsabilidades y proximidad, deben asumir su inspección y evaluación (…), mediante una genuina y cualificada equidad en su aplicación –determinada por un panel de jueces humanos– escenario donde un algoritmo es aceptado en una aplicación transparente y rechaza negras intenciones (p. 317) (como se cita en Gómez 2016)”.

Es importante la regulación en cuanto al uso de los datos, en Europa la GDPR (por su sigla en inglés General Data Protection Regulation) establece seis principios que deben cumplir las organizaciones que administran datos personales mostrando sus deberes en cuanto el uso de estos:

1. Legalidad, equidad y transparencia.
2. Limitación de propósito.
3. Minimización de datos.
4. Exactitud.
5. Limitación de almacenamiento.
6. Integridad y confidencialidad.

**Resaltando en el último punto:**

Este principio final requiere que las organizaciones procesen datos personales de una manera que garantice la seguridad adecuada de los datos personales, incluida la protección contra el procesamiento no autorizado o ilegal y contra la pérdida, destrucción o daño accidental. En el lenguaje de la seguridad de la información, la confidencialidad es la propiedad de que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados. Esto significa que los datos personales deben clasificarse como confidenciales incluso dentro de la organización, ya que es extremadamente improbable que cada persona en la organización necesite tener acceso a los datos personales. En muchos casos, puede que no haya ningún requisito para que nadie acceda a los datos personales. (ITGP Privacy Team, 2017)

# **Glosario De Términos Informáticos**

**1. Aplicaciones:** Son programas diseñados para realizar funciones específicas que pueden ejecutarse en equipos de escritorio o en dispositivos móviles (multiplataforma).

**2. Bots:** Empleado como aféresis de robot, su definición estándar (un programa o agente informático autónomo, diseñado para imitar el comportamiento de usuarios humanos en tareas concretas y repetitivas) no proporciona una idea muy precisa de la variedad de aplicaciones con las que pueden asociarse. Suelen estar programados para funcionar.

**3. Dron:** Aeronaves no tripuladas pilotados a distancia que pueden albergar componentes auxiliares como cámaras, sensores e incluso armamento. Todas las operaciones de vuelo, incluyendo el despegue y el aterrizaje, se realizan sin un piloto humano a bordo.

# **Referencias**

Félix, L. C. (2002). semanticscholar.org. Obtenido de https://pdfs.semanticscholar.org/79dd/0829a48a91a7b299457a18b15122db4c69c6.pdf

Gil, E. (2016). Big data, privacidad y protección de los datos. Madrid: Agencia Española de Protección de Datos.

Prieto, J. V. (2018). Problemas jurídico penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante inteligencia artificial. Monografías de derecho penal.

Muñoz, M. M. (2017). Privacidad y procesado automático de datos personales mediante aplicaciones y bots. (C. I. Consejo Superior de Investigaciones Científicas, Ed.) *Dilemata*(24), 23. Obtenido de <https://dialnet.unirioja.es/servlet/articulo?codigo=6066827>

Villalba Gómez, J. A. (2016). Problemas bioéticos emergentes de la inteligencia artificial. (e. C. Red de Revistas Científicas de América Latina, Ed.) *Diversitas: Perspectivas en Psicología* (1), 12. Obtenido de <https://www.redalyc.org/articulo.oa?id=67945904010>

Martínez Devia, A. (2019). La Inteligencia Artificial, el Big Data y la Era Digital: Una Amenaza para los Datos Personales. Rev. Prop. Inmaterial, 27, 5. <https://heinonline.org/HOL/LandingPage?handle=hein.journals/revpropin27&div=3&id=&page=>

Colle, R. (2017). Algoritmos, grandes datos e inteligencia en la red. Una visión crítica. Obtenido de <https://rua.ua.es/dspace/bitstream/10045/64707/1/Algoritmos-grandes-datos-e-inteligencia-en-la-red.pdf>

ITGP Privacy Team, (2017). *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide - Second edition,* Londres UK, IT Governance Publishing.

Carmona, David (2019).*The AI Organization*, Sebastopol EU, O'Reilly Media, Inc.

Zambrano, R. D. F. (2009). *¿qué es inteligencia artificial?* Retrieved from <https://ebookcentral-proquest-com.unipanamericana.basesdedatosezproxy.com>

VV.AA. (2017). Foro: Revista de derecho, no. 27. la protección de datos personales en la era digital. Retrieved from <https://ebookcentral-proquestcom.unipanamericana.basesdedatosezproxy.com>

Derecho de los drones. (2018). Retrieved from <https://ebookcentral-proquest->com.unipanamericana.basesdedatosezproxy.com