

Delitos contra la intimidad personal en el marco de la inteligencia artificial en Colombia

Drimes against personal privacy in the context of artificial intelligence in Colombia.

Gustavo Andrés López Rincón

Estudiante de derecho

Orcid: <https://orcid.org/0009-0006-4448-5689>

correo: galopezr@ufpso.edu.co

Universidad Francisco de Paula Santander Seccional Ocaña

Laura Marcela Quintero Sánchez

Abogada

Orcid: <https://orcid.org/0009-0009-4889-713X>

Correo: Lmquinteros@ufpso.edu.co

Universidad Francisco de Paula Santander Seccional Ocaña

Cómo citar: López, G. A. Delitos contra la intimidad personal en el marco de la inteligencia artificial en Colombia. Postulados: Revista Sociojurídica, 2(2), 57-71. <https://doi.org/10.22463/29816866.4300>

Fecha de recibido: 15 de diciembre de 2023

Fecha aprobación: 09 de octubre de 2024

Fecha publicación: 18 de junio de 2025

RESUMEN:

Este artículo describe la evolución de la legislación colombiana frente a los delitos informáticos, teniendo como base los mecanismos en el uso de las nuevas tecnologías y la vulnerabilidad que resulta para los asociados del Estado colombiano el uso de estas herramientas en relación con los derechos fundamentales, se debe garantizar el goce de una vida digna, protegiendo especialmente la intimidad de los individuos. Al mismo tiempo podemos encontrar la legislación más relevante en cuanto a la protección de los derechos fundamentales como lo es la intimidad en Colombia y lo que significa el uso de la inteligencia artificial en nuestra sociedad y cuál es la protección del derecho a la intimidad por medio de las aplicaciones de inteligencia artificial, por último, para concluir sobre cuáles son los delitos que más afecta el derecho a la intimidad llevados a cabo por medios electrónicos.

Palabras clave:

Delito informático, Ciberdelitos, Globalización, Derecho Penal, Penalización, Derecho a la Intimidad.

ABSTRACT:

This document describes the evolution of Colombian legislation regarding computer crimes, based on the mechanisms in the use of new technologies and the resulting vulnerability for Colombian state partners in the use of these tools, against fundamental rights for the enjoyment of a dignified life such as privacy. At the same time, we can find the most relevant legislation regarding the protection of the right to privacy in Colombia and what the use of artificial intelligence means in our society and what is the protection of the right to privacy through artificial intelligence applications.

Keywords:

Computer crime, Cybercrime, Globalization, Criminal law, Criminalization, Right to privacy.

Autor para correspondencia

Correo electrónico: galopezr@ufpso.edu.co (Gustavo Andrés López Rincón)



La revisión por pares es responsabilidad de la Universidad Francisco de Paula Santander Ocaña
Artículo bajo la licencia CC BY-NC (<https://creativecommons.org/licenses/by-nc/4.0/deed.es>)

Introducción

Esta investigación se organiza en cuatro acápites. En el primero, se abordará el concepto y el alcance de la inteligencia artificial, así como los delitos informáticos comúnmente perpetrados a través de esta tecnología. Se discutirá, además, la relevancia actual del uso responsable de las aplicaciones basadas en inteligencia artificial y los riesgos asociados con su utilización indebida.

En el segundo capítulo, se analizará la protección de los derechos fundamentales de las personas, en particular el derecho a la intimidad, en el contexto del ordenamiento jurídico colombiano. Colombia ha sido uno de los países pioneros en la regulación de los delitos informáticos, particularmente a través de la Ley 1273 de 2009. No obstante, la Constitución Política reconoce el derecho a la intimidad como un derecho fundamental, estableciendo límites claros en cuanto al uso de datos personales por parte de entidades del Estado y particulares. Desde esta perspectiva, se argumentará que es necesario que el Estado colombiano regule de manera más estricta el manejo de los datos personales, con el fin de proteger adecuadamente los bienes jurídicos tutelados.

En los capítulos tercero y cuarto, se examinará en detalle cómo funciona la inteligencia artificial, las aplicaciones más utilizadas y aquellas que presentan mayores riesgos para el derecho a la intimidad de las personas. Se analizará también la protección de este derecho fundamental frente a los desafíos que plantea el uso de la inteligencia artificial. Finalmente, se concluirá con una reflexión sobre la necesidad urgente de implementar nueva legislación que prevenga los delitos informáticos y proteja el derecho a la intimidad, respondiendo a la siguiente pregunta: ¿Cuáles son los delitos informáticos que afectan el derecho a la intimidad personal, a propósito de la implementación de la inteligencia artificial?"

Explicaciones Argumentadas

Si bien es cierto que las innovaciones tecnológicas permiten un amplio crecimiento en diferentes artes, profesiones, actividades económicas, estas deben ir en concordancia con los derechos inherentes a la persona, que nada tienen que ver con su nacionalidad, su estado civil, su estado judicial etc., pues una de las características de los derechos humanos es la universalidad.

Para Márquez y Mousalli, (2016), en la actualidad el uso de las innovaciones tecnológicas tiene una relevancia significativa para la sociedad pues esta permite la simplificación de acciones cotidianas que anteriormente requerirían de más tiempo o de procesos más complejos, sobre todo en la posibilidad de comunicación y conexión con el mundo.

Sin embargo, frente a dichos avances que permiten la facilidad de ciertas tareas y la exploración de nuevas experiencias en varios ámbitos de aplicación y varias disciplinas necesarias para la misma vida del planeta tierra, también con ellas surgen desafíos que implican reinventarnos como estados en cuanto a su regulación y los límites de los mismos, es así como lo exponen Fernández y Sarmiento, (2020) frente a su investigación

de los riesgos éticos y jurídicos que conlleva el uso y aplicación de la inteligencia artificial y las consecuencias y cambios en el sistema penal colombiano y como este mismo surge y se renueva frente a las herramientas que permiten el avance y la agilidad de los procesos judiciales.

Desde la aplicabilidad e implementación de la inteligencia artificial la cual se ha desarrollado para mejorar y optimizar ciertas funciones que a los seres humanos nos costaría más tiempo y dedicación, se ha podido evidenciar que la misma está inmersa en la vulneración de ciertos derechos humanos, es así que Fernández y Sarmiento (2020) lo dejan ver con la aplicación PRISMA, esta es utilizada en la Fiscalía General de la Nación, que se utiliza para el perfil de riesgos de reincidencia para la solicitud de medidas de aseguramiento, la cual le ayuda a la fiscalía por medio del derecho penal de autor a determinar la necesidad de solicitar una medida de aseguramiento privativa de la libertad, y esta tiene sesgos discriminatorios, que claramente vulnera derechos como el debido proceso, la libertad, la igualdad, el habeas data y la intimidad.

En los últimos años se ha venido hablando de los beneficios de las nuevas tecnologías, especialmente de la inteligencia artificial, pero a su vez se ha advertido sobre los riesgos y las implicaciones que tiene el auge de esta innovación tecnológica, como lo manifestó Michel Bachelet alta comisionada de las Naciones Unidas, (2015) pues en su artículo indica que la inteligencia artificial ha invadido todos los aspectos de la vida de las personas, e incluso toma decisiones importantes como la necesidad de otorgar un servicio público o quienes pueden tener ciertos empleos, situaciones que trasgreden derechos relativos a la salud, la libertad de movimiento entre otros.

En este artículo se intentará establecer la necesidad de ampliar nuestra legislación frente al uso, aplicabilidad, alcance y responsabilidad de la inteligencia artificial en todas sus formas y sobre cuál es la necesidad de implementar otra categoría o generación acerca de los derechos vinculados a la denominada Revolución 5.0, concepto que hace referencia a las innovaciones tecnológicas, adquieren una relevancia creciente en el contexto jurídico contemporáneo. En este sentido, Sánchez (2021), en su trabajo de grado, aborda la necesidad de implementar el control humano sobre la inteligencia artificial, proponiéndolo como un nuevo derecho dentro de nuestro ordenamiento jurídico. Esta propuesta se enmarca dentro de la necesidad urgente de regular los avances tecnológicos para garantizar la protección de los derechos fundamentales en un entorno cada vez más digitalizado.

Es así que es necesario abordar en nuestro planteamiento del problema cuales son los delitos informáticos y ciberdelitos que más afectan el derecho a la intimidad personal de los individuos, pues como se ha dicho anteriormente el mismo uso de herramientas diseñadas para el mejoramiento de ciertas funciones o disciplinas permiten la vulneración de derechos fundamentales, mucho más lo es la creación y disponibilidad en el mercado de herramientas hechas con base de inteligencia artificial que tienen como función crear imágenes o videos falsos que ponen el riesgos varios bienes jurídicos de la sociedad, como la intimidad, el libre desarrollo de la personalidad, la libre expresión, la dignidad entre otros.

Por lo anterior, es necesario abordar este tema desde la perspectiva de la normativa legal vigente en Colombia, evaluando la suficiencia de la regulación actual y la necesidad de legislar de manera más específica sobre las responsabilidades directas de ciertas herramientas tecnológicas que, de manera autónoma, generan contenidos que vulneran derechos fundamentales como la dignidad, la libertad, la igualdad y, en particular, el derecho a la intimidad personal, que es el objeto central de este análisis

Metodología

Para llevar a cabo esta investigación, se empleó un enfoque hermenéutico jurídico, sustentado en una metodología cualitativa y un análisis sistemático. Se procedió a la recopilación y revisión de bases de datos públicas, así como de normativas legales relevantes, con el propósito de realizar un análisis detallado sobre la protección jurídica frente a los delitos informáticos. Adicionalmente, se llevó a cabo un estudio de las implicaciones jurídicas derivadas de la implementación de la inteligencia artificial en diversos sectores de la sociedad, con el fin de evaluar sus efectos y desafíos en el marco legal vigente.

Resultados

A partir de la realización de esta investigación y en virtud del estudio de documentos, leyes y sentencias pertinentes, es posible concluir que los delitos cibernéticos o informáticos, materializados a través de medios electrónicos y virtuales, que operan en espacios no físicos o cuyos efectos se traducen en la afectación real de las víctimas, constituyen una vulneración del derecho a la intimidad, de manera directa o subsidiaria. Aunque en muchos casos la intención del ciberdelincuente no sea atacar este bien jurídico específico, las acciones llevadas a cabo para ejecutar dichos delitos terminan, inevitablemente, afectando la privacidad de las personas.

En este contexto, los delitos cibernéticos como el hurto, la extorsión, la suplantación de identidad, que en Colombia se denomina falsedad personal, entre otros que afectan al patrimonio económico, tienen efectos colaterales que comprometen gravemente la intimidad personal, el buen nombre, la libertad sexual, entre otros derechos fundamentales. Asimismo, los delitos que atentan contra el software o la información de entidades públicas y privadas, cuyo objetivo es vulnerar la confiabilidad, confidencialidad e integridad de los datos, están intrínsecamente vinculados a la protección de la privacidad de dichas entidades. Esta relación evidencia una vez más que el derecho a la intimidad es sistemáticamente afectado en la comisión de delitos informáticos, independientemente de su propósito principal.

Particularmente, los delitos que involucran la manipulación de imágenes, como la difusión no autorizada de fotografías previamente alteradas mediante el uso de inteligencia artificial, constituyen una grave vulneración de la intimidad personal. La intimidad es, sin duda, uno de los bienes jurídicos más preciados para los individuos, y por ello, resulta imperativo que los Estados, incluido Colombia, implementen una legislación adecuada para prevenir estos delitos, establecer responsabilidades y regular

las consecuencias jurídicas de tal acto.

1. Delitos informáticos en la implementación de la inteligencia artificial.

En la actualidad es muy común hablar de las nuevas tecnologías para el desarrollo de muchas actividades de la sociedad y más en un momento de nuestra civilización en donde se ve con más auge los efectos de la globalización, sin embargo, junto a estos beneficios se ven añadidos otros factores que muchas veces no son muy benéficos para quien las usa.

Dentro de los especímenes de la era de la revolución 5.0, encontramos entre tantas, las herramientas de la inteligencia artificial, que permite interactuar de manera virtual con otras personas, crear imágenes, mejorar fotografías, controlar la temperatura de las casas, la luz entre otras, pero debemos preguntarnos si realmente somos conscientes de los riesgos a los que estamos sometidos debido al uso de esta tecnología, pues con ella además de los muchos beneficios que trae, también existen graves riesgos que atentan contra nuestro derechos patrimoniales, a la identidad y el que nos atañe en este escrito, la intimidad.

Es necesario para los efectos de este artículo definir qué es un delito informático o ciberdelincuencia, por ello podemos decir que “son todos los actos ilícitos cometidos mediante el uso inadecuado de la tecnología, atentando contra la privacidad de la información de terceras personas dañando o extrayendo cualquier tipo de datos que se encuentren almacenados en servidores o gadgets” (Acosta, et al. 2020).

Como lo mencionó Serrano, “por otra parte, podríamos decir que es toda aquella acción, típica antijurídica y culpable, dada por vías informáticas cuyo objeto es destruir y dañar ordenadores, medios electrónicos, y redes de internet”. (Serrano E. 2014).

Queda claro con estas definiciones que son conductas que el legislador ha previsto como lesivas y que afectan en gran manera los intereses de la población.

Dentro de los delitos informáticos, los más comunes son: prácticas como el fraude, hurto, suplantación de identidad, extorsiones, chantajes, software malicioso, y como nueva modalidad falsificación de imágenes o videos para uso de pornografía o contenido sexual, afectando gravemente la intimidad y el buen nombre de las personas víctimas de estos delitos, especialmente mujeres.

Ahora es necesario aclarar que los delitos informáticos y los ciberdelitos, tienen diferencias sustanciales, pues así lo deja ver el convenio de Budapest en sus artículos 2 y 6 que hace alusión a los ciberdelitos y los artículos 7 y 8 que refleja lo que son los delitos informáticos. (Ayala y Duque, 2022)

Los ciberdelitos han demostrado que es necesario un replanteamiento de los conceptos dogmáticos tradicionales acerca del delito, lo que sin duda permitirá establecer un nuevo prototipo delictivo que se caracteriza por contener un espacio no físico, sino virtual,

llevado a cabo por medios electrónicos, los mismos que permiten una interconexión con el mundo y abre las puertas al comercio, a la política, al mundo social, pero igualmente permite que los delitos ya conocidos estén de igual forma evolucionando y abarcando otro tipo de modalidades.

En Colombia existe un marco normativo que conduce a la prevención de estas conductas por ejemplo la ley 1273 del 2009 por la cual se modifica el código penal colombiano y se adhieren artículos para imponer penas y multas a los sujetos activos de estos delitos. (Congreso de la República de Colombia, ley 599 del 2000).

Por medio de esta ley se crea un nuevo bien jurídico tutelado denominado “De la protección de la información y los datos” el cual se ubica en su título VII Bis, del que se desprenden 2 capítulos, en el primero están descritos de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, (Ciberdelitos) y en su capítulo segundo de los atentados informáticos y otras infracciones (delitos informáticos), para un total de 10 artículos, los cuales imponen pena de prisión de 48 a 96 meses de prisión y multas de 100 a 1000 salarios mínimos legales vigentes.

El crimen informático ha alcanzado niveles organizacionales, lo que ha permitido su expansión en diversos sectores. En este sentido, Fernández (2013), citado por Acosta et al. (2020), en su estudio titulado Delitos informáticos: impunidad organizacional y su complejidad en el mundo de los negocios, destaca cómo estos delitos se han sofisticado y han sido incorporados en estrategias organizacionales, complicando así la lucha contra la impunidad y la evasión de responsabilidades.

Destaca la importancia que reviste la complicidad interna, por intermedio del personal que labora en la misma, quienes, sin importar los valores de respeto y lealtad, perjudican la vulnerabilidad de la información de la organización, volviéndose inclusive en algunos casos, en algo codiciado que, además, es muy bien remunerada por los delincuentes cibernéticos, que buscan el desprestigio o robo de información confidencial, con la intención de chantajear o liquidar las empresas.

2. Protección al derecho a la intimidad en el ordenamiento jurídico colombiano

La protección del derecho a la intimidad en el ordenamiento jurídico colombiano es fundamental para resguardar la esfera personal de los individuos y contribuir con la organización del tejido social del territorio colombiano.

Desde la constitución Política de Colombia de 1991, podemos encontrar el reconocimiento del derecho a la intimidad como inherente a la persona en relación con la dignidad humana, estableciendo límites de ciertas entidades estatales y personas jurídicas o naturales, en la medida en que se involucran en la vida privada y datos de las personas. (Asamblea Nacional Constituyente, 1991, art 15). Ejerciendo protección al derecho fundamental del habeas data.

Es importante destacar quiénes son los responsable de los datos y la información y quienes son o los encargados de los mismos, pues para poder establecer esta reglamentación demos mencionar que llega a Colombia a través del convenio de Budapest, el cual tiene dentro de sus objetivos la necesidad de aplicar una política penal común, con el objeto de proteger a la sociedad contra la ciberdelincuencia, esta introduce medidas de protección a la confidencialidad, la integridad, la seguridad y la disponibilidad de los datos y sistemas informáticos, el deber de adoptar medidas legislativas y de otro tipo, que resulten necesarias para tipificar como delitos en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático, interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema, abuso de los dispositivos, falsificación informática, fraude informático, delitos relacionados con la pornografía infantil, delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines, responsabilidad de las personas jurídicas, sanciones, medidas y también disposiciones en el derecho procesal como ámbito de aplicación de las disposiciones del procedimiento entre otras. (Convenio de Budapest, 2001).

Podemos encontrar que el Estado colombiano hace un esfuerzo para lograr mantener una legislación que permita tutelar el derecho a la intimidad de todos sus asociados, es por esto que encontramos la ley estatutaria 1581 del 2012, la cual regula el manejo de datos personales y establece principios para su tratamiento adecuado, este marco normativo busca garantizar la privacidad de la información, imponiendo obligaciones a quienes recopilan, almacenan y usan datos personales, con el fin de proteger la privacidad, intimidad, el patrimonio de los individuos. (Congreso de la República de Colombia, 2012, ley 1581, art. 2).

Por otra parte, la corte constitucional a través de su jurisprudencia ha reforzado la protección del derecho a la intimidad, reconociéndolo como un derecho importante y fundamental para la dignidad de las personas, igualmente ha limitado la obtención y divulgación de información sensible, especialmente en contextos laborales y médicos, donde la privacidad adquiere una relevancia particular, como la sentencia T-143-22, T-450-22, T-364-18, las cuales protegen el derecho del habeas data y la intimidad.

Adicionalmente encontramos la ley 1273 del 2009, con la cual se penalizan delitos informáticos bajo el nombre de protección de la información y de los datos, con el fin de proteger la seguridad de la información, los datos y el adecuado funcionamiento de los sistemas informáticos, haciendo énfasis en la integridad, confidencialidad, confiabilidad, disponibilidad, no repudio y recuperación del acceso, procesamiento, almacenamiento y la transmisión eficaz la información, los datos y los sistemas informáticos, que intrínsecamente protege otros bienes jurídicos como la intimidad y el patrimonio. (Congreso de la República de Colombia, 2009).

Anterior a esta ley podemos encontrar la ley 44 de 1993 sobre derechos de autor y el código penal colombiano que introduce los delitos contra los derechos de autor, la propiedad intelectual, la fe pública entre otros. (Congreso de la República de Colombia, 1993).

La ley 679 del 2001 previene la explotación, la pornografía y el turismo sexual con menores de edad, lo que impulso tomar medidas jurídicas más específicas frente al aumento de este flagelo.

También encontramos la ley 1928 del 2018 la cual establece en su artículo 12 la responsabilidad de las personas jurídicas por acción o por omisión de delitos informáticos. (Congreso de la República de Colombia, 2018, ley 1928, art 12).

A pesar del marco jurídico mencionado anteriormente para proteger la intimidad de las personas, realmente hace falta una implementación más severa frente al aumento de casos en los cuales mediante la inteligencia artificial que abusa de su poder y pone en riesgo la intimidad y los demás bienes jurídicos de los individuos, estas no son suficientes, además de existen ciertos vacíos normativos que permiten la interpretación de las normas por parte de los jueces de acuerdo a su criterio o actualización de la información.

3. Inteligencia artificial

Con el avance de la sociedad y de la civilización de manera conjunta va el crecimiento de las nuevas tecnologías, en un mundo cada vez más interconectado, en donde las grandes industrias comerciales informáticas generan innovaciones que pretenden facilitar la vida de las personas del común, además de buscar facilitar, agilizar y potencializar algunas profesiones y por qué no, tratar de generar acciones similares a las del ser humano.

La inteligencia artificial hoy en día, no solamente la encontramos en actividades para el desarrollo económico, académico o médico, también hace parte de la vida cotidiana de las personas, pues hacen parte de la diversión, el ocio o incluso para sofisticar nuestros lugares de residencia.

Equívocamente se podría pensar que la inteligencia artificial es un concepto nuevo, pero realmente, tiene sus antecedentes desde los años 50 con las ideas de Alan Turing con sus conceptos sobre máquinas inteligentes. (López y Meseguer, 2017, Qué sabemos de la inteligencia artificial, pag.10).

Sin embargo, la inteligencia artificial hace presencia en su forma casi perfecta en nuestra sociedad, y pertenece a lo que se le puede considerar como la cuarta revolución, lo que significa nuevos retos para la legislación del mundo entero.

La inteligencia artificial podríamos definirla como un conjunto de algoritmos y herramientas que permiten resolver problemas que requieren de cierto grado de inteligencia y es que uno de los objetivos de esta tecnología es la búsqueda de una máquina que emule los comportamientos y la forma de pensar humana.

Como ya se menciona en apartados anteriores la forma en que la inteligencia artificial ha invadido varios aspectos de la vida del hombre, y los efectos positivos que generan en algunos sectores, también desafortunadamente debemos ocuparnos por los efectos negativos que esta genera.

Muestra de lo anterior son los sesgos discriminatorios de los datos ingresados en los sistemas de inteligencia artificial, que utilizan big data y que producen decisiones tales como asociar los cargos mejores remunerados con los hombres y las vacancias laborales inferior con las mujeres, o considerar como sospechosos de delitos a los hombres negros, por encima de los hombres blancos. (Sánchez V. 2021)

Es pertinente decir que el solo uso de plataformas, software o herramientas que aplican inteligencia artificial vulnera ciertos derechos, como se citó en el párrafo anterior, como se puede mitigar estos riesgos a la discriminación, al debido proceso, al uso de datos, a la igualdad.

Por ejemplo el COMPAS, lo que fue una plataforma de predicción de reincidencia de personas con antecedentes judiciales, señalaba a los hombres negros como los más propensos a reincidir, sin duda alguna esta herramienta vulneraba el derecho a la igualdad.

Es en estos casos en donde debemos preguntarnos, ¿cómo se puede controlar la programación de dichos programas? ¿Cómo evitar la automatización de datos que pueden generar resultados nocivos?, estas y muchas más son las preguntas sin resolver que hoy por hoy tenemos con la aplicación de la inteligencia artificial, pues si bien es cierto que ha traído mucho avance en ciertas áreas, también ha generado efectos nocivos como la delincuencia o dicho en otras palabras la delincuencia ha avanzado en conjunto con la tecnología.

Surgen nuevos planteamientos de cara con aplicativos que funcionan como herramientas para la toma de decisiones judiciales, como lo es en el caso de Colombia la plataforma PRISMA (perfil de riesgos de reincidencia para la solicitud de medidas de aseguramiento), la cual ayuda en las decisiones que tienen que ver con la imposición de medidas de aseguramiento intramural de los capturados, en casos como este es necesario preguntar por el derecho al debido proceso, la intimidad, la presunción de inocencia.

PRISMA toma estas decisiones basado en la teoría de derecho penal de autor, lo que resulta discriminatorios para el imputado. (Fernández y Sarmiento, (2020). la aplicación de la inteligencia artificial en el derecho penal: consecuencias éticas y jurídicas frente a la medida de aseguramiento, Repositorio institucional Universidad de los Andes).

Razones Como la anterior demuestra que es necesario que las aplicaciones basadas en inteligencia artificial tengan un cumplimiento con las normas establecidas en Colombia y se ajuste al marco de legalidad, es necesario la implementación de un control de todos los estados frente a la creación y manipulación de dichas herramientas para de esta manera proteger los bienes jurídicos tutelados.

Como Estado y como sociedad debemos preguntarnos ¿cómo proteger nuestros derechos cuando la tecnología avanza a grandes pasos y cada vez con menos legislación que la regule? ¿Sabemos realmente quién maneja nuestros datos personales cuando

entregamos información para acceder el uso de estas herramientas? respuestas para resolver estos cuestionamientos permite hablar de la creación de nuevos derechos que se derivan de la implementación de las nuevas tecnologías como la inteligencia artificial que cada vez cobra más importancia en todos los ámbitos de la vida y que pueden hacer realidad nuestras peores pesadillas o llegar a creer que las películas de ciencia ficción están más cerca de convertirse en una realidad.

4. Delitos cibernéticos y delitos informáticos

Coloquialmente se suele mencionar que los delitos informáticos y los ciberdelitos son lo mismo, pero desde el convenio de Budapest, el cual es la guía para la regulación de estas conductas criminales, genera unas diferencias importantes que para nuestro estudio es necesario abordar.

“La Convención se basa en el reconocimiento fundamental de que se necesita armonizar las leyes nacionales. Es decir, contar a nivel de Latinoamérica con una herramienta común tanto sustantiva como adjetiva para procesar este tipo de manifestaciones delictivas, procurando con este elemento comunitario en la parte sustantiva el mejoramiento de la cooperación internacional de los países miembros, ya que solamente existiría en esta materia, la aplicación de una ley común de carácter supranacional que permita a los gobiernos intercambiar información y pruebas.” (Ayala y Duque, 2022, que diferencias en ciberdelitos existe entre Colombia y España, repositorio institucional Universidad CES).

Este convenio se crea mediante la Unión Europea, frente a la preocupación por el aumento de dichos delitos en el mundo entero.

Dentro de estos tenemos los delitos como el hurto y la estafa que con la implementación de nuevas tecnologías han evolucionado a nuevas modalidades.

El convenio de Budapest se fracciona en los artículos 2 y 6, por otro lado, en los artículos 7 y 8, de los cuales los dos primeros protegen la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos, por su parte los segundos con conductas como el fraude, hurto lo que permite la gran diferencia entre ciberdelitos y delitos informáticos. (Ayala y Duque, 2022, que diferencias en ciberdelitos existe entre Colombia y España, repositorio institucional Universidad CES).

La gran diferencia entre estos dos es que los delitos informáticos son aquellos que a través de medios informáticos ejercen conductas que se exteriorizan en el mundo, como el hurto, la extorsión, estafa, y los ciberdelitos son los que se ejecutan y se materializan y afectan los mismos medios electrónicos, como quien ingresa de manera remota sin autorización ingresa a un software y altera, modifica o daña una información allí contenida.

Los delitos informáticos se caracterizan, además, por vulnerar la intimidad personal, el buen nombre, la libertad sexual, la fe pública, el patrimonio económico y junto a estos los datos personales.

5. La protección de la intimidad en la inteligencia artificial

La protección del derecho a la intimidad desde el punto de partida de la inteligencia artificial implica grandes desafíos, teniendo en cuenta el uso de algoritmos y sistemas de automatización que permiten el análisis de datos personales, lo que aumenta el riesgo de violaciones a los datos de las personas que las usan y con ello la intimidad.

Hoy en día con la implementación de la inteligencia artificial se hace necesario crear dentro de las mismas políticas de consentimiento informado y que los datos solicitados por ellas sea minimizado, para así proteger la privacidad y la intimidad en el desarrollo y la aplicación de la inteligencia artificial.

La organización de Naciones Unidas (ONU), ha manifestado que la IA, ha llegado a invadir no solo los rincones de las vidas, sino que además alcanza los estados emocionales de las personas, e incluso están ayudando a los gobiernos a decidir quién puede recibir los servicios públicos, y quien aún no los tiene. Además de ello afecta y causa conmoción en la información que los usuarios consumen en las redes, y puede llegar a perjudicar psicológicamente a los consumidores de la internet. La ONU, ha realizado ciertos informes en donde ha manifestado su preocupación sobre la manera deliberada en que se hace uso de la IA, y de cómo está afectando a la humanidad, y en algunos casos, menciona como ejemplo, como esta tecnología es quien en algunos países decide quien es apto para recibir su seguro social y quienes no lo son, e incluso ha indicado casos de personas que han sido arrestadas como consecuencia de errores en los sistemas de reconocimiento facial, y todo ello por el uso indiscriminado y precipitado de la incorporación de tecnologías de IA. (Revista arbitrada de ciencias Jurídicas, Iustitia Socialis, vol. 8. Edición especial, 2023)

Debido al incremento de los delitos cibernéticos ocasionados por el uso reiterativo de la IA, las organizaciones internacionales han hecho pronunciamientos y les ha solicitado a los diferentes estados en implementar normatividad dentro de su ordenamiento interno reglas y límites frente al uso y solicitud de datos personales de los usuarios, hasta que no se tenga la certeza de que es totalmente segura y que sus datos estarán seguros.

Es necesario en este aspecto que haya una atención cuidadosa por parte de legisladores, desarrolladores y sociedad en general para así se combine la innovación tecnológica con la salvaguarda de datos, lo que permite la protección de diferentes derechos fundamentales.

Se hace necesario establecer leyes concretas enfáticas y dirigidas al uso de datos por personas jurídicas o naturales y así mismo el uso de la inteligencia artificial frente a la dignidad e intimidad de las personas es necesario establecer una responsabilidad penal a quienes utilicen estos medios para tratar de dañar la imagen, el trabajo, los bienes de quienes los usuarios.

La alta comisionada de las Naciones Unidas Michel Bachelet, manifestó la urgencia de establecer una norma moratoria para el uso de sistemas de inteligencia artificial que sean usados en contra de los derechos humanos de las personas. (Organización de Naciones

Unidas, oficina del alto comisionado).

En el auge de las nuevas tecnologías es muy común escuchar en las noticias que ciertas personas son víctimas de los malos usos que le dan las personas a la inteligencia artificial, puesto que pretenden despojar de su ropa a personas que quedan en fotografías, videos o también se generan plagios en ciertas obras, música y demás, sin establecer directamente un responsable de dichos actos.

“Sorprendentemente, ClothOff advierte en los términos y condiciones del servicio que el internauta “es el único responsable de las imágenes generadas” o “es el responsable de no usar la aplicación para fines ilegales o no autorizados” como la creación de contenido objetable y la infracción de derechos de propiedad intelectual. Asimismo, recalca que “no reclama la propiedad del contenido resultante” porque el servicio “está destinado para uso personal y no comercial”, agregando que el usuario “acepta que sus imágenes no infringen los derechos de autor, marcas comerciales u otros derechos de propiedad intelectual de terceros”. (Artículo 20 minutos editora, S.L).

Lo anterior deja al descubierto lo flexible que es la legislación frente a las condiciones de uso que tienen estas herramientas, que de una u otra manera permiten los vacíos normativos para acceder a usos poco éticos y que generan violaciones de derechos como la intimidad, la dignidad y el buen nombre.

Discusión

Dentro de la investigación se pudo vislumbrar varios hallazgos, que sugieren que si bien la innovación de las nuevas tecnologías conlleva a una evolución de la misma sociedad y las herramientas con las que esta elabora sus acciones diarias, desde lo más común hasta usos sofisticados y científicos, que permiten en gran manera potencializar y hacer eficientes las mismas, también con ello y su falta de conocimiento por parte de algunos estados como el nuestro, pone el riesgo y lesiona varios bienes jurídicos tutelados.

Este trabajo ha permitido notar como la inteligencia artificial, más específicamente, arroja predicciones, resultados y conclusiones muchas veces con sesgos de discriminación a cierto grupo de personas como las mujeres, las personas de color, la comunidad LGTBI entre otros, pues los datos con los que son alimentados o los seres humanos que cumplen con esta labor lo hacen desde ciertos aspectos subjetivos, que ha permitido que esta herramienta hoy en día no la podamos usar de forma completamente segura.

Por medio de este artículo se puede establecer la respuesta a nuestra pregunta que busca establecer cuáles son los ciberdelitos o delitos cibernéticos que vulneran el derecho a la intimidad con la implementación de la Inteligencia Artificial, pues si bien tenemos un ordenamiento jurídico que permite penalizarlos y unas instituciones que se ha esmerado por implementar medidas de ciberseguridad, también es cierto que dentro de ellos mismos existen vacíos normativos que permiten su uso sin prever ciertas consecuencias.

Es así que se encuentra hoy en día la inteligencia artificial generativa, que permite tener cierta “autonomía” y autoaprendizaje que, como su palabra lo indica, genera contenido que vulnera derechos importantes para la humanidad y que permiten el goce y disfrute efectivo de la vida misma, como lo son el buen nombre, la dignidad, la igualdad, la libertad de expresión, el libre desarrollo de la personalidad, la libre locomoción, el patrimonio económico, el debido proceso y con estos el derecho a la intimidad que si bien no siempre es el principal bien jurídico objeto de perjuicio, resulta lesionado subsidiariamente por su vínculo e inherencia a la persona humana, lo que indica que en su mayoría de delitos informáticos la intimidad es el derecho que más se ve afectado.

Conclusión

Podemos concluir con el desarrollo de este artículo, lo que representa un acto ilícito como los delitos informáticos y por su parte los ciberdelitos que se presentan en redes de información, de los cuales con el surgimiento de las nuevas tecnologías han migrado o cambiado sus modalidades tratando de perfeccionarlos y por supuesto los cometidos a través de la inteligencia artificial, los cuales atentan contra muchos derechos de la sociedad como la propiedad intelectual, contra el patrimonio económico, derechos de autor, el libre desarrollo de la personalidad, el derecho a la salud, el acceso a la justicia, el derecho a la educación, derechos civiles y políticos y por su puesto el derecho a la intimidad, la fe pública, la integridad personal, el debido proceso entre otros en donde los sujetos pasivos no solo suelen ser las personas del común, sino también entidades del Estado.

Los delitos informáticos han ido en ascenso y se van modificando en la medida que las tecnologías van avanzando, al punto de intentar contra la imagen, la sexualidad y la intimidad de las personas, situación que se presenta por el descuido de la protección a los datos personales, la falta de legislación que regule las aplicaciones que son utilizadas con inteligencia artificial, pues lo que no está regulado se entiende por permitido.

En Colombia la regularización de los delitos informáticos han sido reconocidos con la promulgación de la ley 1273 del 2009, con la cual se sanciona y se multa a los sujetos activos de estos delitos, lo que hace que Colombia haya sido en su momento uno de los países pioneros en la implementación de leyes que regulan y penalizan estos delitos, pero también es necesario decir que ante el aumento de los delitos informáticos y ciberdelitos, además de la innovación constante teniendo como premisa la inteligencia artificial, hoy en día podemos decir que no existe una ley específica que permita tener unos lineamientos frente a su uso y consecuencias jurídicas, lo que deja entre ver el desinterés político por ejercer acciones contra los mismos.

Sin embargo, la falta de conocimiento, por parte de las víctimas, el miedo a denunciar, la falta de credibilidad en la institucionalidad, permite que la efectividad del código penal frente a ciertos delitos de contenido virtual no se ejecute como se esperaría.

Se puede evidenciar que es necesario y urgente que Colombia comience a planificar mediante su órgano legislativo una robusta normatividad frente al uso, consecuencias,

responsabilidades directas y prohibiciones de la inteligencia artificial, además de generar un control previo a las aplicaciones que pretendan introducirse al país, como medio de protección a quienes decidan hacer uso de ellas.

Por otra parte, es importante tener políticas públicas institucionales que eduquen a los diferentes sectores sobre las implicaciones que tiene este tipo de ayudas tecnológicas, para que desde el conocimiento se puedan utilizar de una forma más consiente y responsable y tratar de mitigar riesgos que pueden terminar en la vulneración de derechos importantes para nuestra vida, la educación y la implementación de medidas legislativas son la fuente de seguridad para los individuos de las nuevas generaciones.

Referencias Bibliográficas

Acosta, Benavides, García, 2020, Delitos informáticos: impunidad organizacional y su complejidad en el mundo de los negocios, Universidad de Zulia. <https://www.redalyc.org/journal/290/29062641023/html/#:~:text=Resumen%3A%20Los%20delitos%20inform%C3%A1ticos%2C%20son,almacenados%20en%20servidores%20o%20gadgets>

Ana Higueroa, septiembre 2023, así es como se utiliza de manera ilegal la inteligencia artificial para crear imágenes falsas de personas desnudas. <https://www.20minutos.es/tecnologia/inteligencia-artificial/asi-es-como-se-esta-utilizando-inteligencia-artificial-para-crear-imagenes-falsas-personas-desnudas-5174108/>

Asamblea Nacional Constituyente. (1991). Constitución Política de Colombia de 1991.

Ayala y Duque, mayo 2022, ¿Qué diferencias en ciberdelitos existen entre Colombia y España? Universidad CES, Trabajo de pregrado derecho, repositorio institucional. <https://repository.ces.edu.co/bitstream/handle/10946/6025/Trabajo%20de%20grado.pdf?sequence=6&isAllowed=y#:~:text=Con%20todo%20esto%20se%20puede%20definir%20un%20ciberdelito%20como%20un,se%20utilizan%20los%20sistemas%20como>

Congreso de la República de Colombia, 2018, ley 1928, art 12, Por medio de la cual se aprueba el “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest. http://www.secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html

Congreso de la República de Colombia. (2000), ley 599 del 2000 por la cual se expide el código penal colombiano. http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

Congreso de la República de Colombia. (2009), ley 1273 del 2009 por la cual se se dictan disposiciones generales para la protección de datos personales. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso de la República de Colombia. (2012), ley 1581 del 2012 por la cual se se

dictan disposiciones generales para la protección de datos personales. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>.

Convenio Budapest, 2001, https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Fernández y Sarmiento, (2020). La aplicación de la inteligencia artificial en el derecho penal: consecuencias éticas y jurídicas frente a la medida de aseguramiento, Universidad de los Andes, (trabajo de pregrado) Repositorio institucional. <http://hdl.handle.net/1992/49210>.

Gaceta Constitucional 116 de 20 de julio de 1991. http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

López y Meseguer, 2017, ¿Qué sabemos de la inteligencia artificial? <https://elibro-net.sibdigital.ufpso.edu.co/es/ereader/ufpso/42319>

Márquez, Neila y Mousalli, Gloria (2016), Internet, usos y riesgos. Revista Teuken BidiKay, Año 9, No. 12, Medellín, Colombia, PP. 177-191.

Organización de Naciones Unidas, septiembre 2021, los riesgos de la inteligencia artificial para la privacidad exigen medidas urgentes- Michel Bachelet. <https://www.ohchr.org/es/press-releases/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet>

Sánchez, C. (2021). El derecho al control humano en la inteligencia artificial Una propuesta de regulación del control humano como un nuevo derecho en el ordenamiento jurídico colombiano. <https://repository.eafit.edu.co/bitstream/handle/10784/30580/Carolina-Sanchez-2021.pdf?sequence=2&isAllowed=y>

Serrano, E.R. (2014). La práctica de delitos informáticos en Colombia, Universidad Militar Nueva Granada. (Especialización en Administración de la seguridad) Repositorio institucional. <https://repository.unimilitar.edu.co/bitstream/handle/10654/13452/Ensayo%20%20Edison%20Serrano%20EAS.pdf?sequence=1&isAllowed=y>

Tecnologías de la información y las comunicaciones, entre otras disposiciones. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.