UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Regulación del uso del Reconocimiento Facial en espacios públicos

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogado

AUTOR:

Morales Cáceres, Edwin Francis (ORCID: 0000-0002-5550-8608)

ASESOR:

Dr. Barrionuevo Fernández, Jose Roberto (ORCID: 0000-0001-9679-7015)

LÍNEA DE INVESTIGACIÓN:

Derecho Constitucional

LIMA — PERÚ

2021

DEDICATORIA:

A mi madre por ser una persona consecuente que siempre está motivando a ser mejor día a día.

A dios que siempre está con nosotros y nos permite seguir adelante a pesar de las dificultades que se nos presentan.

A mi familia por ser apoyo incondicional en cualquier momento.

AGRADECIMIENTO:

Agradecer infinitamente a la Universidad César Vallejo, por habernos hecho parte de su casa de estudios y familia; así mismo por brindarme las herramientas necesarias para llevar a cabo la elaboración de mi tesis, y de manera muy especial a nuestro metodólogo Dr. José Roberto Barrionuevo Fernandez, por su paciencia y excelente enseñanza, por la cual se hizo posible culminar el presente trabajo de investigación.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

RESUMEN

Esta investigación referida sobre la regulación del uso de reconocimiento facial en espacios públicos, en cuanto al problema, esta investigación evidenció ¿ Cómo se desarrolla la regulación del reconocimiento facial en espacios públicos?, asimismo el propósito de la investigación ha sido analizar el desarrollo de la regulación del reconocimiento facial en espacios públicos, hay que hacer notar, que el Perú aún no ha implementado la regulación jurídica específica para métodos de vigilancia con reconocimiento facial, sin embargo, aún no se ha evidenciado restricciones para el uso de esta tecnología biométrica, comprometiendo la afectación de los derechos fundamentales y exponiendo nuestros datos sensibles, para finalizar, el enfoque de la presente investigación es cualitativa, de tipo básico, el método es inductivo, el diseño es hermenéutica jurídica, el nivel es explicativo, asimismo, se aplicó instrumento con preguntas abiertas a abogados, llegándose a la siguiente conclusión entre otras: Por un lado estamos ante un nuevo desafío, traído por la necesidad de una tecnología emergente, por otro lado, este desafío nos enfrenta un vacío normativo donde el análisis ha mostrado que las tecnologías evolucionan todos los días, y que la falta de protección legal a las personas por el proceso legislativo es necesario evaluar siempre los principios constitucionales y legales ya consolidados antes de insertar una novedad tecnológica en el ordenamiento jurídico peruano.

Palabras claves: Regulación del reconocimiento facial, tecnologías de reconocimiento facial, inteligencia artificial, derechos fundamentales de la persona, protección de datos personales, datos biométricos, datos sensibles, consentimiento de datos.

ABSTRACT

This research referred to the regulation of the use of facial recognition in public spaces, regarding the problem, this research evidenced How is the regulation of facial recognition in public spaces developed? Likewise, the purpose of the research has been to analyze the development of the regulation of facial recognition in public spaces, it should be noted that Peru has not yet implemented the specific legal regulation for surveillance methods with facial recognition, however, restrictions have not yet been evidenced for the use of this biometric technology, compromising the affectation of fundamental rights and exposing our sensitive data, finally, the focus of this research is qualitative, basic type, the method is inductive, the design is legal hermeneutics, the level is explanatory, likewise, an instrument was applied with open questions to lawyers, reaching the following conclusion between others as: On the one hand we are facing a new challenge, brought about by the need for an emerging technology, on the other hand, this challenge confronts us with a regulatory vacuum where the analysis has shown that technologies evolve every day, and that the lack of protection legal to people through the legislative process it is necessary to always evaluate the constitutional and legal principles already consolidated before inserting a technological innovation in the Peruvian legal system.

Keywords: Regulation of facial recognition, facial recognition technologies, artificial intelligence, fundamental rights of the person, protection of personal data, biometric data, sensitive data, data consent.

I. INTRODUCCIÓN

La presente investigación trata acerca de la problemática por la falta de regulación del marco legal del reconocimiento facial en el ordenamiento jurídico peruano. Es en este contexto la presente investigación titulada: *Regulación del uso del Reconocimiento Facial en espacios públicos,* tiene como finalidad responder a la interrogante ¿Cómo se desarrollará la regulación del uso del reconocimiento facial en espacios públicos?, teniendo en cuenta que la seguridad y la privacidad a menudo se mencionan al mismo tiempo e incluso se tratan como sinónimos, estos pueden funcionar realmente en contradicción, ya que en un intento de mejorar la seguridad, podría afectar derechos fundamentales.

Actualmente en el mundo existe preocupación por el uso de la inteligencia artificial ya que a través del reconocimiento facial se esta recogiendo infinidad de datos sensibles que están siendo almacenados en bases de datos inteligentes lo cual permite el rastreo permanente de personas sospechosas y no sospechosas con lo cual, en algunos o muchos casos se desconoce su debido uso.

Múltiples soluciones tecnológicas con la necesidad de conciliar la persecución del delito han derivado en soluciones altamente intrusivas las cuales poseen una incipiente regulación superponiendo intereses de seguridad en desmedro de los derechos fundamentales de la persona.

Si bien el reconocimiento facial puede utilizarse como un aliado para la seguridad pública, su uso puede suponer un gran riesgo, permitiendo que se produzca una verdadera vigilancia. Esto se debe a que permite no solo identificar al titular individualmente, sino también rastrear su ubicación y definir perfiles de comportamiento. Además, dos factores agravantes lo hacen aún más perjudicial: (i) las cámaras pueden estar en cualquier lugar, incluso camufladas, sin que la persona que tiene la imagen captada lo perciba; (ii) la abundante y creciente disponibilidad de bases de datos, lo que permite potenciar la efectividad del reconocimiento facial. Las técnicas que identifican a las personas sin su debido consentimiento amenazan derechos fundamentales como la privacidad o la

privacidad de datos personales generando graves consecuencias para la persona al no poder ejercer libre consentimiento sobre su tratamiento.

Esta investigación tiene como objetivo principal analizar la regulación del uso del reconocimiento facial en espacios públicos; complementado por los siguientes objetivos específicos, Analizar el marco de la protección de datos en el desarrollo del uso del reconocimiento facial en espacios públicos, analizar el marco del consentimiento de datos en el en el desarrollo del uso del reconocimiento facial en espacios públicos y analizar el marco de la libertad de expresión en el desarrollo del uso del reconocimiento facial en espacios públicos.

La justificación teórica, es que el reconocimiento facial no solo es una tecnología con múltiples beneficios como la ubicación de personas desaparecidas sino que trae consigo amenazas a los derechos fundamentales, por ello ante la ausencia de un marco que la regule, controle y corrija los perjuicios dirigidos hacia la persona, es necesario que esta tecnología tenga un riguroso control de vigilancia a través de su regulación considerando la protección de los datos biométricos que son especialmente sensibles pudiendo ser afectados por terceros con fines ilegítimos, por ello, el estado debe garantizar la protección de las personas de tal manera que no se abuse de esta tecnología, fortalecimiento el marco legal para la implantación de la industria del reconocimiento facial frente a los derechos fundamentales.

La justificación metodológica, es que en la presente investigación se realizará una recolección de datos y se materializará, un instrumento que nos permita explicar cómo las tecnologías de reconocimiento facial inciden en la afectación de los derechos fundamentales y por otro lado conocer la ausencia de protección de datos sensibles especiales ante la falta de una regulación jurídica especifica.

La justificación práctica, es que en el presente trabajo se tratara de dar a conocer posibles recomendaciones explicando que la vigente regulación jurídica es genérica frente la necesidad de implementar la tecnología de reconocimiento facial en el Perú. Esta investigación parte de la necesidad de estudiar la protección de los datos

y su transparencia a nivel de consentimiento en su relación con la tecnología de reconocimiento facial.

Esta investigación es importante ya que analizará la regulación del uso del reconocimiento facial en espacios públicos, porque no hay legislación, esto hace que surjan anomalías legales y constitucionales. La disponibilidad de dispositivos para videovigilancia conectados crea oportunidades para la recolección excesiva, almacenamiento y proceso de una gran variedad de bases de datos, comprometiendo significativamente la vida de los ciudadanos. El Estado tiene el deber como guardián de las Leyes de cumplir y velar por su cumplimiento, buscando el equilibrio entre el uso de los mecanismos de combate al delito, sin vulnerar los derechos y garantías inherentes a la persona humana. Se enfatizará la importancia de este trabajo para la comunidad, entendiendo la legalidad del reconocimiento facial a través de la protección de los derechos y garantías fundamentales, creando un escenario favorable para la protección de datos personales y cumpliendo requisitos de legalidad, equidad, necesidad y proporcionalidad.

II. MARCO TEÓRICO

Antecedentes de estudio

Internacionales

Pabón, J. (2020). Fue quien realizó el articulo: *El uso estatal de las tecnologías biométricas de vigilancia afectación de los derechos a la privacidad, a la intimidad y a la propia imagen.* En este trabajo se describe escenarios de vulneración de garantías y derechos fundamentales, se indica que la tecnología biométrica contribuye en la posibilidad de identificación, contraste, verificación o reserva de los datos personales. Los datos atienden a diferentes clasificaciones en los ordenamientos jurídicos pueden ser públicos, reservados, privados, pero de manera específica atienden a la denominación de sensibles, entendidos como la clase de información que requiere de un especial tratamiento por parte de las personas obligadas al demandar circunstancias preferentes para su acceso como es de suerte exclusiva en casi todas las legislaciones el consentimiento otorgado por el titular.

Del mismo modo se refiere, a que las técnicas de identificación biométricas, debido a su probada eficacia y los bajos costos de implementación, sumado al auge comercial de tecnologías como el reconocimiento facial que se ha integrado con agencias de aplicación de la ley en la certeza de que a través de estas se puede ver, oír, grabar, contrastar, verificar, transmitir en vivo, sin requerir el consentimiento del titular. Violentando su privacidad e intimidad, además de propiciar situaciones que reprimen entre otras el libre desarrollo de la personalidad, generan discriminación, desigualdades, al vulnerar de forma palmaria el concepto de estas garantías y derechos fundamentales.

Concluye refiriendo que la consolidación la Inteligencia Artificial se presenta como una deshumanización del individuo, en un derroche de información en que todo es conocido, visible, transparente, la privacidad en el hogar está siendo vulnerada por la tecnología con sus artefactos que captan datos en múltiples formas y dispositivos. Más no todo debería ser del publico conocimiento, al Estado correspondería respetar este sacro lugar de recogimiento individual, familiar y social con lo que allí acontece evidenciado como información en los denominados datos sensibles o

definidos como aquellas situaciones particulares a veces incomodas aún para el propio sujeto que al estar imbricadas en lo más profundo de los sentimientos y actividades que solo al titular conciernen pertenecen por tanto a su núcleo esencial de intimidad.

Referente a los datos sensibles corresponden en cada legislación a la categoría de información acreedora de un especial trato y cuidado, la que debe ser preservada de su conocimiento a los demás. Legislativamente se han diseñado instrumentos que atiendan a su protección de tal modo se tienen herramientas de alcance continental como es el caso de RGPD en el que se integran de igual modo para su observación los denominados datos biométricos. Asimismo otros ordenamientos jurídicos se han armonizado con la medida, en Colombia esta dispuesta en la ley 1581 en la cual a tenor de lo anterior también se han constituido la jurisprudencia para la protección de los datos relativos a la pertenencia a organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o garanticen los derechos y garantías de partidos políticos de oposición.

Las tecnologías biométricas suponen un escenario escalofriante para la privacidad de las personas, los colectivos y las jurisdicciones que se oponen basan sus apuestas no solo en pedir la moratoria mientras se realiza una legislación que la regule, sino en su prohibición de manera total en el entendido de que es una arma de control tan nefasta como lo son las biológicas que deshumanizan el ser humano haciéndolo previsible, plano, mensurable, inerme al control que de él quieran hacer los Estados y quien tenga el poder de almacenar o de analizar estos datos. Además, esta tecnología se supone falible, proclive al robo, al hackeo, es altamente discriminatoria, sesgada y como se ha demostrado con afinidad por un determinado tipo de raza pudiendo así ser usada en detrimento de los grupos sociales más vulnerables. Hoy los Estados se justifican en principios como el de interés general y para muchos en la actualidad la seguridad es el leitmotiv para proceder con la vigilancia o el monitoreo, especialmente a partir del 09/11, los gobiernos se enfrentan cara a cara con sus propios demonios, el ascenso de doctrinas populistas, la lucha por el poder y los recursos, el control de las economías y la

contención de los flujos migratorios han facilitado aún en la más robusta democracia el ejercicio paralizante de estas prácticas, (Dockendorff, 2013) . Esto cuando no se refiere a las pugnas intestinas en las democracias menos fuertes de los grupos de poder o partidos políticos que organizan una labor nefasta en su beneficio y que tiene como producto la recopilación masiva de datos, los falsos positivos, la vulneración de derechos fundamentales. La biometría tiene un amplio trasegar como técnica de control así desde las antiguas practicas marcarias hasta los sistemas de control tipo panóptico y el desarrollo de tecnologías digitales que van dejando atrás los sistemas análogos que presumen un mayor control de la información, para acoger con beneplácito y de manera vertiginosa prácticas que desbordan el control humano, la IA contribuye de esta forma al reemplazo de la razón por previsiones y análisis basados en números o datos. Finalmente se debe poner sobre el tapete de que también es una sumisión consciente y voluntaria de los individuos al ceder su libertad a cambio de una interacción constante, el ciudadano digital en estas labores debe poder resignarse en todo momento a dejar no solo sus datos si no también parte de su personalidad al acceder a un sistema inteligente.

Los Estados previsivos han vislumbrado esta inmensa oportunidad de control y hacia esta apuntan de manera definitiva e irreversible. En Colombia se realiza un tratamiento indebido de los datos personales sensibles a cargo de algunas agencias de seguridad que contrariando las disposiciones legales realizan una labor de monitoreo o vigilancia sobre determinados grupos de personas con el propósito de extraer información que pueda ser usada con fines de control especialmente político. Se vulneran de esta forma los derechos a la intimidad, a la privacidad y a la imagen con el subsidiario desarrollo de la personalidad. Igual desmedro a estas garantías acontece en los U.S con el notable aumento de la tecnología biométrica de reconocimiento facial, auge que ha permitido una complicidad entre un sector del comercio y las agencias de aplicación de la ley, esta práctica se ha considerado en las prohibiciones como muy grave porque aparte de violentar las enmiendas constituye un trabajo constante de cosificación del ser humano.

Domingo, C. (2021). Quien realizó el articulo: *Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana.* En este articulo da a conocer que el uso de las nuevas tecnologías de la información y la comunicación ha irrumpido con fuerza y se ha extendido a cada vez más ámbitos de la sociedad. El de la seguridad, como no podía ser de otro modo, tampoco ha permanecido impasible ante tal expansión, pues cada vez son más los instrumentos utilizados para salvaguardar la seguridad pública. Entre otros, destacan aquellos que se basan en la biometría, al permitir la identificación de una persona a través de parámetros fisiológicos.

Especialmente significativo es el reconocimiento facial, al ofrecer la posibilidad de detectar a una persona, incluso entre una gran multitud, a través de los parámetros del rostro. A pesar de que se ha puesto en práctica en algunos países, con el fin de detectar a delincuentes conocidos, mostrando ciertas garantías de éxito. Los principales obtaculos que plantea, se derivan de la eventual conculcación de los derechos y libertades fundamentales de la ciudadanía. Por este motivo, es necesario abordar el estudio de las implicaciones éticas y legales que la utilización del sistema de reconocimiento facial supondría, con el fin de determinar si se podría aplicar en todo caso o bajo ciertas condiciones establecidas específicamente en una Ley.

Este trabajo concluye refiriendo que el uso de las nuevas tecnologías se está extendiendo cada vez más y ampliando sus funciones en una sociedad digitalizada que reclama mayores niveles de seguridad. El reconocimiento facial, como todo sistema informático, no es ajeno a este expansionismo, pues se ha implementado ya en varios países con diversos propósitos, principalmente para preservar la seguridad, tanto pública como privada.

Nos topamos ante una técnica revolucionaria, capaz de captar en cuestión de segundos y entre una gran multitud, el rostro de una persona, cuya identidad se encuentra inserta en una plantilla. Esto puede reportar grandes beneficios de seguridad, pues agiliza a los agentes de las FCS la labor de detección y detención de peligrosos delincuentes, así como la localización de personas desaparecidas.

Aun así, los perjuicios que suponen a los derechos y libertades fundamentales son muchos y no se pueden obviar.

Particularmente significativas, las injerencias que conllevan en la intimidad personal, a lo que se añaden otros problemas como los relacionados con el derecho a la no discriminación. De este modo, el ejercicio legítimo de tales derechos entra en colisión con la seguridad ciudadana, ante lo cual nos planteamos qué debe prevalecer en semejante caso. A nuestro juicio, aunque los derechos pueden limitarse bajo determinadas condiciones relacionadas con el principio de proporcionalidad, el reconocimiento facial sobrepasa en mucho dichas condiciones, por lo que no estaría legitimada su implantación en nuestro país, ya que hay otras técnicas menos intrusivas en aquellos para garantizar la seguridad. A lo que hemos de añadir que, en caso de aplicarse, puede utilizarse de forma fraudulenta por las personas encargadas del tratamiento de los datos personales recogidos por este sistema (principalmente empleados del sector privado aunque también los agentes policiales), pudiendo incurrir en los ilícitos de descubrimiento y revelación de secretos.

Todo lo señalado hasta el momento, debemos concluir que el sistema de reconocimiento facial con fines de preservación de la seguridad en lugares públicos, no debe ser asumido, al menos hasta que exista una Ley que recoja expresamente los objetivos, límites y condiciones de su utilización, respetando en lo esencial el derecho a la intimidad personal –y demás derechos fundamentales que su uso puede conculcar–. De lo contrario, una utilización inadecuada del mismo puede derivar en serias vulneraciones de aquella que, como bien jurídico tutelado por el Derecho Penal, legitima la intromisión de este último en aras a su protección, cuando sea lesionado de gravedad.

Abbas, L. (2021). Quien realizó el articulo: *Lo que los ojos no pueden ver, las cámaras monitorean: reconocimiento facial para la seguridad pública y la regulación en América Latina.* En este artículo informa que el avance en el uso de la tecnología de reconocimiento facial con fines de seguridad pública en varios países de América

Latina, se han hecho evidentes los efectos discriminatorios o nocivos sobre otras garantías individuales provocados por el uso de estos sistemas. Las incertidumbres sobre la magnitud del potencial negativo del monitoreo biométrico en los espacios públicos, así como la opacidad derivada del uso de la inteligencia artificial, hacen necesario comprender el escenario actual de garantías legales que enfrenta este nuevo instrumento de vigilancia. El presente trabajo pretende investigar la situación regulatoria del uso de tecnologías de reconocimiento facial en el campo de la seguridad en países de América Latina que cuentan, al menos, con legislación de protección de datos personales. Además de presentar casos de uso de tecnología de reconocimiento facial en Argentina, Brasil, Chile Colombia, Costa Rica, México, Nicaragua Panamá, República Dominicana y Uruguay, se verificaron estándares a nivel nacional que eventualmente regulan este uso o están conectados directamente con la temática, así como las leyes sobre tratamiento de datos personales por organismos públicos, videovigilancia y seguridad pública.

El trabajo concluye refiriendo que la ausencia de un marco legal específico para el uso de sistemas de reconocimiento facial es un problema comprobable en varios países de América Latina. La mayoría de los países terminan apoyando la base legal para su uso en la legislación para proteger datos que son, a su vez, textos generales -que muchas veces superan los límites de la recogida de datos personales con fines de seguridad pública, a través de otros documentos no vinculantes, que intentan (incipientemente) llenar los vacíos por negligencia de los reguladores. Este escenario, verificado a lo largo del texto, pone en riesgo los derechos fundamentales y produce impactos perversos que deberían llevar a los países a cuestionar la posibilidad misma del uso de la tecnología.

La regulación de los sistemas de reconocimiento facial basada única y exclusivamente en predicciones normativas sobre protección de datos, como ocurre en los países analizados, es problemática principalmente por dos motivos. Primero, porque estas regulaciones solo autorizan el uso de esta tecnología para la seguridad pública como una excepción general. En otras palabras, no existe una decisión expresa de la Legislatura para permitir específicamente el uso del

reconocimiento facial a gran escala y en los entornos más diversos. En segundo lugar, y quizás más importante, porque más allá del mero permiso para adoptar la tecnología, esta base normativa no ofrece absolutamente ningún faro o guía sobre cómo deben operar tales sistemas, qué niveles de transparencia y responsabilidad deben respetar, cuáles son las tasas de falsos positivos y falsos negativos. tolerable en qué situaciones, cuál es el procedimiento para la auditoría periódica independiente de estas tasas, etc. El mero permiso a través de una excepción generalizada dista mucho de ser una regulación sensible y juiciosa. El avance del reconocimiento facial en estos países es evidente y se viene dando desde hace algunos años, exigiendo ya una respuesta de los órganos de control y, principalmente, del Legislador, considerando el grado de novedad y complejidad de esta aplicación de la inteligencia artificial.

Puesto que, el uso del reconocimiento facial en los espacios públicos, al cambiar la percepción del espacio, redefine su uso, ya que las personas cambian su comportamiento cuando saben o sospechan que están siendo observadas o vigiladas. Por tanto, el debate que antes podía centrarse solo en las preocupaciones sobre la eficiencia de la instalación de cámaras de vigilancia y los respectivos costos de mantenimiento e implementación ante una posible obligación de Su uso también se convierte en un debate de control social, ya que el intenso flujo de información personal que producen las cámaras instaladas en ambientes públicos se vuelve operativo debido al uso de sistemas de reconocimiento facial y la recolección de datos sensibles.

La regulación en los países latinoamericanos analizados no presta la debida atención a los daños a la libertad de expresión y asociación y parece centrarse en las garantías de protección de datos, aun así, de forma tímida. La Asociación por los Derechos Civiles recomienda estudios para certificar que esta es la mejor medida para enfrentar los problemas de seguridad, que el debate legislativo tiene una amplia participación social y que la legislación tiene disposiciones expresas sobre transparencia, supervisión y control del funcionamiento de las herramientas de reconocimiento facial. para prevenir el abuso.

Y esta disputa necesita ser contextualizado, para que los individuos de los grupos más vulnerables al control social estén adecuadamente protegidos por la regulación. La elección de ubicaciones para la instalación de cámaras con reconocimiento facial y otros sistemas de vigilancia la realizan en la mayoría de los casos grupos de poder ya centralizados, que clasifican y tipifican a los grupos sociales como peligrosos y sospechosos. basado en creencias a menudo discriminatorias ya fuertemente arraigadas en la sociedad, estableciendo severas limitaciones a la posibilidad de autodeterminación de grupos históricamente marginados. Al optar por incluir dichos recursos tecnológicos solo en localizaciones donde exista una incidencia de faltas asociadas a determinados colectivos, como centros de prostitución, venta de productos por vendedores ambulantes o consumo de drogas, las autoridades encargadas de gestionar las cámaras realizan una elección. sobre qué grupos requieren más seguimiento social. La limitación de la autonomía y el control sobre la propia vida no llega, por ejemplo, a los lugares donde se practican los delitos de cuello blanco, reforzando representaciones estereotipadas que consideran solo a grupos objetivo de prejuicios históricos como desviados del estándar de normalidad.

Al analizar y reflexionar sobre las posibilidades regulatorias, es importante que exista un texto legal de aplicación obligatoria e inmediata a cualquier autoridad, que establezca los criterios para la instalación, administración y gestión del funcionamiento de los sistemas de videovigilancia, incorporando el principio de proporcionalidad y preceptos que limitan los procesos discriminatorios para el uso de la tecnología. Para considerar el principio de proporcionalidad, el autor también sugiere que se realicen estudios previos sobre los impactos de la implementación de sistemas de videovigilancia en la configuración del espacio urbano. Además, el autor también sugiere la creación de comisiones estatales y municipales, con miras a reducir la opacidad antes mencionada de esta aplicación de inteligencia artificial, los cuales deben contar con la presencia tanto de instituciones gubernamentales como de grupos de la sociedad civil, especialmente aquellos que históricamente

han sido discriminados y que pueden verse más afectados por los cambios en la dinámica socioespacial provocados por la tecnología.

Como se da a conocer a lo largo del texto, el uso de tecnologías de reconocimiento facial con el propósito de proteger la seguridad pública se basa en realidad en un régimen excepcional, presente en leyes de datos personales, leyes de videovigilancia obsoletas u otros instrumentos normativos. Existe, por tanto, una incorporación de estos sistemas a las estructuras tradicionales de vigilancia en el ámbito penal, principalmente, las que tradicionalmente son discriminatorias, sin ningún debate, estudio previo o legislación adecuada.En un contexto de alta inseguridad social, en el que se hace más apropiado el llamado a la implementación de sistemas de vigilancia por parte del Gobierno, motivado con el propósito de reducción de daños, es fundamental que la discusión sobre la aplicación de esta tecnología vaya acompañada de inquietudes éticas. relacionados con los posibles procesos discriminatorios y estratificación del espacio urbano que pudieran derivarse de su instalación.

El debate también debe abarcar discusiones sobre la protección de la privacidad y los datos personales de las personas sometidas a esta forma de control, pero es fundamental entender que un sistema de reconocimiento facial en pleno y riguroso respeto a todo un marco regulatorio sobre la protección de datos también puede ser problemático por varias otras razones relacionadas con la prohibición de la discriminación, el derecho de circulación y la libertad de expresión.

Antecedentes Nacionales

No se encontraron antecedentes referentes a Reconocimiento Facial en el Perú

La videovigilancia es una tecnología operada por medio de cámaras de video donde el fin es llevar un registro permanente de los acontecimientos que ocurren en los sitios en donde se hallan instaladas, estableciendo puntos estratégicos de las cámaras con la intención de facilitar la investigación para la lucha contra la delincuencia.

La mayor parte de las cámaras de video vigilancia se encuentran reguladas, tanto en su ubicación como también en su operatividad y el método de las grabaciones para que sean entregadas a la Policía Nacional del Perú y/o al Ministerio Público.

Al respecto, la **Ley N° 30037 (2013),** exige la instalación de las video cámaras en un área de 5 cuadras a la redonda alrededor de los recintos, obligando a que la información se conserve y sea entregada sin mediar mandato judicial previo a la Policía Nacional el último día hábil del mes siguiente después del espectáculo deportivo o ya sea si esta se solicita.

Al respecto, la **Ley N° 30120 (2013),** impone a toda empresa o persona de haber instalado cámara de video en el frontis del inmueble a entregar los videos a la Policía Nacional o al Ministerio Público, si se sospechara de algún un delito o si es que se le solicitara. Para ello se creará una base de datos con aquellos que cuenten con estos dispositivos el cual estará a cargo del Centro Nacional de Videovigilancia y Radiocomunicación para la Seguridad Ciudadana.

Al respecto, el **Decreto Legislativo N° 1218 (2015),** obliga a personas o empresas que administran bienes públicos instalar cámaras de video deacuerdo a normas vigentes de seguridad ciudadana, así como también para aquellas que brinden servicio público de transporte y de aquellos que tengan establecimientos comerciales por lo menos de 50 personas. Ante la sospecha de delitos facilitar la entrega a la Policía Nacional o al Ministerio Público.

Un aspecto importante al momento de hacer uso de las cámaras de video vigilancia es lo que se registra lo cual hace referencia a la imagen de las personas.

El derecho a la propia imagen es un derecho autónomo de protección frente a reproducciones de la imagen de la persona, para que esta no se vea afectado, salvaguardando su vida íntima de terceros, donde se evite mostrar su aspecto físico, cual fuese la finalidad de quien la capta o la difunde.

Constitucionalmente el plano patológico se encuentra protegido el cual está dirigido a conductas infractoras, asimismo el Tribunal Constitucional garantiza la libertad de la persona a través de características como la voz, imagen, nombre, que son inherentes de toda persona, es así como el derecho a la imagen protege la información gráfica, vale decir, los rasgos físicos ante una difusión pública no autorizada.

El Tribunal Constitucional de España considera que en ciertas circunstancias una imagen que es consentida por una persona podría afectar el derecho fundamental, Sentencia 81/2001, fundamento 2, ello si llegara a vulnerar la dignidad de la persona afectando derechos fundamentales, debiéndose probar y sustentar deacuerdo al marco constitucional protegido.

El derecho a la propia imagen no esta sujeto a un espacio geográfico es así que la persona podría oponerse a ser captada en la vía publica en base al principio de proporcionalidad. Prieto (2003) señala que el derecho a la propia imagen podría verse afectado por otro derecho constitucional lo cual podría producir un conflicto, el cual se resolvería en base a jerarquías.

Constitucionalmente no hay tutela de daños pero si se puede presentar demandas constitucionales. La acción de amparo permite proteger el derecho a la propia imagen, justificándose la protección respecto a la video vigilancia.

Por ello, la aplicación del principio de proporcionalidad debe establecer un equilibrio entre derecho de las personas y las obligaciones del estado para con la persona

respecto a la seguridad ciudadana. Esto es aplicable para juzgados, cortes y Tribunal Constitucional.

El Principio de proporcionalidad, respecto a las cámaras de video vigilancia no incluye el tipo de cámaras que han de considerarse, solo establece la justificación de su instalación con un fin legítimo. En referencia a la conservación de los datos no debe exceder de los 60 días, en el cual se debe asegurar confidencialidad ante terceras personas.

El uso de video cámaras en lugares públicos posee obligaciones dentro de las cuales es garantizar la seguridad de las imágenes ante posibles alteraciones, perdida, tratamiento o accesos no autorizados y lo más importante la confidencialidad es por ello que ante todo se debe mantener un estricto cumplimiento del principio de proporcionalidad.

En la actualidad, el Perú ha normado el uso e implementación de las cámaras de video vigilancia, como parte de la seguridad ciudadana frente actos delincuenciales, sin embargo, países en Europa, Norteamérica, Centroamérica y Sudamérica ya vienen haciendo uso de tecnologías más avanzadas y especializadas como el reconocimiento facial.

En lo concerniente al reconocimiento facial, la biometría tiene que ver con características de conducta y rasgos físicos de las personas. Podemos clasificar el reconocimiento facial dentro de la biometría estática mientras que la biometría dinámica comprendería la conducta y las características psicológicas, es por ello que podremos identificar a una persona a través de estos rasgos.

A nivel tecnológico, se cuenta con una base de datos que almacena los datos biométricos, pero alguno de los rasgos con el pasar del tiempo podrían sufrir modificaciones ya sea en la piel o el rostro.

Los datos biométricos son considerados únicos por ello no hay forma que estos sean iguales al de otra persona, mas bien los riesgos, a juicio de los expertos, se

encuentra en el tratamiento de la base de datos, ya que el operador de estos datos debe asegurar confidencialidad y cumplimiento de las normas.

También podría considerarse otros riesgos a nivel de estado, como el de individualizar a la persona en la base de datos biométrica al realizar una vigilancia masiva, no para asegurar la seguridad de las personas, sino al contrario, como uso discriminatorio y desproporcional afectando los derechos fundamentales de la persona.

El reconocimiento facial automático es un procedimiento técnico de inteligencia artificial consistente en evaluar si dos imágenes faciales representan a la misma persona. El sistema se basa en la comparación entre dos fuentes de información:

- Una base de datos con los datos biométricos faciales (propiedades geométricas, tales como la distancia entre las pupilas, la posición de la nariz o la distancia entre la comisura de los labios) de una serie de imágenes faciales de personas identificadas -por ej., las que provienen de las fotografías que se realizan a las personas detenidas en dependencias policiales. Según el contexto y la finalidad con la que se use el sistema de reconocimiento facial automático, esta base de datos puede estar integrada por todas las imágenes que posea el cuerpo policial, cuando el sistema se utiliza en procesos rutinarios de investigación; o por imágenes de un número limitado de personas seleccionadas, con las que se constituye una lista de observación o vigilancia, cuando el sistema se utiliza para eventos concretos en tiempo real.

- Imágenes de personas no identificadas, de las que un programa informático extrae los datos biométricos faciales. Las fuentes de estas imágenes pueden ser varias: por un lado, aquellas que se pueden obtener, por ej., de grabaciones realizadas por las Fuerzas y Cuerpos de seguridad o por sistemas de vigilancia privados y que con posterioridad son tratadas en dependencias policiales con este fin; y por otro, aquellas que se obtienen y son tratadas en tiempo real mediante un circuito cerrado de televisión (CCTV) en un determinado evento en el que se esté aplicando el sistema de reconocimiento facial automático. Una vez que se tienen las dos fuentes

de información que se quieren cotejar, el sistema realiza una comparación a través del correspondiente programa informático que otorga una puntuación a la similitud entre dos caras, de tal manera que a partir de una determinada puntuación (valor umbral) cuyo nivel se puede configurar, el sistema informa de una posible coincidencia. Ante ese resultado de existencia de una posible coincidencia, el protocolo de actuación prevé que sistema debe valorar si esa coincidencia es correcta o no y, si la considera viable.

Si no se producen coincidencias, como ocurre en la abrumadora mayoría de los casos, el sistema no retiene la imagen facial de las personas ni su plantilla biométrica, que son eliminadas de manera automática e inmediata. No obstante, la grabación realizada por el circuito cerrado de televisión se conserva durante una cantidad de tiempo conforme a la normativa aplicable. Los datos asociados con una coincidencia se retienen dentro del sistema de reconocimiento facial automático durante 24 horas. La plantilla biométrica, aunque haya coincidencia, se elimina inmediatamente; y la lista de observación -con sus imágenes y plantillas biométricas- también se elimina en el plazo de 24 horas.

Los sistemas de video vigilancia comunes y el reconocimiento facial podrían estar integrados, de tal manera que a través de estas tecnologías se pueda hacer el tratamiento de datos biométricos pero la cual tendrá que someterse a los principios de ley según corresponda.

Deacuerdo a la ley de protección de datos personales de España en su artículo 9.2, la instalación de sistemas de reconocimiento facial en sistemas de video vigilancia puede integrarse ya sea por razones de interés público o medicina preventiva cumpliendo requisitos de seguridad y confidencialidad.

El reconocimiento facial es una tecnología altamente intrusiva, que obliga la recolección y almacenamiento de un dato sumamente íntimo, como es nuestro rostro. En tareas de vigilancia del espacio público, su uso conlleva la recolección masiva e indiscriminada de información altamente sensible y, al menos

potencialmente, permite la creación de perfiles detallados de rutinas diarias de todas las personas.

La implementación del reconocimiento facial podría ser una amenaza a la dignidad, al debido proceso o a la presunción de inocencia para grupos vulnerados como mujeres, personas de color y también personas trans por el uso de técnicas de sesgos.

Singularmente cuando se utiliza para la vigilancia del espacio público y el combate del delito común, pues erosiona la autonomía de las personas en favor de un sistema que pretende el control absoluto, mediante la gestión técnica de las identidades, reproduciendo las desigualdades y exclusiones que históricamente han puesto en desventaja a las comunidades no hegemónicas.

A través de los datos biométricos los procedimientos de identificación podrían recoger información como raza, genero, estado emocional, enfermedades, discapacidades, características genéticas, consumo de sustancias, entre otros sin que el individuo se pueda negar a dar la información, sin duda, la licitud y la debida transparencia podrán establecer proporcionalidad y respeto a los principios del tratamiento de datos personales.

El Motivo propuesto por el Comité Europeo de Protección de Datos (EDPB) contempla prohibir cualquier IA de reconocimiento de rostros, voz y movimientos, huellas dactilares, ADN, pulsaciones de teclas, y otras señales biométricas o de comportamiento, independientemente del contexto, siempre y cuando sea en áreas de acceso público. Los organismos creen que debería ser ilegal que los sistemas de inteligencia artificial utilicen datos biométricos para categorizar a las personas, especialmente en grupos basados por etnia, género, orientación política o sexual, o cualquier otra clasificación por la cual podrían ser discriminados.

Otra de las peticiones del organismo también es la prohibición del uso de la IA para “inferir en las emociones de una persona”: solo debería estar permitido en situaciones específicas, por ejemplo, por razones médicas. Dicho documento propone una prohibición de la IA basándose en niveles de riesgo y con severas

sanciones en caso de un mal uso, mientras que las autoridades tendrían mayor libertad de uso, por ejemplo, para prevenir amenazas inminentes o para encontrar menores desaparecidos.

Se viene discutiendo el tema del fin del anonimato por el uso de la identificación biométrica en espacios públicos, por ello muchos países del mundo están trabajando sobre un marco legal de la inteligencia artificial centrado en el ser humano a fin de evitar discriminaciones sociales.

Debido a la existencia de técnicas ocultas que amenazan la filtración de datos personales conllevaría a graves consecuencias para ejercer libre consentimiento lo cual resulta en un tratamiento de datos no proporcionado.

Teniendo en cuenta lo que se podría hacer con este tipo de datos si se usa de una manera incorrecta, debemos recordar que la cara se trata de un dato especialmente protegido por el RGPD puesto que identifica de una manera unívoca a una persona a través de sus características físicas o fisiológicas.

En concreto, el reconocimiento facial en vivo (LFR por sus siglas en inglés) impacta directamente a los derechos fundamentales, por lo que es importante ser precavidos ante este uso de la tecnología. Además, la solicitud de prohibición por parte del EDPD va más allá del reconocimiento facial y también pide que se prohíba la IA capaz de reconocer las emociones de las personas.

Por tal motivo lo que se propone es una prohibición general de esta tecnología como punto de partida, así como la mencionada prohibición de IA para la puntuación social, una proposición totalmente opuesta a la que se utiliza en países como China con programas de reconocimiento facial masivos que permiten al país asiático clasificar ciudadanos entre aquellos que son considerados “mejores ciudadanos”. Sin embargo, dados los beneficios que también aporta esta tecnología debemos tener otros factores en cuenta la hora de su implementación:

– Necesidad y proporcionalidad: la necesidad está incorporada en los principios de protección de datos del RGPD (los requisitos de los datos de categoría especial en

el artículo 9 y los requisitos de la EIPD en el artículo 35). Según indica la ICO: “Para que el tratamiento sea necesario, debe ser “razonablemente necesario”. Esto significa que el tratamiento debe ser más que deseable, pero no tiene que ser indispensable o absolutamente necesario”. El tratamiento no será necesario sin la adecuada finalidad legítima del responsable del tratamiento, y tampoco será necesario si la finalidad legítima del responsable del tratamiento puede alcanzarse razonablemente con un enfoque menos restrictivo o intrusivo.

– La proporcionalidad está estrechamente relacionada con la necesidad, y los responsables del tratamiento deben considerar si su finalidad es lo suficientemente importante como para justificar cualquier intrusión en la intimidad o cualquier otro impacto que surja para el individuo.

La tecnología de reconocimiento facial supervisa, recopila, almacena datos biométricos sensibles de manera masiva e indiscriminada afectando los derechos a la privacidad, libertad de expresión y reunión pacifica llegando a clasificar a las personas debido a la ausencia de protocolos que permitan disminuir arbitrariedades sobre las personas.

En lo que concierne al reconocimiento facial en el Perú, municipalidades como la Victoria, San Martin de Porres, Miraflores, entre otros, están realizando monitoreo de vigilancia biométrica en espacios públicos con esta nueva tecnología apoyados junto a la Policía Nacional, se viene utilizando sin ninguna restricción ya que el marco legal aun no esta configurado, sin embargo, hay propuestas de parte de organizaciones pro-derechos humanos como Hiperderecho.

En América latina países como Brasil, Ecuador, Uruguay, Colombia, Bolivia, México ya vienen implementando sistema de reconocimiento facial, mientras que en Estados Unidos se viene evitando usar la tecnología ya que de acuerdo con su regulación se han presentado riesgos que atentan a la protección de datos personales.

La regulación del reconocimiento facial debe establecer derechos a ser protegidos de tal manera que haya un alto nivel de regulación evitando que ocurran abusos, protección a las poblaciones vulnerables o minorías a través de derechos universales, transparencia dentro del marco de recolección de datos biométricos, atención a sesgos injustos, se debe evitar una supervisión automática y finalmente, se deben incluir los protocolos necesarios para el uso en espacios públicos asegurando que no haya usos discriminatorios.

Con relación a los derechos fundamentales los cuales son reconocidos en la constitución peruana debemos mencionar que la Cuarta Disposición Final reconoce la Declaración Universal de Derechos Humanos, tratados y acuerdos. Dentro de los derechos fundamentales a proteger se encuentra el derecho a la privacidad o intimidad.

La privacidad o intimidad es un derecho fundamental reconocido como protección de los ciudadanos, en la cual, considera evitar la apropiación de la imagen para la obtención de beneficios de terceros.

Por consiguiente, la privacidad distingue aspectos fundamentales como la autonomía, la tranquilidad y el control de la información.

La autonomía esta relacionada a la toma de decisiones sin interferencias directas o indirectas, la tranquilidad relacionada a la protección contra la intromisión y el control de la información relacionado de la reserva de ciertos aspectos de la vida y control de la circulación de la información confiada a un tercero, lo cual permitirá el libre desarrollo y autónomo de la persona.

Por ello, se debe evaluar la necesidad de publicar captura de imágenes que no sean de interés publico en detrimento con los derechos constitucionales como la integridad moral y el honor de las personas, bajo los límites que considera el derecho a la imagen.

Hoy en día, la instalación de cámaras de video en lugares públicos ha sido colocadas para evitar la proliferación de la delincuencia, pero con ello se debe

determinar los ámbitos de privacidad a los cuales se puede acceder para evitar la intromisión de terceros basándose en derechos humanos de seguridad y de privacidad o intimidad.

Para que el individuo pueda vivir en sociedad, es necesario estar en medio del público en general, mediante el uso de lugares comunes para uso colectivo, a saber, plazas, restaurantes, bibliotecas, museos, clubes, etc. De manera directa, dicho uso se da dentro de la rutina de los ciudadanos. Por tanto, la permanencia del individuo en estos lugares no puede interpretarse como ausencia de amparo constitucional. Es la protección que aún logra la vida privada (y también la protección constitucional que otorga a la imagen). (TAVARES, 2012).

El derecho a la intimidad no se puede interpretar de manera restringida, pues de ser así, los individuos tendrían que vivir presos en sus domicilios, no pudiendo gozar de libertad fuera de dicho entorno.

Los métodos de identificación biométrica, tal como se están aplicando, atentan contra el derecho a la privacidad protegido por la Constitución Federal, al recolectar datos y monitorear al ciudadano de manera constante y sin su consentimiento. Así, respecto al uso de tecnologías, se puede decir que:

Es claro que hay que reconocer que hay un agotamiento paulatino de la privacidad, especialmente de las posibilidades efectivas de su protección real, lo que no significa que no haya más espacios para un mayor blindaje y al menos, aunque las intervenciones sean en el ámbito privado, mecanismos de reparación a posteriori. (SARLET; MARINONI; MITIDIERO, 2017, p. 493).

Todo ciudadano, incluso si se encuentra en lugares públicos, tiene un cierto grado de anonimato, dado que la mayoría de las personas que se encuentran allí no tienen el menor conocimiento de quién es ese individuo en particular, siempre que quede claro que no es una figura pública. Esa persona puede viajar en metro, autobús y cualquier otro medio de transporte, sin ser reconocida en ningún momento. Sin embargo, sucede que, si una cámara de seguridad realiza un reconocimiento facial

al identificarlo, puede vincular su identidad física a su identidad digital y hacerlo sin obtener primero su consentimiento.

Los avances tecnológicos en la sociedad no han podido evitar afectar derechos fundamentales, tal es el caso de la privacidad o intimidad, el cual salvaguarda un determinado espacio con carácter exclusivo sin que se tenga acceso de terceros.

No solo podría darse una intromisión de la parte civil sino también de parte del gobierno, utilizando medios no regulados que no garanticen la seguridad del ciudadano afectando la esfera privada del individuo.

Conforme va transcurriendo el tiempo se va perdiendo el aspecto privado a consecuencia del avance tecnológico, ya que por un interés legitimo en salvaguarda de la seguridad inicialmente se ha implementado el uso de cámaras de vigilancia y hoy en día se vienen implementando cámaras de vigilancia con reconocimiento facial haciendo uso de algoritmos de inteligencia artificial que proponen una mayor seguridad al ciudadano pero también un mayor peligro a su privacidad y libertades.

Esto conlleva a que los países del mundo vienen implementando marcos reguladores para no afectar al ciudadano y que no se vean afectadas sus derechos fundamentales minimizando los riesgos al cual se podrían enfrentarse.

Mucha de la información valorizada del ciudadano esta contemplada en los datos personales, por ello, esta información debe ser protegida en base a instrumentos de tutela jurídica.

Cada ciudadano que se encuentra registrado en un banco de datos se encuentra expuesto a una vigilancia masiva dado que sus datos sensibles se encuentran disponibles a operadores o terceros que podrían utilizar la información malintencionadamente, es por ello que se comienza a exigir reconocimiento sobre el uso y control de los datos.

La protección del derecho a privacidad o intimidad no implica un proceso de impedimento para su uso de reconocimiento facial, al contrario, lo que se quiere es asegurar su debido funcionamiento y aplicabilidad protegiendo los derechos fundamentales de la persona.

Ante ello, el derecho a la protección de datos implica como un derecho fundamental en salvaguarda de los principios fundamentales asegurando y controlando la os datos personales posibilitando a la persona decidir si desea o no compartir los datos, quien puede tener acceso a ellos y por cuanto tiempo, debido a que razones o también la modificar los datos que le pertenezca.

Asimismo, en cuanto a los derechos de libertad y de no intervención son importantes para que una persona pueda desenvolverse libremente en la sociedad, el cual se encuentra reconocido constitucionalmente, de tal manera que permita la autonomía de la persona.

Los datos personales es información que permite conocer a una persona como nombre, apellidos, fecha de nacimiento, dirección, teléfono, RUC, placa de vehículo, huella digital, ADN, imagen, numero de seguro social entre otros datos esto de manera directa o indirectamente.

Los datos personales se rigen en base a principios como la legalidad, consentimiento, finalidad, proporcionalidad, calidad y seguridad.

La legalidad prohíbe la recopilación de los datos personales por medios ilícitos, el consentimiento es la autorización de parte del titular para con sus datos personales, la finalidad es el fin de la recopilación de los datos, la proporcionalidad esta alineado al fin establecido debiendo ser imprescindible, suficiente y sin excesos, la calidad refiere a que los datos deben ser veraces y exactos y finalmente, la seguridad de los datos refiere en que el titular del banco de datos y el encargado del tratamiento deben garantizar seguridad y confidencialidad.

Los datos sensibles caracterizan a cada individuo ya que forman parte de la información privada de cada persona como origen étnico, opiniones políticas, convicciones religiosas, afiliación sindical, información de salud u orientación sexual, los cuales han debido ser registrados en base a un fin que justifiquen razones de interés general con su debido consentimiento expreso siendo protegidos jurídicamente de tal manera que se puedan evitar daños a la persona.

Los datos deben estar sujetos a un control estricto de tal manera que la manipulación de la información no vaya en perjuicio del titular o que sea entregada a personas sin el consentimiento del titular. De esta forma, la audeterminacion informativa ejerce control sobre la información vinculada a la persona que se encuentre almacenada en banco de datos buscando garantizar la vida privada de la persona.

En el Perú, la Ley 29733, la cual corresponde a la Protección de Datos Personales a través de la Autoridad Nacional de Protección de Datos establece los procedimientos para su debida protección ante cualquier tratamiento desproporcionado, abusivo o irregular. Hoy en día, los riesgos siguen aumentando, y es que ante esta nueva tecnología del reconocimiento facial será necesario establecer un marco jurídico que pueda proteger al ciudadano.

La privacidad de la información es conocida como protección de datos personales la cual es una garantía legal de los datos públicos y datos sensibles relacionada a intereses de igualdad, libertad o intimidad.

Cualquier sitio o servicio que almacene, procese, indexe o transmita esos datos hace tratamiento de datos personales; conviene entonces analizar si esas conductas afectan o no los derechos fundamentales de los titulares de dicha información y en qué medida lo hacen.

El titular de los datos personales tiene el derecho a ser informado respecto al tipo de finalidad o al desino que tendrá sus datos, el titular podrá acudir ante la Autoridad

Nacional de Protección de Datos Personales o Poder Judicial para la protección total o parcialmente de sus datos y tendrá derecho a la indemnización en caso sea afectado por algún incumplimiento de la Ley de Protección de Datos Personales.

La información del titular podrá ser recogida y almacenada en banco de datos que deacuerdo al presente marco jurídico, esta debe permanecer por un tiempo, pero ello está referido a ciertos tipos de datos que actualmente la Ley protege.

Los datos al cual nos referimos al hacer uso del reconocimiento facial corresponden a los datos biométricos, los cuales son altamente sensibles y aun no existe un marco regulatorio para ello.

Los bancos de datos son aquellos que su titularidad es publica o privada y se encuentran organizados de manera automática o manual. Los de titularidad publica son administradas por el estado, mientras que los de titularidad privada corresponden a personas naturales o jurídicas de derecho privado, pero no vinculadas a empresas públicas.

El titular del banco de datos establece el fin para recopilar y almacenar los datos personales, así como también el tratamiento y las medidas de seguridad que este aplicará.

El encargado del tratamiento de datos personales es quien realiza el tratamiento de datos personales en nombre del titular del banco de datos, siendo responsables ante tratamientos ajenos asumiendo así las responsabilidades pertinentes.

A través de los procedimientos de anonimizacion y disociación se evita identificar al titular, mientras que el procedimiento de anonimizacion es irreversible, el procedimiento de disociación es reversible.

Como se comentó con anterioridad a través del consentimiento expreso, es que los datos personales podrían permanecer dentro de un banco de datos, pero también

podría a través del interés publico permanecer en un banco de datos, es así como por temas de seguridad nacional se establece un consentimiento tácito.

El principio de consentimiento ampara habilitar su uso justificando su tratamiento, este principio es el inicio para el tratamiento de los datos personales, sin el consentimiento expreso del titular no se podrá realizar algún tratamiento a los datos, asimismo a través del consentimiento se manifiesta la voluntad libre e informada e inequívoca autorizando el tratamiento a los datos personales.

El principio de consentimiento considera para el tratamiento de datos personales aquellos de manera expresa y tacita. El consentimiento expreso, se da través de la firma del interesado o traves de un escrito en el cual se autoriza el tratamiento de la información privada del titular, mientras que el consentimiento tácito, se da autorización de los datos personales sin haber realizado una acción concreta, este hecho podría al titular de los datos personales oponerse o revocar el tratamiento de sus datos y registro en los bancos de datos.

Se podrán considerar ciertas excepciones para el caso de la cesión de los datos sin el consentimiento del titular, si esta fuera por norma con rango de ley, si fueran datos recogidos de fuentes accesibles al publico o si se diera por la aceptación de una relación jurídica siempre y cuando se limite la finalidad justificada.

En cuanto la cesión entre administraciones publicas esta se dará con fines históricos, estadísticos o científicos, elaboración de una administración pública a otra, ejercicio de competencias sobre materias idénticas o cesión de datos entre organismos de salud correspondientes al Sistema Nacional de Salud para atenciones sanitarias.

Referente a la revocación del consentimiento solo podrá darse si existe causa justificada y que además no haya efectos retroactivos.

Finalmente, para el tratamiento de datos de menores de edad se requerirá el consentimiento de los padres.

En cuanto la legislación internacional, el artículo 12 de la Declaración Universal de Derechos Humanos, el sistema de reconocimiento facial al realizar un seguimiento de 24 horas y 7 días a la semana genera opresión sobre las personas captando situaciones que no necesariamente deben estar almacenadas en los bancos de datos, esto es una clara injerencia a la vida privada de las personas, en muchos casos su implementación no es necesaria ni proporcionada.

En el artículo 2 de la Declaración Americana de los Derechos y Deberes del Hombre, se hace hincapié respecto a la igualdad ante la ley, lo que hoy en día es más común es la presentación de fallas, debido a que las personas de color no son identificadas correctamente, las personas trans también tienen problemas al momento de su identificación, es así que se debe respetar la igualdad no solo a través de los marcos jurídicos existentes sino también de las propuestas específicas para la protección del ciudadano.

En el articulo 13 de la Convención Americana sobre Derechos Humanos o Pacto de San Jose, refiere a la libertad de expresión, en la cual su efecto inhibidor afecta gravemente a las distintas expresiones publicas de las personas alterando la libertad de reunión, la libertad de expresión debido a su permanente vigilancia.

Respecto a la legislación Peruana, el articulo 2 de la Constitución Política del Perú refiere la vida privada del individuo, como se comentó para la legislación internacional, esta protege que la persona no se sienta hostigado ante la permanente vigilancia de parte del estado sobre todo en situaciones en las cuales no cumpla el principio de proporcionalidad.

Es por ello, que en el articulo 200 de la Constitución Política del Perú, se establecen las garantías ante amenazas de parte de cualquier acción del estado que afecten directamente los derechos fundamentales de la persona, por consiguiente, el

sistema de reconocimiento facial tendrá que alinearse a la regulación jurídica específica para su debido uso.

Asimismo, el articulo 154 del Código Penal Peruano, hace notar que la captación de una imagen a través de cámaras de video vigilancia es espacios públicos no colisiona con la su esfera intima de la persona.

Mas bien si el que hace el tratamiento de los datos personales es quien se vale de la información para comercializarla ilegítimamente, será condenado a cierta cantidad de años

De acuerdo al Código Civil Peruano, en su articulo 17, se prevé un mecanismo procesal civil que habilita la llamada tutela inhibitoria. (León, 2007). Vía en la cual se solicita la cesación de la vulneración y se puede adicionalmente solicitar una pretensión resarcitoria por daños calificados como daño emergente, daño a la persona o daño moral, cuando estemos ante una vulneración que afecte la imagen personal; o como lucro cesante, cuando estemos ante una vulneración que corresponda a lo que dejó de percibir por un uso comercial o lucrativo.

Cabe mencionar, que nuestros derechos se encuentran protegidos de acuerdo al artículo 37 del Código Procesal Constitucional Peruano, estableciendo igualdad ante la ley y protección contra actos discriminatorios. Esta igualdad enmarcada a la presunción de inocencia de parte de toda persona, no por el uso de una tecnología inteligente podríamos partir que uno u otro es culpable. Esto debe evitar que por error se detenga a personas con medios probatorios fallidos.

La Ley de Protección de Datos Personales en su articulo 2, menciona a los datos biométricos, pero ante el uso del reconocimiento facial, se debería ampliar la definición del dato biometrico facial, de tal manera que se tenga mayor control sobre este tipo de dato sensible.

La ley de datos personales en el articulo 14, establece temas relacionados a la videovigilancia, pero se tendría que ampliar el tema hacia el reconocimiento facial

considerando derechos de ARCO, tipos de consentimiento, y la manera de salvaguardar el interés legitimo del titular de los datos personales.

Finalmente, el articulo 25 de la Ley de Protección de Datos Personales, se refiere a un resarcimiento por incumplimiento de la Ley, tal es el caso de los sesgos de parte del sistema.

La presencia del efecto inhibitorio debido al uso del reconocimiento facial podría considerarse como un método de control social debido al monitoreo continuo e invasivo alterando la conducta de las personas. Se da el caso en que muchas personas por la presencia del reconocimiento facial podrían abstenerse de realizar ciertas actividades autocensurando actividades licitas y actividades ilícitas por temor a que las autoridades realicen seguimiento de ellos. Este efecto inhibitorio en cierta forma limitaría las libertades de la persona como derecho fundamental debido a las sanciones que se determinen si es que se hallara alguna conducta anormal, y si no fuera así, el individuo no podría saber cómo actuar debido al desconocimiento jurídico.

Es por ello, que la presencia de la tecnología de reconocimiento facial en espacios públicos no debería hacerse de manera secreta, sino al contrario de manifestarse de manera transparente a las personas de tal manera que haya un fundamento legal de su presencialidad. Así también, el exceso de la vigilancia a través de la instalación de la tecnología del reconocimiento facial en todo lugar público generaría una presión sobre el individuo cuasi amenazante perjudicando en cierta manera el libre ejercicio de sus derechos fundamentales.

Las tecnologías como el reconocimiento facial tienen un gran impacto dentro de la sociedad, sobre todo en la esfera privada de las personas a pesar de que se encuentra dentro un espacio público, ya que tiene que ver mucho con las conductas de las personas.

El reconocimiento facial en espacios públicos funcionaria como un mecanismo equivalente a que nos estén solicitando documentos en todo momento sin motivo alguno o consentimiento de parte de las personas atentando de alguna manera

contra la presunción de inocencia y/o afectando las libertades públicas respecto a los derechos fundamentales.

Es importante que en el espacio público se establezca el orden y la tranquilidad del ciudadano de tal manera que no se alteren las garantías constitucionales, como la presunción de inocencia o el debido proceso. Por ello será necesario regular las políticas de tal manera que se legitime el reconocimiento facial dentro espacios públicos.

El reconocimiento facial tiene distintos fines, dentro de los cuales se encuentra el de investigación terrorista e investigación criminal lo cual interfiere con distintos derechos fundamentales asumiendo que hay culpabilidad de todas las personas que son captadas por el reconocimiento facial a través de la recolección de los datos biométricos.

La vulneración a la presunción de inocencia podría darse por problemas del software, al hacer discriminaciones en los rasgos faciales de las personas y no ubicar a las que se busca. La precisión del software es muy importante ya que deberá reconocer los rostros dejando de lado los posibles sesgos y asi evitar la discriminación de las personas de tal manera que no se culpe a alguien que no cometió delito.

En el espacio público el uso del reconocimiento facial de manera masiva y desproporcionada podría ser perjudicial a las garantías constitucionales de tal manera que dificulta los derechos fundamentales por la criminalización incorrecta de personas a través de errores o de personas erróneamente identificadas, lo cual implica que una persona podría ser hasta condenada sin tener las suficientes pruebas de cargo.

En este caso, cualquier sospechoso deberá probar su inocencia, que a pesar del error del software, deberá presentar los medios probatorios necesarias revirtiendo la acusación. Esta problemática va en contra de los derechos humanos de la persona respecto a sus derechos fundamentales, ya que no debería esperarse una sentencia ejecutoria si es que la persona es inocente. Las pruebas que se

presenten a través de la videovigilancia con reconocimiento facial no deberían ser determinantes, sino que debe existir la garantía procesal del procesado tomando en cuenta que toda persona es inocente hasta que se pruebe lo contrario.

En garantía del debido proceso se deben establecer los protocolos necesarios para la captación de los datos biométricos. Es importante considerar los protocolos ya que así se podrá formalizar acusación estableciendo las pruebas necesarias para incriminar a las personas que hayan cometido algún delito a través de la captación de los datos biométricos.

El algoritmo debería ser conocido por la parte reguladora de tal manera que exista transparencia y determinar que no existan sesgos malintencionados. Este protocolo determinado por la parte reguladora evitaría las discriminaciones ante afectaciones de la presunción de inocencia y se aseguraría el debido proceso.

Esta problemática de determinar un protocolo o la transparencia del algoritmo establece que aun los gobiernos no tienen el conocimiento del daño que puede causar la vigilancia masiva a través del reconocimiento facial. Si bien es cierto, algunos países están tratando de regular o están en la búsqueda de un mejor enfoque de la presente tecnología de inteligencia artificial, se están afectando los derechos fundamentales de muchas personas en el mundo, más aun si esta tecnología estará presente en espacios públicos donde miles de personas tienen acceso.

La protección igualitaria garantiza el debido proceso, ya que la presente tecnología biométrica no cometería excesos, mostrando datos convincentes sobre su precisión y cumplimiento de estándares constitucionales, evitando la discriminación y el sesgo. Cabe recalcar que la clasificación de las personas establece discriminación, la imprecisión del software determina falsos positivos y la falta de transparencia determina arbitrariedades, estos aspectos no garantizan un debido proceso y tutela jurisdiccional.

Se debe establecer proporcionalidad según los fines y acorde a las leyes para el uso del reconocimiento facial en espacios públicos sin afectar el debido proceso.

Definición de términos básicos

Consentimiento:

Elemento principal, que tiene por función legitimizar la utilización por terceros de la imagen personal, tanto en el ámbito del derecho patrimonial de imagen como en el derecho de la propia imagen, ya que el consentimiento del titular del derecho es el que otorga la facultad de reproducir, difundir o modificar, así como el comercializar y explotar económicamente la imagen personal por terceras personas

Privacidad:

Protección de la esfera personal libre de la intromisión del estado, de tal manera que se preserve la tranquilidad, la autonomía, la decisión y el control de la información los cuales han de mantenerse de manera reservada.

La privacidad se considera un derecho de afuera hacia adentro siendo lo contrario de la intimidad, al otorgar consentimiento lo más probable que esté relacionado a la privacidad. Asimismo, la privacidad territorial se encuentra el espacio público el cual considera los lugares públicos.

Derechos Fundamentales.

Son libertades jurídicas que garantizan el derecho positivo, delimitados por el sistema jurídico.

Protección de datos personales:

La Ley de Protección de Datos Personales, define un dato sensible, el cual consiste en el control de los datos que faculta a decidir que datos proporcionar a un tercero, al Estado o un particular, o que datos podrá recabar, pudiendo oponerse a la posesión o uso.

Regulación legal:

La regulación está establecida en el marco de garantizar la protección de los derechos fundamentales de la persona y conforme al sistema jurídico.

Tecnología reconocimiento facial:

El reconocimiento facial es aquella tecnología que permite identificar a una persona en base a algoritmos inteligentes por medio de comparaciones dentro una base de datos de acuerdo a sus características faciales.

No se considera una tecnología similar a las cámaras de videovigilancia, ya que el sistema inteligente de reconocimiento facial permite individualizar a la persona en base a datos biométricos considerados datos de una categoría especial.

Inteligencia artificial:

La inteligencia artificial son sistemas automatizados están cada vez más presentes en la vida diaria de las personas. Ellos entienden un de técnicas de Inteligencia Artificial (IA), que, en general, buscan identificar patrones del análisis de datos a través de lógica matemática (algoritmo) y aprendizaje automático (aprendizaje automático).

Datos sensibles:

Los datos sensibles son datos reservados que caracterizan a cada individuo y forman parte de su privacidad, podrían exponer conductas discriminatorias por ello el estado protege. Un tipo de datos sensible son los biométricos que por si mismos identifican a la persona.

Efecto inhibitorio:

Describe una situación en la cual se reprime un discurso o una conducta por el temor a sufrir una penalización o represalia en los intereses de un individuo o un grupo.

Autodeterminación informativa:

Consiste en determinar quién, qué y con qué ocasión pueden conocer información de cada sujeto, garantizando control sobre sus datos, con el único fin de evitar tráfico de datos que afecte la dignidad y derechos de cada persona, es así que podríamos considerarlo como un derecho al secreto para que un tercero no conozca lo que somos o hacemos.

Interés público:

El interés público es el interés general de la comunidad, el cual no legitima cualquier tratamiento, sino que exige proporcionalidad como requisito para evitar injerencias a su privacidad. Si hubiera colisión con otros derechos se tendrían que ponderarse los intereses ya sea a través de su consentimiento o el interés público existente.

Datos Biométricos:

Los datos biométricos son aquellos que permiten 'el reconocimiento sistemático de individuos basado en sus características conductuales y biológicas'. Tienen la finalidad identificar de manera unívoca a una persona física, siendo ello un problema que puede atentar contra los derechos humanos y, el más importante, la privacidad

Los datos biométricos faciales se utilizan para distinguir a esa persona de cualquier otra persona para que pueda llevarse a cabo el proceso de análisis de correspondencia. En definitiva, los datos biométricos faciales claramente comprenden datos personales porque, per se, permiten la identificación inmediata de una persona. Los datos biométricos que son especialmente sensibles y que pueden ser vulnerados por terceros con fines ilegítimos.

Videovigilancia Publica

Los sistemas de videovigilancia son, por definición, una estructura de captación de imágenes, e incluso sonido, en un espacio concreto, cuyas imágenes puedan ser

visualizadas, grabadas y/o reproducidas, sin que pueda por sí mismo revelar la identidad de las personas.

Los tratamientos de videovigilancia regulados no incluyen los tratamientos de reconocimiento facial, que es un tratamiento radicalmente distinto al incorporar un dato biométrico.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Tipo de investigación: Básico

Cepeda (2013), define el tipo básico:

Este tipo de investigación tiene como propósito enriquecer teorías en base a conocimientos que coexisten en su tiempo y espacio, identificando cánones o patrones similares para hallar respuesta o solución a la problemática planteada. Se requiere de un análisis crítico que permita incorporar conceptos a teorías y planteadas, permitiendo un resultado óptimo, delimitado y estandarizado (p.130).

A partir de lo señalado en líneas arriba podemos decir que el presente trabajo de investigación es de tipo básico, se elaborara teoría científica del problema planteado.

Diseño de investigación:

Hermenéutica jurídica

Dueñas O. (2006), Esta investigación tendrá un diseño de hermenéutica jurídica que consiste en la interpretación de los conceptos y términos científicos que nos ayuden a analizar el problema.

Método de la investigación

Córdova, Medina, Calla y Tapia (2019), definen el método inductivo:

Lo contrario u opuesto al deductivo, y por ende marcha desde lo más particular hacia lo más general. Es decir, se emplea la observación, registro y contraste de la información, para construir premisas generales que puedan servirles de sustento o de explicación. De una parte, a un todo. (p.74).

A partir de lo señalado en líneas arriba podemos decir que la presente investigación aplicará el método inductivo, ya que tratara de analizar los fenómenos y características del problema planteado por lo tanto no existe hipótesis ni existen variables medibles.

3.2. **Categorías, Subcategorías y matriz de categorización**:

Categoría 1	**Subcategoría 1**	**Definición Conceptual**
Regulación para el tratamiento de categorías especiales de datos	Protección de datos	Legitimación para el tratamiento lícito de los datos personales
Categoría 2	**Subcategoría 1**	**Definición Conceptual**
Identificación biométrica remota en espacios públicos	Consentimiento de datos	Finalidad de uso necesidad y respeto al principio de proporcionalidad

Tabla 1: Matriz de Categorización

3.3. **Escenario de estudio**

Se tuvo como escenario al distrito judicial de Arequipa, puesto que nuestra materia de estudio es la propuesta de la regulación del Reconocimiento Facial en espacios públicos, por lo que se recolectó datos de los abogados, como conocedores del ordenamiento jurídico.

3.4. **Participantes**

Las fuentes de información se constituyen en los entrevistados como son los abogados especialistas en materia constitucional fueron seleccionados por su experiencia profesional y conocimientos respecto a procesos contenciosos y su regulación en el Perú, teniendo como entrevistados a las siguientes personas:

Nombre	Cargo / Profesión	Centro de Trabajo	Especialidad
Ronald Marco Antonio Suclla Portocarrero	Abogado	Poder Judicial	Derecho Constitucional
Fanny Zamira Diaz Barriga	Abogado	Poder Judicial	Derecho Constitucional
Nihell David Chacón Dueñas	Abogado	Poder Judicial	Derecho Constitucional

Tabla 2: Cuadro de Participantes

3.5 **Técnicas e instrumentos de recolección de datos**

Técnicas e instrumentos de recolección de información

Técnica

Según Behar (2008), define a la entrevista como:

Es una forma específica de interacción social que tiene por objeto recolectar datos de una indagación. Son las que nos conducen a la verificación del problema planteado. (p. 55).

Por tanto, la técnica a utilizar será la entrevista. En tal sentido, la entrevista está dirigido a personas especialistas en la materia y se encuentran relacionados con la problemática propuesta.

3.6 Método de análisis de información

Según Hernández (2014) “considera que, dentro de las investigaciones del tipo cualitativa, el análisis de los datos dentro de las mismas pueden ser su lado más oscuro.”… “La presente investigación se ha desarrollado con un enfoque cualitativo y con un método hermenéutico”

3.7. Aspectos éticos

Se ha ejecutado el trabajo de investigación garantizando la confiabilidad e integridad de contenido, se ha respetado los derechos de los autores para ello se utilizó el manual de normas APA.

IV. RESULTADOS Y DISCUSIÓN

Los resultados que se han generado para el objetivo general: Analizar el desarrollo de la Regulación del reconocimiento facial en espacios públicos.

La regulación del reconocimiento facial no debe surgir como una ocurrencia repentina. En realidad, se trata de un proceso de maduración. A medida que este tiene lugar es necesario sentar las bases de lo que se puede y no se puede hacer con una tecnología respecto con las normas o derechos fundamentales.

El uso del reconocimiento facial para monitorizar ciudadanos de forma masiva podría implicar evidentes peligros, al manejarse gran cantidad de datos y en el caso de una brecha de seguridad los ciudadanos podrían verse desprotegidos, por tanto, asumir que se debe buscar una regulación específica para este nuevo uso de la inteligencia artificial.

Una de las cuestiones más preocupantes en la implementación de los sistemas de reconocimiento facial es la falta de transparencia en su adquisición y funcionamiento. El potencial daño que tiene cualquier tecnología de vigilancia masiva sobre derechos humanos hace que la transparencia sea fundamental.

El reconocimiento facial es una tecnología biométrica que permite reconocer e identificar a las personas mediante sus rasgos faciales. Los datos biométricos están vinculados a nuestra identidad, ya que forma parte de quienes somos como persona, nuestras características y comportamientos. El estado actual de la tecnología de reconocimiento facial, junto con una falta de legislación específica se encuentran inadecuados para afrontar los desafíos del procesamiento biométrico, los cuales resultan obstáculos insalvables para cualquier iniciativa que pretenda respetar los derechos de los ciudadanos en la actualidad.

Un error de un sistema de vigilancia basado en video puede significar que una persona inocente es seguida, investigada e incluso arrestada y acusada de un delito que no cometió, un error de un sistema de vigilancia de escaneo facial podría ser letal.

La grabación de imágenes y su almacenamiento, unido a la aplicación de tecnologías basadas en la IA y el desarrollo de los algoritmos, podrían desvirtuar la finalidad para la que originariamente se instalaron dichos dispositivos y utilizar la información para otros fines, como análisis de audiencias, publicidad o servicios dirigidos.

El marco jurídico actual protege los datos personales a través de la Constitución Política del Perú, que prevé que los servicios informáticos, computarizados o no, públicos o privados, no suministren información que afecte la intimidad personal y familiar de las personas, la Ley 29733, Ley de Protección de Datos Personales, la cual desarrolla los derechos de los titulares de datos personales, los principios y las condiciones que se deben aplicar en su tratamiento, el Decreto Supremo 003-2013-JUS, Reglamento de la Ley de Protección de Datos Personales, el cual regula la inscripción en el Registro Nacional de Protección de Datos Personales así como el régimen sancionador ante la inobservancia de la normatividad sobre protección de datos personales.

Ante la ausencia de un marco regulador para atenuar y corregir los perjuicios que puedan causar el uso de sistemas de vigilancia “es imprescindible que los Estados limiten el uso de estas tecnologías a las que consideren legales, sometiéndolas a un riguroso control de vigilancia y autorización dentro del ámbito de los derechos humanos.

Es necesario recordar que toda injerencia a los derechos de las personas sea o no utilizando tecnología, debe estar debidamente sustentada, ser legal, necesaria y proporcional.

Los resultados que se han generado para el objetivo específico 1: Analizar el marco de la protección de datos en el desarrollo de la Regulación del reconocimiento facial en espacios públicos.

El dato biométrico es un dato sensible dirigido a identificar de una manera unívoca a una persona física, en un proceso de búsqueda de correspondencias uno-a-varios, el cual requiere mejores mecanismos de salvaguarda que actualmente la Ley no contempla, desafíos para garantizar el cuidado de los datos ante posibles prácticas discriminatorias que se podrían realizar a partir de la identificación de la persona.

La conformación de bases de datos biométricas podría suponer la vulneración de derechos fundamentales en materia de protección de datos sensibles de la ciudadanía y la dinámica de implementación impide a las personas tener conocimiento sobre la recolección, procesamiento, uso y eventual destrucción de los datos recolectados en la esfera pública.
Los datos biométricos deben ser recogidos para unos fines determinados, el principio de necesidad implica que los datos biométricos que se vayan a recabar deben ser los adecuados. y nunca excesivos, para los fines que se vayan a tratar, el principio de idoneidad y proporcionalidad hace referencia a los riesgos que puedan existir para la protección de los derechos y libertades fundamentales de las personas, por tanto, habrá que realizar un juicio de proporcionalidad entre la finalidad perseguida y el medio que pretendo utilizar.

El reconocimiento facial automático podrá estar conforme con la exigencia de proporcionalidad siempre que se trate de identificar a personas sobre las que exista razones fundadas para pensar que puedan estar en la zona afectada sobre las que haya un interés fundado, y concurran otras circunstancias vinculadas con el evento o espacio público en el que se pretenda utilizar.

Es importante que exista un texto legal de aplicación obligatoria e inmediata, que establezca los criterios para la instalación, administración y gestión del funcionamiento de los sistemas de videovigilancia, incorporando el principio de proporcionalidad y preceptos que limitan los procesos discriminatorios para el uso de la tecnología.

La Ley de Protección de Datos Personales debe ser clara en el alcance de la presente tecnología para el procesamiento de datos con fines exclusivos de seguridad pública y persecución penal, debiendo cumplir con criterios de proporcionalidad, necesidad de servir al interés público, debido proceso legal, principios generales de protección y los derechos del titular.

Los resultados que se han generado para el objetivo específico 2: Analizar el marco del consentimiento de datos en el desarrollo de la Regulación del reconocimiento facial en espacios públicos.
Los protocolos de seguridad, privacidad y confidencialidad deben garantizar la privacidad de la información de las personas, recopilada desde su captura hasta su procesamiento en lo referente a las cámaras que captan imágenes públicas. El marco jurídico peruano lo protege a través de la Ley N° 27489, vigente desde julio del 2001.

El reconocimiento facial es una especie de tratamiento de datos personales, el cual debería contar con el consentimiento del titular, a menos que exista una habilitación legal expresa. Por lo que, al tratarse de captación de imágenes para identificar a una persona, estamos ante datos biométricos no regulados, estos datos requerirán consentimiento expreso del interesado.

El establecer pautas normativas y éticas que regulen el uso de los datos personales y la inteligencia artificial, se puede garantizar la seguridad, privacidad y otros derechos fundamentales de los ciudadanos, además de proteger frente a abusos de estas tecnologías desarrolladas para empresas y poderes públicos. Por ello, esta tecnología aplicada sin la transparencia adecuada y una regulación sólida podría incurrir en una violación de los derechos humanos, como la privacidad, la protección de datos, la discriminación, la presunción de inocencia, el debido proceso, así como la propia democracia.

El uso del reconocimiento facial en los espacios públicos, al cambiar la percepción del espacio, redefine su uso, ya que las personas cambian su comportamiento

cuando saben o sospechan que están siendo observadas o vigiladas. Asimismo, esta vigilancia del espacio público pone en jaque el ejercicio de derechos fundamentales y garantías constitucionales.

Como se destaca en la introducción, los datos obtenidos en la investigación bibliográfica demuestran que es necesario la regulación de esta nueva tecnología, donde su ausencia permite, en cierto modo, una falta de respeto a los derechos fundamentales garantizados por la Constitución, es por ello que la inclusión de cualquier tipo de tecnología integrada a nuestra sociedad debe prevalecer la privacidad, protección de datos y libertades civiles desde el punto de vista jurídico, sin duda, la normatividad actual no ayuda a mantener esta protección de la persona. Estos resultados difieren con la aplicabilidad existente en algunos países del mundo y Latinoamérica como es el caso de China y Argentina. La tecnología de reconocimiento facial podría ser considerada una amenaza a las sociedades si es que no se llegara a proteger los datos biométricos de la persona. El país aún no cuenta con una legislación para promover la vigilancia estatal a través del reconocimiento facial, pero para una debida regulación se debe delinear los requisitos legales para que exista vigilancia de las personas, con límites para que el Estado invada la privacidad de las personas y donde el ciudadano conozca hasta dónde puede llegar el Estado.

V. CONCLUSIONES

Se debe tener en cuenta, que el uso de la tecnología del reconocimiento facial debe limitarse a casos específicos, la cual permita implantar medidas de seguridad necesarias, garantizando confidencialidad, integridad y resiliencia permanente a tipo de datos especiales, sobre todo por la amenaza que podría suponer el acceso de terceros afectando la privacidad de las personas y su efecto inhibitorio en espacios públicos.

El marco normativo peruano vigente resulta insuficiente, hoy en día, para permitir la utilización de técnicas de reconocimiento facial en sistemas de videovigilancia, asimismo por falta de un marco regulatorio especifico, por lo que es necesario que se apruebe una norma con rango de ley alineado a la ley de protección de datos personales.

Cualquier interferencia por parte del Estado debe estar basada en fundamentaciones sólidas, sustentadas en datos y diagnósticos serios e independientes, a fin de cumplir con las condiciones de necesidad y proporcionalidad requeridas para la legitimidad de toda medida que pretenda limitar derechos fundamentales.

La falta de cumplimiento de los requisitos comunes para la protección de datos personales y la excepcionalidad prevista en las leyes y en la directiva de videovigilancia, la práctica de la monitorización a gran escala por cámaras, especialmente con un sistema de reconocimiento facial, no encuentra límites en la legislación peruana cuando se contraponen valores como la protección de la seguridad y la seguridad pública, por un lado, y la privacidad, protección de datos y libertades civiles, por otro.

VI. RECOMENDACIONES

Se debe pretender implementar un marco jurídico que permita garantizar el tratamiento de los datos biométricos de forma adecuada por parte del Estado. Ante abusos o filtraciones de datos biométricos, el Estado debe tener previsto una autoridad competente para velar por la protección de los derechos de las personas.

Establecer normas jurídicas, estándares técnicos y directrices éticas necesarias para proteger los derechos fundamentales, cumpliendo con sus obligaciones legales antes de la implementación de la tecnología de reconocimiento facial.

Proponer la realización de evaluaciones de impacto e invoque el principio precautorio hasta tanto no se corrobore la necesidad y proporcionalidad de la medida adoptada.

La regulación no solo debe autorizar el uso de la tecnología de reconocimiento facial para la seguridad pública como una excepción general, sino que esta debiera permitir específicamente el uso del reconocimiento facial a gran escala y en los ambientes más diversos.

La base normativa debiera establecer el procedimiento de cómo deben operar la tecnología de reconocimiento facial, qué niveles de transparencia y responsabilidad deben respetar, qué tasas de falsos positivos y falsos negativos son tolerables, en qué situaciones, cuál es el procedimiento para la auditoría periódica independiente de estas tasas, entre otros.

La regulación debiera prestar atención de los daños a la libertad de expresión y asociación y centrarse en las garantías de protección de datos, de tal manera que pueda enfrentar los problemas de seguridad, y que la legislación tenga disposiciones expresas sobre transparencia, supervisión y control del

funcionamiento de las herramientas de reconocimiento facial para prevenir el abuso.

La discusión sobre la aplicación de esta tecnología debiera ir acompañada de inquietudes éticas relacionados con posibles procesos discriminatorios y estratificación del espacio público que pudieran derivarse de su instalación.

Para considerar el principio de proporcionalidad, se sugiere que se realicen estudios previos sobre los impactos de la implementación de sistemas de videovigilancia en la configuración del espacio público.

REFERENCIAS

Abad, S. (2017). El proceso constitucional de amparo (3a ed.). Lima: Gaceta Jurídica.

Agencia Española de Protección de Datos. (s.f.). Guía sobre el uso de videocámaras para seguridad y otras finalidades. Recuperado de: https://www.aepd.es/media/guias/guia-videovigilancia.pdf

Barona, S. (2019). Inteligencia Artificial o la algoritmización de la vida y de la justicia: ¿Solución o problema?. Bolivia: Revista Boliviana de Derecho, 28, 18-49.

Bel, I. (2013). Derecho a la intimidad personal, uso de cámaras ocultas y otras amenazas a los derechos personales. En L. Corredoira & A. Cotino (Eds.), Libertad de expresión e información en Internet (pp. 375-393). Madrid: Centro de Estudios Políticos y Constitucionales.

Bernal, C. (2014). El principio de proporcionalidad y los derechos fundamentales (4a ed.). Bogotá: Universidad Externado de Colombia.

Cavero, E. (2012). El right of publicity y los derechos sobre la imagen y reputación de las celebridades en la industria del entretenimiento. Ius et Veritas, 22(44), 212-223.

Chavez, J. (2019). Brace yourselves! La Videovigilancia ya viene: situación de la videovigilancia en el ordenamiento jurídico peruano. Perú. Derecho PUCP, n. 83, 2019, p. 133-178.

Christopher Hood et al, 'Risk Management' in The Royal Society (ed), Risk: Analysis, Perception and Management - A Report of a Royal Society Study Group (The Royal Society 1992).

Cotino, L. (2017). Big Data e Inteligencia Artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales. Dilemata, 24, 131-150.

De Hert Paul and Vagelis Papakonstantinou, “The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?” Computer Law and Security Review [2016] 32 (2) 179–94.Available at http://daneshyari.com/article/preview/466369.pdf -last accessed 3 of September 2017.

En B. Aláez (Ed.), Conflictos de derechos fundamentales en el espacio público (pp. 37-69). Madrid: Marcial Pons.

Gellert R.,'We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection' [2016] 4(2) European Data Protection Law Review (EDPL) 481-492. Available at https://www.researchgate.net/publication/312652929_We_Have_Always_Managed_Risks_in_Data_Protection_Law_Understanding_the_Similarities_and_Differences_Between_the_Rights-Based_and_the_Risk-Based_Approaches_to_Data_Protection - last accessed 10 of July 2017.

Gil, C. (2019). Videovigilancia y protección de datos. Especial referencia a la grabación de la vía pública desde el espacio privado. Madrid: Wolters Reuters.

Gonzaíni, O. (2011). Derecho procesal constitucional: habeas data. Protección de datos personales. Santa Fe: Rubinzal-Culzoni.

Goñi, J. (2007). La videovigilancia empresarial y la protección de datos personales. Madrid: Civitas.

Grenoble, R. (12 de diciembre de 2017). Welcome to the Surveillance State: China's AI Cameras See All. HuffPost. Recuperado de https://www.huffpost.com/entry/china-surveillance-camera-big-brother_n_5a2ff4dfe4b01598ac484acc

Guastini, R. (2016). Lecciones de derecho constitucional. Lima: Legales.

Hakansson, C. (2019). Curso de derecho constitucional (3a ed.). Lima: Palestra.

Iglesia, A. de la (2017). Videovigilancia, espacio público y derechos fundamentales.

Kokott Juliane and Christoph Sobotta, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law, Vol. 3, No. 4 (2013). Available at http://oxfordindex.oup.com/view/10.1093/idpl/ipt017 -last accessed 23 of August 2017.

Kuner Cristopher and others , Risk management in data protection, International Data Privacy Law, Vol. 5, No. 2, (2015), 95. Available at https://academic.oup.com/idpl/article/5/2/95/645238/Risk-management-in-data-protection -last accessed 23 of August 2015.

León, L. (2007). El problema jurídico de la manipulación de información personal.Lima: Palestra.

Marciani, B. (2004). El derecho a la libertad de expresión y la tesis de los derechos preferentes. Lima: Palestra.

Mendoza, M. (2007). Conflictos entre derechos fundamentales: expresión, información y honor. Lima: Palestra.

Rosado, G. (2004). La titularidad de derechos fundamentales por la persona jurídica. Valencia: Tirant lo Blanch.

Sagüés, N. (2017). Derecho constitucional (Vol. 3). Buenos Aires: Astrea.

Salomé, L. (2011). La doble dimensión de los procesos constitucionales de libertad. En autores varios, Derecho procesal constitucional (pp. 11-43). Lima: Palestra.

Zambrano, A. (2019). Cámaras de videovigilancia: ¿Nos cuidan o nos vigilan?. Brasil: IPANDETEC.

ANEXOS

MATRIZ DE CONSISTENCIA

Regulación del uso del Reconocimiento Facial en espacios públicos

Problemas	Objetivos	Supuesto	Categorías	Metodología
Problema general ¿Cómo se desarrolla la Regulación del reconocimiento facial en espacios públicos? **Problema específico** -¿En el marco de la protección de datos cómo se desarrolla la Regulación del reconocimiento facial en espacios públicos? -¿En el marco del consentimiento de datos cómo se desarrolla la Regulación del reconocimiento facial en espacios públicos?	**Objetivo general** Analizar el desarrollo de la Regulación del reconocimiento facial en espacios públicos. **Objetivo específico** -Analizar el marco de la protección de datos en el desarrollo de la Regulación del reconocimiento facial en espacios públicos -Analizar el marco del consentimiento de datos en el desarrollo de la Regulación del reconocimiento facial en espacios públicos.	Es importante Analizar el desarrollo de la Regulación del reconocimiento facial en espacios públicos.	**Categoría 1** Regulación para el tratamiento de categorías especiales de datos **Subcategoría 1** -Protección de datos **Categoría 2** Identificación biométrica en espacios públicos **Subcategoría 1** - Consentimiento de datos	Enfoque: cualitativo Tipo: Básico Método: Inductivo Diseño: Hermenéutica jurídica Nivel: explicativo Población: abogados de Arequipa Muestra: 3 especialistas Técnica: entrevista Instrumento: Guía de entrevista con preguntas abiertas

Tabla 3: Matriz de Consistencia

Instrumento: Guía de entrevistas

Título: Regulación del uso del Reconocimiento Facial en espacios públicos

Objetivo general:

Analizar el desarrollo de la Regulación del reconocimiento facial en espacios públicos

Problema General:

¿Qué entiende Ud. por regulación y en que se fundamenta?

¿Qué entiende Ud. por tecnologías de reconocimiento facial, considera que es necesaria su implementación para el control de seguridad ciudadana?

¿De qué manera las políticas públicas en el marco jurídico peruano actual brindan protección a los datos personales?

¿Cuáles son los riesgos del uso de tecnologías de reconocimiento facial para el control y seguimiento masivo de personas?

¿Qué requisitos legales debe cumplir la implementación de tecnologías de reconocimiento facial en espacios públicos?

OBJETIVO ESPECÍFICO 1:

Analizar el marco de la protección de datos en el desarrollo de la Regulación del reconocimiento facial en espacios públicos.

PROBLEMA ESPECÍFICO 1

¿En qué se diferencian los datos sensibles de los datos biométricos?

¿Cree Ud. que la implementación de tecnologías de reconocimiento facial debe cumplir con el principio de proporcionalidad y necesidad?

¿Considera Ud. que el incumplimiento de los requisitos de la protección de datos origina la vulneración de datos sensibles por el uso de tecnologías de reconocimiento facial?

¿Qué obligaciones debe tener el titular y el encargado del tratamiento de datos personales frente al uso de las tecnologías de reconocimiento facial?

OBJETIVO ESPECÍFICO 2:

Analizar el marco del consentimiento de datos en el desarrollo de la Regulación del reconocimiento facial en espacios públicos.

PROBLEMA ESPECÍFICO 2

¿De qué manera las políticas públicas en el marco jurídico peruano actual protegen la confidencialidad de los datos personales?

¿Cree Ud. que la regulación jurídica respecto a la biometría facial debe exigir un consentimiento explícito?

Desde su punto de vista, ¿considera Ud. que es posible tener derecho a la privacidad en un lugar público?