Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

VULNERACIÓN DE LA PRIVACIDAD DE DATOS PERSONALES POR EMPLEO DE LA CÁMARA DE RECONOCIMIENTO FACIAL

Línea de investigación:

Procesos jurídicos y resolución de conflictos

Tesis para optar el grado académico de Doctora en Derecho

Autora:

Reyes Trujillo, Felicinda

Asesor:

Guardia Huamani, Efraín Jaime

(ORCID:0000-0002-7715-2366)

Jurado:

Jiménez Herrera, Juan Carlos

Gonzales Loli, Martha Sofia

Vigil Farías, José

Lima - Perú

2023

Reporte de Análisis de Similitud

Archivo:	1A_REYES_TRUJILLO_FELICINDA_DOCTORADO_2023.docx
Fecha del Análisis:	24/02/2023
Analizado por:	Astete Llerena, Johnny Tomas
Correo del analista:	jastete@unfv.edu.pe
Porcentaje:	7 %
Título:	"VULNERACIÓN DE LA PRIVACIDAD DE DATOS PERSONALES POR EMPLEO DE LA CÁMARA DE RECONOCIMIENTO FACIAL"
Enlace:	https://secure.urkund.com/old/view/152218358-684306-148384#FYY7DsJAEMXusrWF5rezk1wFUaAIUArSpETcnUXy8/Onvc+2XlVQndic87/pQDua6EALXTBMMMVmBJY4Lrjihnd84EUQQhgxoxNFd5IUUslBLhSV1LjRzv117M99ux/bo61ykfT06KFhVktpfn8=

UNIVERSIDAD NACIONAL FEDERICO VILLARREAL
OFICINA DE GRADOS Y GESTIÓN DEL EGRESADO
ESCUELA UNIVERSITARIA DE POSGRADO

DRA. MIRIAM LILIANA FLORES CORONADO
JEFA DE GRADOS Y GESTIÓN DEL EGRESADO

Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

VULNERACIÓN DE LA PRIVACIDAD DE DATOS PERSONALES POR EMPLEO DE LA CÁMARA DE RECONOCIMIENTO FACIAL

Línea de investigación:
Procesos jurídicos y resolución de conflictos

Tesis para optar el grado académico de Doctora en Derecho

Autor:
Reyes Trujillo, Felicinda

Asesor:
Guardia Huamani, Efraín Jaime
(ORCID:0000-0002-7715-2366)

Jurado:

Jiménez Herrera, Juan Carlos

Gonzales Loli, Martha Sofia

Vigil Farías, José

Lima- Perú

2023

DEDICATORIA:

Ofrezco esta investigación al Altísimo

Por guiar mis pasos por sendas

Seguras y no dejarme desfallecer

Ante las dificultades.

A mi familia por su comprensión

Y apoyo incondicional.

REYES TRUJILLO FELICINDA

AGRADECIMIENTO:

Mi especial agradecimiento a los miembros del jurado:

Jiménez Herrera, Juan Carlos
Gonzales Loli, Martha Sofia
Vigil Farías, José

Asimismo, mi agradecimiento para mi asesor:

Guardia Huamaní, Efraín Jaime

Por su incalculable colaboración
Y oportunas recomendaciones.

REYES TRUJILLO FELICINDA

Índice

Índice de tablas

Índice de figuras

Resumen

Objetivo: Exponer los motivos por los que el empleo de la cámara de reconocimiento facial vulnera la privacidad de los datos personales. **Metodología**: tipo de investigación básico, nivel: explicativo, diseño: no experimental- transaccional. Población 50 y muestra 44 sujetos. Instrumento aplicado cuestionario, procedimientos: exegético, histórico y sistemático análisis de datos: programa SPSS, organizados en tablas y gráficos. **Resultados**: de los sujetos encuestados: el 88% estuvo de acuerdo con que el empleo de la cámara de reconocimiento facial vulnera la privacidad de los datos personales a través del consentimiento otorgado por el titular para su rostro captado por la cámara sea tratado y, por la falta de regulación de su empleo; el 87% concordó con que el consentimiento del titular para que su rostro captado por la cámara de reconocimiento facial sea tratado. vulnera la privacidad de los datos personales al permitir el acceso a los datos en todos los ámbitos de la vida de la persona; y, el el 89% estuvo de acuerdo con que la falta de regulación del empleo de la cámara de reconocimiento facial vulnera la privacidad de los datos personales, porque no están autorizadas para captar, tratar y trasferir las imágenes del rostro de la persona o usuario.

Palabras claves: derecho a la privacidad, derecho a la protección de datos personales, inteligencia artificial, cámaras de reconocimiento facial.

Abstract

Objective: to expose the reasons why the use of the facial recognition camera violates the privacy of personal data. **Methodology:** basic type of research, level: explanatory, design: non-experimental-transactional. Population 50 and sample 44 subjects. Instrument applied questionnaire. Procedures: exegetical, historical and systematic Data analysis: SPSS program, organized in tables and graphs. **Results:** of the subjects surveyed: 88% agreed that the use of the facial recognition camera violates the privacy of personal data through the consent granted by the owner for their face captured by the camera to be processed and, therefore, the lack of regulation of their employment; 87% agreed that the holder's consent for his face captured by the facial recognition camera to be processed. violates the privacy of personal data by allowing access to data in all areas of the person's life; and, 89% agreed that the lack of regulation of the use of the facial recognition camera violates the privacy of personal data, because they are not authorized to capture, process and transfer the images of the person's or user's face.

***Keywords**:* right to privacy, right to personal data protection, artificial intelligence, facial recognition cameras.

Sommario

Obiettivo: esporre i motivi per cui l'uso della telecamera per il riconoscimento facciale viola la privacy dei dati personali. **Metodología**: ricerca di tipo base, livello: esplicativo, disegno: non sperimentale-transazionale. Popolazione 50 e campione 44 soggetti. Questionario applicato allo strumento. Procedure: esegetiche, storiche e sistematiche Analisi dei dati: Programma SPSS, organizzato in tabelle e grafici. **Risultati**: dei soggetti intervistati: l'88% ha convenuto che l'utilizzo della telecamera per il riconoscimento facciale viola la privacy dei dati personali attraverso il consenso concesso dal titolare al trattamento del proprio volto ripreso dalla telecamera e, quindi, la mancata regolamentazione dei il loro impiego; L'87% ha concordato che il consenso del titolare per il suo volto catturato dalla telecamera di riconoscimento facciale venga elaborato. viola la privacy dei dati personali consentendo l'accesso ai dati in tutte le aree della vita della persona; e, l'89% ha convenuto che la mancanza di regolamentazione dell'uso della fotocamera per il riconoscimento facciale viola la privacy dei dati personali, perché non sono autorizzati a catturare, elaborare e trasferire le immagini del volto della persona o dell'utente.

***Parole chiave*:** diritto alla privacy, diritto alla protezione dei dati personali, intelligenza artificiale, telecamere per il riconoscimento facciale.

I. Introducción

A pesar de que el desarrollo tecnológico contribuye significativamente al desarrollo de la vida del hombre, existen situaciones en las que, simultáneamente, resulta perjudicial, tal es el caso de las cámaras de reconocimiento facial empleadas para coadyuvar con la seguridad ciudadana y para brindar seguridad al momento de realizar actividades financieras o de presentar exámenes virtuales, entre otros; dado que, vulneran los derechos fundamentales de los usuarios entre ellos el de la privacidad de los datos personales, tal como se analizó en esta investigación conformada por nueve secciones discriminadas así:

I. Introducción: En esta sección se aborda la problemática a examinar, se reseñan los antecedentes del estudio, se presentan los objetivos a alcanzar en la investigación y se formulan la hipótesis, como solución tentativa de la problemática.

II. Marco teórico: Esta sección incluye el sustento científico y legal de la investigación.

III. Método: Esta sección comprende los aspectos metodológicos de la investigación.

IV. Resultados. Esta sección contiene la presentación de los resultados alcanzados al desarrollar la investigación.

V. Discusión de resultados. En esta sección se confrontan los resultados alcanzados con los antecedentes y con los postulados teóricos considerados en la investigación.

VI. Conclusiones: En esta sección se presentan las deducciones realizadas por la investigadora al culminar su labor investigativa.

VII. Recomendaciones: En esta sección se formulan propuestas para remediar la problemática de vulneración de la privacidad de datos personales que entraña el empleo de las cámaras de reconocimiento facial.

VIII. Referencias. Contiene las propuestas de la investigadora para superar la problemática estudiada.

IX. Anexos. Documentos en los que se sustentó el estudio.

1.1. Planteamiento del problema

Es innegable la contribución que el desarrollo tecnológico tiene en la vida del hombre, dado que, ella se ha orientado a través de la historia a hacerla más sencilla, además que ha contribuido a restaurar la salud cuando ha sido atacada por enfermedades, no de otra manera se puede entender el invento: del teléfono por parte de Antonio Meucci, en 1854; el celular inventado por Martin Cooper creando el Motorola DynaTAC 8000X en 1973; de la computadora en 1941 por parte de Konrad Zuse; del automóvil por Karl Benz, en 1886; el marca pasos por Rune Elmqvist, la ecografía por Langevin y Chilowsky, la resonancia electromagnética nuclear por Raymond Vahan Damadian etc., etc., a partir de los cuales, por ejemplo, la comunicación a cualquier parte del mundo se hizo cada vez más sencilla, así como el acceso a la información de cualquier tipo o se facilitó la detección y tratamiento de las enfermedades.

No obstante, en ocasiones a esos inventos o avances tecnológicos, llegan a ser perjudiciales para las personas, tal como acontece con: i) el uso excesivo del celular que puede producir dolores articulares, insomnio, así como afectar su privacidad y el uso indebido de los datos personales al publicar 24X7 todas sus actividades; y, ii) su empleo para defensa de los Estados contra agresiones externas, o contra la inseguridad interna, sin tener en consideración el grado de afectación o violación de los derechos fundamentales reconocidos a las personas por el ordenamiento jurídico nacional y los instrumentos internacionales, como ocurre con los sistemas de identificación biométricos que, a través de las huellas digitales, la voz o el rostro de una persona, entre otros; valiéndose de un software por medio de un proceso técnico obtienen datos que convertidos a un formato digital, posibilitan la identificación de una persona.

Estos datos, desde la óptica jurídica se adscriben en la categoría del derecho fundamental a datos personales que por estar vinculados a la privacidad de la persona son objeto de protección reforzada por parte del Estado.

1.2. Descripción del problema

En la actualidad una de las formas de identificación biométrica que más polémica ha despertado es el sistema de identificación facial, coloquialmente conocido como cámara de identificación facial; a través del cual, como su nombre lo indica, se logra que el sistema identifique los rasgos de un rostro captado por fotografía o en tiempo real a través de algoritmos matemáticos, comparándola con imágenes previamente archivadas.

En nuestro país, al igual que en otros países, esta técnica es utilizada para desbloquear celulares, como sistema de seguridad para acceder a la App y validar operaciones bancarias, como ocurre con el BBVA y para la seguridad ciudadana, tal como lo ha propuesto el distrito de La Victoria el cual desde inicios del mes de abril de dos mil diecinueve instaló nueve cámaras de reconocimiento facial en las puertas de acceso gamarra. (Andina, 2019), así como los distritos de Miraflores, San Martin de Porres y las Universidades Mayor de San Marcos y Federico Villarreal, para sus exámenes de ingreso virtuales del año 2021.

Las personas del común que emplean esta tecnología, lejos están de comprender que ésta atenta contra de su derecho a la intimidad, en el que, para el caso peruano, se comprende el derecho a la protección de las imágenes propias. (Constitución Política del Perú, Art. 2.7, 1993), sino que, por el contrario, se sienten orgullosos de emplear esa tecnología pues a su juicio, es demostrativa de estar a la vanguardia tecnología, y en el caso de Gamarra se pretendió usar con el argumento de contribuir con la seguridad ciudadana al permitir la identificación de personas que se encuentren delinquiendo o que cuenten con requisitoria vigente, no obstante, en el 2022, tras una denuncia cuidada ante la Autoridad Nacional de Protección de Datos

Personales, se conoció que estas no se habían entrado en funcionamiento al carecer de convenio con la Policía Nacional. (Villena, 2022).

No obstante, como ya se ha anticipado, el uso de estos mecanismos, atendiendo a la poca confiabilidad que ofrecen pues la identificación del rostro depende entre otros: de la iluminación y posición del rostro por identificar, así como al empleo de maquillaje, las enfermedades en la piel, etc., pueden llevar a falsos positivos y falsos negativos debido a lo cual su empleo se ha prohibido en EEUU: San Francisco, Somerville, Oakland, California; Brasil, Argentina, etc. pues, no se trata solo de almacenar el rostro del cliente, usuario o transeúnte en la base de datos de la empresa o institución que instaló el dispositivo sino que, esta información es empleada para compararla con otros rostros disponibles en bases de datos.

En el caso de nuestro país, si bien existe una Legislación de protección de datos personales, Ley N° 29733 (2011), y su Reglamento Decreto Supremo Nº 003-2013-JUS (2013); el empleo de del sistemas biométricos para el reconocimiento facial no ha sido normado, y la autoridad de protección de datos tampoco se ha pronunciado sobre el particular, aunque en la práctica como se mencionó se utiliza, circunstancia que origino la realización de esta investigación con el propósito de analizar de qué manera las cámaras de reconocimiento facial vulnera el derecho a la protección de datos de las personas.

1.3. Formulación del problema

1.3.1. Problema general

¿Cuáles son los motivos por los que el empleo de la cámara de reconocimiento facial vulnera de la privacidad de los datos personales?

1.3.2. Problemas específicos

¿Por qué motivo el consentimiento del titular para que el rostro captado por la cámara de reconocimiento facial sea tratado vulnera de la privacidad de los datos personales?

¿Por qué causa la falta de regulación del empleo de la cámara de reconocimiento facial vulnera de la privacidad de los datos personales?

1.4. Antecedentes

1.4.1. Antecedentes internacionales

El artículo de Simón y Dorado (2022), titulado Límites y garantías constitucionales frente a la identificación biométrica. Luego de analizar la actuación de Agencia española de protección de datos, la legislación europea y la jurisprudencia concluyeron que los métodos de detección biométrica, particularmente de captura de "imagen que funcionen con algoritmos de identificación de personas naturales". (p. 11), que hacen parte de un banco de datos, constituyen un procesamiento de datos con rango especial, por lo que su empleo a futuro debe sobrepasar un riguroso juicio de constitucionalidad.

Este juicio se expresa: i) desde la óptica del individuo, se requiere que al encargado del procesamiento de datos se le deben haber asignado explícitamente y legalmente las facultades oficiales en esta esfera; así como, el interés público alegado debe ser reconocido por ley; y, ii) desde el enfoque material o del objeto, que constituye la cuestión analizada en el juicio de proporcionalidad, se debe resolver analizando "la idoneidad, necesidad y proporcionalidad estricta respetando el núcleo material del derecho fundamental en cuestión". (Simón y Dorado, 2022, p. 11).

La investigación titulada: Los sistemas de reconocimiento facial: una mirada a la luz del examen de proporcionalidad, en la que el investigador luego de realizar un juicio de proporcionalidad entre el empleo de esta técnica, con relación a la afectación de derechos fundamentales como: la presunción de inocencia, el derecho a la igualdad y no discriminación y el fin mayoritariamente perseguido con su implementación, la seguridad pública, concluyó que:

A consecuencia de lo investigado, no resulta extraño que esta técnica se haya prohibido, aun cuando, parcial y aisladamente. En su examen cobra mayor peso, la violación de los derechos fundamentales, la cual es irreparable y que puede abrir un portal cuya clausura con el tiempo no será sencilla. (Simón y Dorado, 2022).

No obstante, este el momento para reconsiderar sí efectivamente vale la pena otorgar a esta técnica un papel esencial en la comunidad, pese a los beneficios que produce en ciertos ámbitos. En esta investigación, se han analizado los inconvenientes que acarrea su uso en el ámbito público. Si los Estados optan por continuar aplicándola, se le debe proveer de una protección más estricta. De otro modo, se saldrá de control produciendo más inconvenientes que beneficios.

La investigación titulada: Reconocimiento facial en América Latina: tendencias en la implementación de una tecnología perversa; en la que, luego de analizar la implementación de la tecnología de reconocimiento facial, de manera general se concluyó que: "el reconocimiento facial no nos protege, nos vulnera". (Venturini y Garay, 2021, p. 20). Varios Estados han comenzado a prohibir o diferir la instalación de esta tecnología y compañías que desarrollan este software han limitado su comercialización en ciertos casos es así como IBM, Microsoft y Amazon lo han hecho por problemas de racismos en EEUU en 2020. Estas medidas son apoyadas por expertos (as) atendiendo su incidencia en los derechos humanos.

En concreto respecto al derecho a la protección de los datos personales, se concluyó que esta clase de tecnología supone la violación del "derecho a la privacidad y, de manera asociada, al derecho a la protección de datos personales". (Venturini y Garay, 2021, p. 21).

La investigación titulada: Tecnología de reconocimiento facial en Colombia: un análisis regulatorio en relación con la protección de los datos personales en el sector privado en la que se concluyó que esta técnica es el prototipo de la "tecnología blanda y flexible" cuya operatividad se fundamenta en la información biométrica, los que a la vez son tratados por

métodos algorítmicos que posibilitan la identificación de la persona. Esta técnica se puede emplear en multitud de ámbitos, verbi gratia en la comprobación de la identidad en operaciones financieras, o ayuda a discapacitados, etc. De ahí que, la regulación de esta metodología es trascendente, debido al peligro que supone para los usuarios son considerables, en vista no solo de los imple que es obtener los datos, sino, igualmente la contingencia de que se dé un ilícito procesamiento de la información, dado que no son técnicas totalmente eficientes y "poseen altos márgenes de error". (Camelo, 2021).

1.4.2. Antecedentes nacionales

En nuestro país, se han realizado investigaciones sobre las cámaras de reconocimiento facial, pero a nivel de pregrado y especialmente de la ingeniería de sistemas que nos permiten conocer el funcionamiento técnico de esta técnica, pero que no constituyen antecedentes de la investigación. Los únicos referentes que se pueden citar son:

El artículo titulado: Cámaras con reconocimiento facial en Lima, en el que luego de analizarse el anuncio de los distritos de Miraflores, San Martin de Porres y La Victoria, sobre la implementación de cámaras de seguridad, se analizó la problemática que su funcionamiento entrañaría, al: i) crear un peligro para la privacidad y tratamiento de datos personales de quienes transitan por los calles y sitios públicos; ii) todo individuo captado por la cámara se trasforma en sospecho al ser comparado y vigilado permanentemente, se puede conocer su identidad "se pierde el anonimato". (Arroyo, 2019); iii) al posibilitar la clasificación de las personas puede derivar en discriminación; iv) la falta de precisión de esta técnica lo que lleva a "gran cantidad de resultados falsos positivos". (Arroyo, 2019); v) no hay información disponible sobre la adquisición de los equipos; y, vi) la inexistencia de protocolos para reducir los peligros que supone afecta el debido proceso. (Arroyo, 2019).

De la misma forma se advierte que, toda intromisión en los derechos fundamentales, a través de la tecnología o no debe estar debidamente fundamentada, además de licita, necesaria y proporcional. (Arroyo, 2019).

El articulo signado como: Denunciamos a la Universidad Nacional Mayor de San Marcos por el uso de software biométrico en su examen virtual, la denuncia se fundamenta en el empleo del programa de reconocimiento facial software SMOWL basados en datos biométricos, para cuidar en tiempo real a los postulantes a la universidad periodo 2020-II, para evitar el fraude y la suplantación y no proporcionar información de la manera como se tratarán los datos sensibles que almacenará el software, es decir las fotografías que el sistema toma de forma continua y que luego proporciona a la Universidad para que examinen los comportamientos evaluadas como "sospechosas" con fundamento en las cuales se puede o no anular el examen. (Guerrero, 2020).

1.5. Justificación de la investigación

1.5.1. Justificación teórica

El sustento teórico de la investigación se sustenta en el hecho de proveer argumentos constitucionales, legales, y doctrinales para demostrar la forma como el empleo de la cámara de reconocimiento facial vulnera la privacidad de los datos personales.

1.5.2. Justificación metodológica

La fundamentación metodológica de la investigación reside en que producto de la metodología aplicada por la investigadora, de proporcionaran datos demostrativos de los motivos por los que el empleo de la cámara de reconocimiento facial vulnera de la privacidad de los datos personales; lo que permitirá ampliar el conocimiento que se tiene sobre la materia.

1.5.3. Justificación práctica

Desde el punto de vista práctico esta investigación reside en emprender la discusión en torno a la problemática que implica el empleo de la cámara de reconocimiento facial para vulneración de la privacidad de los datos personales, de manera que el derecho se adecue al desarrollo tecnológico.

1.6. Limitaciones de la investigación

La principal limitación que se presentó para la ejecución de esta investigación consistió en la confusión entre las cámaras de video vigilancia y de reconocimiento facial que tienen las personas, sin embargo, esta limitante se superó.

1.7. Objetivos

1.7.1. Objetivo general

Exponer los motivos por los que el empleo de la cámara de reconocimiento facial vulnera la privacidad de los datos personales

1.7.2. Objetivos específicos

Explicar el motivo por el que el consentimiento del titular para que el rostro captado por la cámara de reconocimiento facial sea tratado vulnera de la privacidad de los datos personales

Indicar el motivo por el cual la falta de regulación del empleo de la cámara de reconocimiento facial vulnera de la privacidad de los datos personales.

1.8. Hipótesis

1.8.1. Hipótesis general

El empleo de la cámara de reconocimiento facial vulnera la privacidad de los datos personales a través del consentimiento otorgado por el titular para que el rostro captado por la cámara sea tratado y, por la falta de regulación de su empleo.

1.8.2. Hipótesis específicas

El consentimiento del titular para que su rostro captado por la cámara de reconocimiento facial sea tratado vulnera la privacidad de los datos personales, al permitir el acceso a los datos en todos los ámbitos de la vida de la persona.

La falta de regulación del empleo de la cámara de reconocimiento facial vulnera la privacidad de los datos personales, porque no están autorizadas para tratar captar, tratar y trasferir las imágenes del rostro de la persona.

II. Marco teórico

2.1. Marco conceptual

2.1.1. Conceptos relacionados con privacidad de datos personales

Banco de DadPe. Cumulo de información personal de infinidad de usuarios, estructurado, automatizado o no, sin consideración a que su suporte sean material, magnético, informático, visual o se hayan constituido, conservado, estructurado o sean accesibles de cualquiera otra manera.

Derechos ARCO: acróstico de las facultades reconocidas legalmente a los titulares de DadPe para que en el momento en que lo consideren conveniente soliciten, al titular del banco de datos personales o al responsable de su tratamiento, se le permita acceder a ellos, se rectifiquen, corrijan o su oposición al procesamiento. Si su requerimiento no es atendido puede acudir a la autoridad nacional de protección de datos personales o iniciar una acción judicial, en la que puede optar por una indemnización.

Encargado de tratamiento de DadPe. Persona natural o de derecho que independientemente o colectivamente, que por convenio con del titular de la base de datos, en el que se precisa el contexto de su labor; trata o procesa los datos personales.

Titular de DadPe: persona natural a la que pertenece la información procesada o tratada por el banco de datos o el encargado.

Tratamiento DadPe. Toda acción o proceso especializado, automático o no, que posibilita la recolección, inscripción, organización, acopio, preservación, creación, reforma, supresión, acceso, empleo, bloqueo, eliminación, notificación de trasferencia o divulgación "o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales". (D. S. Nº 003-2013-JUS, Art. 2.19, 2013).

2.1.2. Conceptos relacionados con empleo de cámara de reconocimiento facial

Consentimiento para tratamiento del rostro: manifestación de la voluntad inequívoca, expresa, previa e informada del titular para que los rasgos de su rostro sean procesados o incorporados a bancos o bases de datos.

Falso negativo o falso rechazo. El sistema no identifica a una persona pese a que sus datos biométricos están almacenados en los bancos de datos.

Falso positivo o falsa aceptación. El sistema de reconocimiento facial hace una identificación equivocada.

Huella facial. Imagen digital de la cara del individuo, se emplea para confrontarla con la información archivada en los bancos de datos o para identificar a un determinado individuo.

Identificación biométrica: individualización de una persona a partir de las medidas del cuerpo, en el caso de reconocimiento facial del rostro: como longitud de la nariz, distancia entre los ojos, etc. y de la cabeza.

Imagen de consulta: rostro del individuo captada por la cámara, es la que emplea para realizar la huella facial.

Verdadero positivo. El sistema realiza un reconocimiento que concuerda con los datos biométricos están almacenados en los bancos de datos.

2.2. Bases teóricas de la investigación

2.2.1. Derecho a la privacidad

En la noción de privacidad, como precisan Bennett y Raab (2003) se incorporan los valores que la persona y la comunidad le atribuyen, lo que conlleva a que pueda ser concebida desde diferentes aristas: “como un reclamo, un derecho, un interés, un valor, una preferencia o simplemente un “estado de existencia”. (Nissenbaum, 2009, p. 3), debido a lo cual, las nociones resultan parciales o imprecisas. No obstante, aun cuando no hay un criterio generalizado respecto a la noción de privacidad, lo cierto es que, por ser un ingrediente de la dignidad de la

persona debe ser tutelada legalmente como el derecho que le asiste al individuo para sustraer su vida privada del conocimiento público.

Como explica Corral (2000), solo hasta fines del siglo XIX la vida privada empezó a ser protegida por la normatividad anglosajona. Hasta esta época, cualquier intromisión en la vida privada, atendiendo que, conforme a los postulados del liberalismo, la propiedad constituía la piedra angular de todos los derechos; se concebían como intromisiones ilícitas en el territorio privado. De manera que, para obtener una tutela legal de la privacidad era suficiente invocar la violación al derecho de la propiedad, a través de cualquiera de los mecanismos jurídicos existentes, debido a lo cual, la defensa de la privacidad o vida íntima emergía como la salvaguarda del área geográfica sobre la que recae la propiedad.

Este modelo se trasformó con la conceptualización del derecho a la privacidad (en adelante Do. Pri.) en la literatura norteamericana a fines del S. XIX, por Warren y Brandeis (1890) con la finalidad de defender al individuo de las creaciones tecnológicas, para la época representadas por las fotografías instantáneas, dado que, producto de la propagación realizada por los medios de comunicación escritos, habían irrumpido en el aspecto más inviolable de la vida privada y personal. Los investigadores comprendieron que a las personas les asiste el Do. Pri., concibiéndolo como "*the right to be let alone* (el derecho a no ser molestado)". (García, 2013, p. 1045), como un derecho diferente a los existentes, orientado, se reitera; a la defensa de los individuos contra las violaciones a su vida privada. (Corral, 2000).

El crédito asignado por la doctrina a Warren y Brandeis (1890) se fundamenta en sus apotres: i) haber precisado los elementos del Do. Pri.; y, ii) formularlo como un derecho de índole abierta y de naturaleza fundamental cambio su sustento del derecho a la propiedad "a la inviolabilidad y dignidad del ser humano, es decir, al ámbito del derecho a la personalidad". (p. 74).

Posteriormente, en la década del 70 *Westin* amplio este concepto incorporando al Do. Pri., la potestad que le asiste a la persona para establecer la forma, el momento y el límite de divulgación de su información privada. (García, 2013).

De lo expuesto se puede colegir que el Do. Pri., tiene dos manifestaciones: i) el que tiene la persona para apartase de los otros, incluyendo la familia, la sociedad o instituciones públicas, refugiarse física y psicológicamente del escrutinio público; y, ii) el que le faculta para controlar la información personal pese a haberse hecho pública, vertiente denominada a partir del análisis realizado en 1983 por el Tribunal Constitucional de Alemania (en adelante TCA) como "derecho a la autodeterminación informativa". España es una de las legislaciones qua ha adoptado este nombre, concibiendo al derecho a la auto determinación normativa como autónomo aun cuando no relacionado con la vida privada. (Herrán, 2003).

Conforme a la interpretación que el TCA realizo del libre desarrollo de la personalidad supone, en el marco de las actuales circunstancias para el tratamiento de datos la defensa de las personas "frente a la ilimitada recolección, archivo, empleo y retransmisión de sus datos personales. El derecho fundamental garantiza de esta manera la capacidad del individuo principalmente para determinar la transmisión y empleo de sus datos personales". (García, 2013, p. 1046).

Pese a lo anterior, hay cuestiones de la privacidad, como los vinculados "con los espacios, las decisiones o los comportamientos, que no pueden ser reducidos simplemente a la "información" o "datos". (García, 2013, p. 1047), que no están comprendidos en Do PDadPe. No obstante, como precisa Bennett la tutela de la privacidad se ha orientado a proteger, por medio de leyes, a cuestiones de la vida personal formulados en términos informacionales, en tanto que los magistrados salvaguardan los no informacionales. (García, 2013, p. 1047).

De lo anterior se desprende que, la privacidad debe ser salvaguardada por la acción conjunta de la administración pública y la actuación de los magistrados quienes cuentan con la

capacidad para decidir el conflicto que se presente entre el derecho a la privacidad y cualquiera otro derecho fundamental.

2.2.1.1. Noción. Respecto al Do. Pri. se han formulado múltiples nociones entre las que se destacan: la de García (2013), de acuerdo con la cual el Do. Pri. abarca la tutela de los datos personales (en adelante DadPe), así como de la intimidad, "lo cual consiste en controlar la información de uno mismo". (p. 8). En concreto este derecho incluye:

a) el derecho a la vida privada y la protección que el Estado debe garantizar para que esta sea velada; b) domicilio; c) vida sexual; d) conversaciones telefónicas; e) derecho a la honra y a la reputación; f) intimidad, cuya información se encuentra restringida a los familiares; g) identidad sexual; h) inviolabilidad de las comunicaciones; i) créditos fiscales j) protección de datos personales. (García, 2013, p. 8-32).

Desde un punto de vista amplio Altamirano concibe al Do. Pri., o intimidad como, el derecho humano, de conformidad con el cual, la persona jurídica o natural, posee la capacidad o potestad impedir o denegar a los otros individuos, "del conocimiento de su vida". (Estrada, 2002, p. 3), así como para establecer en que porcentaje esos aspectos de su vida personal pueden ser lícitamente trasmitidos a los demás.

En el ámbito jurisprudencial, a partir de lo manifestado por la Corte Constitucional de Colombia, se colige que el Do. Pri. o intimidad puede ser considerado como el derecho que asegura a los ciudadanos, el poseer un ámbito o área de su vida personal no susceptible de la intromisión ilegal de los otros individuos y posee dos magnitudes: i) negativa materializada en el "secreto de la vida privada"; y, ii) positiva materializada en una libertad; dentro de este contexto: la magnitud negativa proscribe toda intromisión ilegal, en la vida privada y la publicación ilícita de sucesos o documentos íntimos. La su magnitud positiva, salvaguarda el derecho del individuo para decidir sobre aspectos de su vida íntima o personal da a conocer. (Sentencia C-094/20, considerando 65, 2020).

Acorde con lo manifestado, la privacidad constituye un derecho fundamental orientado a salvaguardar de toda injerencia el área privada y familiar que el individuo "excluir del conocimiento" e injerencias de terceros contra su voluntad. (Megías, 2002, p. 530).

De esta manera, el Do. Priv., puede ser considerado como aquel que le asiste a todo individuo para impedir que terceros puedan conocer su vida personal, así como, para determinar qué aspectos de su vida personal pone al conocimiento de las demás personas.

2.2.1.2. En instrumentos internacionales de Derechos Humanos. Para iniciar se debe puntualizar que en el contexto de los instrumentos internacionales de Derechos Humanos no se emplea el vocablo derecho a la privacidad, sino que alude al derecho a la protección de las injerencias arbitrarias en la vida privada. Con esta precisión, se puede señalar Do. Pri., ha sido regulado en los instrumentos internacionales, de la siguiente forma:

La Convención Americana sobre Derechos Humanos (1969), coloquialmente conocida como pacto de San José; en este instrumento continental de Derechos Humanos, el Do. Pri., no se regula de forma autónoma sino como un aspecto de protección de la honra y dignidad, al señalar que: "Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación". (Convención Americana sobre Derechos Humanos, Art. 11.2, 1969).

La Declaración Americana de los Derechos y Deberes del Hombre (1948), este instrumento si consagra el Do. Pri., como una de las manifestaciones del derecho que tiene toda persona a la "protección la honra, la reputación personal y la vida privada y familiar". (Declaración Americana de los Derechos y Deberes del Hombre, Art. 5, 1948).

La Declaración Universal de Derechos Humanos (1948), respecto al Do. Pri. señala que:

Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a

la protección de la ley contra tales injerencias o ataques. (Declaración Universal de Derechos Humanos, Art.12, 1948).

El pacto internacional de derechos civiles y políticos (1966), por su parte, se limita a reproducir en su artículo 17 lo normado por la declaración universal de derechos humanos.

La carta de los derechos fundamentales de la unión europea (2000), como instrumento de derechos humanos regional, prevé la protección de datos de carácter personal como un derecho que le asiste a todo individuo, aclarando simultáneamente que:

Estos datos se tratan en de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

El respeto de estas normas quedará sujeto al control de una autoridad independiente. (Carta de los Derechos Fundamentales de la Unión Europea, Art. 8. 2 y 3, 2000).

A través del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (2016). Se regulo la: protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Consiente de los avances científicos en materia de comunicación, la Organización de las Naciones Unidas, reglamentó el derecho a la privacidad en la era digital, en la que se reafirma conforme a lo establecido en la Declaración Universal de Derechos Humanos y Pacto Internacional de Derechos Civiles y Políticos el Do. Pri., conforme al cual: “nadie debe ser objeto de injerencias arbitrarias o ilícitas en su vida privada, su familia, su domicilio o su correspondencia, y el derecho a la protección de la ley contra tales injerencias”. (Resolución A/HRC/28/L.27, núm. 1, 2015).

Con fundamento en lo normado por los instrumentos internacionales mencionados, se colige que el Do. Pri., se enmarca en la categoría de Derecho Fundamental en virtud del cual,

el individuo puede gozar íntegramente de su ámbito privado, familiar, su residencia, entre otros1; sin ser objeto de intromisiones, excepto cuando la Ley así lo disponga.

2.2.1.3. ¿Se puede diferenciar la intimidad y la privacidad? En criterio de Bautista (2015) en la doctrina se han empleado equivocadamente los vocablos intimidad y privacidad, esencialmente debido a dos causas: i) la jurisprudencia, los ha empleado como sinónimos; y, ii) por la dificultad que se presenta para diferenciarlos. Por este motivo a continuación se abordan aspectos doctrinales y jurisprudenciales que, para un sector de la doctrina posibilitan diferenciarlos, para luego analizar si ello es posible. Para tal efecto, se parte de establecer el origen etimológico de cada uno de los términos, se proporcionan nociones doctrinales y jurisprudenciales.

Como refiere Rebollo (2005), el origen etimológico del vocablo intimidad proviene de la locución latina *intimus,* superlativo de la palabra *inter,* que alude al área psíquica privada de un individuo, de un colectivo o grupo familiar. Es una noción, que aun cuando es extensamente empleada por la doctrina, posee un significado reduccionista, con respecto a la zona en la que las personas son libres para determinar su comportamiento personal y social, dado que, conforme con Toscano (2017), la intimidad atañe a lo confidencial del individuo, a "su fuero interno" por lo cual, únicamente él, puede acceder a ella, de manera que no requiere de seguros ni rejas que imposibiliten la injerencia de terceros en el área personal.

En el mismo sentido, la Corte Constitucional de Colombia conceptualiza a la intimidad como: el área particular de todo individuo; el ámbito reservado para cada uno, y del que todo individuo debe disponer; que procura el aislamiento o defensa de la persona respecto a la intromisión de terceros, debido a la socialización innata de la persona. (Sentencia C-094/20, considerando 65, 2020).

A partir de lo expuesto, se tiene que la intimidad es un concepto vinculado con la identidad y ámbito interior del individuo, es un área personalísima a la que terceros no pueden

acceder, que le posibilita permanecer aislado hasta el momento en que voluntariamente opta por dar a conocer sus emociones e ideas a otros individuos de su elección, con lo cual prescinde de su intimidad y deposita estas emociones o ideas en su ámbito privado.

En lo que concierne a la privacidad, de acuerdo con lo señalado por Vítores (2018), su origen etimológico se ubica en el vocablo latino *privatus,* que equivale a "quitar, despojar, desposeer o prohibir". Ahora bien, respecto a la noción de privado el diccionario de la Real Academia Española (2022), lo define como un adjetivo, asignándole entre otros el significado: "1. Que se ejecuta a la vista de pocos, familiar y domésticamente, sin formalidad ni ceremonia alguna; y, 2. Particular y personal de cada individuo". (RAE, 2022). Al respecto, originalmente Warren y Brandeis (1890), consideran que la privacidad alude al nivel de asequibilidad, o supervisión que realizamos sobre la accesibilidad de terceros, a nuestra área privada conformada por ideas, emociones, etc. (Toscano, 2017). Así mismo, lo privado como indica Fernández (2019), sirve de nexo entre lo público y lo íntimo, al aceptar la presencia de un área que debe mantenerse aislada del circulo público, debido a lo cual, se le debe mantener en secreto.

Siguiendo esta línea, la Corte Constitucional de Colombia, conceptualiza la privacidad o lo privado como, aquellos temas que inicialmente conciernen únicamente con los intereses concretos y personales del individuo, que no perjudiquen o aludan a las otras personas, respecto de los cuales no existen la obligación legal de darlos a conocer o trasmitirlos. Por el contrario, si un asunto se considera legalmente público su esencia privada cambia. (Sentencia T787/04, considerando 9, 2004).

De lo expuesto, se puede colegir que la privacidad hace referencia a la vigilancia que la persona despliega sobre su área intima, en la que almacena la información, ideas y emociones; a fin de impedir que personas no autorizadas por ella o que no pertenezcan a su entorno accedan o los conozcan.

Análogamente, a partir de lo explicado por Rebollo (2000), colegimos que, a veces equiparamos la noción "de lo irreductible (intimidad) con lo que es exterior, con lo que además de aquello, se compone de otros elementos (vida privada)". (p. 52) se adscribe a esta categoría lo relacionado con el matrimonio, los descendientes, los ascendientes; y, a la categoría de lo íntimo como lo realizo o conformo. Se conoce mi estado civil, si mis ascendientes viven o si soy padre (vida privada). Conforme a mi albedrio puedo divulgar mis orientaciones sexuales o sus pormenores (intimidad). De manera que, desde la óptica de lo público, la intimidad es lo lejano y la vida privada lo cercano.

Dentro de este contexto, *grosso modo,* la diferencia esencial entre intimidad y privacidad radica en que: i) la intimidad en el área en la que el individuo deposita sus sentimientos, ideas, deseos, etc. más personales, cuyo conocimiento está vedado para terceros; y, ii) la privacidad pertenece a la vigilancia que el sujeto despliega sobre sus cuestiones e información personal, para que no sean conocidos por todas las personas sino únicamente aquellas a quienes ella autorice.

No obstante, un sector de la academia considera que la vida privada y la intimidad son sinónimos, en este sentido Ferreira (1982) señala que, aun cuando, en sentido estricto pueden diferenciarse vida privada e intimidad esta diferenciación no tiene consecuencias legales en la mayor parte de regímenes jurídicos. No se debe olvidar que, las tipologías se justifican cuando acarrean consecuencias y no constituyen un fin en sí mismas. (p. 92).

De lo expuesto, se considera que, pese a que en principio se pueden diferenciar la intimidad de la vida privada, esta diferencia es intrascendente pues, la línea que los separa es muy sutil y legalmente esta distinción no tiene implicancias, ya que no conlleva consecuencias diferentes, de ahí que, en la mayoría de los casos la jurisprudencia emplee indistintamente estos términos.

2.2.2. Derecho a la privacidad en Perú

2.2.2.1. Regulación. En nuestro país, tal como ocurre en otras legislaciones, solo se regula el derecho a la intimidad y el Do. Pri. se considera como una de sus expresiones, de manera que, las normas que regulan el derecho a la intimidad contienen aspectos del Do. Pri., por ello, en este acápite se analizarán las principales normas que regulan el Derecho a la intimidad en el Perú, así:

i) ***La constitución política.*** Nuestra norma fundamental prevé que: toda persona tiene derecho:

"Al honor y a la buena reputación, a la intimidad personal y familiar, así como a la voz y a la imagen propias. Toda persona afectada por afirmaciones inexactas o agraviada en cualquier medio de comunicación social tiene derecho a que éste se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley. (Constitución Política del Perú, Art.2, inc.7, 1993).

De la norma mencionada se puede colegir que ella salvaguarda los derechos: al honor, a la intimidad como tal, a la reputación y de rectificación, cuyo contenido se refiere a continuación:

Derecho al honor. El honor es un patrimonio inherente al individuo, dado que hace parte de su esencia. El derecho al honor, conforme expresa Chanamé (2015), corresponde a la defensa "del sentimiento de autoestima o de la apreciación positiva que la persona hace de sí misma. Se atenta contra este honor cuando se nos ofende –en público o en privado– o se agrede sin sustento nuestro prestigio". (p. 205). Es el status jurídico que se asigna al individuo por su valor intrínseco y exclusiva dignidad, respeto al cual se le defiende con relación a los "juicios de valor que se puedan hacer de ella". (Chanamé, 2015, p. 2010). Existen dos tipos de honor: i) subjetivo u honra, en este caso el juicio de valor es realizado por el mismo individuo; y, ii) objetivo o reputación, el juicio de valor lo realiza la sociedad.

Derecho a la reputación. Como lo preciso Chanamé (2015), la reptación corresponde al honor objetivo, pues corresponde a la opinión que los otros poseen o suponen del individuo. Se vulnera cuando la imagen que nuestro entorno posee de notros se afecta. Esta afectación puede provenir de una información cierta o inexistente

Derecho a la intimidad. En concepto de Chanamé (2015), entendido como la situación legal, en la que se protege el ámbito personal y familiar del individuo, constituido por las vivencias previas, las circunstancias presentes, rasgos físicos y psicológicos que no se puede apreciar y en general, toda la información que la persona desea conservar en secreto, porque de ser divulgados, sin su aquiescencia le causarían inconvenientes y alteraciones.

Derecho a la rectificación. Su finalidad es la defensa de la intimidad respecto de los medios de comunicación, es decir, de la libertad de prensa y en la actualidad respecto de los bancos de datos y redes sociales, en nuestro país se encuentran protegidos por la Ley N° 29733 (2011), bajo la denominación Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).

ii) Código civil. Respecto al derecho a la intimidad el Código Civil peruano (1984), regula explícitamente la intimidad personal y familiar; y, prevé normas relacionadas con ella, como se explica a continuación:

Efectivamente, la norma civil protege la intimidad al impedir su divulgación sin el consentimiento del individuo en tratándose de personas vivas y "del cónyuge, descendientes, ascendientes o hermanos, excluyentemente y en este orden" cuando la información pertenece a una persona fallecida. (Código Civil, Art. 14, 1984); esta misma autorización se requiere para el empleo de la imagen o voz de un individuo, excepto cuando ese empleo se justifica por:

La notoriedad de la persona, por el cargo que desempeñe, por hechos de importancia o interés público o por motivos de índole científica, didáctica o cultural y siempre que se relacione con hechos o ceremonias de interés general que se celebren en público. No rigen estas

excepciones cuando la utilización de la imagen o la voz atente contra el honor, el decoro o la reputación de la persona a quien corresponden. (Código Civil, Art. 15, 1984).

Otro aspecto protegido por la legislación civil es la confidencialidad de la correspondencia y demás comunicaciones

La correspondencia epistolar, las comunicaciones de cualquier género o las grabaciones de la voz, cuando tengan carácter confidencial o se refieran a la intimidad de la vida personal y familiar, no pueden ser interceptadas o divulgadas sin el asentimiento del autor y, en su caso, del destinatario. La publicación de las memorias personales o familiares, en iguales circunstancias, requiere la autorización del autor.

Muertos el autor o el destinatario, según los casos, corresponde a los herederos el derecho de otorgar el respectivo asentimiento. Si no hubiese acuerdo entre los herederos, decidirá el juez.

La prohibición de la publicación póstuma hecha por el autor o el destinatario no puede extenderse más allá de cincuenta años a partir de su muerte. (Código Civil, Art. 16, 1984).

No obstante, se debe tener presente que las normas mencionadas son las únicas que regulan el derecho a la intimidad en la legislación civil, aunque son las más relevantes.

iii) Código penal. La legislación penal por su parte, protege el derecho a la intimidad en el capítulo II: violación de la intimidad, artículos 154 y ss. Al tipificar las conductas de: violación de la intimidad (Código Penal, Art. 154, 2004); el tráfico ilegal de datos personales (Código Penal, art. 154ª, 2004); la difusión de imágenes, materiales audiovisuales o audios con contenido sexual (Código Penal, Art. 154B, 2004); revelación de la intimidad personal y familiar (Código Penal, art. 156); uso indebido de archivos computarizados (Código Penal, Art. 157, 2004); aunque para su juzgamiento se requiere de la acción privada, salvo para los tipos previstos en los artículos 154 A y 155 que se procede por acción pública.

2.2.2.2. Noción. El Do. Pri. en opinión del T.C. peruano, se basa en la vida privada la cual como lo indica el máximo defensor de la Norma Fundamental, se formuló como derecho-regla y está conformado por varios aspectos: i) el "derecho a la intimidad personal y familiar". (Constitución Política, Art 2, inc. 7, 1993); ii) el impedimento de que los servicios informáticos no suministren informaciones que afecten la intimidad personal y familiar (inciso 6); la inviolabilidad de domicilio. (Constitución Política del Perú, Art. 2, inc. 9, 1993); el secreto e inviolabilidad de comunicaciones y documentos privados (Constitución Política del Perú, Art. 2, inc., 10, 1993); entre otros. Luego de analizar la regulación internacional de este derecho-regla, el T.C. expuso que, la normatividad nacional se diferencia a la internacional, por lo cual, con fundamento en la Cuarta Disposición Final y Transitoria de la Norma Superior y del Código Procesal Constitucional, se debe procurar formular una noción única de la vida privada, de acuerdo con lo cual concluye que: "el derecho--principio reconocido es la vida privada, y la intimidad, uno de sus derechos-regla". (Expediente N.º 6712-2005-HC/TC, fd. 37).

En relación con el bien jurídico: vida privada, protegido por la Norma Fundamental, su entendimiento es complicado, al extremo que un sector de la doctrina plantea que constituye un concepto legal indefinido. Aun así, el T.C. se empeñó por formular una noción básica y tentativa, su labor partió de reconocer que hay muchos enfoques sobre la vida privada, algunos lo conceptualizan como el área del individuo que no es publica, de ahí que ninguno puede ingresar a ella. No obstante, es más adecuado procurar asignarle un aspecto positivo. De esta manera, con fundamento en el *right to be alone* o derecho a estar en soledad, formulado por Warren y Brandeis (1890), es acertado sostener que la vida privada, es la esfera personal en la que la persona está facultada para "desarrollar y fomentar su personalidad". (Expediente N.º 6712-2005-HC/TC, fd. 38), de manera que, está conformada por: la información, sucesos o situaciones ocultos a la sociedad, que pese a ser ciertos, son confidenciales y solo pueden ser

conocidos por el mismo individuo y un conjunto pequeño de individuos que al ser difundidos o conocidos por terceros generan un perjuicio, como lo precisó Ferreira (1982).

Dentro de este contexto, se ha logrado formular una noción positiva de vida privada en los términos de Zavala (1982), como: el refugio de lo personal que no está limitado por la individualidad, sino que sirve de foro de inserción de la persona con la esfera de determinados parientes y está conformado por: "un ambiente físico (el domicilio) y con el ambiente inmaterial de sus manifestaciones espirituales (la correspondencia, las comunicaciones de todo tipo, los papeles privados)". (Expediente N.º 6712-2005-HC/TC, fd. 38).

El concepto jurisprudencial positivo de la vida privada supone, irreparablemente, apartar a los terceros dado que, salvaguarda una esfera eminentemente personal y como tal, es esencial para el desempeño del individuo, por medio del libre desarrollo de su personalidad, conforme a la lo preceptúa la Norma Fundamental (Constitución Política, art. 2, inc. 1)

En el mismo sentido, el Tribunal Europeo de Derechos Humanos en el caso Hannover (2004), Aplicación N.º 59320/00, estableció que:

La importancia fundamental de la protección de la vida privada desde el punto de vista del desarrollo de la personalidad que tiene todo ser humano. Esa protección, se extiende más allá de círculo privado familiar e incluye también la dimensión social. El Tribunal considera que cualquier persona, aun si es conocida por el público, debe poder gozar de una "legítima expectativa" de protección y respeto de su vida privada. (Expediente N.º 6712-2005-HC/TC, fd. 38).

De expuesto se colige, que solo, mediante el reconocimiento de la vida privada al individuo, éste logrará consolidar su propia identidad, lo que facilita su inserción en la comunidad, dado que, el conocimiento y ámbito psicológico que posee.

La vida privada es un derecho fundamental en primordial relación con la intimidad. El último de ellos tiene una protección superlativa dado que configura un elemento infranqueable

de la existencia de una persona; la vida privada, por su parte, la engloba y también incluye un ámbito que sí admite algunas intervenciones que habrán de ser consideradas como legítimas, vinculándose inclusive con otros derechos como la inviolabilidad de domicilio, prevista, en el artículo 2º, inciso 9 de la Norma Fundamental. (Expediente N.º 6712-2005-HC/TC, fd. 38).

2.2.3. Derecho a la protección de datos personales

Previo al análisis del Derecho a la protección de datos personales (en adelante Do PDadPe) conviene precisar el significado de datos personales, al ser un constructo legal, de esta forma tenemos que:

En el ámbito de la Comunidad Europea se entiende por datos personales: "toda información sobre una persona física identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación" (Reglamento (UE) 2016/679, Art.4.1, 2016), así como, su ubicación por medio de localizador virtual o de un componente (s) de la identidad biológica, psíquica, hereditario, moral, financiero, social y/o cultural del individuo.

En la legislación peruana de protección de datos personales, lo concibe como: "aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados". (Decreto Supremo Nº 003-2013-JUS, Art. 4.1, 2013).

A partir de lo preceptuado por las legislaciones mencionadas, se puede colegir que, los datos personales corresponden a la información proporcionada por la propia persona, que permite identificarla y conocerla en su integridad. Debido a lo cual, se considera acertado lo manifestado por Quiroz (2016), pues Do PDadPe está estrechamente vinculado con

autodeterminación de la información," la privacidad y con el proceso de agravio constitucional de Hábeas Data". (p. 25).

Pese a que nuestro país, como la mayoría de Estados Latinoamericanos ha promulgado la Ley de protección de datos personales (en adelante DaPer), la comunidad y en la mayoría de instituciones oficiales y particulares está en proceso de formación la cultura de defensa de estos datos, las personas ignoran que es uno de sus derechos fundamentales y que son titulares de sus datos personales "cuyo registro manipulación y transferencia sin su consentimiento, en particular con las nuevas tecnologías de la información, puede ocasionar daños y perjuicios con graves repercusiones en su vida personal, social o profesional". (Quiroz, 2016, p. 26), dado que están conformados por la información que posibilite la identificación y que vienen a constituir su perfil, pues permite conocer su nombre, sexo, raza, edad, los padecimientos de salud que presenta, estado civil, profesión, residencia, el culto que profesa, sus preferencias políticas, etc., etc., etc.

En la actualidad resulta vital proteger los DaPer, dado que su empleo se ha incrementado ostensiblemente a través de los registros múltiples registros que la sociedad, de acuerdo a las actividades que se pretendan realizar ha implementado, *verbi gratia*: cuando adquirirnos un celular se proporciona el D.N.I., la dirección de residencia, etc., al igual que, cuando se solicita la instalación de servicios públicos, se apertura una cuenta bancaria, se abre una cuenta en redes sociales, etc., por ello Falcón (1996) en lista los registros en:

1) Personales (del estado civil, de trabajo, escolares y estudiantiles, bancarios, de mandatos, testamentos, reincidencia, policiales, militares, etc.);

2) Comerciales, que pueden ser societarios (de sociedades y asociaciones, acciones y balances, etc.) o de comerciantes (como el Registro Público de Comercio);

3) Impositivos (sobre las actividades y bienes de las personas individuales, colectivas o patrimonios indivisos);

4) De propiedad (inmuebles; muebles registrables; buques; intelectual de marca; etc.);

5) Políticos (padrones, fichas de los partidos, etc.);

6) Sanitarios (de antecedentes y fichas médicas, historias clínicas, etc.);

7) Registros de información y de simple registración (según qué datos sean para su libre conocimiento; por ej., cuando se quieren dar los datos de un producto, o cuando simplemente están para el cumplimiento de determinadas funciones y reservados a ciertas áreas);

8) Públicos, registros semipúblicos, registros privados, registros secretos. (Chanamé, 2003, p. 158)

2.2.3.1. Desarrollo histórico. La protección de DaPer, a partir de lo manifestado por Korff y Georges (2019), se puede sostener que, hizo imprescindible para proteger la información militar a partir de la creación del computador, con objetivos bélicos a fines de la Segunda Guerra Mundial; pues en el Reino Unido con la orientación de Turing se crearon modelos primigenios de descifradores de comunicaciones alemanas codificados por Enigma y Lorenz. En Estado Unidos, por su parte, la compañía IBM creo, con la orientación de Watson, una cantidad importante de dispositivos de "tratamiento de datos para el ejército y comenzó a experimentar con computadoras analógicas, empleadas por los alemanes para calcular la trayectoria de misiles cohete V2". (p. 11).

Ahora bien, en cuanto a la protección de los derechos humanos y libertades en el Estado respecto "al tratamiento automatizado" DaPer (Korff y Georges, 2019, p. 60), apareció mucho después en los años 60's cuando las computadoras empezaron a emplearse como herramienta en el ámbito privado y público. No obstante, esa protección no se universalizó, sino que, se circunscribió aquellos países que podían asumir los altísimos precios de las computadoras en esa época y, además contaban con el espacio para ubicarlas habida cuenta el gran tamaño que tenían; en los que, a su vez, fue empleada por las instituciones gubernamentales y grandes negocios. Las computadoras, inicialmente se emplearon para pagar nóminas de trabajadores,

para el registro de enfermos ingresados a las instituciones de salud, para los censos oficiales y estadísticas, al igual que, para los historiales policiales.

Igual situación se presentó a finales de los 60's y comienzos de los 70's en Alemania, concretamente en la población de Hesse, respecto de los expedientes policiales; Suecia, Noruega, Francia, Estados Unidos, Inglaterra, etc.; y, en el Consejo de Europa; respecto de los archivos de la violencia y otros documentos oficiales, sobre actuación Nazi en la Segunda Guerra Mundial. Los debates iniciales, los protagonizaron profesionales sometidos a deberes éticos, *verbi gratia*: en Estados Unidos entre ingenieros de sistemas y médicos, producto de los cual surgieron lineamientos respecto de "Prácticas de información justas". (Korff y Georges, 2019, p. 12).; también fueron atores en esos debates, los políticos preocupados por el mal uso, el uso ilegitimo o la seguridad de los datos personales automatizados.

Posteriormente, a mediados de la década de los 70's y comienzos de los 80's, esta discusión de popularizo; en Francia se presentaron dos situaciones trascendentales: uno la disertación respecto del proyecto oficial para constituir un banco de datos nacional de ciudadanos y residentes en este país europeo, asignándoseles un "número de identificación único". (Korff y Georges, 2019, p. 12); y, dos, el debate respecto a la presencia de expedientes policiales conflictivos. En Alemania, se presentó un rechazo absoluto, dentro de un ambiente político agitado: al censo previsto para 1983, la discusión no giraba sólo sobre el peligro de la vulneración de la privacidad debido al empleo de nuevas tecnologías, sino, también respecto a: i) los efectos de las equivocaciones en los datos y respecto del poder que significaba el acceder a los datos aglutinados y emplearlos con distintas finalidades; y, ii) el empleo de "identificadores únicos para la interconexión de archivos". (Korff y Georges, 2019, p. 12); estas situaciones sirvieron de sustento para la demanda de "protección de datos" o "informática y libertades" que se presentó en Europa con el propósito que ésta tuviera amparo legal,

jurisprudencial a través de los pronunciamientos de los Tribunales Constitucionales y Superiores, así como, por instrumentos internacionales.

Dentro de este contexto, la expresión "protección de datos" o Datenschütz -en alemán-, se empleó por primera vez en la Ley de protección de datos" o Datenschütz en el año 1970, en el Estado Alemán de Hesse, escrita por el jurista Spiros Simitis considerado como "el padre de la protección de datos". (Korff y Georges, 2019, p. 12). No obstante, en opinión de Burkert, la denominación que se dio a la Ley no era la apropiada, pues su objeto no era el proteger los datos como tal, sino a los individuos titulares de los datos que se manejaban. (Korff y Georges, 2019, p. 12).

Sin embargo, la expresión se conservó hasta la actualidad en donde ha alcanzado un uso generalizado mundialmente.

2.2.4. Protección de datos personales en Perú

En nuestro país los DaPer se encuentran protegidos por la Ley de protección de datos personales, Ley N° 29733 (2011) y su Reglamento Decreto Supremo Nº 003-2013-JUS (2013), conforme a la cual:

El objeto de la legislación de protección de DaPer es salvaguardar este derecho fundamental establecido en la Norma fundamental. (Constitución Política del Perú, Art. 2 inc. 6, 1993), procurando que: i) sean tratados adecuadamente; y, ii) la observancia de los demás derechos fundamentales previstos en la Constitución. (Decreto Supremo Nº 003-2013-JUS, Art.1, 2013).

Los datos sensibles, son DaPer conformados por la información: i) biométrica que *per se* hacen posible la identificación de su titular; ii) sobre la procedencia "racial y étnica"; iii) la economía; iv) la ideas u opiniones políticas, de credo, ideológicas o éticas; vi) sobre pertenencia a sindicatos; y, vii) la vinculada con la salud o tendencia sexual. (D. S. Nº 003-2013-JUS, Art. 2.5, 2013).

La normativa de protección de DaPer es aplicable a: los DaPer almacenados en las bases de datos personales gestionados por instituciones oficiales o particulares "cuyo tratamiento se realiza en el territorio nacional. Son objeto de especial protección los datos sensibles". (D. S. Nº 003-2013-JUS, Art. 3, 2013).

No están amparadas por las normas de protección DaPer a: 1. Los datos almacenados en bases de datos constituidos por el individuo con propósitos vinculados a su vida personal o de su familia; 2. Los almacenados en bases de datos oficiales, en la medida que su tratamiento se requiera para el cumplimiento de las funciones establecidas por Ley a las respectivas instituciones oficiales "para la defensa nacional, seguridad pública, y para el desarrollo de actividades en materia penal para la investigación y represión del delito". (D. S. Nº 003-2013-JUS, Art. 3.1 y 3.2, 2013).

2.2.4.1. Principios rectores de los DaPer. Conforme a Ley de protección de DaPer estos principios no taxativos tiene una doble función: 1. son de observancia obligatoria por los titulares, quienes manejen DaPer y quienes se vinculen con su tratamiento; 2. sirven de "criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de esta Ley y de su reglamento, así como de parámetro para la elaboración de otras disposiciones y para suplir vacíos en la legislación sobre la materia". (D. S. Nº 003-2013-JUS, Art. 12, 2013). Los principios que se regulan son:

1. Legalidad: Los DaPer se tratan dentro del marco legal. Se proscribe la recolección de DaPer a través de procedimientos engañosos, desleales o ilegales (Ley N° 29733, art. 4, 2011).

2. De consentimiento: para que el tratamiento de DaPer sea licito exige del consentimiento o permiso "libre, previo, expreso, informado e inequívoco". (D. S. Nº 003-2013-JUS, Art. 7, 2011), del titular, no son de recibo modelos de consentimiento que no se ajusten a esta exigencia o por la que se presuma el consentimiento o que este contenido en otra

manifestación del titular de DaPer, este principio por ser de interés en esta investigación se abordara de forma pormenorizada en un acápite independiente.

3. De finalidad: la norma regula tres aspectos:

i) la formalidad que debe observarse al momento de da a conocer la finalidad o propósito para recoger los DaPer debe ser "manifestado con claridad, sin lugar a confusión y cuando de manera objetiva se especifica el objeto que tendrá el tratamiento de los datos personales". (D. S. Nº 003-2013-JUS, Art. 8, 2013);

ii) la finalidad de constituir banco de datos sensibles debe ser "legítima, es concreta y acorde con las actividades o fines explícitos del titular del banco de datos personales". (D. S. Nº 003-2013-JUS, Art. 8, 2013).

iii) impone a los profesionales que procesan o manejas DaPer a circunscribirlos al servicio que prestan y a "guardar secreto profesional". (D. S. Nº 003-2013-JUS, Art. 8, 2013.)

4. De proporcionalidad: "Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados". (Ley N° 29733, Art. 7, 2011).

5. De calidad: este principio comprende dos aspectos del tratamiento de los DaPer al prescribir: i) que deben ser verdaderos, correctos y preferentemente actualizados, indispensables, convenientes y apropiados en relación con el propósito con el que se recolectaron; y, ii) deben preservarse en condiciones de seguridad por el lapso requerido para alcanzar el propósito por el que son tratados. (D. S. Nº 003-2013-JUS, Art. 8, 2013).

6. De seguridad: el titular de la base de DaPer y el responsable de su tratamiento, están obligados a implementar "medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales", las cuales deben ser idóneas y coherentes con el tratamiento que se desee realizar y el nivel de DaPer en cuestión. (Ley N° 29733, Art. 9, 2011).

7. De disposición del recurso. Alude a la facultad que asiste al titular de DaPer para acceder a procedimientos administrativos y procesos judiciales para demandar y hacer efectivo sus derechos, en el momento que sean vulnerados por el tratamiento de DaPer. (Ley N° 29733, Art. 10, 2011).

8. De nivel de protección adecuado para el flujo internacional de DaPer, se debe asegurar un apropiado nivel de defensa adecuado a los DaPer "que se vayan a tratar o, por lo menos, equiparable a lo previsto por esta Ley o por los estándares internacionales en la materia". (Ley N° 29733, Art. 11, 2011).

2.2.4.2. Excepciones aplicación de legislación de protección de DadPe. La Ley de protección de datos personales – Ley N° 29733 (2011) y su reglamento- D. S. Nº 003-2013-JUS (2013), no se aplican cuando el tratamiento de datos se realiza con propósitos: i) "domésticos, personales o relacionados con su vida privada o familiar". (D. S. Nº 003-2013-JUS, Art.4, 2013), en tratándose de personas físicas; ii) para formar parte de los bancos de datos oficiales y estén orientados a: "defensa nacional. La seguridad pública y, El desarrollo de actividades en materia penal para la investigación y represión del delito". (D. S. Nº 003-2013-JUS, Art.4, 2013).

2.2.4.3. Del Consentimiento para tratamiento de DadPe. El consentimiento del titular de los DadPe a tratar: i) debe ser recabado por el titular o encargado de su tratamiento; ii) la solicitud de consentimiento debe señalar de forma precisa el propósito (s) para los que se recogen los DadPe, así como las demás situaciones que se puedan presentar; y, iii) informársele si ellos van a ser objeto de trasferencia a nivel local o al extranjero, su finalidad
"el tipo de actividad desarrollada por quien recibirá los mismos". (D. S. Nº 003-2013-JUS, Art.11, 2013).

Características. El consentimiento del titular de DadPe debe ser:

a) Libre: Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular de los datos personales. (D. S. Nº 003-2013-JUS, Art.12.1, 2013), esta autonomía no se afecta por las dadivas o incentivos que se ofrezcan al titular de DadPe. La libertad o autonomía de consentimiento de afecta: i) cundo se ofrecen dadivas o incentivos a menores de edad; ii) se condiciona la prestación de un servicio, se apercibe o coacciona con no permitir o negar "el acceso a beneficios o servicios que normalmente son de acceso no restringido". (D. S. Nº 003-2013-JUS, Art.12, 2013), a condición de que los datos solicitados no se requieren para los beneficios o servicios que se pretenden denegar.

b) Previo: El consentimiento debe preceder el tratamiento de los DadPe.

c) Expreso e inequívoco: El consentimiento se debe expresa de manera que no suscite vacilaciones que su conducta demuestre que esa era la voluntad de titular y no otra. El consentimiento se puede otorgar de forma: i) verbal manifestador oralmente in situ o por medios técnicos que posibiliten emitirlo a viva voz; y, ii) escrito expresado a través de un documento rubricado por el titular de los DadPe o dispositivo legal en que se pueda hacer constar o imprimir en papel o análogo.

El carácter de expreso del consentimiento no está subordinado a que se manifieste de manera verbal o por escrito.

"Tratándose del entorno digital, el consentimiento considera prestado por: i) expresa la manifestación consistente en "hacer clic", "cliquear" o "pinchar", "dar un toque", "touch" o "pad" u otros similares". (D. S. Nº 003-2013-JUS, Art.12.3, 2013); y, ii) por medio de la rúbrica electrónica, o escrito del que quede constancia que posibilite su lectura o impresión "o que por cualquier otro mecanismo o procedimiento establecido permita identificar al titular y recabar su consentimiento, a través de texto escrito". (D. S. Nº 003-2013-JUS, Art.12.3, 2013); y, iii) a través de texto predeterminado, sencillo de percibir, inteligible, redactado de forma sencilla

“que el titular pueda hacer suyo, o no, mediante una respuesta escrita, gráfica o mediante clic o pinchado”. (D. S. Nº 003-2013-JUS, Art.12.3, 2013).

Informado: “Cuando al titular de los datos personales se le comunique clara, expresa e indubitablemente, con lenguaje sencillo”. (D. S. Nº 003-2013-JUS, Art.12.4, 2013), como mínimo:

a. la identificación y domicilio o residencia del titular del banco de DadPe o del encargado de su tratamiento al que puede recurrir para anular el consentimiento o “ejercer sus derechos”. (D. S. Nº 003-2013-JUS, Art.12.4, 2013);

b. el propósito de los datos procesados;

c. identificación de los reales o potenciales receptores de los DadPe;

d. el banco de datos en que archivaran;

e. la condición de imperativa o facultativa de responder las preguntas que se le formulen:

f. los efectos que acarrea suministrar los DadPe y de la denegación de hacerlo;

g. de ser procedente la trasferencia de datos y su naturaleza,

2.2.4.4. Negación, revocación y alcances del consentimiento. El titular de DadPe está facultado para: i) revocar el consentimiento en todo momento sin motivación previa y sin que de ello se deriven consecuencias retroactivas, la revocación está sometida a las mismas formalidades de consentimiento excepto que se haya pactado lo contrario; y, ii) negar o revocar el consentimiento para propósitos complementarios al tratamiento autorizado, sin que esta revocación o negación se haga extensiva al consentimiento inicial.

En tratándose de revocatoria, el responsable del tratamiento de DadPe está obligado a “adecuar los nuevos tratamientos a la revocatoria y los tratamientos que estuvieran en proceso de efectuarse, en el plazo que resulte de una actuación diligente, que no podrá ser mayor a cinco (5) días”. (D. S. Nº 003-2013-JUS, Art.16, 2013).

De producirse el revocatorio total del consentimiento, el titular o encargado del banco de datos está obligado a: i) ejecutara las normas de cancelación o supresión de DadPe; y, ii) "establecer mecanismos fácilmente accesibles e incondicionales, sencillos, rápidos y gratuitos para hacer efectiva la revocación". (D. S. Nº 003-2013-JUS, Art.16, 2013).

2.2.4.5. Derechos de los titulares de DaPer. Corresponden a los derechos que se reconocen a los titulares de los DaPer contra el titular del banco de datos o contra el responsable del tratamiento de los DaPer y están conformados por: i) el Derecho de información; ii) los Derechos designados por la doctrina ARCO; iii) Derecho a evitar que sean suministrados, iv) Derecho al tratamiento objetivo; v) Derecho a la tutela administrativa o judicial; y, v) Derecho a indemnización.

i) Derecho de información: Faculta al titular de los DaPer a disponer de información pormenorizada, accesible, explicita, precisa y por anticipado sobre diversos aspectos: -el propósito por el sus DaPer son tratado; -los destinarios reales o presuntos de los DaPer; -la base de datos en que se archivarán, al igual que la identidad y domicilio de su titular, y de requerirse, del responsable del tratamiento de los datos; -la naturaleza imperativa o potestativa de sus respuestas al cuestionario que se le formule, particularmente tratándose de datos sensibles; - la posibilidad de que sus datos sean trasferidos; - los efectos de suministrar sus DaPer, así como de negarse a suministrarlos; - el plazo de almacenamiento de DaPer; -la facultad de ejercitas los derechos reconocidos por la Ley y los mecanismos para ello. En tratándose de DaPer recolectados en línea o "por redes de comunicaciones electrónicas" este derecho se satisface por medio de las políticas de privacidad, a las que se pueda acceder de forma sencilla y cuya identificación sea fácil. (D. S. Nº 003-2013-JUS, Art. 18, 2013).

De producirse: el cambio del responsable del tratamiento de DaPer luego de emitido el consentimiento por su titular; o la trasferencia de los DaPer "fusión, adquisición de cartera, o supuestos similares", el nuevo responsable o el nuevo titular de la base de datos, deben tomar

medidas eficaces para que el titular conozca esa nueva circunstancia fácil (D. S. Nº 003-2013-JUS, Art. 18, 2013).

ii) Derechos designados por la doctrina ARCO. Como se adelantó se les denomina de esta forma por el acrónimo que la doctrina elaboro con su primera letra conforme a la figura 1

Figura 1

Conformación de Derechos ARCO

Nota. Elaboración propia

Derecho de acceso. Faculta al titular de los DaPer a conocer la información que sobre él tratan las bases de datos oficiales o particulares; la manera y razones para ser recolectados, la identidad de quien los recogió, las trasferencias de que fueron objeto o que se realizaran. (D. S. Nº 003-2013-JUS, Art. 19, 2013).

Derecho de rectificación y cancelación. Faculta al titular de DaPer "a la actualización, inclusión, rectificación y supresión de sus datos personales materia de tratamiento, cuando estos sean parcial o totalmente inexactos, incompletos, cuando se hubiere advertido omisión, error o falsedad". (D. S. Nº 003-2013-JUS, Art. 20, 2013), cuando no se requieran para el propósito para el que se recolectaron o el termino establecido para su tratamiento finalizo.

El responsable del tratamiento de DaPer, en caso de que se hayan trasferido, está obligado a comunicar estas circunstancias al nuevo responsable del tratamiento, quien debe proceder conforme lo manifestado por el titular.

Cuando el titular ejerza alguna de las atribuciones mencionadas, el responsable del tratamiento de DaPer debe bloquearlos para que personas ajenas no puedan acceder a ellos. Este Bloqueo no se aplica a los DaPer que reposan en bases de datos oficiales, pues solo deben informar de la actuación del titular.

La supresión de datos personales contenidos en bancos de datos personales de administración pública se sujeta a lo dispuesto en el artículo 21 del Texto Único Ordenado de la Ley N° 27806 (2002).

Derecho de oposición. En la medida en que la Ley no lo ordene y no se haya otorgado el consentimiento el titular de DaPer está facultado para oponerse a su tratamiento por motivos fundados y legales respecto a un acontecimiento personal, Si se considera fundada la oposición el responsable del tratamiento de DaPer debe suprimirlos. (D. S. Nº 003-2013-JUS, Art. 22, 2013).

iii) Derecho a impedir el suministro: Faculta al titular de DaPer a evitar que sean proporcionados cuando ello vulnera sus derechos fundamentales, aunque no opera para "la relación entre el titular del banco de datos personales y el encargado de tratamiento de datos personales para los efectos del tratamiento de estos". (D. S. Nº 003-2013-JUS, Art. 21, 2013).

iv) Derecho al tratamiento objetivo: Garantiza al titular de DaPer a que no se afecte con determinaciones con consecuencias legales o que lo perjudique gravemente, fundamentada solamente en el tratamiento de los DaPer orientado a apreciar ciertos rasgos de su personalidad o comportamiento, excepto que esto se dé en el ámbito de "la negociación, celebración o ejecución de un contrato o en los casos de evaluación con fines de incorporación a una entidad pública, de acuerdo a ley" asistiéndole el derecho de hacer valer sus argumentos en defensa de sus DaPer. (D. S. Nº 003-2013-JUS, Art. 23, 2013).

v) Derecho a la tutela administrativa o judicial: Acción que puede ejercer el titular de DaPer en el evento en que el titular o el responsable de la base de datos, le niegue, "total o

parcialmente, el ejercicio de los derechos" reconocidos por la Ley de protección de DaPer, acudiendo ante la Autoridad Nacional de Protección de DaPer a través de la reclamación o ante el poder judicial a través de la acción de habeas data. (D. S. Nº 003-2013-JUS, Art. 24, 2013).

vi) Derecho a ser indemnizado: Faculta al titular de DaPer que se perjudique por el desconocimiento de la Ley de protección de DaPer por el titular o encargado de su tratamiento o por terceros a ser indemnizado de acuerdo a lo previsto en la Ley. (D. S. Nº 003-2013-JUS, Art. 25, 2013).

2.2.4.6. Autoridad nacional de protección de datos personales. Organismo que representa al Ministerio de Justicia como encargado del manejo o procesamiento de los DadPe, por lo que regularmente debe remitir a esta entidad el reporte sobre sus acciones. En el desempeño de sus funciones además de lo establecido en la Ley de protección de DadPe y su reglamento, debe observar las normas que le sean aplicables del Reglamento de organización y funciones del Minjus. Se le ha dotado de facultad: i) sancionatoria con observancia de lo dispuesto en la Ley N° 27444 (2001) -; y, ii) coactiva con observancia de la Ley N° 26979 (1998) - (Ley 29733, Art. 32, 2011).

2.2.5. Empleo de cámaras de reconocimiento facial

2.2.5.1. Inteligencia artificial. Dentro del ámbito del creciente y permanente desarrollo informático moderno, se ha hecho común el uso de la expresión inteligencia artificial respecto de la cual se han formulados múltiples definiciones tales como:

La proporcionada por Benítez et al. (2013) conforme a la cual: "la inteligencia artificial es una disciplina académica relacionada con la teoría de la computación cuyo objetivo es emular algunas de las facultades intelectuales humanas en sistemas artificiales". (p.10).

En concepto de Escolano et al. (2003), la inteligencia artificial es la disciplina que permite la creación de artefactos, para que realicen las acciones, que, de ser realizadas por personas, demandarían de inteligencia.

Finalmente, en criterio de Rouhiainen (2018), la inteligencia artificial es una capacidad de los computadores, para realizar labores que habitualmente precisan de la inteligencia humana. Bajo un criterio más técnico preciso que "es la capacidad de las máquinas para usar algoritmos, aprender de los datos y utilizar lo aprendido en la toma de decisiones tal y como lo haría un ser humano". (p. 17).

Analizando las nociones presentadas, se puede colegir que, la inteligencia artificial es la competencia de la que el hombre dota a una máquina para que realice actividades que, habitualmente la persona realiza empleando su inteligencia. Contexto dentro del cual, Boden (2022), plantea dos tipos de la inteligencia artificial: i) tecnológico, al emplear computadores para crear artículos útiles; y, ii) científico, al emplear nociones y prototipos de la inteligencia artificial para contribuir en la solución de dificultades de las personas y las otras especies vivas.

2.2.5.2. La biometría. Como lo informa Díaz (2013), etimológicamente el vocablo "biometría" y "biométrico", proviene del "latín "bios", vida, y "metría", medidas" y, corresponde a los datos relativos a los rasgos biológicos o anatómicos de los individuos recolectados a través de métodos manuales o mecánicos, con un doble propósito: i) individualizar al individuo, empleado su información para confrontarla con un banco de datos; y, ii) certificar o confirmar su identidad. (pp. 29-30), debido a lo cual; concluye que, su funcionamiento se fundamenta en el empleo de información archivada con anticipación para cotejarla con la información conseguida.

Al igual que Díaz (2013), muchos otros investigadores han conceptualizado la biometría algunos de los cuales se refieren a continuación con la finalidad de arribar a una noción propia.

Dentro de este contexto, Martínez (2004), concibe la biometría como un método de reconocimiento humano fundamentado en tipologías corporales y de comportamiento, cuyo

objeto es la identificación de individuos para evitar fraudes, robo de información, bloquear el acceso a redes sociales si como, para verificar la identidad de criminales.

En criterio de Carrión (2009), a través de la ciencia biométrica se reconocen las características particulares de los individuos, efectúa por medio de un proceso, habitualmente empleado en seguridad y vigilancia para el ingreso a diversos sitios, recurriendo a un hardware de reconocimiento por medio de modelos proporcionados constituidos "por secuencias de números, y software, mediante algoritmos de identificación" (p. 15)

Con la misma perspectiva Thill (2011), afirma que a través de la biometría se identifica a una persona por sus huellas digitales, rasgos de su cara "patrón de las venas, iris, voz y el tecleo, entre otros". (Lechner, 2016, p. 28).

Acorde con lo expuesto, se puede afirmar que la biometría es una técnica que, posibilita la identificación de una persona por sus impresiones digitales, rasgos de su rostro y otros datos biológicos o fisiológicos.

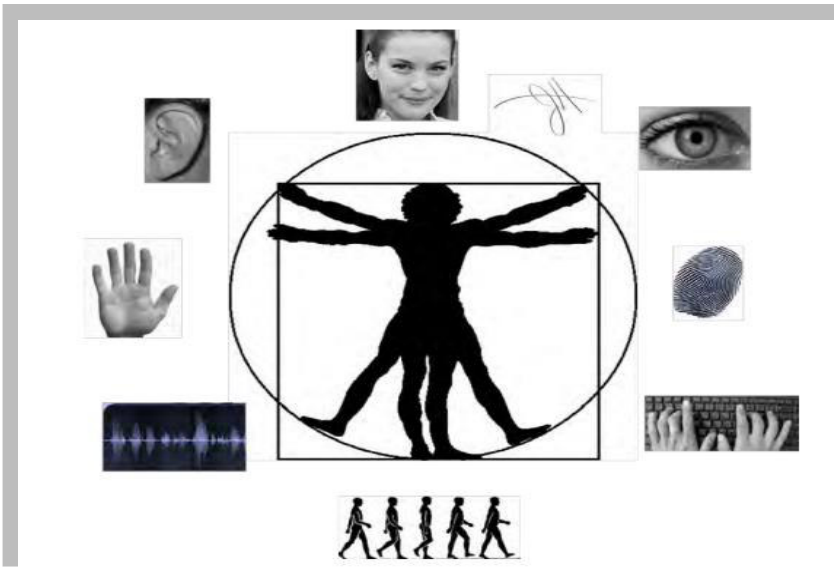
A. Rasgos biométricos. Como precisa Vázquez (2014), los rasgos biométricos corresponden a los atributos "fisiológicos o de conducta del cuerpo humano. Éstos deben ser elementos que puedan ser registrados, cuantificados y procesados mediante ordenadores" (p.7) a través del software de reconocimiento. La figura 3 muestra algunos de los rasgos biométricos del individuo.

En cuanto a estos dos tipos de rasgos Vázquez (2014), precisa que los rasgos: i) fisiológicos corresponden a particularidades esenciales del cuerpo humano, que se pueden obtener de "la mano, del rostro, del iris, de la retina, de la oreja, de la voz, de los patrones vasculares, el ADN entre otros". (p. 8); y, ii) los de conducta corresponden a las muecas o postura que asume el cuerpo frente a determinados sucesos, verbi gracia: la forma "de hablar de escribir, de caminar, la dinámica del uso del teclado, la firma, entre otros". (Vázquez, 2014, p. 8). No obstante, el investigador advierte que con el desarrollo actual la biometría abarca otras

“características del cuerpo como son los electrocardiogramas (ECG), los rayos X, el análisis de la luna de las uñas, el análisis del movimiento de los labios y la expresión corporal al hablar”. (p. 8).

Figura 2

Ejemplos rasgos biométricos



Nota: Tomada de Vázquez (2014).

Características rasgos biométricos. Para Vázquez (2014), los rasgos biométricos tienen como particularidades:

Su universalidad: dado que los rasgos biométricos que el sistema requiere deben estar presentes en las personas a identificar.

Su singularidad: los rasgos de las personas a identificar son exclusivos e irrepetibles

Su cuantificabilidad: los rasgos corresponden a datos que se pueden almacenar, evaluar y procesar.

Su aceptabilidad: quienes acuden al sistema de identificación biométrico deben confiar en él.

Su evasión o usurpación: el sistema de identificación biométrica debe superar los métodos ilícitos, como el robo de identidad o modificación de los rasgos para eludirlo, imposibilitando la identificación de la persona. B

2.2.5.3. Sistema biométrico. En opinión de Ortiz (2010), se denomina sistema biométrico al reconocimiento de determinadas pautas que individualizan a una persona a través de sus rasgos fisiológicos o de comportamiento, conforme a lo conceptualizado por Vázquez (2014). Es decir, es el cotejo de los rasgos biométricos con un padrón previamente archivado en el sistema. Los rasgos se cotejan individualmente para comprobar que la identidad de un individuo sea verdadera.

Respecto al sistema biométrico, señala Vázquez (2014), tiene como finalidad identificar o confirmar, automáticamente la identidad de un usuario (individuo registrado en el sistema), en virtud del examen de uno o varios rasgos biométricos o de cuerpo de la persona. Los sistemas biométricos funcionan con fundamento en tres aspectos: "1) Lo que el usuario sabe. 2) Lo que el usuario posee. 3) Quién realmente es el usuario". (p. 9).

En este contexto, el sistema biométrico es aquel que, a través del empleo de software en el que se han archivado previamente los rasgos biométricos de la persona, posibilita su identificación producto de la comparación de los datos o información obtenida con la almacenada.

2.2.5.4. Reconocimiento facial. El reconocimiento facial (en adelante ReFa), es una forma de inteligencia artificial, concebido por Llerena y La Madrid (2021), como la identificación biométrica que emplea las proporciones del cuerpo para comprobar la identidad de un individuo, en este caso posee un subgrupo de datos biométricos que permiten la identificación del individuo a partir de la configuración y configuración de su cara. "Permite establecer la identidad de los individuos mediante sus rasgos faciales, copiando las

características de las personas, en la identificación de la imagen del rostro, tras analizar un conjunto de imágenes preestablecidas". (p. 10).

Desde una perspectiva más técnica Galván et al. (2015), indican que ReFa es un método para "identificar a las personas por sus rasgos faciales. Utilizan el algoritmo de Eigenfaces, que reconoce las características del rostro de un individuo en un espacio multidimensional". (p. 16). Conforme explican los investigadores, de esta forma los computadores pueden realizar rastreos en bancos de datos faciales o efectuar comparaciones en tiempo real de uno a uno o entre varios en pocos segundos con gran exactitud.

Conforme explican Galindo et al. (2021) el propósito del sistema de reconocimiento facial, es adquirir "una imagen de prueba de un rostro "desconocido" y encontrar una imagen de ese mismo rostro en un conjunto de imágenes "conocidas" o imagen de entrenamiento". (p. 37).

En criterio de Garvie et al. (2016), el ReFa es el procedimiento automatizado de confrontar dos fotografías de rostros para establecer si corresponden a una misma persona. Previo a esta identificación, un algoritmo debe ubicar el rostro del individuo en la fotografía, esta acción corresponde a la denominada detección de la cara. Luego de detectado el rostro se "normaliza". (p. 12), se escanea, se gira y se rectifica de manera que cada rostro que se procese tenga la misma postura. En seguida, el algoritmo obtiene los rasgos del rostro, como la ubicación de los ojos, la contextura de los labios, el color de la piel, etc. las cuales se representan numéricamente. Por último, el algoritmo examina por pares los rostros y suministra una calificación numérica que corresponde a la semejanza de los rasgos. Esta técnica es de naturaleza binaria, pues está orientado a detectar semejanzas más factibles y menos factibles.

En virtud de lo expuesto, se puede sostener que el ReFa es una forma de inteligencia artificial pues, a través de ella la computadora a la que previamente se le ha instalado el

correspondiente programa de reconocimiento basado en algoritmos, puede identificar el rostro que se le pone de presenta de entre los que se han almacenado previamente en su base de datos.

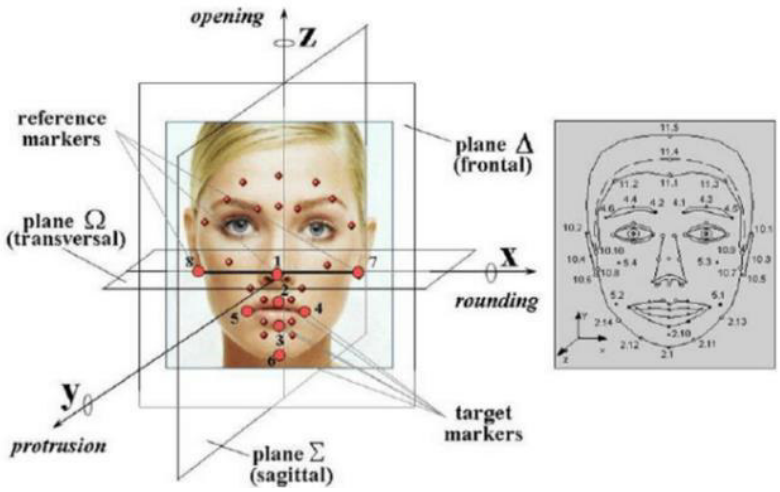
A. Evolución del reconocimiento facial. En las últimas décadas del siglo XX el reconocimiento facial, se consideraba como una técnica irreal, no obstante, en el siglo XXI este método se ha hecho realidad, extendiéndose su uso. A continuación, se detallan los acontecimientos más importantes en el desarrollo de esta técnica, tal como se ha consignado en el artículo titulado: Una breve historia del reconocimiento facial.

B. Las mediciones manuales de Bledsoe en los años 60s. La literatura considera a Woodrow Wilson Bledsoe como el precursor o padre del reconocimiento facial, debido a que en los años sesenta ideó un método que conseguía catalogar fotografías de rostros de forma manual empleando la tableta "RAN", equipo que podía ser utilizados por los individuos introduciendo "coordenadas horizontales y verticales" usando un bolígrafo electromagnético. A través de esta técnica, no solo se registraba la localización por medio de las coordenadas, sino, además, los rasgos faciales: boca, nariz, ojos y el pelo. Estos datos se incorporaban a un banco de datos y en el momento que el sistema recibió una foto de una persona, logro recuperar del archivo la imagen que mayor similitud tenía con esa persona.

C. ***Mayor exactitud con veintiún marcadores del rostro (años 70's)*** Una breve historia del reconocimiento facial (2019***).*** Gracias a las investigaciones de Goldstein et al (1971). El sistema de reconocimiento facial manual experimentó un adelanto en los años 70's, el emplear 21 marcadores subjetivos concretos que comprendían el espesor de la boca y el tono del pelo para identificar el rostro mecánicamente, los datos continuaban archivándose a mano. Conforme se ilustra en la figura 3.

Figura 3

Reconocimiento facial manual



Nota: Elaboración propia

D. Eigenfaces (rostros propios) (fines años 80's e inicio de los 90's). Una breve historia del reconocimiento facial (2019), en este período se buscó reproducir imágenes faciales a baja escala e inicia con el empleo por Sirovich y Kirby (1988), del algebra lineal al reconocimiento facial, lo que les permitió revelar que: i) el examen de los rasgos en un compendio de imágenes de rostros podría constituir una serie de rasgos fundamentales; y, ii) que con menos de cien valores era factible codificar "con precisión una imagen facial normalizada". (Una breve historia del reconocimiento facial, 2019). Posteriormente, Turk y Pentland (1991), ampliaron la perspectiva del plano adecuado al identificar la forma de identificar rostros en los retratos, estas propuestas llevaron al reconocimiento facial automático. No obstante, la aplicación de perspectiva al reconocimiento facial no tuvo mayor desarrollo por circunstancias técnicas y medio ambientales.

E. Programa Feret (1993–2000. Una breve historia del reconocimiento facial (2019). Este programa de reconocimiento fue promovido por la "Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) y el Instituto Nacional de Estándares y Tecnología". a inicios de los noventa con la finalidad de promover la comercialización del reconocimiento facial. La propuesta era la de constituir un banco de datos de imágenes de rostros, la cual se incrementó en el 2003 incorporando fotografías a color y con alta definición

de 24 bits, el ensayo se efectuó con dos mil cuatrocientas trece fotos de rostros, correspondientes a ochocientos cincuenta y seis individuos. Se pretendió que con este amplio archivo de fotografías de prueba para el reconocimiento estimular investigación para crear un método de reconocimiento más eficaz.

F. Super bowl XXXV (2002). Una breve historia del reconocimiento facial (2019)**.** En 2002 los miembros de la Policía emplearon reconocimiento facial, como manifestación de la tecnología para el cumplimiento de sus funciones. A pesar de que con él se logró el reconocimiento de criminales que habían llegado a la mayoría de edad, el proyecto se consideró como un fiasco. "Los falsos positivos y las reacciones violentas de los críticos demostraron que el reconocimiento facial no estaba del todo". (Una breve historia del reconocimiento facial, 2019), ello debido esencialmente, que no tenía funcionabilidad en archivos constituidos por multiplicidad de fotografías, circunstancia que es esencial en el funcionamiento del reconocimiento facial.

G. Pruebas de vendedores de reconocimiento facial (2000s). Una breve historia del reconocimiento facial (2019). Estas pruebas fueron realizadas a inicios del dos mil por el "Nacional de Estándares y Tecnología (NIST)". Con fundamento en el programa Feret, estas pruebas se formularon para realizar análisis oficiales diferentes de las técnicas de reconocimiento faciales que se comercializaban por la época, al igual que de los métodos de modelos. La finalidad de este análisis consistió en suministrar a las agencias de seguridad y al gobierno de los Estados Unidos datos para mejorar la técnica de reconocimiento facial.

H. Base de datos forense (2009). Una breve historia del reconocimiento facial (2019). Este archivo forense fue creado en dos mil nueve por el alguacil del Condado de Pinellas en el Estado de la Florida, para que los policiales ingresaran al historial "fotográficos del Departamento de Seguridad de Carreteras y Vehículos Motorizados (DHSMV)", lo cual ocasiono que para el dos mil once, aproximadamente a ciento setenta diputados se le había

provisto de cámaras fotográficas, con la que fotografiaban a sospechosos para ser confrontadas con el archivo, llegando a incrementarse las detenciones y causas penales sin precedentes.

I. Medios sociales (2010-presente). Una breve historia del reconocimiento facial (2019). Desde el dos mil diez, la red social Facebook puso en práctica el reconocimiento facial para individualizar a los individuos cuyos rostros figuraban en las fotografías que sus usuarios publican habitualmente. Aun cuando esta iniciativa fue atacada por los medios informativos por atentar contra la privacidad, la red social no tuvo en cuenta estos ataques. Dado que esta medida fue aceptada por los usuarios de Facebook hoy en día "más de 350 millones de fotos se cargan y etiquetan con reconocimiento facial cada día". (Una breve historia del reconocimiento facial, 2019).

El dos mil once, fue muy significativo para el desarrollo del reconocimiento facial esencialmente por dos acontecimientos: i) "Primera instalación principal del reconocimiento facial en un aeropuerto en el año 2011". (Una breve historia del reconocimiento facial, 2019). El primer país en implementar una cámara de reconocimiento facial en un terminal aéreo fue Panamá con el apoyo de los Estados Unidos en el dos mil once, con la finalidad de mitigar las acciones ilegales en la terminal de Tocumen en el que predominaba el narcotráfico y la criminalidad organizada. Esta medida fue positiva, ya que posibilito el incremento de aprehensiones por la organización Internacional de Policía Criminal o Policía Internacional (Interpol); y, ii) Osama Bin Laden identificado en el año 2011. (Una breve historia del reconocimiento facial, 2019). El reconocimiento facial contribuyo a la identificación del cadáver de Bin Laden.

J. Ley que aprueba el reconocimiento facial en el año 2014). Desde el dos mil catorce el "Sistema de información de justicia regional automatizado (ARJIS, por sus siglas en inglés), red de instituciones de justicia que fomenta el intercambio de información entre agencias locales, estatales y federales de justicia". (Una breve historia del reconocimiento facial, 2019),

empezó a dotar a las entidades asociadas de una plataforma móvil de reconocimiento facial, con el propósito de solucionar una grave problemática: la individualización inmediata de individuos que poseían documentos de identidad o que no deseaban ser reconocidos. Dentro de las agencias que emplearon base se cuentan: "la policía de San Diego, el Departamento de Justicia, el FBI, la DEA, la CBP y los EE. UU. Marshalls". (Una breve historia del reconocimiento facial, 2019).

K. Reconocimiento facial "inevitable" para los retailers (2017)". Una breve historia del reconocimiento facial (2019) El incremento de la comercialización al menudeo del reconocimiento facial coadyuvó a su desarrollo.

L. IPHONE X (2017)". Una breve historia del reconocimiento facial (2019). El iPhone X lanzado por Apple en dos mil diecisiete, trajo como su principal novedad el reconocimiento facial como mecanismo de seguridad del equipo. A partir del hecho de la veloz venta de este dispositivo, se deduce que la personas aceptan esta técnica como sistema de seguridad en los celulares.

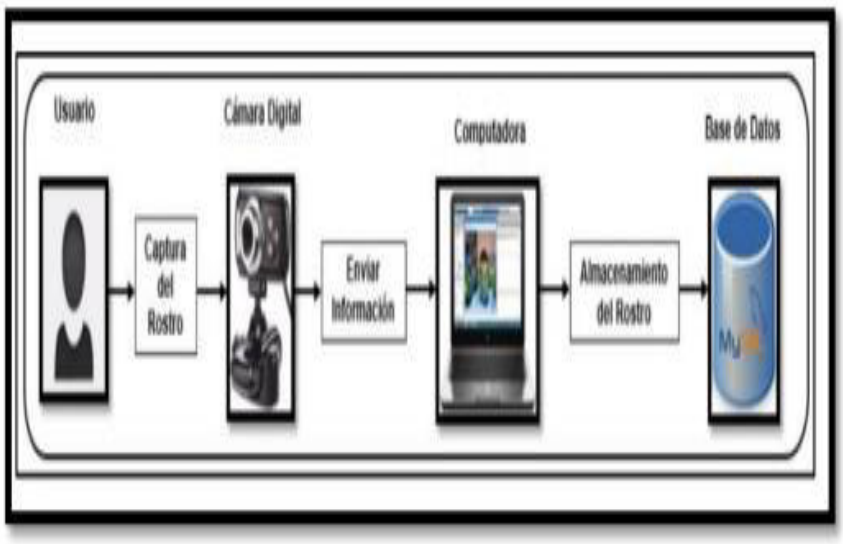
M. Listado de vigilancia como servicio (2018) Desde dos mil dieciocho la técnica del reconocimiento facial se difundió más, facilitando que las instituciones accedan a ella. "Este año, en la conferencia NRF Protect presentó el futuro de los retails con WatchList as a Service (WaaS). WaaS es una nueva plataforma de datos de reconocimiento facial". Una breve historia del reconocimiento facial (2019). creada para coadyuvar en la disuasión de robos en comercio y crímenes violentos, al ofrecer un banco de datos de criminales reconocidos que constituyen un peligro para la seguridad. No obstante, este banco de datos no opera autónomamente sino asociada con una plataforma de monitoreo biométrico que coteja los rasgos para dar aviso sobre peligros en tiempo real". (Una breve historia del reconocimiento facial, 2019).

N. Configuración del sistema de ReFa. El sistema de ReFa está constituido por: i) el usuario individuo a ser reconocido; ii) el mecanismo que va a administrar la imagen, puede ser

o bien una cámara digital o una biométrica; iii) el sistema que gestiona y confronta la imagen, -ordenador- con el banco de datos para recoger los datos del individuo – usuario, conforme se ilustra en la figura. (Neyra, 2019).

Figura 4

Constitución sistema de reconocimiento facial



Nota. Tomada de Neyra (2019)

O. Funcionamiento del ReFa. Conforme lo exponen Galindo et al. (2021), sucintamente explicado el funcionamiento del ReFa consiste en exhibir frente a una cámara especial los rostros de los individuos la cual los compara con las caras almacenadas en su memoria. Este archivo o "listas de observación" contiene fotografías de muchas personas y pueden de las redes sociales o de cualquier sitio. Aunque, existen varios sistemas de ReFa sus funciones básicas son:

i) el ReFa. La cámara localiza la imagen de la cara y la ubica, pues la fotografía debe presentar al individuo en "primer plano". (Galindo et al., 2021, p. 38);

ii) examen facial. se registra la fotografía de una cara y estudia: "distancia entre los ojos, la profundidad de las cuencas de los ojos, la distancia desde la frente hasta el mentón, la forma de los pómulos, los contornos de la boca, los oídos y el mentón". (Galindo et al., 2021, p. 38); dado que su finalidad es localizar parámetros de semejanza trascendentes para diferenciar entre otras caras.

iii) trasformación de imagen en información. la captura de rostros convierte la información analógica (rostros) en un conjunto de información digital (datos) en función de los rasgos faciales de la persona. Los códigos digitales se denominan impresión de rostros". (Galindo et al., 2021, p. 39).

iv) indagar por coincidencia. Como se indica en Kaspersky lab, las fotos etiquetadas en Facebook ingresan a su banco de datos y pueden ser empleadas para ReFa, con el propósito "de establecer si la huella facial coincide con la imagen en la base de datos de reconocimiento facial. Y se concluye que, de todas las medidas biométricas, el reconocimiento facial se considera la más natural". (Galindo et al., 2021, p. 39).

En el mismo sentido Binford et al. (2019), explican las cuatro fases del ReFa así:

- ***Detección de caras "face detection":*** se tiene una fotografía o imagen, en la que además del rostro se parecían más cosas o un fondo. De hecho, pueden aparecer múltiples rostros. En esta etapa se detecta el o los rostros y se encierran en un rectángulo.

- ***Alineamiento de cara "face alignment"*** o ***"face normalization"*:** Comúnmente conocida como eta de normalización, dado que se ajustan los componentes en cuanto a su "tamaño, geometría o fotometría para conseguir consistencia entre todas las imágenes que se almacenan en una base de datos, y poderlas hacer de alguna forma comparables". (Binford et al., 2019, p. 67).

- ***Extracción de características "feature extraction"*:** En esta fase, lo que inicialmente era una imagen se convierte, en realidad, en una serie de características que de

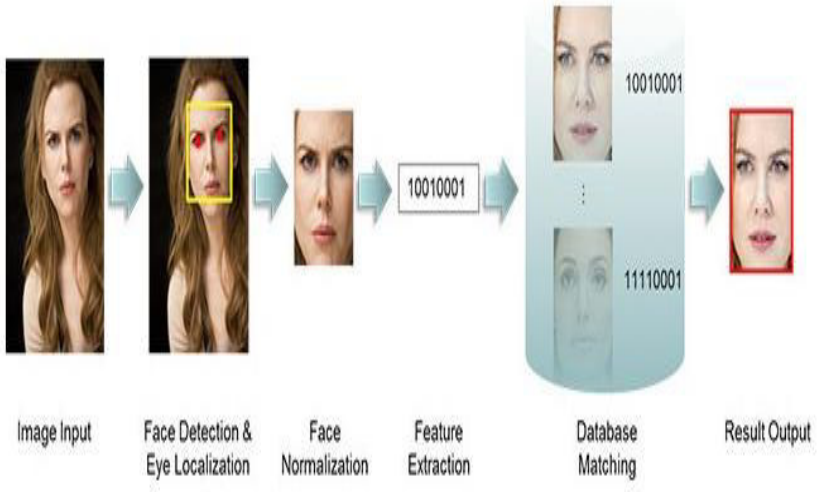
alguna forma definen esa imagen, esa cara, reduciéndola a esas características que le confieren singularidad. El resultado suele ser un vector de características. (Binford et al., 2019, p. 67).

- ***Reconocimiento de cara "face recognition"*** o **"*matching*":** Una vez reducida la imagen de la cara a un vector de características se busca en una base de datos alguna cara que presente esas mismas características. Si la encontramos, habremos culminado con éxito el reconocimiento. (Binford et al., 2019, p. 67).

En este contexto, advierten los investigadores que en cada una de estas etapas se emplean algoritmos diferentes, graficando las fases en la figura 5

Figura 5

Fases del reconocimiento facial



Nota. Nota. Elaboración propia

2.3. Marco filosófico

2.3.1. Los imperativos en Kant

En la filosofía kantiana los imperativos pertenecen a la filosofía práctica, pese a que los imperativos hipotéticos (en adelante ImHip) por ser normas técnicas, pertenezcan también a las ciencias, la filosófica teórica y el arte. Kant (1989), aborda los imperativos y su distinción: ImHip e imperativos categóricos (en adelante ImCat), en el II capítulo de la "Fundamentación de la Metafísica de las costumbres" al señalar: "La representación de un principio objetivo, en

tanto que es constrictivo para una voluntad, llámese mandato (de la razón), y la fórmula del mandato llámese imperativo". (Kant, 1989, p. 414), agregando que los imperativos (ImCat e ImHip) se enuncian por medio de un "deber ser" y de esta forma evidencian el vínculo de una norma "objetiva de la razón a una voluntad que, por su constitución subjetiva, no es determinada necesariamente por tal ley (una constricción)". (Kant, 1989, p. 414).

Respecto a los principios prácticos en criterio de Kant (1997). "Son proposiciones que encierran una determinación universal de la voluntad, a cuya determinación se subordinan diversas reglas prácticas". (p. 39). En cuanto a la norma práctica, a partir de lo planteado por Kant (1997), se deduce que, es creada por la razón al establecer la acción como modo para alcanzar un resultado o efecto, identificando tres principios prácticos: i) subjetivos que corresponden a las máximas; ii) objetivos, que son de dos categorías: ImCat e ImHip.

En consecuencia, se puede aseverar que los principios prácticos se pueden amparar de forma i) objetiva que corresponden a los imperativos con validez universal y son de dos categorías: ImCat e ImHip; y, ii) subjetiva que corresponden a las máximas.

Los ImHip "son los que determinan las condiciones de la causalidad del ente racional como causa eficiente sólo respecto del efecto que se espera conseguir y contienen únicamente preceptos de habilidad". (Kant, 1997, p. 38). No obstante, los que definen la voluntad de forma irrestricta, independientemente, la consecuencia que origine, son los ImCat.

Acorde con lo manifestado, se concluye que Kant (1997), formula tres principios prácticos: i) las máximas; ii) los ImHip o condicionales; y; iii) los ImCat o incondicionados.

La característica esencial de las máximas es la carencia de obligatoriedad y como principio practico subjetivo kantiano, deben comprenderse como norma o regla de conducta o comportamiento. De manera que, para "Kant la máxima es el principio subjetivo de obrar que contiene la regla práctica que determina la voluntad de conformidad con las condiciones del sujeto". (Kant, 1946), esto es, el principio en virtud del cual procede el individuo. Y debido a

su naturaleza subjetiva solo tienen validez para quien las reconoce, admite y actúa de conformidad con ellas. Desde el enfoque ético, las máximas o normas de conducta se catalogan como: i) buenas, por ejemplo: no perjudicar a los demás, no robar, socorrer al prójimo, etc.; ii) malas, ver gratia: conseguir lo que se desee sin considerar el medio empleado, etc.; y, iii) neutro.

Respecto a las máximas malas, no son éticas por lo cual jamás pueden constituir un mandato o imperativo, dado que serían contrarias con la ley moral o superior de la razón, que persigue la creación de máximas que puedan llegar a universalizarse. Es decir, la máxima adquiera la categoría de ley cuando su tenor coincide con la ley moral, por cuanto ella establece "Obra de tal manera que la máxima de tu acción pueda convertirse en ley moral". (Kant, 1946, p. 423).

Al contrario de los principios prácticos subjetivos, los principios prácticos objetivos para Kant (1998). son obligatorios, dado que son válidos para todas las personas, por ende, universales. El motivo de su naturaleza imperativa sus sustenta en el libre albedrio de la persona, conforme con el cual, se pueden obedecer o no, toda vez que "son siempre producto de la razón". (p. 39).

2.3.2. Imperativo categórico

Acorde con el problema planteado en esta investigación, solo se ahondará en el ImCat que conforme a lo expresado por Kant (1998), es una formulación de la ley universal de la razón o ley moral y su génesis se ubica en la "razón práctica pura. Este es un mandato que no está sometido a ninguna condición, razón por la cual es categórico. Puesto que es categórico, es irrenunciable". (p.12).

El ImCat, apriorísticamente se puede considerar como el sustento de la moral y del derecho, de manera que posibilita la comprensión de la libertad, pues como lo sostiene Kant (1989), únicamente se comprende la libertad, de la que se originan las leyes morales, derecho

y obligaciones; por medio “del imperativo moral, que es una proposición que manda, el deber, y a partir de la cual puede desarrollarse después la facultad de obligar a otros, es decir, el concepto de derecho”. (p. 241).

Prosiguiendo con el desarrollo de la teoría de ImCat, Kant (1989), formula tres modalidades del ImCat, los cuales en su criterio son recíprocamente análogos, esto es, se contienen mutuamente, signados conforme a lo explicado por Rivera (2004), como:

i) “la ley universal”. (Rivera, 2004, p. 5), conforme a la cual “Obra sólo según una máxima tal que puedas querer al mismo tiempo que se torne ley universal”. (Rojas, 2015, p. 123), que es la más divulgada.

ii) “de la humanidad”. (Rivera, 2004, p. 5), en virtud de la cual se debe “Obra de tal modo que consideres a los demás siempre como un fin en sí mismo y nunca solamente como medio”. (Rojas, 2015, p.123).

iii) “de la autonomía”, (Rivera, 2004, p. 5), con arreglo a la cual se debe “Obra de tal modo que tu voluntad pueda considerarse como legisladora universal”. (Rojas, 2015, p.123), es decir, se debe actuar conforme a la máxima por la que se opte autónomamente.

Kant (1989), afirma que las tres modalidades del ImCat son manifestaciones de un solo principio. Proceder de conformidad con las máximas, de manera que estas puedan tenerse como leyes universales, equivale “a tratar a la humanidad siempre como fin y nunca como un mero medio, lo cual, a su vez, es lo mismo que actuar de manera autónoma”. (Rivera, 2004, p. 5).

La segunda modalidad, la de la humanidad; comprende la significación de la dignidad del ser racional, tal como se desprende de lo manifestado por Kant (1989). “La humanidad misma es una dignidad porque el hombre no puede ser utilizado únicamente como un medio por ningún hombre (ni por otros, ni siquiera por sí mismo), sino siempre a la vez como fin, y en esto consiste precisamente su dignidad (la personalidad)”. (p. 464), lo cual permite distinguir

al individuo de los otros seres humanos, sobre los que prevalece gracias a la dignidad, que se sustenta en el hecho de ser un fin en sí mimo.

Por consiguiente, afirma Kant (1989), el individuo en "en cuanto a ser racional debe pensarse a sí mismo como inteligencia y por tanto como perteneciente, no al mundo sensible, sino al inteligible". (p. 454). Adicionalmente, alude a quien vulnera los derechos de los individuos, afirmando que se vale de los demás "simplemente como medio, sin tomar en consideración que en cuanto seres racionales deben ser apreciados siempre al mismo tiempo como fines, o sea, como seres que también habrán de poder albergar en sí el fin de esa misma acción". (Kant, 1946, p. 432).

La ley fundamental, es decir la humanidad contenida en el ImCat, es caracterizada por Kant (1988), como un hecho de la razón, dado que no se puede deducir de información precedente de la razón verbi gratia "de la conciencia de la libertad". (p. 52) pues ella no la poseemos con anterioridad

"Sino que se impone por sí misma a nosotros como proposición sintética a priori, la cual no está fundada en intuición alguna, ni pura ni empírica, aun cuando sería analítica si se presupusiera la libertad de la voluntad, pero para ello requeriría, como concepto positivo, una intuición intelectual, la cual no se puede admitir aquí de ningún modo. Sin embargo, para considerar como dada esta ley, sin lugar a malas interpretaciones, hay que notar bien que ella no es un hecho empírico, sino el único hecho de la razón pura, la cual se anuncia por él como originariamente legislativa (sic volo, sic iubeo 6)". (Kant, 1988, p. 52).

En este contexto, el fáctum, en este caso supone a priori la conciencia de la ley moral o universal (humanidad) y, por ende, no es licito la estructuración de un régimen moral o legal deseando que sea válida para todos los individuos, dado que para Kant (1988), el ImCat es el sustento a priori de la moral y el derecho como ya se indicó precedentemente.

Adicionalmente, al ser el ImCat el fundamento o norma de cuantificación de las acciones de los individuos, en la filosofía kantiana, establece las que son buenas y las que no, por ende, cuales se debe cumplir y cuáles no, es decir las nociones del bien y del mal. Sobre el particular, Kant (1997), sostiene que el bien y el mal no existen de forma autónoma, sino que están vinculadas con el propósito y los efectos de las acciones del hombre, de manera que, "no es el concepto de bien como objeto el que el que determina y hace posible la ley moral sino al revés, la ley moral la que determina y hace posible el concepto de bien". (p. 88).

III. Método

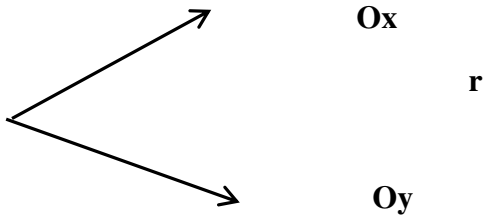
3.1. Tipo de investigación

El enfoque de la investigación fue cuantitativo

El tipo de investigación fue básico. Las variables del estudio privacidad de datos personales y empleo de cámara de reconocimiento facial, se analizaron en el ámbito legal y tecnológico.

El nivel de la investigación fue explicativo. Se precisó la forma como el empleo de la cámara de reconocimiento facial vulnera la privacidad de los datos personales.

El diseño de la investigación fue no experimental-transaccional, las variables privacidad de datos personales y empleo de cámara de reconocimiento facial no fueron manipuladas, solo se observó su comportamiento en el lapso de la investigación para luego establecer el vínculo que existió entre ellas.



Dónde:

M: Muestra

Ox: Observación realizada a Variable independiente: prueba de absorción atómica

Oy: Observación realizada a la Variable dependiente: causas de ineficacia de la prueba de absorción atómica

R: Relación que existe entre las variables sometidas a estudio

3.2. Población y muestra

La investigación conto con una población de 50 sujetos entre: cuentahabientes del Banco BBVA que emplean el reconocimiento facial para abrir la app del banco y realizar sus

transacciones, usuarios de celulares que emplean el reconocimiento facial para activarlos, Jueces, secretarios y especialistas de Juzgados Constitucionales de Lima, profesores de Derecho Constitucional y egresados del doctorado en Derecho de la Escuela Universitaria de Posgrado de la Universidad Nacional Federico Villarreal (en adelante EUPG-UNFV) y Abogados.

De la población, empleando el muestreo no probabilístico y fórmula matemática indicada a continuación, se obtuvo la muestra conformada por 44 sujetos y configurada como se ilustra en la tabla 1:

$$\mathbf{n = \frac{(p.\ q)\ Z^2\ N}{e^2\ N - 1 + (p.\ q)\ Z^2}}$$

En la cual:

n: Tamaño de la muestra de investigación

p, q: Probabilidad de la población estándar, no comprendida en la muestra. Se les asigna a p y q el valor de 0.5 cada uno.

Z: Unidades de desviación estándar con probabilidad de error de 0.05, lo que indica que el intervalo de confianza de 95% en la estimación de la muestra, el valor asignado a Z = 1.96.

N: Total de la población: 50 sujetos.

EE: Error estándar de estimación, aceptado en la investigación, corresponde a 5.00%.

Sustituyendo:

$n = (0.5 \times 0.5 \times (1.96)^2 \times 50) / (((0.05)^2 \times 50) + (0.5 \times 0.5 \times (1.96)^2))$

n = 44

Tabla 1

Configuración muestra

Sujeto	Número	%
Jueces, secretarios y especialistas de juzgados constitucionales de Lima.	09	20.45
Profesores de derecho constitucional UNFV	03	6.84
Egresados del doctorado en Derecho EUPG-UNFV.	15	34.09
Abogados	17	38.63
TOTAL	44	99.98

Nota: Elaboración propia.

3.3. Operacionalización de variables

Tabla 2

Operacionalización de variable independiente y dependiente

VARIABLE	DEFINICION CONCEPTUAL	DEFINICION OPERACIONAL	INDICADORES
INDEPENDIENTE X. PRIVACIDAD DE DATOS PERSONALES	Toda información que identifica o hace identificable a una persona natural y que solo puede ser conocida por voluntad de su titular, como: el nombre, D.N.I., edad, sexo, localización, clase social, de naturaleza médica, profesional, financiera "numérica, alfabética, gráfica, fotográfica, etc.	Se medirá en encuesta	X.1. Derecho fundamental. X.2. Protección legal. X.3. Información privada.
DEPENDIENTE Y. EMPLEO DE CÁMARA DE	Forma de identificación biométrica que opera con un dispositivo que hace parte de un sistema dotado de un software que se usa para que, a partir de la comparación en tiempo real o por medio de	Se medirá en la Encuesta	Y.1. Consentimiento del titular. Y.2. Trasferencia de datos.

RECONOCIMIENTO FACIAL.	fotografías o videos o cualquier medio audiovisual, de los rasgos del rostro puede identificar a una persona.	Y.3. Falta de regulación.

Nota: Elaboración propia.

3.4. Instrumento

El instrumento de que se valió la investigadora fue:

El cuestionario*:* estructurado con preguntas cerradas, para averiguar la opinión de la población respecto a la privacidad de los datos personales y el empleo de cámara de reconocimiento facial.

3.5. Métodos de investigación

En esta investigación se usaron los métodos:

Exegético. Para conocer el sentido otorgado por el legislador a regulación de la privacidad de los datos personales y el empleo de la cámara de reconocimiento facial

Histórico. Para conocer la evolución en el tiempo de la privacidad de los datos personales y el empleo de la cámara de reconocimiento facial

Sistemático: Para conocer la forma como el régimen internacional y el interno regulan la privacidad de los datos personales y el empleo de la cámara de reconocimiento facial.

3.6. Análisis de datos

Para el análisis de los datos alcanzados se empleó el programa SPSS en el que se ingresaron los resultados de la encuesta, para obtener datos estadísticos mostrados por medio de gráficos y tablas.

IV. Resultados

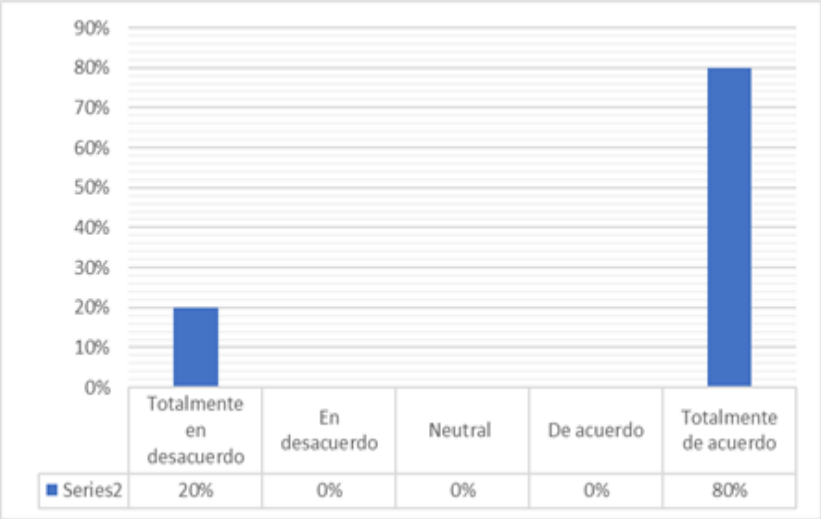
4.1. Análisis de la encuesta

En este acápite se presentan los resultados de la encuesta formulada a los sujetos de la muestra, ingresados al programa SPSS formulados en figuras.

1. ¿Sabía que la privacidad de datos personales es un Derecho Fundamental?

Figura 6

Resultado pregunta No. 1 de encuesta



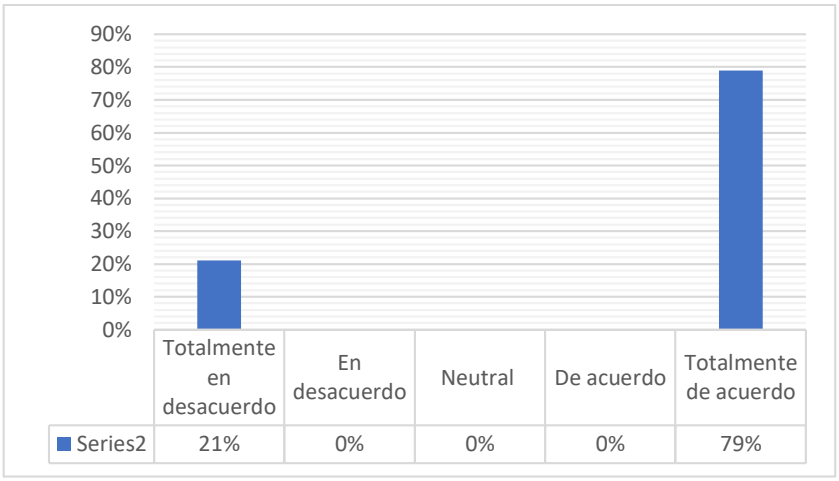
Nota. Elaboración propia, fuente encuesta.

Evaluación: La respuesta a la pregunta 1, confirma el tipo de investigación aplicado por la investigadora, dado que, de la figura 6 se extrae que el 80% de los sujetos encuestados admitió saber que la privacidad de los datos personales es un Derecho Fundamental, en tanto que el 20% estuvo totalmente en desacuerdo con ello.

2. ¿Está de acuerdo con que los derechos fundamentales tienen protección reforzada?

Figura 7

Resultado pregunta No. 2 de encuesta



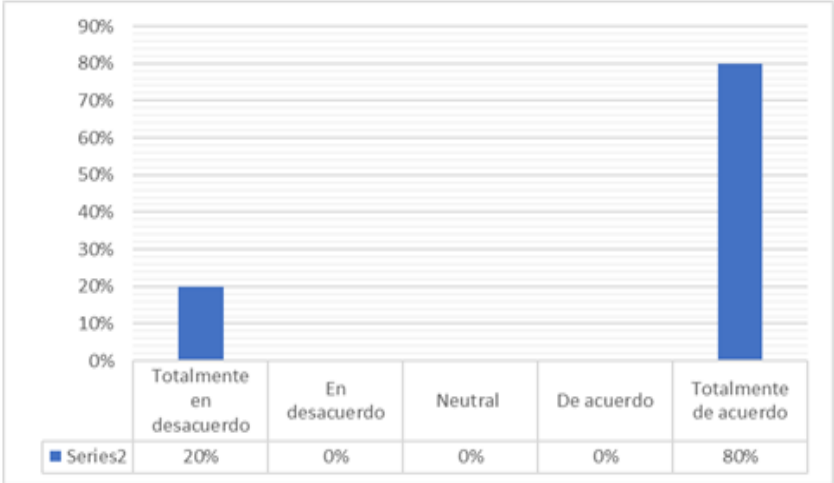
Nota. Elaboración propia, fuente encuesta.

Evaluación: La respuesta a la pregunta 2, confirma el tipo de investigación aplicado por la investigadora, dado que, de la figura 7 se extrae que el 79% de los sujetos encuestados estuvo de acuerdo con que los derechos fundamentales tienen protección reforzada, en tanto que el 21% estuvo totalmente en desacuerdo con ello.

3. ¿Concuerda Ud. con que la privacidad de los datos personales está garantizada legalmente por Ley de protección de datos personales?

Figura 8

Resultado pregunta No. 3 de encuesta



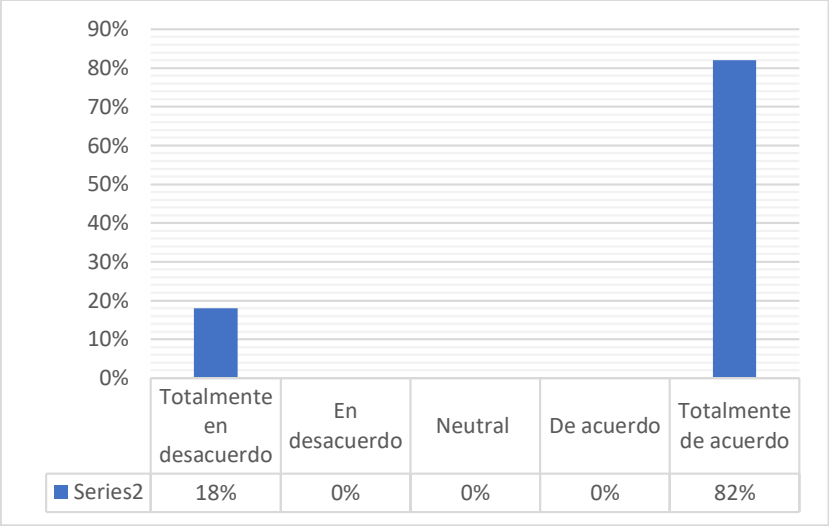
Nota. Elaboración propia, fuente encuesta.

Evaluación: La respuesta a la pregunta 3, confirma el tipo de investigación aplicado por la investigadora, dado que, de la figura 8 se extrae que el 80% de los sujetos encuestados concordó con que la privacidad de los datos personales está garantizada legalmente por Ley de protección de datos personales, en tanto que el 20% estuvo totalmente en desacuerdo con ello.

4. ¿Concuerda con que los datos personales corresponden a información privada del individuo?

Figura 9

Resultado pregunta No. 4 de encuesta



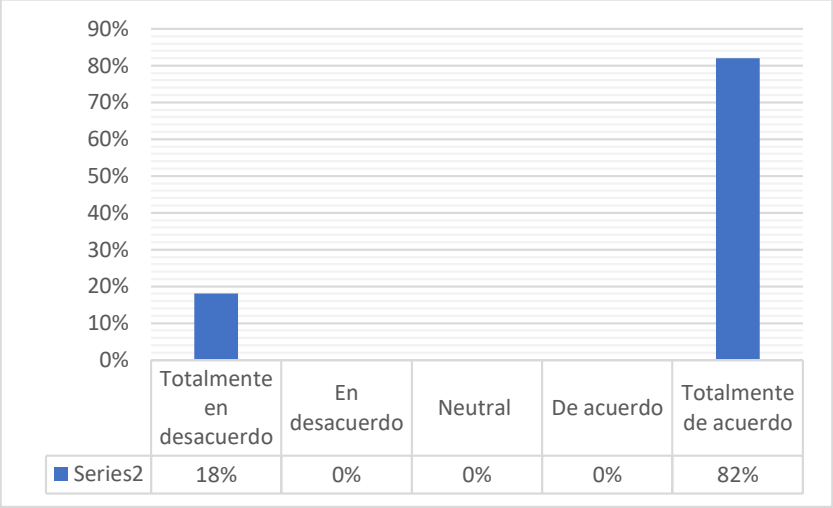
Nota. Elaboración propia, fuente encuesta.

Evaluación: La respuesta a la pregunta 4, confirma el tipo de investigación aplicado por la investigadora, dado que, de la figura 9 se extrae que el 82% de los sujetos encuestados concordó con que los datos personales corresponden a información privada del individuo, en tanto que el 18% estuvo totalmente en desacuerdo con ello.

5. ¿Está de acuerdo con que los datos personales solo pueden divulgarse sino por voluntad de su titular?

Figura 10

Resultado pregunta No. 5 de encuesta



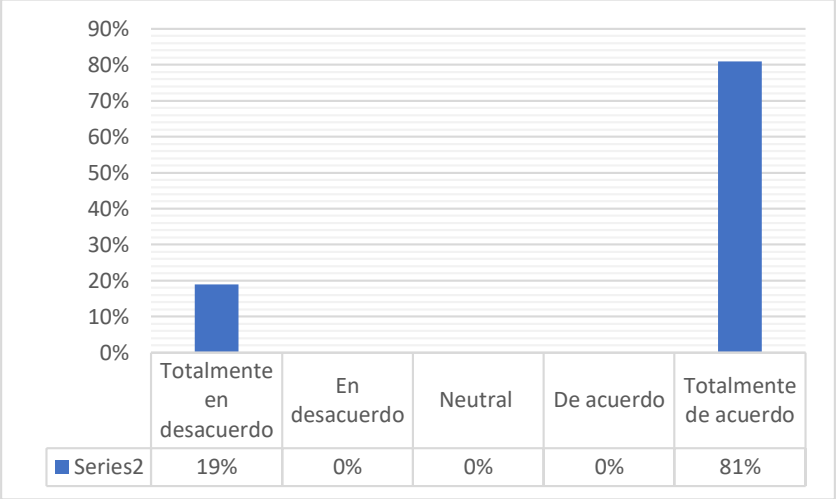
Nota. Elaboración propia, fuente encuesta.

Evaluación: La respuesta a la pregunta 5, confirma el tipo de investigación aplicado por la investigadora, dado que, de la figura 10 se extrae que el 82% de los sujetos encuestados concordó con que que los datos personales solo pueden divulgarse sino por voluntad de su titular, en tanto que el 18% estuvo totalmente en desacuerdo con ello.

6. ¿Está de acuerdo con que el tratamiento del rostro de la persona permite conocer todos sus datos personales?

Figura 11

Resultado pregunta No. 6 de encuesta



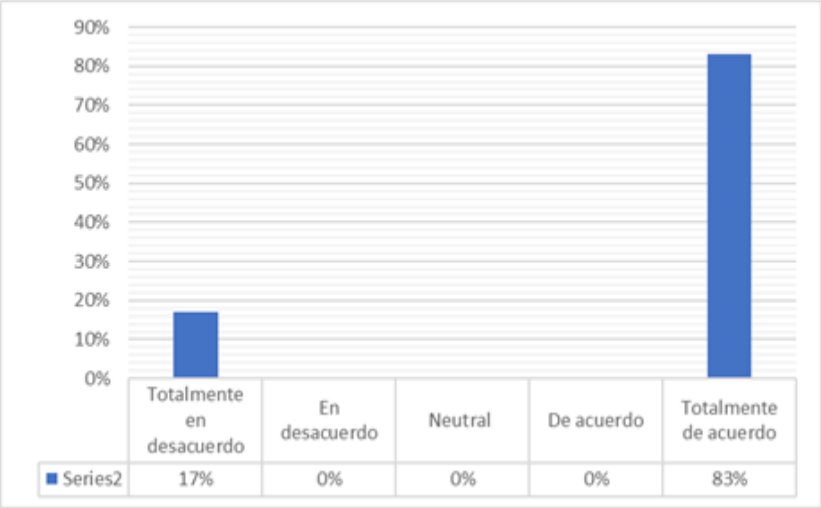
Nota. Elaboración propia, fuente encuesta.

Evaluación: La respuesta a la pregunta 6, confirma el tipo de investigación aplicado por la investigadora, dado que, de la figura 11 se extrae que el 81% de los sujetos encuestados estuvo de acuerdo con que el tratamiento del rostro de la persona permite conocer todos sus datos personales, en tanto que el 19% estuvo totalmente en desacuerdo con ello.

7. ¿Sabía Ud. que para que el rostro de una persona sea captado por la cámara de reconocimiento facial se necesita de su consentimiento?

Figura 12

Resultado pregunta 7 de encuesta



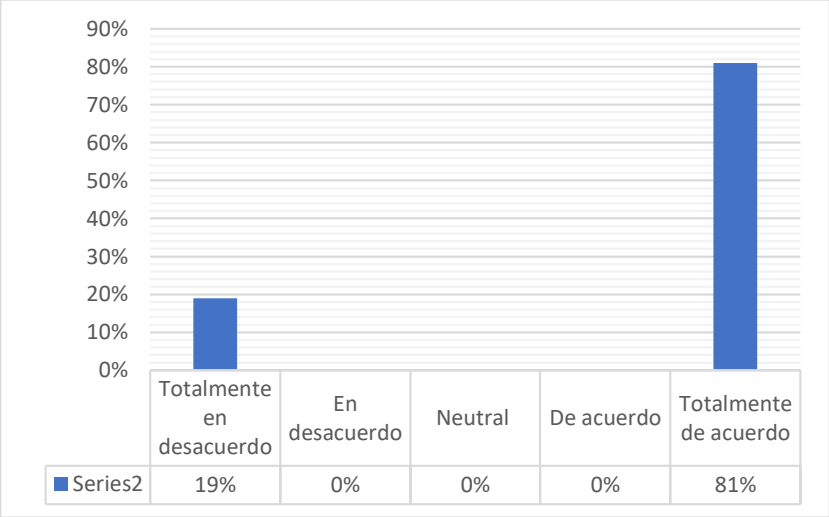
Nota. Elaboración propia, fuente encuesta.

Evaluación: La respuesta a la pregunta 7, confirma el tipo de investigación aplicado por la investigadora, dado que, de la figura 12 se extrae que el 83% de los sujetos encuestados acepto saber que para que el rostro de una persona sea captado por la cámara de reconocimiento facial se necesita de su consentimiento, en tanto que el 17% estuvo totalmente en desacuerdo con ello.

8. ¿Concuerda Ud. con que el consentimiento referido en el numeral anterior debe ser claro, expreso y previo?

Figura 13

Resultado pregunta No. 8 de encuesta



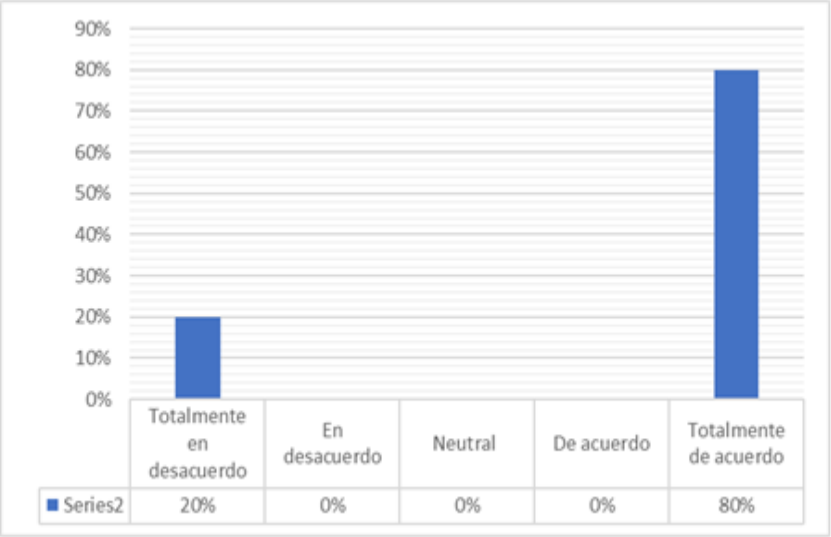
Nota. Elaboración propia, fuente encuesta.

Evaluación: La respuesta a la pregunta 8, confirma el tipo de investigación aplicado por la investigadora, dado que, de la figura 13 se extrae que el 81% de los sujetos encuestados concordó con que el consentimiento referido en el numeral anterior debe ser claro, expreso y previo, en tanto que el 19% estuvo totalmente en desacuerdo con ello.

9. ¿Sabia Ud. que luego reconocido el rostro por la cámara de reconocimiento facial se convierte en un dato?

Figura 14

Resultado pregunta No. 9 de encuesta



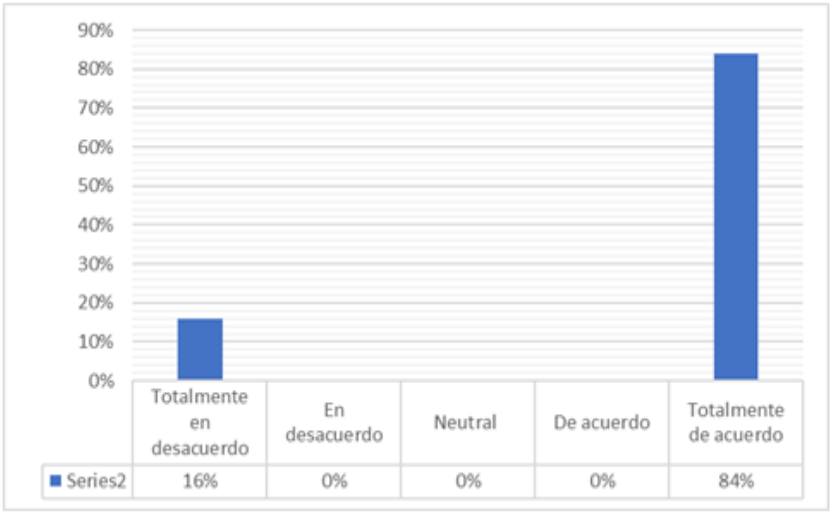
Nota. Elaboración propia, fuente encuesta.

Evaluación: La respuesta a la pregunta 9, confirma el tipo de investigación aplicado por la investigadora, dado que, de la figura 14 se extrae que el 80% de los sujetos encuestados acepto saber que luego reconocido el rostro por la cámara de reconocimiento facial se convierte en un dato, en tanto que el 20% estuvo totalmente en desacuerdo con ello.

10. ¿Concuerda Ud. con que el rostro como dato personal puede ser trasferido?

Figura 15

Resultado pregunta No. 10 de encuesta



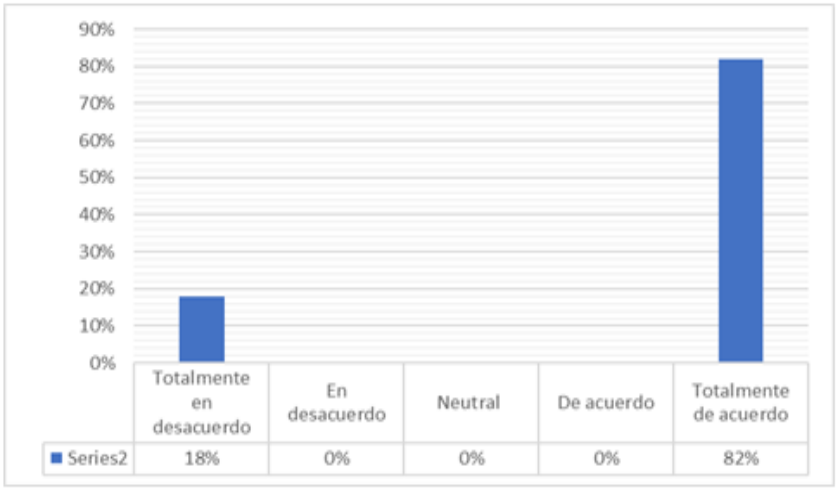
Nota. Elaboración propia, fuente encuesta.

Evaluación: La respuesta a la pregunta 10, confirma el tipo de investigación aplicado por la investigadora, dado que, de la figura 15 se extrae que el 84% de los sujetos encuestados concordó con que el rostro como dato personal puede ser trasferido, en tanto que el 16% estuvo totalmente en desacuerdo con ello.

11. ¿Sabia Ud. que la trasferencia de datos personales puede darse a nivel nacional y/o internacional?

Figura 16

Resultado pregunta No. 11 de encuesta



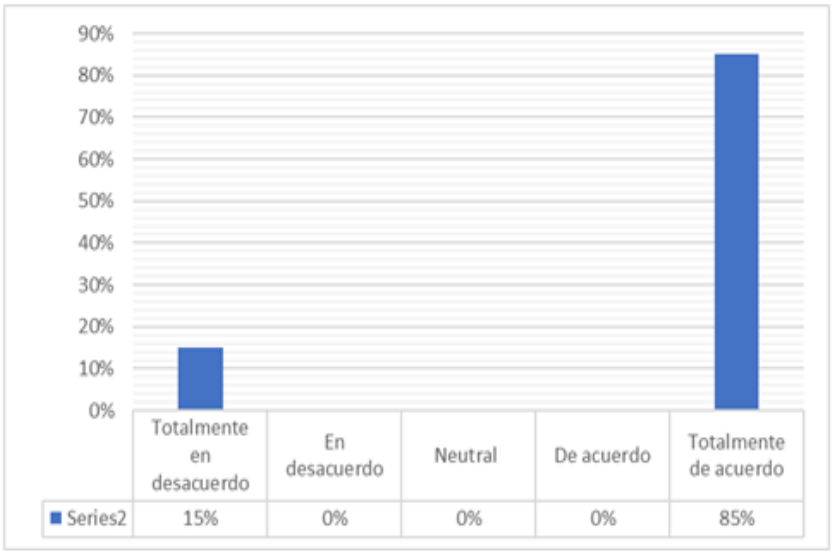
Nota. Elaboración propia, fuente encuesta.

Evaluación: La respuesta a la pregunta 11, confirma el tipo de investigación aplicado por la investigadora, dado que, de la figura 16 se extrae que el 82% de los sujetos encuestados acepto saber que la trasferencia de datos personales puede darse a nivel nacional y/o internacional, en tanto que el 18% estuvo totalmente en desacuerdo con ello.

12. ¿Conocía Ud. que el empleo de cámara de reconocimiento facial en Perú no está regulado?

Figura 17

Resultado pregunta No. 12 de encuesta



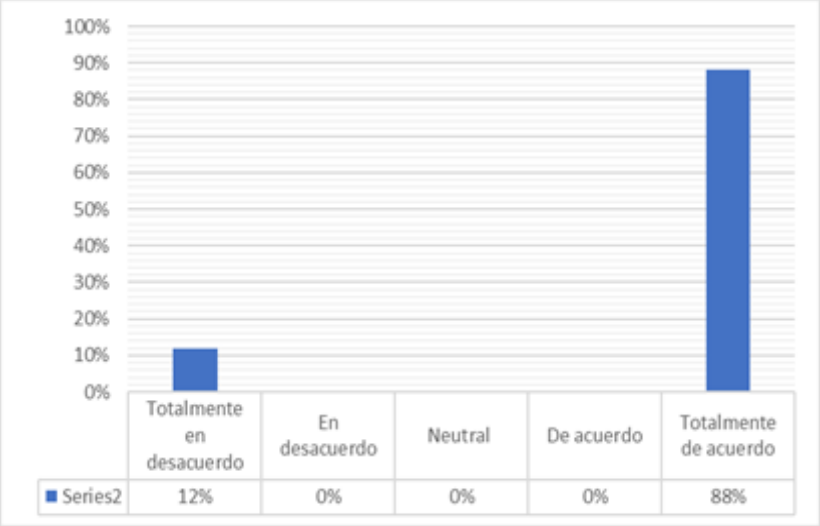
Nota. Elaboración propia, fuente encuesta.

Evaluación: La respuesta a la pregunta 12, confirma el tipo de investigación aplicado por la investigadora, dado que, de la figura 17 se extrae que el 85% de los sujetos encuestados acepto conocer que el empleo de cámara de reconocimiento facial en Perú no está regulado, en tanto que el 15% estuvo totalmente en desacuerdo con ello.

13. ¿Está de acuerdo con que el empleo de la cámara de reconocimiento facial vulnera la privacidad de los datos personales a través del consentimiento otorgado por el titular para que el rostro captado por la cámara sea tratado y, por la falta de regulación de su empleo?

Figura 18

Resultado pregunta No. 13 de encuesta



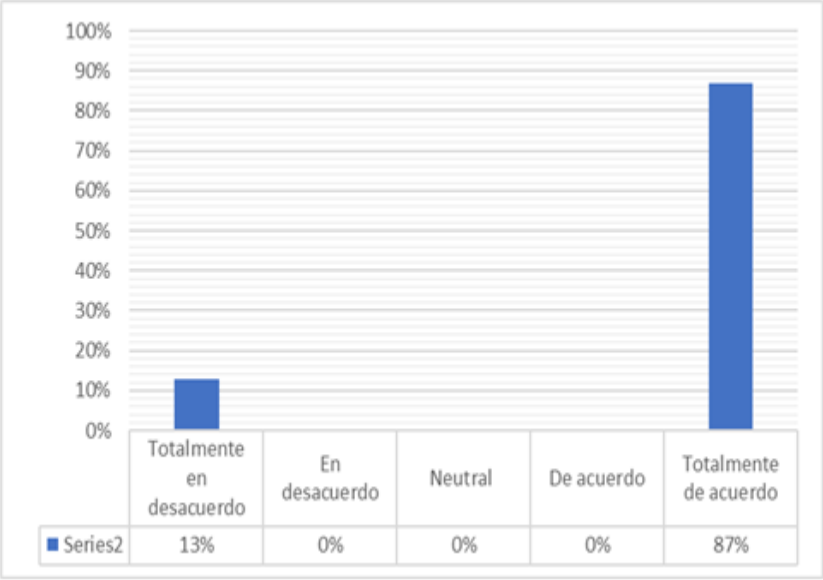
Nota. Elaboración propia, fuente encuesta.

Evaluación: La respuesta a la pregunta 13, confirma el tipo de investigación aplicado por la investigadora, dado que, de la figura 18 se extrae que el 88% de los sujetos encuesta estuvo de acuerdo con que el empleo de la cámara de reconocimiento facial vulnera la privacidad de los datos personales a través del consentimiento otorgado por el titular para que el rostro captado por la cámara sea tratado y, por la falta de regulación de su empleo, en tanto que el 12% estuvo totalmente en desacuerdo con ello.

14. ¿Concuerda con que el consentimiento del titular para que su rostro captado por la cámara de reconocimiento facial sea tratado vulnera la privacidad de los datos personales, al permitir el acceso a los datos en todos los ámbitos de la vida de la persona?

Figura 19

Resultado pregunta No. 14 de encuesta



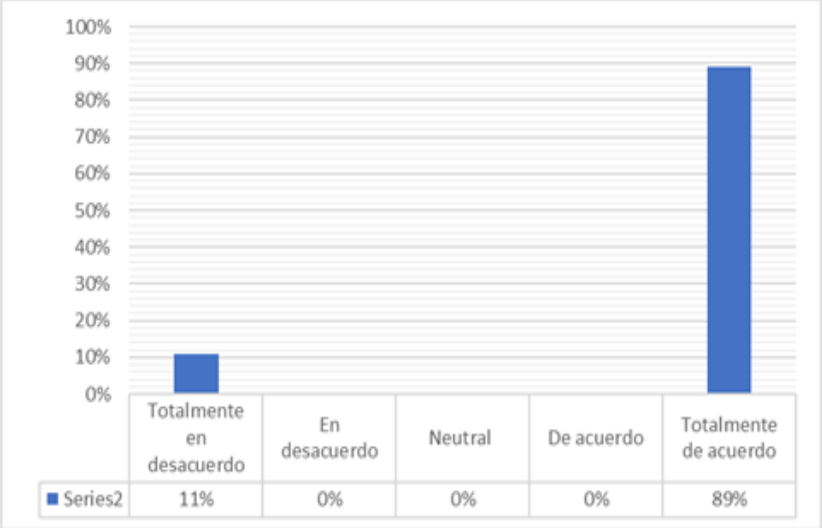
Nota. Elaboración propia, fuente encuesta.

Evaluación: La respuesta a la pregunta 14, confirma el tipo de investigación aplicado por la investigadora, dado que, de la figura 19 se extrae que el 87% de los sujetos encuesta concordó con que el consentimiento del titular para que su rostro captado por la cámara de reconocimiento facial sea tratado vulnera la privacidad de los datos personales, al permitir el acceso a los datos en todos los ámbitos de la vida de la persona, en tanto que el 13% estuvo totalmente en desacuerdo con ello.

15. ¿Está de acuerdo con que la falta de regulación del empleo de la cámara de reconocimiento facial vulnera la privacidad de los datos personales, porque no están autorizadas para tratar captar, tratar y trasferir las imágenes del rostro de la persona?

Figura 20

Resultado pregunta No. 15 de encuesta



Nota. Elaboración propia, fuente encuesta.

Evaluación: La respuesta a la pregunta 15, confirma el tipo de investigación aplicado por la investigadora, dado que, de la figura 20 se extrae que el 89% de los sujetos encuesta estuvo de acuerdo con que la falta de regulación del empleo de la cámara de reconocimiento facial vulnera la privacidad de los datos personales, porque no están autorizadas para tratar captar, tratar y trasferir las imágenes del rostro de la persona, en tanto que el 11% estuvo totalmente en desacuerdo con ello.

4.2. Contrastación de la hipótesis

Al contrastar la hipótesis se calculó, mediante el coeficiente estadístico de correlación de Rho de Spearman.

Contrastación de la hipótesis general

Hipótesis Alternativa (H_1): El empleo de la cámara de reconocimiento facial vulnera la privacidad de los datos personales a través del consentimiento otorgado por el titular para que el rostro captado por la cámara sea tratado y, por la falta de regulación de su empleo.

Hipótesis Nula (H_0): El empleo de la cámara de reconocimiento facial NO vulnera la privacidad de los datos personales a través del consentimiento otorgado por el titular para que el rostro captado por la cámara sea tratado y, por la falta de regulación de su empleo.

Tabla 3

Tabla de frecuencias observadas de la hipótesis general

Variables	Totalmente de acuerdo	Totalmente en desacuerdo	Total
Privacidad de datos personales	32	12	44
Empleo de cámara de reconocimiento facial	32	12	44
TOTALES	32	12	44

Nota. Elaboración propia.

Tabla 4

Tabla de frecuencias esperadas de la hipótesis general

Variables	Totalmente de acuerdo	Totalmente en desacuerdo	Total
Privacidad de datos personales	35	09	44
Empleo de cámara de reconocimiento facial	35	09	44
TOTALES	35	09	44

Nota. Elaboración propia.

Método de contrastación:

El método de contrastación fue el siguiente:

1) Supuestos: La muestra fue aleatoria simple, constituida por 44 sujetos

2) Estadística de contrastación:

$$X^2 = \sum \frac{(\text{Observed frequencies} - \text{Expected frequencies})^2}{\text{Expected frequencies}}$$

$$= \sum \frac{(Fo - Fe)^2}{Fe}$$

3) Criterio de decisión: desestimar la hipótesis nula (H_0) si X^2 es mayor o igual a 0.05 = 5.00% es decir, $X^2 = \geq 0.05 = 5.00\%$

4) Resultado de obtenido al resolver la estadística de contrastación:

$X^2 = ((32-35)^2) / 35) = 0, 2571$

5) Decisión estadística: por cuanto 25,71% > 5.00%, se desestima la hipótesis H_0 y se estima H_1.

6) Conclusión: Se estima que el empleo de la cámara de reconocimiento facial vulnera la privacidad de los datos personales a través del consentimiento otorgado por el titular para que el rostro captado por la cámara sea tratado y, por la falta de regulación de su empleo.

Contrastación de la hipótesis especifica N° 1

Hipótesis alternativa (H_1): El consentimiento otorgado por el titular para que el rostro captado por la cámara de reconocimiento facial sea tratado vulnera la privacidad de los datos personales, al permitir el acceso a los datos en todos los ámbitos de la vida de la persona.

Hipótesis nula (H_0): El consentimiento otorgado por el titular para que el rostro captado por la cámara de reconocimiento facial sea tratado NO vulnera la privacidad de los datos personales, al permitir el acceso a los datos en todos los ámbitos de la vida de la persona.

Tabla 5

Tabla frecuencias observadas de las hipótesis general N° 1

Variables	Totalmente de acuerdo	Totalmente en desacuerdo	Total
Privacidad de datos personales	31	13	44
Empleo de cámara de reconocimiento facial	31	13	44
TOTALES	31	13	44

Nota. Elaboración propia.

Tabla 6

Tabla frecuencias esperadas de las hipótesis general N° 1

Variables	Totalmente de acuerdo	Totalmente en desacuerdo	Total
Privacidad de datos personales	36	08	44
Empleo de cámara de reconocimiento facial	36	08	44
TOTALES	36	08	44

Nota. Elaboración propia.

Método de contrastación:

El método de contrastación fue el siguiente:

1) Supuestos: La muestra fue aleatoria simple, constituida por 44 sujetos

2) Estadística de contrastación:

$$X^2 = \sum \frac{(\text{Observed frequencies} - \text{Expected frequencies})^2}{\text{Expected frequencies}}$$

$$= \sum \frac{(Fo - Fe)^2}{Fe}$$

3) Criterio de decisión: desestimar la hipótesis nula (H_0) si X^2 es mayor o igual a 0.05 = 5.00% es decir, $X^2 = \geq 0.05 = 5.00\%$

4) Resultado de obtenido al resolver la estadística de contrastación:

$X^2 = ((31-36)^2) / 31) = 0, 806$

5) Decisión estadística: por cuanto 80,64% > 5.00%, se desestima la hipótesis H_0 y se estima H_1.

6) Conclusión: Se estima que el empleo de la cámara de reconocimiento facial vulnera la privacidad de los datos personales a través del consentimiento otorgado por el titular para que el rostro captado por la cámara sea tratado y, por la falta de regulación de su empleo.

Contrastación de la hipótesis especifica 2

Hipótesis alternativa (H_1): La falta de regulación del empleo de la cámara de reconocimiento facial vulnera de la privacidad de los datos personales, porque no están autorizadas para tratar captar, tratar y trasferir las imágenes del rostro de la persona.

Hipótesis nula (H_0): La falta de regulación del empleo de la cámara de reconocimiento facial NO vulnera de la privacidad de los datos personales, porque están autorizadas para tratar captar, tratar y trasferir las imágenes del rostro de la persona.

Tabla 7

Tabla de frecuencias observadas de las hipótesis específicas N° 2

Variables	Totalmente de acuerdo	Totalmente en desacuerdo	Total
Prueba de absorción atómica	34	10	44
Causas ineficacia prueba absorción atómica	34	10	44
TOTALES	34	10	44

Nota. Elaboración propia.

Tabla 8

Tabla de frecuencias esperadas de las hipótesis específicas N° 2

Variables	Totalmente de acuerdo	Totalmente en desacuerdo	Total

Prueba de absorción atómica	38	06	44
Causas ineficacia prueba absorción atómica	38	06	44
TOTALES	38	06	44

Nota. Elaboración propia.

Método de contrastación:

El método de contrastación fue el siguiente:

1) Supuestos: La muestra fue aleatoria simple, constituida por 44 sujetos

2) Estadística de contrastación:

$$X^2 = \sum \frac{(\text{Observed frequencies} - \text{Expected frequencies})^2}{\text{Expected frequencies}}$$

$$= \sum \frac{(Fo - Fe)^2}{Fe}$$

3) Criterio de decisión: desestimar la hipótesis nula (H_0) si X^2 es mayor o igual a 0.05 = 5.00% es decir, $X^2 = \geq 0.05 = 5.00\%$

4) Resultado de obtenido al resolver la estadística de contrastación:

$X^2 = ((34-38)^2) / 34) = 0{,}470$

5) Decisión estadística: por cuanto 47,05% > 5.00%, se desestima la hipótesis H_0 y se estima H_1.

6) Conclusión: Se estima que la falta de regulación del empleo de la cámara de reconocimiento facial vulnera de la privacidad de los datos personales, porque no están autorizadas para tratar captar, tratar y trasferir las imágenes del rostro de la persona.

V. Discusión de resultados

5.1. De la encuesta

a) Se ha podido validar la hipótesis general

De conformidad con la encuesta el 88% de los sujetos encuestados estuvo de acuerdo con que el empleo de la cámara de reconocimiento facial vulnera la privacidad de los datos personales a través del consentimiento otorgado por el titular para que el rostro captado por la cámara sea tratado y, por la falta de regulación de su empleo. La contrastación estadística de esta hipótesis posibilito su estimación, pues el valor de X^2 conforme al criterio de decisión estadístico fue mayor 0.05 = 5.00% esto es X^2= 0, 2571= 25,71% > 5.00%, conforme se había planteado inicialmente.

Este resultado es similar al presentado por Simón y Dorado (2022) quienes, al analizar las cámaras de reconocimiento facial bajo los parámetros de un juicio de proporcionalidad, aluden a que en su examen cobra mayor peso, la violación de los derechos fundamentales, la cual es irreparable y que puede abrir un portal cuya clausura con el tiempo no será sencilla. También coadyuvan este resultado Venturini y Garay (2021, p. 21), al aceptar que la cámara de reconocimiento facial transgrede el derecho a la protección de datos personales y a la privacidad. Finalmente, Arroyo (2019) al analizar las cámaras de reconocimiento facial, ubicadas en sitios públicos para colaborar con la seguridad, concluyo que: crea un peligro para la privacidad y tratamiento de datos personales de quienes transitan por los calles y sitios públicos y vulnera los derechos del individuo captado por la cámara, el cual se trasforma en sospecho al ser comparado y vigilado permanentemente, se puede conocer su identidad "se pierde el anonimato", es decir, de esta forma este mecanismo posibilita el conocimiento del nombre como el principal dato personal.

b) Se ha podido validar la hipótesis especifica N °1

De conformidad con la encuesta el 87% de los sujetos encuestados concordó con que el consentimiento del titular para que su rostro captado por la cámara de reconocimiento facial

sea tratado vulnera la privacidad de los datos personales, al permitir el acceso a los datos en todos los ámbitos de la vida de la persona. La contrastación estadística de esta hipótesis posibilito su estimación, pues el valor de X^2 conforme al criterio de decisión estadístico fue mayor 0.05 = 5.00% esto es X^2= 0.864= 80,64% > 5.00%, conforme se había planteado inicialmente.

Si bien este resultado no pudo ser contrastado, dado que es un aspecto que no ha sido investigado, se considera adecuado y no genera controversia dado que se encuentra respaldada por la doctrina y la Ley de protección de datos personales - Ley N° 29733 (2011) y su Reglamento -Decreto Supremo Nº 003-2013-JUS (2013), en la que se regula en el Titulo III, Capítulo I, artículos 11 y siguientes, de la que se extrae que corresponde a la expresión de la voluntad inequívoca, expresa, previa, etc. de la persona o usuario, para que sus datos sean tratados, para el caso de esta investigación, autorizando el tratamiento o procesamiento de su rostro por la cámara de reconocimiento facial, lo que conlleva a que con la imagen de rostro de la persona se acceda a las esferas de su vida familiar, laboral, social, profesional, etc.

c) Se ha podido validar la hipótesis especifica N° 2

De conformidad con la encuesta el 89% de los sujetos encuestados estuvo de acuerdo con que la falta de regulación del empleo de la cámara de reconocimiento facial vulnera la privacidad de los datos personales, porque no están autorizadas para tratar captar, tratar y trasferir las imágenes del rostro de la persona. La contrastación estadística de esta hipótesis posibilito su estimación, pues el valor de X^2 conforme al criterio de decisión estadístico fue mayor 0.05 = 5.00% esto es X^2= 0,470= 47,05% > 5.00%, conforme se había planteado inicialmente.

Este resultado es análogo a lo manifestado por Simón y Dorado (2022), en su artículo titulado Límites y garantías constitucionales frente a la identificación biométrica, precisaron que ésta, particularmente el reconocimiento facial, constituyen un procesamiento de datos con

rango especial, por lo que su empleo a futuro debe sobrepasar un riguroso juicio de constitucionalidad, el cual desde el enfoque de la persona se requiere que al encargado del procesamiento de datos se le deben haber asignado explícitamente y legalmente las facultades oficiales en esta esfera; así como el interés público alegado debe ser reconocido por ley. Otra coincidencia se encuentra en lo manifestado por Camelo (2021), con respecto a la regulación de esta metodología es trascendente, debido al peligro que supone para los usuarios son considerables, en vista no solo de los imple que es obtener los datos, sino, igualmente la contingencia de que se dé un ilícito procesamiento de la información, dado que no son técnicas totalmente eficientes y "poseen altos márgenes de error". En el mismo sentido vi) la inexistencia de protocolos para reducir los peligros que supone afecta el debido proceso Arroyo (2019) al señalar como uno de los problemas que representa la cámara de reconocimiento facial consiste en la inexistencia de protocolos para reducir los peligros que supone afecta el debido proceso.

VI. Conclusiones

6.1. El empleo de la cámara de reconocimiento facial constituye un peligro latente para los Derechos Fundamentales de las personas por cuanto, no cuentan con mecanismos que

impidan el acceso ilegal a ellos, por el contrario, con fácilmente franqueables posibilitando entre otros la vulneración a la privacidad de los datos personales, el derecho a la no discriminación, la vulneración de la presunción de inocencia, etc. sin que sus productores implementen mecanismos para solucionar esta problemática, pues los mueve únicamente la finalidad de perfeccionar su funcionamiento.

6.2. En cuanto a la vulneración del derecho a la privacidad de los datos personales, en Perú se logró establecer que ello se produce esencialmente por dos motivos: por el consentimiento del titular para su rostro sea procesado o tratado por la cámara de reconocimiento facial y por la falta de regulación de su empleo y/ funcionamiento, pues ellos facilitan que a través del rostro de una persona se conozcan sus datos: personales, familiares, profesionales, su origen étnico, el culto que profesa, etc., etc., etc.

6.3. Aunque parezca absurdo, el consentimiento del titular para que su rostro sea tratado o procesado a través de un sistema de reconocimiento facial, vulnera la privacidad de sus datos personales porque al usuario no se le ha informado explícitamente: en que consiste esta técnica y lo sencillo que resulta que a través de su cara almacenada en un banco datos, las personas puedan acceder a esa información que no se desea compartir públicamente, sino que está reservada para su entorno familiar o para personas a las que conscientemente se les ha permitido conocer, *verbi gratia* cotejando la fotografía captada por la cámara de reconocimiento facial, con las imágenes almacenadas en base de datos oficiales o privadas se puede conocer la identidad completa de las persona, el número de D.N.I., la dirección de la residencia, la identidad de los padres, la edad, etc.

6.4. El acceso a la información en base de datos pública, es posible por cuanto la RENIEC, previo convenio con instituciones públicas o privad, en el que se debe indicar conforme a su giro de negocios o actividad requiere acceder a la información de una persona, constituida por sus el (los) prenombre (s), apellidos, número y expedición del documento de

identificación, “fecha y lugar de nacimiento, estatura, sexo, estado civil, grado de instrucción, nombres del padre y de la madre, fotografía, dirección y domicilio declarado”. (Morachimo, 2018), a cambio de pagar la tasa correspondiente; y en las redes sociales a través del etiquetado de las fotografías subidas.

6.5. La falta de regulación del empleo cámara de reconocimiento facial vulnera el derecho a la privacidad de los datos personales, por cuanto no existe una norma que imponga el protocolo para su empleo, así como las restricciones a los operadores de las bases de datos en los que se almacenan los rostros de los usuarios para su trasferencia y conforme al principio constitucional conforme el cual “Nadie está obligado a hacer lo que la ley no manda, ni impedido de hacer lo que ella no prohíbe”. (Constitución Política del Perú, Art. 2, 1993), el Estado no puede intervenir en esta actividad.

VII. Recomendaciones

Para enfrentar la problemática de vulneración de la privacidad de datos personales por el empleo de las cámaras de reconocimiento facial, se hace necesario:

7.1. Que la Autoridad Nacional de Protección de Datos Personales en ejercicio de lo previsto el numeral 12 del artículo 33 de la Ley N° 29733 (2011), emita una Directiva aprobada por la Resolución Directoral correspondiente en la que se apruebe el protocolo para el empleo de las cámaras de reconocimiento facial, con especial énfasis en el tratamiento y trasferencia de las imágenes del rostro captadas, catalogadas por esta mima normativa como datos sensibles para que puedan ser procesadas a través de este sistema.

7.2. Que la Autoridad Nacional de Protección de Datos Personales cumpla con las obligaciones impuestas: i) por el numeral 4 del artículo 33 y publique en su página institucional la relación de los Bancos de datos públicos y privados pues, en la actualidad solo se puede acceder a ello proporcionando el nombre de la base de datos y su registro; de manera que las personas puedan corroborar que la base en la que se insertan sus datos cuenta con la respectiva autorización y de ser necesario pueda ejercer los derechos que la propia Ley concede a los usuarios: acceso, rectificación, corrección y oposición; y, ii) por el numeral 5 fomentando campanas de educación y protección del rostro de las personas tratados o procesados en las bases de datos personales, pues en la actualidad las personas no son conscientes de los riesgos que ello implica para la privacidad de sus datos personales.

VIII. Referencias

Andina (11 de abril de 2019). Gamarra cuenta con cámaras de seguridad con reconocimiento facial. *Agencia peruana de noticias.*

https://www.andina.pe/agencia/noticia-gamarra-cuenta-camaras-seguridad-reconocimiento-facial-748323.aspx

Arroyo, V. (14 de noviembre de 2019). Cámaras con reconocimiento facial en Lima. *Accessnow*. https://www.accessnow.org/camaras-con-reconocimiento-facial-en-lima/

Bautista, M. (2015). *El derecho a la intimidad y su disponibilidad públic*a. Editorial Universidad Católica de Colombia.

Benítez, R., Escudero, G., Kanaan, S. y Masip, D. (2013). *Inteligencia Artificial avanzada.* Editorial UOC.

Bennett, C. y Raab, Ch. (2003). *The Governance of privacy. Policy instruments in global perspective*. (7ª ed.). Routledge.

Binford, T., Kumar, J., Nedumaan, J., Lepika, J., Ruby, J. y Tisa, J. (2019*). Modern deep learning and advanced computer vision: a perspective approach*. Editor Intel.

Boden, M. (2022). *Inteligencia artificial*. (1ª ed.). Ediciones Turner.

Camelo, A. (2021). "*Tecnología de reconocimiento facial en Colombia: Un análisis regulatorio en relación con la protección de los datos personales en el sector privado".* [Tesis de Materia, Universidad de los Andes]. http://hdl.handle.net/1992/53644

Carrión, R. (2009). "*Desarrollo de un algoritmo de clasificación de la huella dactilar para la Policía Nacional del Perú"*. [Tesis pregrado] Pontificia Universidad Católica del Perú. htttps://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/535

Carta de los Derechos Fundamentales de la Unión Europea [CDFUE]. (2000). *Parlamento Europeo, el consejo unión europea y la comisión.* Diario Oficial de las comunidades europeas.

Chanamé, R. (2003). "*Hábeas data y el derecho fundamental a la intimidad de la persona"*. [Tesis de Maestría, Universidad Nacional Mayor de San Marcos]. https://sisbib.unmsm.edu.pe/bibvirtual/tesis/human/chaname_or/chaname_or.htm

Chanamé, R. (2015). *La Constitución comentada*. (9ª ed.). Ediciones Legales E.I.R.L.

Código Civil Decreto Legislativo Nº 957, 14 de noviembre de 1984 (Perú). http://www.abrahamlincoln.pe/normas/ETT/NL2.pdf

Código Penal (2004). Decreto Legislativo Nº 957. Jurisprudencia del art. 271.3. Audiencia y resolución. 29 de julio de 2004 (Perú). https://www.gob.pe/institucion/presidencia/normas-legales/344687-957

Constitución Política del Perú [Const]. 29 de diciembre de 1993. https://www.congreso.gob.pe/Docs/files/documentos/constitucion1993-01.pdf

Convención Americana sobre Derechos Humanos. (22 de noviembre de 1969). Asamblea legislativa de la Republica de Costa Rica. https://www.corteidh.or.cr/tablas/17229a.pdf

Corral, H. (2000). Configuración jurídica del derecho a la privacidad: Origen, desarrollo y fundamentos. *Revista Chilena de Derecho*,*27*(1), pp. 331-355. https://repositorio.uc.cl/handle/11534/14800

Corte Constitucional de Colombia, Sentencia T 787-04 (18 de agosto de 2004). https://www.corteconstitucional.gov.co/relatoria/2004/t-787-04.htm

Corte Constitucional de Colombia. Sentencia C-094/20 (3 de marzo de 2020). https://www.corteconstitucional.gov.co/Relatoria/2020/C-094-20.htm#_ftnref20

Declaración Americana de los Derechos y Deberes del Hombre. (1948). Comision Interamericana de derechos humanos. Organización de Estados Americanos. https://www.oas.org/es/cidh/mandato/basicos/declaracion.asp

Declaración Universal de Derechos Humanos, (10 de diciembre de 1948). Organización de las Naciones Unidas. https://www.un.org/es/about-us/universal-declaration-of-human-rights

Decreto Supremo Nº 003-2013-JUS. Ley de protección de datos personales. Diario Oficial El Peruano (21 de marzo de 2013). https://diariooficial.elperuano.pe/pdf/0036/ley-proteccion-datos-personales.pdf

Díaz, V. (2013). Sistemas biométricos en materia criminal: un estudio comparado. *Revista lus,7*(31), pp., 28-47. https://doi.org/10.35487/rius.v7i31.2013.19

Escolano, F., Cazorla, M., Alfonso, M., Colomina, O. y Lozano, M. (2003). *Inteligencia artificial: modelos técnicas y áreas de aplicación*. Ediciones Paraninfo.

Estrada, J. (2002). El derecho a la intimidad y su necesaria inclusión como garantía individual. *Órgano Informativo de la Comisión de Derechos Humanos del Estado de México,57(*9), pp. 1-14. http://www.ordenjuridico.gob.mx/Congreso/pdf/86.pdf

Expediente N° 6712-2005- HC/TC-Lima. (17 de octubre de 2005). Tribunal Constitucional del Perú. https://www.tc.gob.pe/jurisprudencia/2006/06712-2005-HC.pdf

Falcón, E. (1996). *Habeas data. Concepto y procedimiento.* (1ª ed.). Editorial Abeledo Perrot.

Fernández, C. (2019). El nuevo concepto de privacidad: la transformación estructural de la visibilidad. *Revista de Estudios Políticos* (185), pp. 139-167. https://recyt.fecyt.es/index.php/RevEsPol/article/view/74389

Ferreira, D. (1982). *El derecho a la intimidad*. Editorial Universidad.

Galindo, D., Huaringa, S. y Samaniego, G. (2021). "Reconocimiento facial para la identificación *de los alumnos en exámenes finales en la modalidad presencial de la*

Universidad Continental – Huancayo, 2021". [Tesis pregrado] Universidad Continental. https://repositorio.continental.edu.pe/handle/20.500.12394/11570

Galván, M., Huerta, M. y Mancilla, M. (2015). *"Sistema biométrico aplicado a la gestión de accesos mediante visión artificial"*. [Tesis pregrado] Instituto Politécnico Nacional. http://tesis.ipn.mx/handle/123456789/22363

García, D. (2013). *Artículo 16 Constitucional Derecho a la Privacidad*. Instituto de Investigaciones Jurídicas, Suprema Corte de Justicia de la Nación, Fundación Konrad Adenauer .https://archivos.juridicas.unam.mx/www/bjv/libros/8/3567/39.pdf

Garvie, C., Bedoya, A. y Frankle, J. (2016). *The Perpetual Line- Up. Unregulated Police face recognition in America*. Georgetown Law, Center on Privacy y Technology.

Gestión. (30 de mayo de 2022) Descubren venta de datos bancarios y personales de 1 millón de peruanos en Wilson. *Redacción Gestión.* https://gestion.pe/noticias/filtracion-de-datos/

Goldestein, A., Harmon, L. y Lesk, A. (1970). *Identification of Human Faces.* Publisher IEEE.

Guerrero, C. (22 de setiembre de 2020). Denunciamos a la Universidad Nacional Mayor de San Marcos por el uso de software biométrico en su examen virtual. *Hiperderecho* https://hiperderecho.org/2020/09/denunciamos-a-la-universidad-nacional-mayor-de-san-marcos-por-el-uso-de-software-biometrico-en-su-examen-virtual/

Hannover, C. (2004): *Corte Europea de Derechos Humanos*. Aplicación N.º 59320/00.

Herrán, A. (2003). El derecho a la Protección de datos personales en la sociedad de la información. *Cuadernos Deusto de Derechos Humanos* (26), pp. 9-21. https://dialnet.unirioja.es/servlet/libro?codigo=114845

Kant, I. (1946). *Fundamentación de la metafísica de las costumbres*. Editorial Espasa Calpe.

Kant, I. (1988). *Crítica de la razón pura.* Ediciones Alfaguara.

Kant, I. (1989). *Metafísica de las costumbres*. Editorial TECNOS.

Kant, I. (1997). *Crítica de la razón práctica.* Editorial Sígueme.

Korff, D. y Georges, M. (2019*).* El Manual del DPD (delegado de Protección de Datos). Guía para los delegados de Protección de Datos en los sectores públicos y semi-públicos sobre cómo garantizar el cumplimiento del Reglamento General de Protección de Datos de la Unión Europea (Reglamento (UE) 2016/679). https://www.aepd.es/es/documento/el-manual-del-dpd-korffgeorges-esp.pdf

Lechner, M. (2016). Tecnologías aplicadas a la seguridad ciudadana: desafíos para la justicia transicional ante nuevos mecanismos de control social. *Revista Divulgatio,1*(1), pp. 21-36. https://dialnet.unirioja.es/servlet/articulo?codigo=7882752

Ley N° 26979 – Ley de Procedimiento de Ejecución Coactiva. (21 de setiembre de 1998). Congreso de la República del Perú. https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/1293121-26979

Ley N° 27444 – Ley Procedimiento Administrativo General. (10 de abril de 2001). Congreso de la República del Perú. https://www4.congreso.gob.pe/historico/cip/materiales/delitos_omision/ley27444.pdf

Ley N° 27806 – Ley de Ley de Transparencia y Acceso a la Información Pública. (02 de agosto de 2002). Congreso de la República del Perú. https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/118374-27806

Ley N° 29733 – Ley de protección de datos personales (14 de junio de 2011). Congreso de la República del Perú.

https://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

Llerena, J, y La Madrid, A. (2021). **"***Guía de estandarización con especificaciones técnicas de las cámaras de video vigilancia, ubicación y posicionamiento para enfrentar la ineficaz identificación facial en la sección de reconocimiento facial digitalizado de la DIRCRI-PNP de Lima Metropolita 2017-2019".* [Tesis de Maestría, Pontificia Universidad Católica del Perú].

http://hdl.handle.net/20.500.12404/21428

Martínez, R. (2004). *Una aproximación critica a la autodeterminación informática*. Editores Civitas.

Megías, J. (2002). Privacidad e internet: intimidad, comunicaciones y datos personales. *Anuario de derechos humanos*, (3), pp. 515-560.

htttps://dialnet.unirioja.es/servlet/articulo?codigo=939136

Morachimo, M. (26 de julio de 2018). ¿Cómo así RENIEC vende nuestros datos personales? *HIPERDERECHO*

https://hiperderecho.org/2018/07/como-asi-reniec-vende-nuestros-datos-personales/

Neyra, M. (2019). "*Sistema de reconocimiento facial para el control de acceso de estudiantes a los laboratorios de la FIIS-UNAC, 2019"*. [Tesis pregrado] Universidad Cesar Vallejo.

https://hdl.handle.net/20.500.12692/44310

Nissenbaum, H. (2009). *Privacy in context: Technology, policy and the integrity of social life*. Stanford University Press.

Ortiz, A. (2010). *"Mejora de imágenes de huellas digitales"*. [Tesis pregrado] Pontificia Universidad Católica del Perú.

http://hdl.handle.net/20.500.12404/540

Pacto Internacional de Derechos Civiles y Políticos. (1966). (10 de diciembre de 1948). Asamblea General de las Naciones Unidas. https://docplayer.es/35657925-Los-imperativos-en-la-filosofia-kantiana-the-imperatives-in-kantian-philosophy.html

Quiroz, R. (2016). El Hábeas data, protección al derecho a la información y a la autodeterminación informativa. *Letras*,*87*(126), pp. 23-27. http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S2071-50722016000200002

Real Academia Española [RAE]. (2022). *Diccionario de la Lengua española.* Edición del tricentenario. https://dle.rae.es/privado?m=form

Rebollo, L. (2005). *El derecho fundamental a la intimidad.* (2ª ed.). Dykinson.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. (27 de abril de 2016). Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=es

Resolucion A/HRC/28/L.27, (24 de marzo de 2015). El derecho a la privacidad en la era digital. Asamblea General – Oficina de Derechos Humanos de las Naciones Unidas. http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_28_L27.pdf

Rivera, F. (2004). El imperativo categórico en la fundamentación de la Metafísica de las Costumbres. *Revista Digital Universitaria,5*(11), pp. 2-6. https://www.revista.unam.mx/vol.5/num11/art81/dic_art81.pdf

Rojas, C. (2015). Los imperativos en la filosofía kantiana. *DIKAIOSYNE* (30), pp. 117-126. *Revista de filosofía práctica Universidad de Los Andes.*

https://docplayer.es/35657925-Los-imperativos-en-la-filosofia-kantiana-the-imperatives-in-kantian-philosophy.html

Rouhiainen, L. (2018). *Inteligencia artificial: 101 cosas que debes saber hoy sobre nuestro futuro*. Editorial Planeta.

Simón, P. y Dorado, X. (2022). Límites y garantías constitucionales frente a la identificación biométrica. *Revista de Internet, Derecho y Política* (35), pp. 1-13. https://doi.org/10.7238/idp.v0i35.392324

Sirovich, L. y Kirby, M. (1988). Low-dimensional procedure for the characterization of human faces. *Journal of The Optical Society of America A-optics Image Science and Vision,4*(3), pp. 519-527. https://www.semanticscholar.org/paper/Low-dimensional-procedure-for-the-characterization-Sirovich-Kirby/2a62d0cca2fabf1d6f6ee15e4c14cef415b657d1

Thill, E. (2011). El rol de la identificación de personas en las políticas de desarrollo e inclusión digital: el Marco para la Identificación Electrónica Social Iberoamericana. En E. Thill (Comp.), *Biometrías 2* (pp. 11-23). Jefatura de Gabinete de ministros.

Toscano, M. (2017). Sobre el concepto de privacidad: la relación entre privacidad e intimidad. *Isegoría. Revista de Filosofía Moral y Política* (57), pp. 533-552. https://isegoria.revistas.csic.es/index.php/isegoria/article/view/994/990

Turk, M. y Pentland, A. (1991). Eigenfaces for Recognition. *Journal of cognitive neuroscience,3*(1), pp. 71 - 86. https://www.scirp.org/(S(i43dyn45teexjx455qlt3d2q))/reference/ReferencesPapers.aspx?ReferenceID=23700

Una breve historia del reconocimiento facial (2019). [Blog] *VISION* . https://spotcloud.medium.com/una-breve-historia-del-reconocimiento-facial-vision-blog-5a76fdfe4865

Vázquez, M. (2014). "*Sistema de reconocimiento facial mediante técnicas de visión tridimensional"*. [Tesis de Maestría, Centro de Investigaciones en óptica, A.C]. https://cio.repositorioinstitucional.mx/jspui/bitstream/1002/436/1/15950.pdf

Venturini, J. y Garay, V. (2021). *Reconocimiento facial en América Latina: tendencias en la implementación de una tecnología perversa.* A1sur.

Villena, D. (2022). Dirección de protección de datos personales sanciona a la Municipalidad de La Victoria por no cumplir con medidas de seguridad en sus cámaras de videovigilancia. *Hiperderecho.* https://hiperderecho.org/2022/07/direccion-de-proteccion-de-datos-personales-sanciona-a-la-municipalidad-de-la-victoria-por-no-cumplir-con-medidas-de-seguridad-en-sus-camaras-de-videovigilancia/

Vítores, S. (2018). Privacidad. *Cadena SER* https://cadenaser.com/programa/2018/09/27/hora_25/1538077085_587111.html

Warren, S. y Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review,4*(5), pp. 193–220. https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

Zavala, M. (1982). *El derecho a la intimidad*. Editorial Abeledo Perrot.

IX. ANEXOS:

Anexo A: Matriz de consistencia

"VULNERACIÓN DE LA PRIVACIDAD DE DATOS PERSONALES POR EMPLEO DE LA CÁMARA DE RECONOCIMIENTO FACIAL"

PROBLEMAS	OBJETIVOS	HIPÓTESIS	MÉTODO
PROBLEMA GENERAL ¿Cuáles son los motivos por los que el empleo de la cámara de reconocimiento facial vulnera de la privacidad de los datos personales? **PROBLEMAS ESPECÍFICOS** 1. ¿Por qué motivo el consentimiento del titular para que el rostro captado por la cámara de reconocimiento facial sea tratado vulnera de la privacidad de los datos personales? 2. ¿Por qué causa la falta de regulación del empleo de la cámara de reconocimiento facial vulnera de la privacidad de los datos personales?	**OBJETIVO GENERAL** Exponer los motivos por los que el empleo de la cámara de reconocimiento facial vulnera la privacidad de los datos personales. **OBJETIVOS ESPECÍFICOS** 1. Explicar el motivo por el que el consentimiento del titular para que el rostro captado por la cámara de reconocimiento facial sea tratado vulnera de la privacidad de los datos personales 2. Indicar el motivo por el cual la falta de protocolos para el empleo de la cámara de reconocimiento facial vulnera de la privacidad de los datos personales.	**HIPÓTESIS GENERAL** El empleo de la cámara de reconocimiento facial vulnera la privacidad de los datos personales a través del consentimiento otorgado por el titular para que el rostro captado por la cámara sea tratado y, por la falta de regulación de su empleo. **HIPÓTEIS ESPECÍFICAS** 1) El consentimiento otorgado por el titular para que el rostro captado por la cámara de reconocimiento facial sea tratado vulnera la privacidad de los datos personales, al permitir el acceso a los datos en todos los ámbitos de la vida de la persona. 2) La falta de regulación del empleo de la cámara de reconocimiento facial vulnera de la privacidad de los datos personales, porque no están autorizadas para tratar captar, tratar y trasferir las imágenes del rostro de la persona.	Enfoque investigación: cuantitativo Tipo de investigación básico. Nivel de investigación: explicativo. Diseño de investigación: no experimental. La población: 50 sujetos La muestra 59 sujetos. Instrumento: cuestionario. Métodos: exegético, histórico y sistemático. Análisis de datos: programa SPSS, gráficos y tablas.

Anexo B. Matriz operacionalización de variables

VARIABLE	DEFINICION CONCEPTUAL	DEFINICION OPERACIONAL	INDICADORES
INDEPENDIENTE **X. PRIVACIDAD DE DATOS PERSONALES**	Toda información que identifica o hace identificable a una persona natural y que solo puede ser conocida por voluntad de su titular, como: el nombre, D.N.I., edad, sexo, localización, clase social, de naturaleza médica, profesional, financiera "numérica, alfabética, gráfica, fotográfica, etc.	Se medirá en encuesta	X.1. Derecho fundamental X.2. Protección legal X.3. Información privada
DEPENDIENTE **Y. EMPLEO DE CÁMARA DE RECONOCIMIENTO FACIAL.**	Forma de identificación biométrica que opera con un dispositivo que hace parte de un sistema dotado de un software que se usa para que, a partir de la comparación en tiempo real o por medio de fotografías o videos o cualquier medio audiovisual, de los rasgos del rostro puede identificar a una persona.	Se medirá en la Encuesta	Y.1. Consentimiento del Titular. Y.2. Trasferencia de datos Y.3. Falta de regulación

Anexo C: Instrumento: encuesta

Instrucciones generales:

Esta encuesta es personal y absolutamente anónima, agradezco de antemano dar su respuesta con la mayor transparencia y veracidad a las diversas preguntas del cuestionario, todo lo cual permitirá tener un acercamiento científico respecto a la privacidad de datos personales y el empleo de la Cámara de Reconocimiento Facial.

Para contestar considere la siguiente Escala Likert:

1= Totalmente en desacuerdo

2= En Desacuerdo

3= Neutral

4= De acuerdo

5= Totalmente de acuerdo

No.	PREGUNTA	1	2	3	4	5
	VARIABLE INDEPENDIENTE. PRIVACIDAD DE DATOS PERSONALES					
01	¿Sabía que la privacidad de datos personales es un Derecho Fundamental?					
02	¿Está de acuerdo con que los derechos fundamentales tienen protección reforzada?					
03	¿Concuerda Ud. con que la privacidad de los datos personales está protegida legalmente por Ley de protección de datos personales?					
04	¿Concuerda con que los datos personales corresponden a información privada del individuo?					
05	¿Está de acuerdo con que los datos personales solo pueden divulgarse sino por voluntad de su titular?					
06	¿Está de acuerdo con que el tratamiento del rostro de la persona permite conocer todos sus datos personales?					
	VARIABLE INDEPENDIENTE. EMPLEO DE CÁMARA DE RECONOCIMIENTO FACIAL					
07	¿Sabía Ud. que para que el rostro de una persona sea captado por la cámara de reconocimiento facial se necesita de su consentimiento?					
08	¿Concuerda Ud. con que el consentimiento referido en el numeral anterior debe ser claro, expreso y previo?					
09	¿Sabia Ud. que luego reconocido el rostro por la cámara de reconocimiento facial se convierte en un dato personal?					
10	¿Concuerda Ud. el rostro como dato personal puede ser trasferido?					
11	¿Sabia Ud. que la trasferencia de datos personales puede darse a nivel nacional y/o internacional?					

12	¿Conocía Ud. que el empleo de cámara de reconocimiento facial en Perú no está regulado?					
13	¿Está de acuerdo con que el empleo de la cámara de reconocimiento facial vulnera la privacidad de los datos personales a través del consentimiento otorgado por el titular para que el rostro captado por la cámara sea tratado y, por la falta de regulación de su empleo?					
14	¿Concuerda con que el consentimiento del titular para que su rostro captado por la cámara de reconocimiento facial sea tratado vulnera la privacidad de los datos personales, al permitir el acceso a los datos en todos los ámbitos de la vida de la persona?					
15	¿Está de acuerdo con que la falta de regulación del empleo de la cámara de reconocimiento facial vulnera la privacidad de los datos personales, porque no están autorizadas para tratar captar, tratar y trasferir las imágenes del rostro de la persona?					

Anexo D: Validación instrumento por experto

Luego de examinado el instrumento empleado en la investigación titulada titulado: "Vulneración de la privacidad de datos personales por empleo de la Cámara de Reconocimiento Facial", presentó la siguiente evaluación:

INDICADORES	CRITERIOS CUALITATIVOS/CUANTITATIVOS	Deficiente 0-20%	Regular 21-40%	Bueno 41-60%	Muy Bueno 61-80%	Excelente 81-100%
1. CLARIDAD	Se formulo con lenguaje apropiado.					90
2. OBJETIVIDAD	Expreso conductas observables.					90
3. ACTUALIDAD	Adecuado al alcance de ciencia y tecnología.					90
4. ORGANIZACIÓN	Existe una organización lógica.					90
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					90
6. INTENCIONALIDAD	Adecuado para valorar aspectos del estudio.					90
7. CONSISTENCIA	Basados en aspectos teóricos-científicos y del tema de estudio.					90
8. COHERENCIA	Entre los índices, indicadores, dimensiones y variables.					90
9. METODOLOGIA	La estrategia responde al propósito del estudio.					90
10. CONVENIENCIA	Genera nuevas pautas en la investigación y construcción de teorías.					90
	SUB TOTAL					90
	TOTAL					90

Opinión de aplicabilidad: Se recomienda aplicar el instrumento por cumplir los requisitos correspondientes.

Validado por: Dr. Efraín Jaime Guardia Huamani (Asesor)

Anexo E: Confiabilidad del instrumento establecida por experto

El instrumento de la Tesis denominada: **"**Vulneración de la privacidad de datos personales por empleo de la cámara de reconocimiento facial", ha obtenido un coeficiente Alfa de Cronbach razonable, lo cual favorece la aplicación de dicho instrumento.

Determinación del coeficiente de confiabilidad

Variables	Coeficiente Alfa de Cronbach	Número de ítems
Privacidad de los datos personales facial	0, 8918	06
Empleo de la cámara de reconocimiento facial	0, 8968	09
Total	**0, 8905**	**15**

Estas son las conclusiones sobre el coeficiente confiabilidad:

1) Para la Variable independiente: Privacidad de los datos personales facial, el valor del coeficiente es de 0.8918, lo que indica alta confiabilidad.

2) Para la variable dependiente: Empleo de la cámara de reconocimiento facial, el valor del coeficiente es de 0.8968, lo que indica una alta confiabilidad.

3) El coeficiente Alfa de Cronbach para la escala total es de 0.8905, lo cual indica una alta confiabilidad del instrumento.

4) Finalmente, la confiabilidad, tanto de la escala total, como de las dos variables en particular, presentan valores que hacen que el instrumento pueda ser útil para alcanzar los objetivos de la investigación

Comentario:

El 89% de confiabilidad del Alpha de Cronbach para el instrumento de investigación del trabajo le da un alto grado de coherencia en la formulación del instrumento de investigación; lo cual se condice con la validación de los expertos académicos.

De este modo, se entiende que los resultados obtenidos con el instrumento en una determinada ocasión, bajo ciertas condiciones, serán similares si se volviera a medir las mismas variables en condiciones idénticas.

Por tanto, este aspecto de la razonable exactitud con que el instrumento mide lo que se ha pretendido medir es lo que se denomina la confiabilidad del instrumento, la misma que se cumple con el instrumento de encuesta de este trabajo.

Confirmada la confiabilidad del instrumento por el asesor

Dr. Efraín Jaime Guardia Huamani

Docente de la Universidad Nacional Federico Villarreal- Lima – Perú.