Maestría en

Derecho Digital

Trabajo de investigación previo a la obtención del título de

Magíster en Derecho Digital con mención en Innovación Jurídica y Legaltch

AUTORES:

Irina Katyuska Silva Echeverría

Gary Alejandro Loor Escobar

Byron Ramiro Villarreal Narváez

Gisela Esperanza Barreiro Cedeño

TUTORES:

Docente titulación

Profesor PBL 1 Francisco Játiva

Profesor PBL 2 Cristian Fabián Martínez Sánchez

Profesor PBL 3 Juan Manuel Faramiñan

El Reconocimiento Facial y su Tratamiento en la Seguridad Pública en el Ecuador

Quito, (enero 2025)

Certificación de autoría

Nosotros, Gisela Esperanza Barreiro Cedeño, Gary Alejandro Loor Escobar, Irina Katyuska Silva Echeverría, Byron Ramiro Villarreal Narváez**,** declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedemos nuestros derechos de propiedad intelectual a la Universidad Internacional del Ecuador (UIDE), para que sea publicado y divulgado en internet, según lo establecido en la Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación (COESCCI), su reglamento y demás disposiciones legales.

Firmado electrónicamente por:
GISELA ESPERANZA BARREIRO CEDENO

Firma del graduando

Gisela Esperanza Barreiro Cedeño

Firmado electrónicamente por:
GARY ALEJANDRO LOOR ESCOBAR

Firma del graduando

Gary Alejandro Loor Escobar

Firmado electrónicamente por:
IRINA KATYUSKA SILVA ECHEVERRIA

Firma del graduando

Irina Katyuska Silva Echeverría

Firmado electrónicamente por:
BYRON RAMIRO VILLARREAL NARVAEZ

Firma del graduando

Byron Ramiro Villarreal Narváez

Autorización

Nosotros, Gisela Esperanza Barreiro Cedeño, Gary Alejandro Loor Escobar, Irina Katyuska Silva Echeverría, Byron Ramiro Villarreal Narváez**,** en calidad de autores del trabajo de investigación titulado ***El Reconocimiento Facial y su Tratamiento en la Seguridad Pública en el Ecuador***, autorizamos a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que nos pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autores nos corresponden, lo establecido Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación (COESCCI) y su Reglamento en Ecuador.

D. M. Quito, (mes año)

Firmado electrónicamente por:
GISELA ESPERANZA BARREIRO CEDENO

Firma del graduando

Gisela Esperanza Barreiro Cedeño

Firmado electrónicamente por:
GARY ALEJANDRO LOOR ESCOBAR

Firma del graduando

Gary Alejandro Loor Escobar

Firmado electrónicamente por:
IRINA KATYUSKA SILVA ECHEVERRIA

Firma del graduando

Irina Katyuska Silva Echeverría

Firmado electrónicamente por:
BYRON RAMIRO VILLARREAL NARVAEZ

Firma del graduando

Byron Ramiro Villarreal Narváez

Aprobación de dirección y coordinación del programa

Nosotros, Juan Manuel de Farmiñán Fernández – Fígares **y Francisco Játiva Yánez,** declaramos que los graduandos: Gisela Esperanza Barreiro Cedeño, Gary Alejandro Loor Escobar, Irina Katyuska Silva Echeverría, Byron Ramiro Villarreal Narváez son los autores exclusivos de la presente investigación y que ésta es original, auténtica y personal de ellos.

DE FARAMIÑAN FERNANDEZ-FIGARES JUAN MANUEL - 74666256E

Firmado digitalmente por DE FARAMIÑAN FERNANDEZ-FIGARES JUAN MANUEL - 74666256E
Fecha: 2025.03.24 08:39:48 +01'00'

Firmado electrónicamente por: FRANCISCO JOSE JATIVA YANEZ

Juan Manuel Faramiñán Fenández-Fígares
Director de la
Maestría en Derecho Digital con mención
Innovación Legal y Nuevas Tecnologías

Francisco Játiva Yánez
Coordinador de la
Maestría en Derecho Digital con mención
Innovación Legal y Nuevas Tecnologías

DEDICATORIA

A todas las personas que han hecho posible llegar a este momento y que cada una con su granito se han convertido en parte de este gran proyecto.

AGRADECIMIENTOS

A todas las personas que han hecho posible llegar a este momento, gracias a su colaboración y sacrificio; de manera especial el agradecimiento a la Universidad y a sus excelentes docentes que han sabido transmitir sus conocimientos de manera extraordinaria.

RESUMEN

La creciente inseguridad en Ecuador ha motivado a la Policía Nacional a implementar sistemas de videovigilancia con reconocimiento facial para identificar y rastrear a individuos en espacios públicos, contribuyendo a la seguridad y prevención del delito. Sin embargo, el uso de esta tecnología plantea preocupaciones en cuanto a la intimidad y protección de datos biométricos de los ciudadanos, especialmente ante la falta de una normativa específica que la regule. La investigación busca evaluar si el uso de esta tecnología por parte de la Policía Nacional del Ecuador es legítimo y compatible con los derechos fundamentales, y examina normativas nacionales e internacionales relevantes, como el Reglamento de IA de la Unión Europea. Además, se revisan estudios y casos internacionales que subrayan la importancia de una regulación que evite la vigilancia masiva y proteja contra posibles abusos. Este proyecto tiene como fin contribuir a políticas públicas en Ecuador que garantiza un equilibrio entre la seguridad ciudadana y los derechos humanos, promoviendo el uso responsable del reconocimiento facial en la seguridad pública.

Palabras Clave: Seguridad pública, videovigilancia, reconocimiento facial, datos personales, dato biométrico, legalidad, proporcionalidad, transparencia.

ABSTRACT

The growing insecurity in Ecuador has motivated the National Police to implement video surveillance systems with facial recognition to identify and track individuals in public spaces, contributing to security and crime prevention. However, the use of this technology raises concerns regarding the privacy and protection of citizens' biometric data, especially in the absence of specific regulations that regulate it. The research seeks to assess whether the use of this technology by the Ecuadorian National Police is legitimate and compatible with fundamental rights, and examines relevant national and international regulations, such as the European Union's AI Regulation. In addition, international studies and cases are reviewed that underscore the importance of regulation that prevents mass surveillance and protects against potential abuses. This project aims to contribute to public policies in Ecuador that guarantee a balance between citizen security and human rights, promoting the responsible use of facial recognition in public security.

***Keywords*:** Public security, video surveillance, facial recognition, personal data, biometric data, legality, proportionality, transparency.

TABLA DE CONTENIDOS

CAPITULO 1

INTRODUCCIÓN

Planteamiento del Problema e Importancia del Estudio

En los últimos años, la inseguridad ha aumentado de forma alarmante en Ecuador, se encuentra como uno de los países más inseguros de América Latina: de acuerdo con investigaciones realizadas en el año 2023 se reporta 7.878 (El Universo, 2024) muertes violentas. Reportes como el de Human Rights Watch, dejan entrever la gravedad de este problema, así una publicación hecha por Juanita Gobertus Estrada, Directora de la División de las Américas, señala que en Ecuador existe una crisis de violencia, la cual ha alcanzado niveles alarmantes, y señala enfáticamente que la tasa de homicidios ha aumentado en un 430% en cinco años, al tiempo que barrios enteros están en zozobra y a merced de grupos criminales organizados que reclutan a niños, matan jueces, fiscales, e inclusive matan a candidatos políticos, como el caso Villavicencio, sonado caso que causo verdadera alarma social, sin dejar a un lado que la delincuencia organizada también se infiltran en las mismas instituciones gubernamentales. Pese a que el gobierno anuncia que la tasa de homicidios ha disminuido en 2024 aproximadamente en un 17% en comparación con 2023, se muestra un aumento en las cifras de extorsión y secuestros en comparación con el mismo año. (Goebertus Estrada, 2025)

Este panorama ha impulsado a las autoridades a implementar diversas medidas tecnológicas para combatir el crimen y proteger a la ciudadanía. Entre estas tecnologías, el reconocimiento facial se ha posicionado como una opción de herramienta relevante dentro de los sistemas de videovigilancia de la Policía Nacional. Esta tecnología permitirá identificar y

rastrear individuos en espacios públicos mediante el análisis de patrones faciales, contribuyendo a la seguridad pública y la prevención de delitos. Sin embargo, el uso de esta tecnología ha suscitado una serie de preocupaciones en el contexto a la privacidad y la protección de datos personales, principalmente los considerados sensibles, como los datos biométricos.

La implementación de la herramienta de reconocimiento facial en el ámbito de la seguridad pública plantea un dilema en el que se deben equilibrar dos aspectos fundamentales: la necesidad de garantizar la seguridad ciudadana y el deber de respetar los derechos fundamentales, entre ellos el derecho a la privacidad y la protección de datos personales. En el contexto ecuatoriano, este equilibrio se vuelve especialmente complejo debido a la ausencia de una normativa específica y actualizada que regule de forma detallada el uso de tecnologías de vigilancia con reconocimiento facial y el tratamiento de los datos biométricos. Aunque existen leyes que abordan la protección de datos personales, como la Constitución (Registro Oficial 449, 20-10-2008) (Registro Oficial 449, 20-10-2008) y la Ley Orgánica de Protección de Datos Personales (Registro Oficial Suplemento 459, 26-05-2021) y su reglamento (Registro Oficial 435, 13-11-2023), estas aún no brindan un marco claro y exhaustivo que determina hasta qué punto el uso de esta tecnología por parte de la Policía Nacional es legítimo y, en particular, cómo debe garantizarse que no se vulneren derechos huma y constitucionales.

Además, la ciudadanía ecuatoriana muestra un respaldo general hacia el uso de sistemas de videovigilancia para mejorar la seguridad. Sin embargo, el desconocimiento sobre el manejo de los datos personales capturados en estos sistemas y la falta de transparencia

sobre su uso han generado inquietud y escepticismo. Esto subraya la importancia de contar con procedimientos claros y normativas específicas que permitan a los ciudadanos entender y confiar en el modo en que la tecnología de reconocimiento facial va a ser usada.

En este contexto, el presente proyecto de investigación pretende evaluar si la utilización de sistemas de videovigilancia con reconocimiento facial por parte de la Policía Nacional del Ecuador, con el fin de garantizar la seguridad ciudadana y el orden público, podría vulnerar derechos fundamentales de los ciudadanos. La pregunta central de esta investigación se plantea si la Policía Nacional cuenta con la legitimidad necesaria para emplear esta tecnología de vigilancia sin poner en riesgo los derechos constitucionales de los ciudadanos. La exploración de esta pregunta permitirá no solo comprender los mecanismos de seguridad y mecanismos que se aplican para el control criminal, sino también ofrecer recomendaciones para un uso responsable de esta tecnología.

Para ello, la investigación se enfoca en varios aspectos claves. En primer lugar, se analizarán los aspectos regulatorios existentes en Ecuador sobre la protección de datos personales y de seguridad pública, así también, se examinará el marco del Reglamento de Inteligencia Artificial de la Unión Europea, que establece lineamientos específicos sobre el uso de datos biométricos en actividades de seguridad pública, para entender en qué casos y en qué condiciones es posible y lícito el uso del reconocimiento facial. Con estos elementos, se pretende identificar retos legales de la protección de datos biométricos necesarios para garantizar que el uso de esta tecnología cumpla con los principios de legalidad, proporcionalidad y transparencia.

Por otra parte, esta incluye la revisión de estudios y análisis de casos previos sobre la implementación del reconocimiento facial en la seguridad pública, con especial énfasis en sus riesgos. En distintas regiones del mundo, el uso de esta tecnología ha generado controversias relacionadas con la invasión de la privacidad, lo cual destaca la importancia de establecer normas que delimiten el uso de estos sistemas de manera específica. Estas investigaciones evidencian la relevancia de adoptar un enfoque crítico y cauteloso al implementar la tecnología de reconocimiento facial, recomendando su uso únicamente en situaciones justificadas y bajo condiciones estrictas de regulación.

El objetivo principal de este proyecto es proporcionar una base sólida de conocimiento que permita contribuir al debate sobre la regulación del reconocimiento facial en el ámbito de la seguridad pública en Ecuador. Esta investigación busca no solo responder a la cuestión de la legitimidad del uso de dicha tecnología, sino también promover que su uso se enmarque en las garantías de los derechos humanos y las libertades fundamentales de los ciudadanos. En última instancia, se espera que los resultados obtenidos puedan aportar a la creación de políticas públicas que regulen de manera adecuada el tratamiento de datos biométricos, facilitando un uso responsable y respetuoso del reconocimiento facial en el contexto ecuatoriano.

Definición del Proyecto

La inseguridad en Ecuador ha impulsado el uso de videovigilancia con reconocimiento facial, lo que ha generado preocupación sobre la privacidad y protección de datos. Aunque la ciudadanía apoya que se implementen sistemas de videovigilancia en la ciudad, en sus barrios,

en espacios privados y públicos, para prevenir y advertir al delincuente que está siendo vigilado e identificable para su captura, generando en el ciudadano el uso de esta herramienta seguridad, pero desconocen cómo se gestionan los datos que se capturan.

Naturaleza o Tipo de Proyecto

Sin descuidar la necesidad de combatir la inseguridad en Ecuador, y para contrarrestar los modernos métodos y sistemas que utiliza la delincuencia, es preciso se norme a las instituciones competentes de la seguridad nacional. Esto garantizará que el uso de la información se realice, al menos, alineados a los estándares internacionales en materia de derechos humanos, aplicando los criterios de legalidad, proporcionalidad y necesidad de transparencia en el uso de la información.

La Policía Nacional reconoce su utilidad para combatir el crimen, pero también la necesidad de que su aplicación respete la Declaración Universal de Derechos Humanos y otros tratados internacionales sobre protección de derechos, la Constitución del Ecuador, y las leyes vigentes los derechos humanos. ¿La Policía Nacional está legitimada para utilizar sistemas de videovigilancia con reconocimiento facial para combatir delitos sin vulnerar derechos fundamentales de los ciudadanos?

Objetivos

Objetivo General

Describir, mediante el uso de instrumentos de investigación, si el tratamiento de datos biométricos de reconocimiento facial por parte de la Policía Nacional en su labor de combate al delito vulnera los derechos fundamentales de los ciudadanos.

Objetivos Específicos:

- Realizar un análisis normativo, doctrinario y crítico sobre los riesgos que implica para los ciudadanos la captura y uso de datos biométricos de reconocimiento facial por parte de la Policía Nacional en la lucha para combatir el delito.
- Conocer qué datos biométricos de reconocimiento facial se capturan, incluyendo el tiempo de permanencia de la información, y las medidas de protección legal aplicables, para no afectar los derechos fundamentales y constitucionales de las personas.

Justificación

Evaluar los riesgos del uso de videovigilancia y reconocimiento facial en Ecuador, donde aún no existe una normativa específica que proteja los derechos a la privacidad y la protección de datos sensibles. Su objetivo es establecer una base de conocimiento para futuros estudios, promoviendo un uso ético de estas tecnologías de seguridad, y contribuyendo al debate sobre cómo equilibrar la tecnología con los derechos humanos, conforme a estándares internacionales de legalidad, proporcionalidad y transparencia.

CAPITULO 2

METODOLOGÍA

La investigación utiliza una metodología de análisis normativo y revisión documental para examinar la protección de datos personales y sensibles en Ecuador. Evalúa la normativa nacional, como la Constitución, la Ley de Protección de Datos, su reglamento, así como las leyes relacionadas con la seguridad pública. Revisa protocolos de actuación policial y la política de privacidad en portales oficiales de la Policía Nacional para entender los términos de tratamiento de conservación. Analiza el alcance del Reglamento de IA de la Unión Europea, para determinar en qué casos es lícito recopilar datos biométricos mediante el reconocimiento facial.

Asimismo, se incluye análisis de estudios previos sobre el uso de reconocimiento facial en seguridad pública, destacando las vulneraciones legales sobre la privacidad y proponiendo su uso en situaciones limitadas y justificadas.

No podemos desconocer el desarrollo de las nuevas tecnologías y su uso tanto por parte de la sociedad civil como en el ámbito público, en este ámbito el reconocimiento facial nace como un elemento muy usado en seguridad para la protección de la ciudadanía, debido a que uso permitiría a la fuerza pública perseguir el crimen y anticipar las crecientes amenazas.

El sistema de videovigilancia en tiempo real, se implementó en las ciudades para prevenir el cometimiento de delitos, o al menos como elemento disuasorio. Con la evolución de la tecnología el sistema de videovigilancia puede contar con programas de reconocimiento facial que recopila y almacena patrones faciales , que en conjunción con las diferentes bases

de datos que están en poder de las instituciones públicas permite identificar a una persona, un infractor o a un presunto delincuente no solo en tiempo real, sino también que sirve para verificar el rastro o la huella de todo su accionar lo que permitiría determinar el potencial riesgo para la sociedad, agilitando las investigaciones.

Está claro que la tecnología no solo que ayuda a la fuerza pública a combatir el delito para la protección de la ciudadanía, pero surge una inquietud en el sentido de que si se justifica el obtener datos personales de diferentes bases en pro de garantizar la seguridad de la población, porque además no se conoce a ciencia cierta cuan efectiva es esta herramienta, sin dejar de ser preocupante el tratamiento que se está dando a estos datos, y la afectación que esto representa a los derechos fundamentales de los seres humanos como son el derecho a la a la intimidad.

De ahí que a nuestro criterio es importante conocer a través de una muestra la opinión de diferentes grupos etarios, a través de una encuesta, sobre si está de acuerdo con que se instalen sistemas de videovigilancia con reconocimiento facial en zonas públicas, si conoce sobre el tratamiento que se dan a los datos que se recogen, si conoce sobre los derechos que tenemos los ciudadanos a la intimidad consagrados en nuestra legislación, si conoce sobre el derecho que tienen los ciudadanos a solicitar a la entidad que recoge los datos personales el acceso a ellos, la rectificación, la cancelación y la oposición a su tratamiento de acuerdo a la Ley Orgánica de Protección de Datos Personales (Registro Oficial Suplemento 459, 26-05-2021), con miras a analizar las conclusiones que se han publicado en informes.

Las respuestas nos permiten analizar el conocimiento de las personas encuestadas para enforcar nuestra investigación a proponer recomendaciones que puedan garantizar la confidencialidad en el tratamiento de datos biométricos capturados a través de sistemas de videovigilancia por parte de la fuerza pública, cumpliendo con los requisitos elementales para precautelar la intimidad, y sobre todo que no se puedan usar con fines políticos, que los datos que se recojan sean los mínimos requeridos, que el tratamiento de esos datos sea para un objetivo específico autorizado, que una vez recogidos no se conserven datos que no sean estrictamente necesarios y que el acceso a los datos sea limitado estrictamente al personal autorizado.

Objetivo de la Encuesta

El objetivo de la encuesta es recopilar la percepción, conocimiento y preocupaciones del público en general sobre el uso del reconocimiento facial en la seguridad pública en Ecuador, centrándose en aspectos como la protección de datos personales, los beneficios percibidos y los riesgos asociados, para evaluar la aceptación de esta tecnología, sus implicaciones éticas y los desafíos legales y técnicos que enfrenta su implementación.

Diseño de la Encuesta

La encuesta se estructuró en cuatro secciones claves, con preguntas cerradas, para obtener información cuantitativa:

- Datos Demográficos: Recogió información sobre los participantes, solo por el rango edad, para identificar patrones de percepción del tema planteado.
- Conocimiento sobre Reconocimiento Facial: Evaluó el nivel de conocimiento de los

encuestados con la tecnología de video vigilancia con reconocimiento facial y su implementación en Ecuador.

- Percepción sobre el Uso de la Tecnología: Midió la utilidad sobre el uso de esta tecnología, positivo y negativo.
- Preocupaciones y Expectativas sobre Protección de Datos: Exploró las principales preocupaciones de los ciudadanos respecto a la seguridad de sus datos personales, además de su opinión sobre la regulación y el control sobre la información capturada.

Muestra

Para conocer la percepción y conocimiento de los participantes, se elaboró una encuesta cerrada para escoger respuestas de Si o No, compartida por Redes Sociales –WhatsApp-, dirigida a cuatro grupos por edades pertenecientes a: adolescencia (de 15-años a 18 años), juventud (de 19 años a 26 años), adultez (de 27 años a 59 años) y personas mayores (de 60 años en adelante), utilizando un formulario digital de Google Forms. No se parametrizó en el programa en el que se elaboró la encuesta, ni se diseñó esta para recolectar información sobre: el género de las personas, educación, número telefónico, números de cédula, dirección de correo electrónico, con la finalidad de no generar desconfianza en las personas que aceptaban rellenar la encuesta. Si bien esta se solicitó a grupos de -WhatsApp- de amigos y conocidos, y de estos a otros grupos de amigos y conocidos, no fue fácil la recolección de la información por la desconfianza hacia el encuestador que en muchos casos no lo conoce y la preocupación sobre si al rellenar la encuesta se estén captando datos personales por el temor

a que estos sean utilizados para otros fines, principalmente delictivos o muy íntimos como el género. Contestaron la encuesta 201 personas.

Instrumento de Recolección de Datos

La encuesta fue aplicada mediante un formulario digital de Google Forms, que fue de fácil acceso desde cualquier dispositivo con conexión a internet, sin necesidad de instalar software adicional.

Proceso de Recolección de Datos

La encuesta se distribuyó a través de plataformas digitales (Redes sociales – WhatsApp).

Procesamiento de Datos

Una vez recolectados, los datos se organizaron y se procesaron mediante una herramienta estadísticas denominadas Google Forms y para el análisis cuantitativo se utilizó tablas dinámicas en Excel, para determinar el número de participantes por edad y su porcentaje para evaluar el nivel de aceptación, conocimiento y percepción del riesgo.

Resultados Esperados

Que los resultados proporcionen una visión general sobre:

- El conocimiento de la población sobre el reconocimiento facial en la seguridad pública y su aceptación.
- La percepción general sobre si es positivo o negativo.
- El riesgo que conoce la ciudadanía en cuanto a la protección de sus datos personales.

Recopilación y evaluación de datos

Durante el análisis de la problemática de nuestra investigación, nos preocupa si la fuerza pública, en el contexto de la seguridad para la prevención del crimen, requiere de alguna autorización específica por parte de los ciudadanos para ser grabados, y aún más con la evolución tecnológica que incorpora el sistema de reconocimiento facial, que permite identificar a las personas mediante una comparación de patrones faciales con bases de datos públicos, como la del Registro Civil.

A pesar de existir una especie de consentimiento tácito de los ciudadanos, por las bondades del servicio de video vigilancia, nos preocupa qué pasa con el derecho a la intimidad de las personas para llevar a cabo sus actividades diarias en libertad y sin vigilancia del Estado, y si es consiente la ciudadanía de que su derecho puede estar siendo afectado a pretexto de combatir la delincuencia.

Visualización de datos y análisis estadístico.

Se encuestó una muestra de 201 personas, quienes respondieron a las preguntas planteadas conforme a lo siguiente:

Tabla 1

Total de Personas Encuestadas por Edades

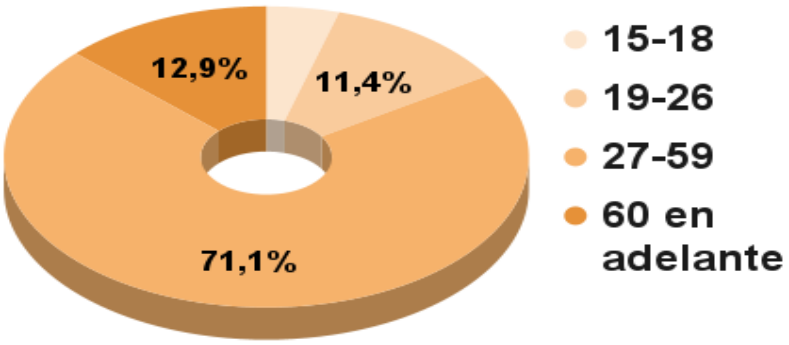
Edades	Votos
15-18	9
19-26	23
27-59	143
60 en adelante	26
Total General	**201**

Nota: Detalle el número de votos por edades

Se receptaron respuestas de todos los rangos de edad, sobresaliendo el grupo de 27 años a 59 años con un 71,1%, considerado dentro de la etapa del ciclo vital como la adultez, dentro de este grupo se encuentran quienes toman decisiones relevantes tanto en el sector público como privado.

Figura 1

Grupos por edades



Nota: El gráfico representa los porcentajes mayores del rango de edad que contestaron a la encuesta.

Tabla 2

Instalación de tecnología de reconocimiento facial en zonas públicas

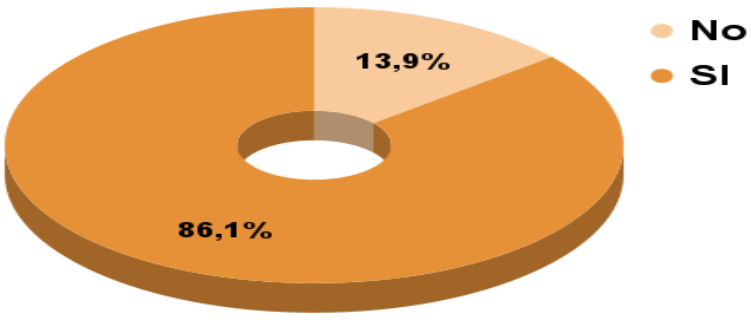
Pregunta 2
¿Estás de acuerdo con qué se instalen sistemas de videovigilancia con tecnología de reconocimiento facial en zonas públicas?

Edades	No	SI	Total
15-18	2	7	9
19-26	4	19	23
27-59	18	125	143
60 en adelante	4	22	26
Total`General	**28**	**173**	**201**

Nota: Los encuestados respondieron en su mayoría SI a esta pregunta como se puede observar en la taba.

Figura 2

Instalación de tecnología de reconocimiento facial en zonas públicas



Nota: Los encuestados respondieron a esta pregunta SI en un 86,1% y solo un 13,9% no está de acuerdo.

Tabla 3

Es positivo el sistema de videovigilancia con tecnología de reconocimiento facial

Pregunta 3.
¿Considera usted que el sistema de videovigilancia con tecnología de reconocimiento facial, en el ámbito de la seguridad ciudadana (pública), es un elemento positivo?

Edades	No	Si	Total
15-18	1	8	9
19-26	3	20	23
27-59	18	125	143
60 en adelante	4	22	26
Total General	**26**	**175**	**201**

Nota: La pregunta tiene una alta votación por el Si.

Para el 87,1% de los encuestados considera que es positivo que el sistema de videovigilancia cuente con reconocimiento facial para la seguridad ciudadana, solo para el 12,9% no lo es.

Figura 3

Es positivo el sistema de videovigilancia con tecnología de reconocimiento facial

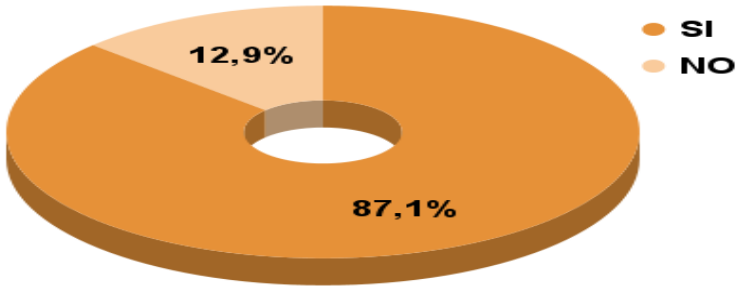


Tabla 4

Dato Biométrico

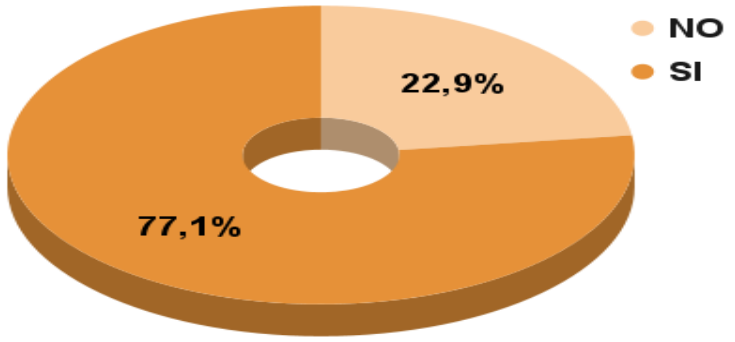
Pegunta 4
¿Sabe qué a través del reconocimiento facial se realiza el tratamiento de un dato biométrico que forma parte de los datos personales de cada individuo?

Edades	No	Si	Total
15-18	3	6	9
19-26	6	17	23
27-59	29	114	143
60 en adelante	8	18	26
Total General	**46**	**155**	**201**

Nota: La tabla muestra el número de votos por el Si a la pregunta cuatro.

Figura 4

Dato biométrico



Nota: El 77,1% de los encuestados sabe que a través del reconocimiento facial se obtiene datos biométricos que son propios de cada individuo, el 22,9% no lo sabe.

Tabla 5

Riesgo en la recopilación de datos personales

Pregunta 5
¿Considera usted que existen riesgos para los ciudadanos, en la recopilación y uso que se hace de los datos personales y sobre todo del reconocimiento facial?

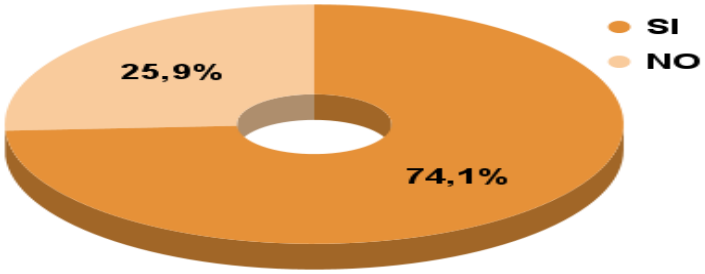
Edades	No	SI	Total
15-18	2	7	9
19-26	4	19	23
27-59	39	104	143
60 en adelante	7	19	26
Total General	**52**	**149**	**201**

Nota: La tabla muestra la votación mayoritaria por el Si a la pregunta

Para el 74,1% de los encuestados existe un riesgo en la recopilación y uso que se hace de sus datos personales y más aún el que se obtiene del reconocimiento facial, para el 25,9% no representa ningún riesgo.

Figura 5

Riesgo en la recopilación de datos personales



Nota: Porcentaje de votación a la pregunta cinco

Tabla 6

Comparativa de datos por la fuerza Pública

Pregunta 6
¿Conoce usted que la fuerza pública utilizará el reconocimiento facial de los sistemas de vigilancia para comparar con otras bases de datos?

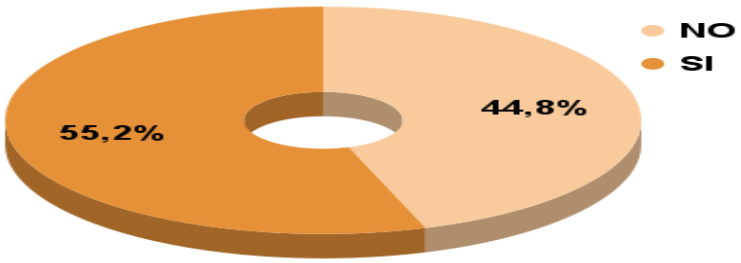
Edades	No	Si	Total
15-18	5	4	9
19-26	8	15	23
27-59	61	82	143
60 en adelante	16	10	26
Total General	**90**	**111**	**201**

Nota: La tabla muestra que el Si es superior a la votación del No

El 55,2% de los encuestados conoce que la fuerza pública utilizará sus datos biométricos para ejecutar comparativas con otros bases de datos públicas, el 44,8% no tiene ningún conocimiento.

Figura 6

Comparativa de datos por la fuerza pública



Nota: Porcentaje de votación a la pregunta seis

Tabla 7

Conocimiento de la existencia de la Ley Orgánica de Protección de Datos Personales

Pregunta 7
¿Tiene conocimiento de que en el Ecuador está en vigencia la Ley Orgánica de Protección de Datos Personales, cuyo objetivo es proteger los datos personales de todos los ciudadanos de su uso indebido o fraudulento?

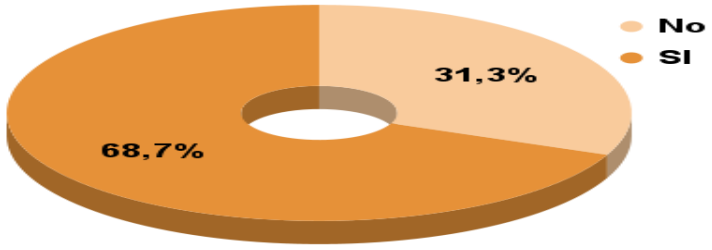
Edades	No	Si	Total
15-18	5	4	9
19-26	8	15	23
27-59	39	104	143
60 en adelante	11	15	26
Total General	63	138	201

Nota: La tabla muestra el número de votos por el Si y el No

Un 68,7% de los encuestados señala que conoce que en el Ecuador existe una ley que protege los datos personales de los ciudadanos, el 31,3% lo no conoce.

Figura 7

Porcentaje de Conocimiento de Ley Orgánica de Protección de Datos Personales



Nota: Porcentaje de votación a la pregunta siete.

Tabla 8

Tratamiento de datos biométricos

Pregunta 8
¿Conoce usted sobre el tratamiento que se dan a los datos que se recogen a través de los sistemas de videovigilancia con reconocimiento facial?

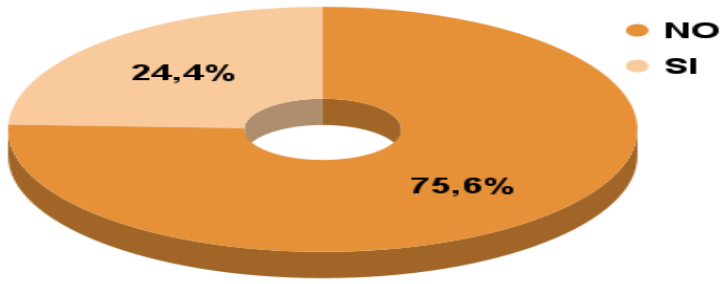
Edades	No	Si	Total
15-18	7	2	9
19-26	16	7	23
27-59	108	35	143
60 en adelante	21	5	26
Total General	**152**	**49**	**201**

Nota: La tabla detalla la votación en mayor número para el No

De los 201 encuestados el 75,6% no conoce cual es el tratamiento que se dan a sus datos biométricos, mientras que el 24,4% si conoce.

Figura 8

Tratamiento de datos biométricos



Nota: Porcentaje de votación a la pregunta ocho

Tabla 9

Derecho a la intimidad

Pregunta 9
¿Conoce sobre el derecho que tenemos los ciudadanos a la INTIMIDAD y a la PRIVACIDAD consagrado en nuestra legislación?

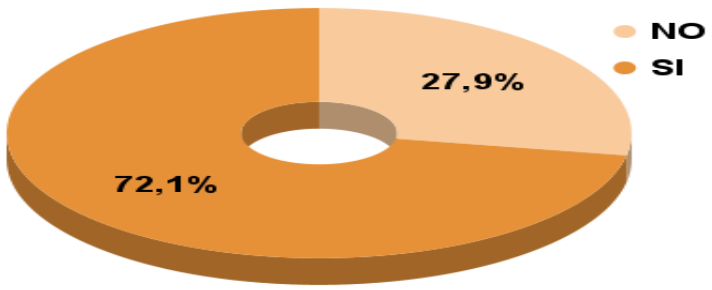
Edades	No	Si	Total
15-18	2	7	9
19-26	8	15	23
27-59	39	104	143
60 en adelante	7	19	26
Total General	**56**	**145**	**201**

Nota: La tabla detalla la votación en mayor número para el SI

A esta pregunta los encuestados dicen que conocen sobre su derecho a la intimidad en un 72,1% y el 27,9% no lo conoce.

Figura 9

Derecho a la intimidad



Nota: El Si tiene el mayor porcentaje de votación a la pregunta nueve.

Tabla 10

El reconocimiento facial trasgrede el derecho a la intimidad

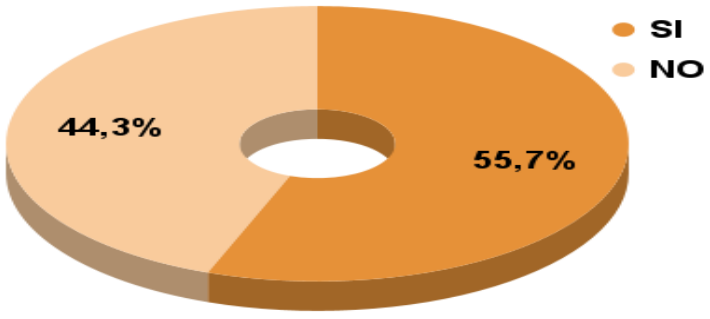
Pregunta 10
¿Considera usted que el reconocimiento facial, en el ámbito de la seguridad pública, trasgrede el derecho de los ciudadanos a la intimidad y a la privacidad?

Edades	No	Si	Total
15-18	3	6	9
19-26	6	17	23
27-59	65	78	143
60 en adelante	15	11	26
Total General	**89**	**112**	**201**

En esta pregunta los encuestados consideran que el reconocimiento facial aplicado al ámbito de la seguridad pública no trasgrede su derecho a la intimidad en un 44,3%, mientras que para el 55,7% considera que sí.

Figura 10

El reconocimiento facial trasgrede el derecho a la intimidad



Nota: El sí tiene el mayor porcentaje en la pegunta diez

Tabla 11

Derecho de acceso, rectificación, cancelación y oposición

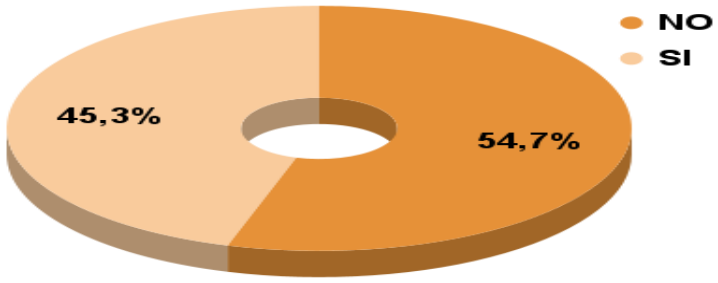
Pregunta 11
¿Conoce sobre el derecho que tiene como ciudadano para solicitar a la fuerza pública que recoge sus datos personales, el acceso a estos, o a solicitar la rectificación, la cancelación u oponerse a que se recojan?

Edades	No	Si	Total
15-18	3	6	9
19-26	10	13	23
27-59	79	64	143
60 en adelante	18	8	26
Total General	**110**	**91**	**201**

El 54.7% de la muestra desconoce sobre este derecho, mientras que el 45.3% conoce que puede solicitar el acceso a su información.

Figura 11

Derecho de acceso, rectificación, cancelación y oposición



Nota: sí tiene el mayor porcentaje de votación a la pregunta once

Identificación de tendencias

Para la mayoría de encuestados, el uso de sistemas de videovigilancia implementados en las ciudades para prevenir delitos, o al menos como elemento disuasorio, es aceptado. No tienen reparos en que estos sistemas cuenten con reconocimiento facial en pro de la seguridad ciudadana, y que los datos biométricos sean utilizados por las instituciones estatales encargadas de la seguridad pública.

La mayoría de los encuestados reconocen que el Estado ecuatoriano está obligado a proteger su derecho a la intimidad, conforme a la norma constitucional y lo establecido en la Ley Orgánica de Protección de Datos Personales y su reglamento.

Al ser preguntados si conoce que el reconocimiento facial es un dato biométrico personal, los encuestados afirmaron estar al tanto y aceptaron su uso por parte de la fuerza pública. Sin embargo, expresaron preocupación y desconocimiento sobre el procedimiento para el tratamiento de datos personales y su uso final.

Un alto porcentaje de encuestados desconoce que tiene derecho a solicitar a la fuerza pública acceso a sus datos personales, así como a solicitar su rectificación, cancelación u oponerse a que su recolección.

Interpretación

El análisis de las encuestas y los datos de la muestra nos permite determinar que en principio la fuerza pública no necesitaría de un consentimiento expreso de los ciudadanos para la implementación de un sistema de videovigilancia con reconocimiento facial en zonas públicas.

El uso de los sistemas de videovigilancia con reconocimiento facial en espacios públicos es valorado positivamente por los encuestados, ya que este sistema ofrece varias ventajas para la seguridad de la ciudanía. En tiempo real, permite prevenir delitos o infracciones, y detectar situaciones de emergencia. En video contribuye a la investigación y esclarecimiento de actos delictivos durante la fase de investigación previa, y facilita la localización de personas extraviadas.

Los sistemas de video vigilancia utilizan un software específico que permite que las imágenes captadas con cámaras de alta resolución sean cruzadas con bases de datos, con el propósito de identificar los patrones faciales captados. Los encuestados manifiestan que conocen que el reconocimiento facial es un dato biométrico sensible, protegido por el derecho a la intimidad; sin embargo, a pesar de esto, aceptan su uso y comparación con otras bases de datos de instituciones estatales. No obstante, desconocen el tratamiento que se les dará a sus datos y desconocen en qué momento serán utilizados. Por ello, es importante generar normativas para el uso de estos datos en situaciones específicas y con una finalidad clara, a fin de garantizar el derecho a la intimidad, privacidad y libertad de las personas.

Presentación de resultados

Para la visualización de los hallazgos identificados se utilizó la herramienta Google Form y Excel. Se tomó en cuenta un muestreo por conveniencia y se realizó un análisis usando tablas dinámicas en las respuestas de la encuesta, basada en grupos etarios específicos, con el objetivo de comprender de manera detallada las diferencias y similitudes entre los distintos segmentos de edad, lo cual permitió identificar los siguientes hallazgos:

1. Los grupos etarios encuestados de 15 a 18 años, de 19 a 26 años, de 27 a 59 años y de 60 años en adelante, a las preguntas dos y tres respondieron que están de acuerdo con la instalación de sistemas de videovigilancia con tecnología de reconocimiento facial en zonas públicas, considerándolos positivos el 87% de los encuestados según la muestra.

Tabla 12

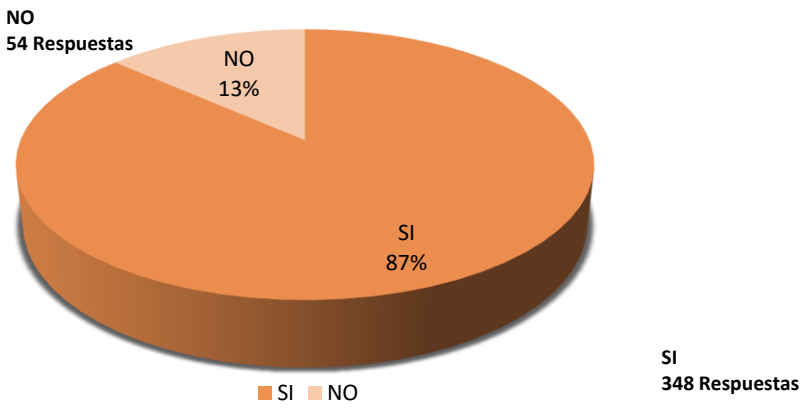
Aceptación de sistemas de videovigilancia con reconocimiento facial

Tabulación	Pregunta 2	Pregunta 3	Total Respuestas	Total Resultados	Porcentaje
SI	173	175	348	348	86,60%
NO	28	26	54	54	13,40%
Total de la muestra				**402**	**100,00%**

En la tabla se refleja los votos para el SI o NO a las preguntas 2 y 3, la sumatoria de los votos determinó el porcentaje de aceptación del sistema de video vigilancia con reconocimiento facial.

Figura 12

Aceptación de sistemas de videovigilancia con reconocimiento facial



Nota: El porcentaje de aceptación en el 87%

2. Los encuestados contestaron a las preguntas cuatro y cinco, que son conscientes de que el reconocimiento facial capta datos biométricos sensibles y consideran que existe un riesgo en la recopilación de estos datos personales y biométricos.

Tabla 13

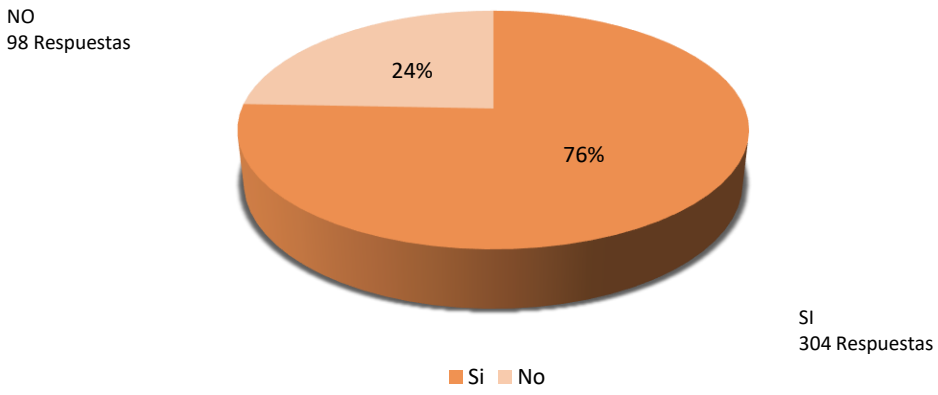
Conocimiento y riesgo en la captación de datos personales y biométricos

Tabulación	Pregunta 4	Pregunta 5	Total respuestas	Total resultados	Porcentaje
Si	155	149	304	304	75,62%
No	46	52	98	98	24,38%
Total de la Muestra				**402**	**100,00%**

La tabla refleja los votos para el SI o NO a las preguntas 4 y 5, la sumatoria de los votos determinó que el 76% de los encuestados consideran que existe un riesgo en la recopilación de datos personales y biométricos.

Figura 13

Porcentaje de conocimiento y riesgo en la captación de datos personales y biométricos



3. Los encuetados contestaron a las preguntas 7, 9, y 10, revelando que solo el 66% del total de la muestra conoce su derecho a la intimidad, consagrado en la Constitución del Ecuador, así como la existencia de la Ley Orgánica de Protección de Datos (LOPD), que garantiza la protección de datos personales contra usos indebidos o fraudulentos. Sin embargo, aún no se ha normado cuales son las limitaciones para la captación de datos sensibles en el uso de los sistemas de videovigilancia con reconocimiento facial.

Tabla 14

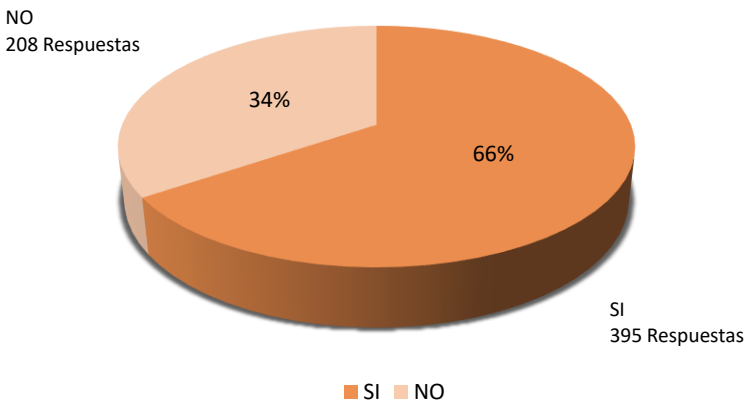
Conocimiento de la normativa

Tabulación	Pregunta 7	Pregunta 9	Pregunta 10	Total respuestas	Total resultados	Porcentaje
SI	138	145	112	395	395	66%
NO	63	56	89	208	208	34%
Total de la muestra					**603**	**100%**

Nota: La tabla detalla el total de votos para el SI o NO

Figura 14

Porcentaje de conocimiento de la normativa



4. Los encuestados en el 55% del total de la muestra son conscientes de que la fuerza pública utilizará sus datos personales y biométricos para compararlos con otras bases de datos. A pesar de conocerlo, no se oponen al uso de sistemas de videovigilancia con reconocimiento facial, ni exigen transparencia en el uso de sus datos para la protección de su derecho a la intimidad consagrada en nuestra legislación.

Tabla 15

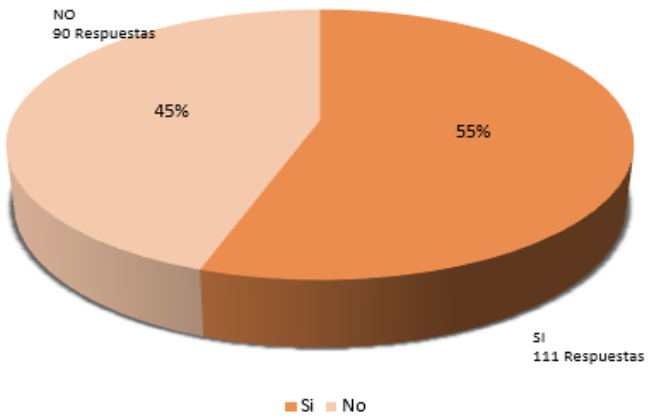
Uso de datos personales y biométricos

Tabulación	Pregunta 6	PORCENTAJE
Si	111	55,22%
No	90	44,78%
Total de la Muestra	201	100,00%

Nota: La tabla detalla el total de votos para el SI o NO

Figura 15

Porcentaje de la votación de uso de datos personales y biométricos



5. Los encuestados en el 76% del total de la muestra desconocen el tratamiento que se dará a los datos biométricos que son recogidos a través de los sistemas de videovigilancia con reconocimiento facial. Por ello, es necesario generar normativa para su uso en casos concretos, implementando medidas que impidan la retención de datos biométricos, para garantizar el derecho a la intimidad, libertar y privacidad de los ciudadanos.

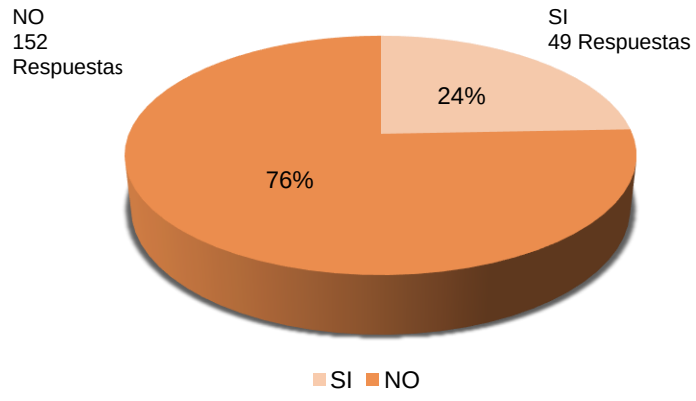
Tabla 16

Tratamiento de datos biométricos

Tabulación	Pregunta 8	PORCENTAJE
SI	49	24,38%
NO	152	75,62%
Total de la Muestra	201	100,00%

Figura 16

Porcentaje de votación sobre la tabla de tratamiento de datos



6. Todos los encuestados en el 55% desconocen su derecho a solicitar a la fuerza pública el acceso a los datos personales recolectados, o solicitar la rectificación, la cancelación y la oposición al uso de sus datos personales conforme a los principios establecidos en la Ley Orgánica de Protección de Datos Personales. Esto hace necesario que dichas instituciones generen campañas de comunicación dirigidas a todos los ciudadanos.

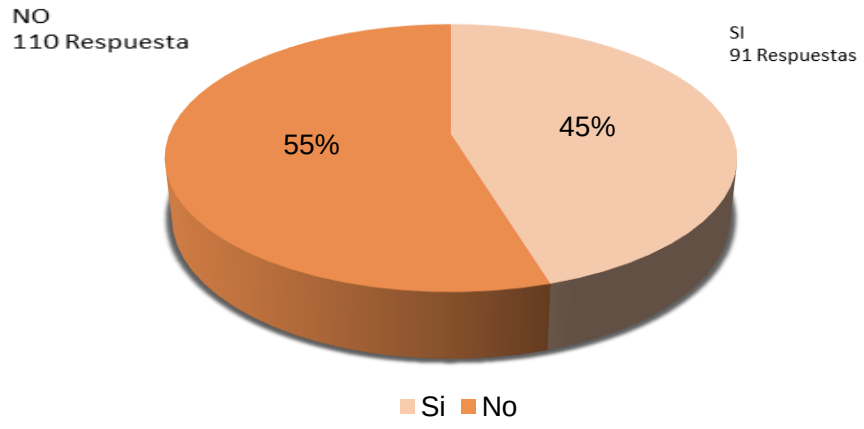
Tabla

Derecho a solicitar a la fuerza pública el acceso a los datos personales

Tabulación	Pregunta 11	PORCENTAJE
Si	91	45,27%
No	110	54,73%
Total de la Muestra	201	100,00%

Figura 17

Porcentaje de votación al derecho a solicitar a la fuerza



CAPITULO 3

Seguridad Pública estrategias de control criminal

Partiendo del conocimiento general la seguridad pública es la erradicación, prevención, detención de delitos o situaciones atípicas al ordenamiento jurídico, es por ello por lo que el estado a través de sus representantes y en apego a la constitución actúa en base a la normativa vigente, velando por que se cumpla con los principios de legalidad, eficacia, celeridad tal cual como lo reconoce el estado ecuatoriano.

La seguridad pública es de gran relevancia en Ecuador, ya que afecta directamente el bienestar de las personas y el crecimiento del país. En los últimos años, la inseguridad ha sido uno de los problemas primordiales que enfrentan todos los ciudadanos, lo que ha llevado a la implementación de políticas y estrategias para el mejoramiento de la seguridad pública ecuatoriana. (Andrade, 2018).

En el derecho comparado con Argentina, tenemos una estrecha relación cuando se menciona:

[…] De la misma manera, la seguridad pública se orienta a disciplinar el comportamiento de la sociedad mediante acciones normativas del orden público de esta, modo nuestro país podrá tener en cuenta una hipótesis del modelo neoliberal ante la situación del control criminal mediante las estrategias que se consolidó en el país de Argentina. **[…]** (Urvio Revista Latinoamericana, 2020).

Para poder controlar este gran acto criminal que atraviesa el Ecuador se debe ejecutar mejores estrategias de seguridad pública desde el punto de vista metodológico consisten en una acción de formulación y establecimiento de objetivos de carácter prioritario con la finalidad de disminuir la problemática de la inseguridad en nuestro país que aparece en el escenario social con nuevas formas y características de acuerdo a un enfoque multifacético, es allí donde se verá reflejado el uso de la tecnología, cooperación, para dosificar los pilares fundamentales del país.

Así mismo, según el artículo 23 de la Ley de Seguridad Pública y del Estado, tipifica que la seguridad ciudadana es una política de Estado, destina a fortalecer y modernizar los mecanismos necesarios para garantizar los derechos humanos, en especial el derecho a una vida libre de violencia y criminalidad, la disminución de los niveles de delincuencia, la protección de víctimas y el mejoramiento de la calidad de vida de todos los habitantes del Ecuador. (Ley de Seguridad Publica y del Estado, 2017).

Por ello, existen evidencias claras de que las estrategias de prevención del delito bien estructuradas no solo previenen el acto criminal, sino que promueven la seguridad de la comunidad contribuyendo al desarrollo del Estado ecuatoriano, las implementaciones de políticas de seguridad eficaces mejoran la calidad de la vida de las personas, además la prevención de actos delictivos ofrece oportunidades para reducir costos generados por la sustracción de bienes debemos tomar en cuenta que todos estos actos afectan directamente el bienestar social de forma que la inseguridad y la violencia generan un clima de temor.

De acuerdo con la teoría de (Arias, 2021) la seguridad pública se define como una serie de políticas y acciones convenientes y articuladas, que tienen como propósito afianzar la protección y el bienestar de la ciudadanía, mediante la precaución y control de los delitos, la violencia y la delincuencia. En Ecuador, la seguridad pública se rige por la Ley de Seguridad Pública y del Estado, la cual establece que la misma es integral para todos los que habitan en el país, pueblos, sectores, nacionalidades, grupos, colectivos y personas.

A lo largo de las últimas décadas, la seguridad pública en Ecuador ha evolucionado de manera significativa. En los últimos años, se han implementado diferentes políticas y estrategias, se ha fortalecido la coordinación entre las diversas instituciones responsables de la seguridad pública, se han creado nuevas unidades especializadas y se ha mejorado la formación y capacitación de los policías. Sin embargo, a pesar de estos avances, la inseguridad y la violencia siguen siendo un problema importante en Ecuador, debido a que han incrementado en los últimos años, lo que ha permitido que se implementen nuevas políticas y estrategias para tratar de mitigarlos.

Ecuador se ha convertido en un país inseguro, se debería aumentar las estrategias de seguridad pública ante los actos criminales de manera eficaz y efectiva, se debe de convertir en un país subdesarrollado en la tecnología actualizada donde sea basado en un proyecto de seguridad virtual como Digital Modelo Neoliberal que existe en el país de Argentina, nuestro país también tiene las herramientas necesarias para combatir todos los actos delictivos donde implemente métodos y políticas de seguridad para reforzar la coordinación entre las

diversidades entidades para la prevención del delito y el acto criminal y así se puedan cumplir el respeto de los Derechos Humanos.

Asimismo, se recomienda llevar a cabo nuevas tecnologías para optimizar tanto a la seguridad pública en el país como a la coordinación entre las distintas instituciones responsables y fortalece el apoyo internacional en tópicos de seguridad pública, con el objetivo de intercambiar información y experiencia para mejorar la seguridad en el país.

Definición y aplicabilidad de la Seguridad Pública en el Ecuador.

La seguridad pública en Ecuador se remonta a la época colonial, donde nacieron las primeras entidades dedicadas al cuidado del orden y la seguridad en el territorio nacional, sin embargo, en la época republicana, aparecen entidades policiales y militares encargadas de la seguridad pública.

Desde 1822, cuando Ecuador llega a forma parte de la Gran Colombia se establecieron ciertos lineamientos para la policía, como encargada de la seguridad pública en el país, durante las décadas siguientes, se implementaron diferentes políticas y estrategias para mejorar la seguridad pública en Ecuador, aunque con resultados limitados, siendo así que, en el año de 1964, mediante la expedición de la Ley Orgánica de la Policía Nacional, se le da el nombre de Policía Nacional, con el objetivo de modernizar la institución y mejorar su eficiencia en la lucha contra la violencia y la incidencia delictiva, creando nuevas unidades especializadas, mejorando la formación de competencias de los policías y se implementaron nuevas tecnologías para optimizar el tema de seguridad pública.

En el pasado se implementaron diferentes políticas y estrategias para mejorar la seguridad pública en Ecuador, sin embargo, muchos de estos esfuerzos no tuvieron los resultados esperados y la inseguridad y la violencia siguieron siendo un problema principal en el país. (Romero Torres, Juan, 2023).

Entre las políticas y estrategias implementadas en el pasado, se pueden mencionar la fundación de la Policía Comunitaria, la puesta en marcha de programas de prevención de la criminalidad y la violencia, la creación de unidades especializadas a fin de combatir el crimen organizado y la aplicación de nuevas tecnologías para mejorar la seguridad pública en territorio, sim embargo, pese a todo este trabajo, la inseguridad y la violencia siguen representando una dificultad notoria en el país, requiriendo la formulación de un nuevo esquema de seguridad pública en el país pueda garantizar la seguridad. (Romero Torres, Juan, 2023).

El gobierno ha tomado varias medidas para abordar la crisis de seguridad en el país, como por ejemplo:

- Plan Nacional de Desarrollo 2017-2021 Toda una Vida, que establece acciones para el mejoramiento de la seguridad pública en el país.
- Fortalecimiento de la coordinación entre instituciones como Policía Nacional, Ministerio de Gobierno y Ministerio de Defensa, que tienen como responsabilidad la seguridad pública.
- Programas de prevención del delito y la violencia, con el fin de minimizar los índices de criminalidad.
- Creación de nuevas entidades expertas y enfocadas en la mitigación del narcotráfico y

el crimen organizado.

- Nuevas tecnologías para el mejoramiento de la seguridad pública en el país, como cámaras de vigilancia y sistemas de monitoreo.
- Inversión en seguridad pública, con el objetivo de optimizar el adiestramiento y capacitación de los policías y la obtención de nuevos equipamientos y aparatos tecnológicos.
- Mayor cooperación internacional en cuanto a lo referente a seguridad pública, con el objetivo de intercambiar información y experiencias para mejorar la seguridad en el país.
- Mejoramiento de la situación carcelaria en el país, con el propósito de disminuir el porcentaje delictivo en las cárceles y mejorar la reinserción social de los privados de libertad.

La inseguridad y la violencia son un problema latente en el país, por ello, es imperante implementar estrategias eficientes para regenerar la seguridad pública y afianzar más el derecho de los individuos a la seguridad. (Dávila Molina , Cristina Maribel, 2003).

Es importante considerar que la respuesta de la sociedad civil a la crisis de seguridad se ha visto demostrada mediante manifestaciones y protestas para exigir al gobierno medidas efectivas para optimizar la seguridad pública en el país, estas manifestaciones también han incluido demandas relacionadas con el acceso a la salud, la educación y el empleo, en igual sentido se han presentado varias críticas a la gestión del gobierno por la falta de medidas efectivas para mitigar el índice de la criminalidad y la violencia en el país

Agentes participantes de la Seguridad Pública

En un estado garantista de derechos, la seguridad ciudadana o seguridad pública, es uno de los pilares fundamentales para su desarrollo, integrando los esfuerzos de la ciudadanía y de las organizaciones del sector público, a fin de que los derechos individuales se puedan ejercer, mediante la consolidación de un conjunto de acciones que van encaminadas a garantizar el respeto de los derechos humanos.

La Seguridad Pública es competencia exclusiva y privativa del Estado, mediante acciones y medidas sistémicas orientadas a mantener y restablecer el orden público, la protección interna y el libre ejercicio de los derechos.

La Seguridad Pública comprende, además, la prevención, investigación, persecución penal y administrativa de las infracciones, su sanción y la rehabilitación social de los infractores. (Ministerio del Interior, 2019).

Es así que como agentes participantes de la seguridad pública en Ecuador, tenemos a las instituciones públicas como Policía Nacional, Fuerzas Armadas, los Gobiernos Autónomos Descentralizados, Consejo de la Judicatura; quienes desempeñan un papel clave en la protección de la seguridad de los ciudadanos y la prevención de delitos, cada uno asumiendo sus responsabilidades específicas de acuerdo con lo que rige la Constitución de la República del Ecuador.

En la Carta Magna, específicamente en el Art. 158 establece “Las Fuerzas Armadas y la Policía Nacional son instituciones de protección de los derechos, libertades y garantías de los ciudadanos

Las Fuerzas Armadas defienden la soberanía e integridad territorial, mientras que la Policía Nacional es responsable del orden público, garantizando el respeto a la dignidad y derechos de las personas sin discriminación y conforme a la ley. (Constitución de la República del Ecuador, 2008).

Aterrizando más al contexto de la presente investigación la misma Carta Magna, establece la misionalidad de Policía Nacional en su Art. 163 ““La Policía Nacional es una institución estatal de carácter civil, armada, técnica, jerarquizada, disciplinada, profesional y altamente especializada, cuya misión es atender la seguridad ciudadana y el orden público, y proteger el libre ejercicio de los derechos”. (Constitución de la República del Ecuador, 2008)

El personal que forma parte de las entidades encargadas de la seguridad tendrá una formación basada en derechos humanos, investigación especializada, prevención, control y prevención del delito y utilización de medios de disuasión y conciliación como alternativas al uso de la fuerza, para el desarrollo de sus tareas la Policía Nacional coordinará sus funciones con los diferentes niveles de gobiernos autónomos descentralizados

La Constitución establece la misión de la Policía Nacional bajo un enfoque integral y moderno de seguridad pública, destacando su compromiso con la protección de los derechos humanos y la seguridad ciudadana, como institución civil y profesional, se diferencia de las Fuerzas Armadas al centrarse en la protección de la población, la prevención del delito y la promoción de la convivencia pacífica, su carácter técnico y especializado exige una capacitación constante para adaptarse a los cambios y aprovechar las tecnologías con el fin de mejorar su servicio, siempre con respeto a los derechos humanos, fortaleciendo su labor

mediante estrategias preventivas y no violentas alineadas a estándares internacionales, contando con el apoyo de las Fuerzas Armadas y los Gobiernos Autónomos Descentralizados para responder de manera más eficaz a las necesidades de seguridad.

La Policía Nacional juega un papel fundamental en la protección de los derechos de la ciudadanía y en la convivencia pacífica, es importante destacar que para dar cumplimiento a esta misión de manera efectiva, es necesario mantener la capacitación constante, y en cuanto al uso de nuevas tecnologías la manera de regular su uso, y fomentar la confianza de la ciudadanía, gracias a la cooperación interinstitucional y la especialización son pilares indispensables para construir una institución más eficiente y comprometida para con la sociedad.

Policía Nacional y almacenamiento de datos

La Policía Nacional del Ecuador, dentro su estructura organizacional cuenta con la Dirección Nacional de Tecnologías de la Información y Comunicación, la misma que de acuerdo con lo que establece el Acuerdo Ministerial 080. "Estatuto Orgánico de Gestión Organizacional por Procesos de la Policía Nacional, tiene la misión de asesorar y promover la innovación y el desarrollo tecnológico institucional, respecto a las tecnologías de la información y comunicación a nivel nacional". (Ministerio del Interior, 2019).

Es así que con el fin de garantizar la atención de la seguridad ciudadana la Policía Nacional desarrolla en el año 2005 una herramienta tecnológica denominada Sistema Informático Integrado de la Policía Nacional-SIIPNE, el cual se constituye como un medio

esencial y fundamental de carácter estratégico que integra, genera y articula la coordinación operativa y administrativa.

En el año 2021 se expide el Reglamento del Sistema Informático Integrado de la Policía Nacional del Ecuador SIIPNE, mediante el cual se regula la estructura funcionamiento y administración del referido sistema, estableciendo procedimientos para el acceso, uso, eliminación y anulación de datos de forma segura, proporcionando información a través de la web y dispositivos móviles a los usuarios de los subsistemas, procesos y componentes de la Policía Nacional; para la ejecución de procesos operativos y de gestión institucional; y, brindar servicios a la comunidad, que contribuyen a la seguridad ciudadana y orden público, bajo los principios de confidencialidad, integridad, disponibilidad y rectificabilidad.

Este sistema informático procesa, produce, comparte e intercambia datos e información provenientes de fuentes internas y externas para respaldar las actividades operativas y administrativas de la Policía Nacional. Las fuentes internas corresponden a las distintas dependencias dentro de su estructura organizativa, mientras que las externas incluyen instituciones públicas y privadas que suministran información para los usuarios del sistema, como el Registro Civil, la Agencia Nacional de Tránsito, el Consejo de la Judicatura, la Fiscalía General del Estado, el Servicio de Rentas Internas, la Subsecretaría de Migración, Interpol, entre otras.

En este contexto los datos tanto de fuentes internas y externas, se almacenan en el Data Center Institucional, el mismo que cuenta con las debidas seguridades a fin de precautelar la integridad, disponibilidad y confidencialidad de esta.

De acuerdo con la Política Tecnológica Institucional, en las directrices generales 8.5 determina que “Toda la infraestructura debe ser implementada en el Data Center Institucional evitando Data Center paralelos con sistemas, aplicaciones y servicios institucionales similares”, (Polícia Nacion del Ecuador-DNTIC, 2023).

Constituyéndose este como el centro de procesamiento de datos, instalación empleada para albergar un sistema de información de componentes asociados, como telecomunicaciones y los sistemas de almacenamiento.

Para el consumo de información desde instituciones públicas, como fuentes externas, se realiza mediante la autorización emitida por parte de la Dirección Nacional de Registro Públicos, mediante convenios para su consumo, estableciendo los mecanismos para garantizar su seguridad.

Aspectos regulatorios

En Ecuador, la seguridad pública está estructurada como una función esencial del Estado, orientada a garantizar la convivencia pacífica y la protección de los derechos ciudadanos, los aspectos regulatorios que rigen la actuación de los agentes participantes de la seguridad pública se fundamentan en la Constitución de la República, leyes específicas y normativas complementarias, estableciendo los roles y responsabilidades de las instituciones involucradas.

La Constitución de Ecuador define claramente las competencias de las instituciones encargadas de la seguridad pública, los artículos 158 y 163 establecen la misionalidad de la Policía Nacional y las Fuerzas Armadas, diferenciando sus roles y subrayando el carácter civil,

técnico y profesional de la Policía en la protección interna y el mantenimiento del orden público, así mismo, las disposiciones constitucionales enfatizan el respeto irrestricto a los derechos humanos y la coordinación interinstitucional.

El marco regulatorio ecuatoriano establece un enfoque integral para la seguridad pública, donde la colaboración entre instituciones y la aplicación de principios éticos son fundamentales, la regulación del uso de tecnologías como el reconocimiento facial requiere ajustes constantes para responder a desafíos emergentes, equilibrando la protección de los derechos humanos con la necesidad de mantener el orden y la seguridad.

Mecanismos de seguridad y control social

El Estado es el encargado de velar por la protección y seguridad de todos los bienes públicos y privados y proteger la seguridad integral de todos los habitantes de un país, a través de sus organismos de control como Fuerzas Armadas y Policía Nacional.

La seguridad ciudadana se considera una política de Estado, a través de la cual se garantiza los derechos fundamentales de los seres humanos, la prevención y control de los delitos, privilegiando para ello el equipamiento tecnológico que permita a las instituciones vigilar, controlar, auxiliar, e investigar los eventos que constituyen una amenaza para la ciudadanía, así lo establece la Ley de Seguridad Pública y del Estado del Ecuador (Registro Oficial Suplemento, 2009).

El Reglamento a la Ley de Seguridad Pública y del Estado del Ecuador (Registro Oficial Suplemento 557, 2024), señala en su artículo treinta y tres que, el Plan Nacional de Seguridad Ciudadana desarrollará objetivos claros y estrategias específicas orientadas a la prevención del

delito, así como a la contención y disminución de la violencia en sus distintas manifestaciones. Este plan define las estrategias y líneas de acción para mejorar la seguridad como un bien público, promover la cultura de paz y legalidad, y fortalecer las capacidades institucionales para una respuesta efectiva ante los fenómenos de violencia y delincuencia. Se busca la integración de tecnologías avanzadas, los sistemas de videovigilancia y prácticas innovadoras en la gestión de la seguridad ciudadana y pública.

La Agenda de Transformación Digital del Ecuador 2022-2025 (Registro Oficial Sumplento 114, 2022), dentro de la estrategia de transformación digital, ha considerado que uno de los mecanismos para el control y seguridad social y equipamiento tecnológico de la Policía Nacional, sea mediante el uso de tecnologías emergentes para el desarrollo sostenible, seguridad y confianza digital y la interoperabilidad y tratamientos de datos, que permita optimizará la gestión de la Policía Nacional.

Dotar a la Policía Nacional de este tipo de tecnología debe ir de la mano de la profesionalización y capacitación de su personal, para que la información que se recabe con la implementación de todas las estrategias planteadas para mejorar la seguridad y control social sea el obtener información comprobable que permita prevenir y castigar el delito, salvaguardando la seguridad ciudadana.

Los avances de la tecnología no podían quedar fuera del ámbito de la seguridad y van encaminados a fortalecer las herramientas que ya está utilizando la Policía Nacional, a los que podrá acceder ampliamente con convenios entre las instituciones públicas como Fiscalía, la Judicatura, Registro Civil, Gobiernos Autónomos Descentralizados Municipales, como lo es el

sistema de videovigilancia implementada por ECU 911 y ciertos Gobiernos Autónomos Descentralizados Municipales.

Video vigilancia

La realidad en la que la ciudadanía lleva a cabo sus actividades cotidianas, y la inseguridad a la que se siente expuesta, determinan que la implementación de sistemas de videovigilancia en espacios públicos, no haya sido rechazada por los ciudadanos ecuatorianos sino más bien que se nota un elevado grado de aceptación; consideran que este tipo de sistemas ayudan a disuadir al delincuente y genera en la ciudadanía un sentimiento de seguridad. Pero desde cuándo este sistema es utilizado para la seguridad pública. De acuerdo con la investigación realizada por la autora (Ramirez 2021, como citó en Uribe, Dennisse, 2024) en el artículo El aviso de Privacidad de Datos Personales en la Era Digital de la Videovigilancia, señala:

La implementación de los sistemas de videovigilancia tuvo su origen en las pruebas realizadas por el ingeniero estadounidense Frank B. Gilbreth, con el principal objetivo de llevar a cabo el monitoreo a operarios y a profesionales destacados a comienzos del siglo XX. El científico Frank Gilbreth, pretendía optimizar aquellos procesos productivos y aumentar la eficacia, utilizando tecnologías visuales y cámaras cinematográficas con la finalidad de optimizar la producción industrial.

> A partir de 1971, en Estados Unidos se comenzaron a utilizar los sistemas de videovigilancia para conocer, prevenir y contender aquellas manifestaciones que ocasionaban desórdenes públicos. Este monitoreo se realizaba a través de circuitos

cerrados de televisión, por lo que, a partir de esa época, diversos países en el mundo comenzaron a utilizar los citados sistemas.

La escritora cita a Soto Galindo José, autor de ¿Qué es la videovigilancia? al señalar que, la primera práctica de implementación en espacios públicos se desarrolló en los años 1970, “cuando se estableció el primer sistema público de vigilancia en la ciudad turística británica de Bournemouth en 1895 como parte de la reunión anual del Partido Conservador del Reino Unido”.

En los años 80, en Norteamérica, el uso de sistemas de videovigilancia no era empleado en la mayoría de los de casos para las áreas públicas, pero en el sector privado los propietarios de tiendas y bancos comenzaron a utilizar dichos sistemas, para contrarrestar la inseguridad.

> Con los atentados ocurrido el 11 de septiembre de 2001 en Estados Unidos, se impuso el tema de la seguridad como una de las prioridades de la agenda mundial, por lo que los sistemas de videovigilancia se han ido implementado en los medios que se consideran vitales para la lucha contra el terrorismo.
>
> Actualmente, en diversos países se han instaurado la tecnología de video vigilancia con CCTV (circuitos cerrados de televisión), la cual es utilizada como un instrumento para supervisar y monitorear los sistemas de transporte, vigilar el mantenimiento de la infraestructura, prevenir incendios y supervisa espacios públicos. Suiza en los 90 adoptó de manera amplia la tecnología de CCTV, con la finalidad de manejar el sistema operativo de áreas públicas… (p. 288,289)

Para Norris (Norris, 2004) la implementación de estos sistemas pasó por cuatro etapas de acuerdo a la complejidad de las experiencias de los diferentes países, la primera pasó por el uso del sector privado para disuadir el robo y el fraude; la segunda fue la introducción de la video vigilancia en el transporte, escuelas, edificios gubernamentales y en zonas de importancia simbólica; una tercera etapa en la que los sistemas de CCTV migran al espacio público de los centros urbanos y a las calles de las ciudades con el fin de disuadir y detectar el delito, estos sistemas se financian con fondos públicos y son administrados por las autoridades municipales o la policía local; en la cuarta etapa el monitoreo urbano tiende hacia la ubicuidad, cientos de cámaras que proporcionen una cobertura total de zonas enteras de la ciudad, integración de sistemas a gran escala con sistemas pequeños preexistentes tanto públicos como privados, el uso de mayor tecnología para habilitar sistemas de reconocimiento facial o de matrículas automáticos vinculados a bases de datos locales o nacionales.

Es así como las cámaras de seguridad ubicadas en sectores privados pasaron al ámbito público, a sistemas de video vigilancia para el monitoreo de espacios públicos, incorporándose cada vez con mayor naturalidad al espacio urbano, donde pasan desapercibidas para muchos ciudadanos, quienes entienden que son parte de las políticas de seguridad municipal o policial para la prevención del delito.

En el Ecuador, en el 2021, Fundamedios realizó una investigación titulada: Ecuador avanza hacia la Vigilancia Biométrica sin Protección Jurídica, en esta investigación se define: “La videovigilancia es un sistema que combina la tecnología audiovisual con redes de comunicación con el objeto de supervisar imágenes, comportamientos, perfiles de ciudadanos y

el entorno en espacios públicos o privados para alertar sobre situaciones de emergencia ..l" (Almeida María, 2021).

En la Resolución 5 (Registro Oficial Suplemento, 634), que establece las normas de Interoperabilidad de los Sistemas Tecnológicos con el ECU 911, señala quien es el organismo que se encargará de la video vigencia y su definición.

El organismo público encargado de regular la normativa y establecer procesos es el Sistema Integrado de Seguridad ECU 911, y define al sistema de videovigilancia: como un conjunto de dispositivos para registrar, vigilar y monitorear imágenes y/o video en distintas zonas, que están conectadas a un sistema tecnológico. El sistema debe incluir cámaras de video, software para administración, gestión y control; así como el hardware para almacenamiento y gestión de analítica de video.

Para los autores del artículo Dispositivos de vigilancia electrónica. Una mirada desde el Ámbito Jurídico (Chipulli Arturo, 2024), el propósito primordial de los dispositivos de vigilancia electrónica, es crear las condiciones de control que prevengan hechos delictivos, que implica una labor compleja de reconocimiento de conductas sospechosas, amenazas y patrones delictivos de estructuras criminales que operan en sectores específicos, para la formulación de políticas de seguridad específicas que vayan de acuerdo a las necesidades de cada ciudad. Identificadas las políticas de seguridad que se requieren aplicar el Estado debe emitir la normativa necesaria para garantizar el uso correcto que se les dé a los dispositivos de vigilancia.

De su estudio también han determinado que ‘’los dispositivos de vigilancia han sido catalogados como mecanismos que sintetizan simultáneamente las fuerzas morales y el mal en una sociedad. En ellos se puede ver un objeto sagrado o puro que garantiza la protección de las personas y colectivos, que permite monitorear peligros latentes, así como transmitir el sentido de obligatoriedad a los ciudadanos a respectar la reglas y, de la misma forma, castigar a quienes las rompen al mismo tiempo hacen posible que los individuos se comporten adecuadamente en los espacios tanto públicos como privados, al tiempo que generan un historial de comportamiento.’’ (pag.44).

Este criterio es compartido por nosotros ya que, en la muestra tomada, los encuestados consideran que este sistema es positivo. Es muy común al ingresar a un barrio en el Ecuador y encontrar carteles que señalan, “él barrio cuenta con cámaras de vigilancia’’, ‘’usted está siendo gravado’’, con la finalidad de disuadir a los delincuentes y a la vez que el habitante del barrio, el vecino o el visitante mantenga un buen comportamiento para evitar sanciones.

> Los autores recogen también en su investigación el criterio de Arteaga Botello, al indicar que estos dispositivos no han tenido la aceptabilidad esperada en algunos casos, pues se les ha concebido como ‘’artefactos impuros que tienden a vulnerar a las personas en su intimidad y privacidad”, denotándolos como un ataque a las libertades, ya que obligan a cumplir con leyes posiblemente injustas, que permiten la delación de actividades políticas y sociales. Lo anterior, toda vez que alteran los límites de lo público y lo privado, permitiendo que el pasado de las personas sea utilizado mediante poderes que lo escrudiñan (pág. 44).

Si bien los sistemas de videovigilancia facilitan el trabajo investigativo de la policía y de todos los involucrados en el plan nacional de seguridad integral del estado, no debe ser utilizado para limitar el derecho de libertad y de intimidad de las personas, menos aún utilizar la información que capturan para otros fines distintos al de la recolección de la información, como por ejemplo para fines políticos.

De acuerdo con la investigación de Fundamedios, los datos recogidos, no solo se utilizó en el sistema de video vigilancia para prevenir delitos sino también para el seguimiento de políticos no afines al régimen que gobernaba en aquel año que se puso en marcha el Sistema Integrado de Seguridad ECU 911.

Uno de los riesgos de crear el ECU 911 bajo un decreto presidencia

es que responde únicamente al poder Ejecutivo, lo cual lo hace más vulnerable de ser instrumentado por intereses políticos y no contar con independencia para cumplir con el objetivo en favor de la seguridad ciudadana. Varias investigaciones periodísticas (Almeida María, 2021) de medios nacionales e internacionales revelaron que, durante los primeros años de creación, el ECU 911 compartió la información obtenida de sus cámaras a través de un sistema espejo con la ex Secretaria de Inteligencia (SENAIN), creada en 2009. A través de la SENAIN, el gobierno de Rafael Correa espió y persiguió a políticos, funcionarios públicos, activistas y periodistas.

La ex Secretaría Nacional de Inteligencia (SENAIN), recibía información de las cámaras del ECU 911 para perseguir a los detractores del régimen, intervenía escuchas telefónicas ilegales e incluso se utilizaba los medios públicos para filtrar información

privada. Así lo publicó un amplio reportaje de investigación del medio estadunidense The New York Times titulado: “Made in China, Exported to the World: The Surveillance State”’. El reportaje devela el aparataje de vigilancia y espionaje de la Senain con cámaras del ECU 911, página 19. (Almeida María, 2021)

La investigación de Fundamedios reseña que la videovigilancia como mecanismo para resguardar la seguridad ciudadana, nace en el Ecuador a partir de la creación del Sistema Integrado de Seguridad ECU 911, en el año 2011. Los investigadores no pudieron analizar el funcionamiento de los sistemas de este organismo porque en el año 2013 por resolución ministerial MICS-2013-046, se clasificó como reservada toda la información contenida en manuales o instructivos generados y los que llegaren a generarse en el ECU 911 como consecuencia o para la prestación de servicio de despacho de recursos para la atención de emergencias, videovigilancia y recepción de llamadas a la línea única 911, la información se mantendrá bajo reserva por 15 años, esto es, hasta el año 2028, por lo que no se puede conocer si el uso y las capturas que realizó y realiza el sistema no vulnero derechos.

Los sistemas de videovigilancia nacieron para instaurar las condiciones de advertencia, prevención y control, para evitar la concurrencia de hechos delictivos, estos equipos mejoran rápidamente debido al avance tecnológico y es así como hoy estamos frente a la implementación de sistemas del reconocimiento facial y sistemas analíticos que los procesan, por lo que su uso está relacionado a la recolección de una gran cantidad de datos con información personal que obliga a que también la normativa se actualice constantemente

para que el uso de estas herramientas vayan de la mano con la protección al derecho a la libertad, intimidad y protección de datos personales.

Reconocimiento facial para combatir delito

Entre las herramientas más deseables para salvaguardar la seguridad pública se encuentran aquellas que permiten la identificación de la persona a través del reconocimiento facial, que permite identificar a una persona, incluso entre una gran multitud, mediante parámetros faciales y el sistema analítico adquirido por las instituciones encargados de la seguridad pública.

Cristina Domingo (Domingo Jaramillo, 2021), en su artículo incluye un pequeño antecedente sobre cómo se fue implementando el uso del reconocimiento facial para preservar la seguridad ciudadana en lugares públicos, la primera ciudad en implementarlo fue Londres en el año 1998, seguida por Tampa (Florida) durante la final de Superbowl XXXV en 2001.

En Ecuador el sistema de video vigilancia se implementó en el año 2019, de acuerdo con la investigación de Fundamedios" (Almeida María, 2021), pese a existir equipos de reconocimiento facial, estos no pudieron implementarse y aplicar la inteligencia artificial debido a la falta de conexión entre los equipos y las bases de datos. Los Gobiernos Autónomos Descentralizados de Quito y Latacunga, el Consejo de Seguridad de Cuenca y la Corporación para la Seguridad Ciudadana de Guayaquil han adquirido cámaras con capacidad de reconocimiento facial, pero no gestionaron el cruce con las bases de datos, que es el principal requerimiento para aplicar la tecnología biométrica (pág.21).

La tecnología de reconocimiento facial permite la identificación automática de un individuo al hacer coincidir dos o más rostros o caras de imágenes digitales, lo hace detectando y midiendo varios rasgos faciales, extrayéndolos de la imagen y en un segundo paso, comparándolos con rasgos tomados de otros rostros. (European Union Agency for Fundamental Rights, 2019 cómo cito Felicitas Escobar, 2001).

El proceso de reconocimiento facial se compone de varios y distintos subprocesos, como adquisición que consiste en capturar la imagen del rostro de un individuo y convertirlo a una forma digital; detección que es: identificar la presencia del rostro dentro de una imagen digital y marcar el área; normalización esto es, suavizar las variaciones en las regiones faciales detectadas para convertirlas a un tamaño estándar, rotar o alinear distribuciones de color; extracción de características, inscripción, almacenar el registro si se trata de una persona que es reconocida por primera vez, y por último, comparación, medir la similitud entre un conjunto de características tomadas de la muestra con lo previamente inscrito en el sistema.(pág. 212)

El reconocimiento facial involucra una multitud de tecnologías que pueden realizar diferentes tareas con diversos propósitos, en tal sentido, es importante distinguir si su objetivo es la verificación, la identificación o la categorización. La verificación permite comparar si el rostro de un individuo se equipara a otro, la identificación, si se lo puede distinguir y encontrar dentro de una base de datos, la categorización involucra deducir si un sujeto pertenece a un grupo específico, basado en sus características biométricas por ejemplo, sexo, edad. (pág. 212)

Si bien, está tecnología avanza y puede mejorar los procesos de adquisición, detención, normalización, extracción de características, inscripción; es importante que el grado de confiabilidad de estos sistemas sea alto, medible y auditable, para que cuando se extraiga las imágenes del presunto autor de un delito previamente captadas por el sistema de videovigilancia, para someterlo al proceso de análisis durante una investigación, las fuerzas encargadas de la seguridad ciudadana obtenga resultados con un elevado grado de certeza sobre la identidad del posible infractor, minimizando errores, y se convierta esta investigación en una prueba clave dentro de un proceso penal, evitando que el infractor alegue que no es la persona que se busca y por tanto argumente ser inocente.

En el Ecuador esta tecnología para el caso de infractores aún no ha sido implementada, la investigación de Fundamedios señala que el ECU 911 no cruza la base de datos con otras instituciones pues, hasta el momento, no se ha hecho operativa la tecnología de reconocimiento facial ni el software para que un rosto sea asociado con la identidad de una persona.

La Policía Nacional del Ecuador suscribió un convenio con la Dirección General del Registro Civil para revisar en línea la condición del cedulado, número de cédula, apellido(s), nombre(s), fecha de nacimiento, nacionalidad, estado civil, nombre del cónyuge, instrucción, profesión u ocupación, fecha de defunción, fecha de expedición de cédula, sexo, lugar de nacimiento y fecha de matrimonio. (Almeida María, 2021).

Las 18 cámaras de reconocimiento de placas que tiene el ECU 911 en el país si funcionan con una base de datos y software que solamente maneja la Policía Nacional. El ECU

911 solamente brinda el medio tecnológico que es la cámara con el algoritmo de lectura de placas, el informe también señala que la Policía tiene asignadas cámaras específicas de vigilancia en “puntos clientes’’ donde hay mayor índice delictivo o problemas de orden público y tienen la base de datos. El ECU 911 no interviene en esa base de datos, solo remite el registro de las cámaras. Policía Nacional hace un chequeo con la base de datos que tienen y determinan si ese vehículo es robado o no, o si está inmerso en algún delito. (Almeida María, 2021).

La experiencia de otros países que utilizan la herramienta de reconocimiento facial y bases de datos interconectadas con diferentes instituciones públicas, ha permitido que las investigaciones en curso lleguen a resultados positivos en beneficio de la seguridad ciudadana y no se puede cerrar los ojos a que seguirá creciendo y será necesaria para fortalecer la investigación policial. La INTERPOL cuenta con esta tecnología desde finales del 2016, que contiene imágenes faciales enviados por sus países miembros, su sistema puede identificar a una persona o comprobar su identidad mediante la comparación y el análisis de rasgos y contornos faciales utilizado para identificar a terrorista, prófugos, persona de interés o desaparecidos. (INTERPOL, 2024),

En el Ecuador no existe una normativa específica que norme la videovigilancia menos aún el reconocimiento facial; la Policía Nacional mantiene convenios con el Registro Civil, GAD Municipal de Latacunga, pero no se ha podido evidenciar si el trabajo que realiza esta institución ha servido como prueba dentro del proceso penal, de ahí que se hace necesario que la implementación de estos sistemas sea regulada.

Aplicación del reconocimiento facial a la videovigilancia

La tecnología del reconocimiento facial se ha vuelto una herramienta transformadora para la video vigilancia, al incorporar los avances de la inteligencia artificial, para mejorar la eficiencia en sistemas de seguridad y monitoreo. En esta área, el reconocimiento facial, basado en tecnologías de aprendizaje automatizado y profundo posibilita el reconocimiento de la identidad de individuos en tiempo real, incluso bajo condiciones desafiantes. No obstante, la implementación de estas tecnologías no es perfecta, lo cual tiene implicaciones éticas y legales ante los sujetos que son vigilados y monitoreados a través de estas tecnologías.

La evolución de la tecnología de reconocimiento facial ha evolucionado a la par de los avances en el aprendizaje automatizado (también conocido como machine learning) y el aprendizaje profundo (también conocido como deep learning). Estos métodos han mejorado la precisión y eficiencia de los sistemas de reconocimiento facial. Los algoritmos aplicados en el aprendizaje automatizado permiten procesar videos en tiempo real, tales como los producidos por las cámaras de videovigilancia en las ciudades, para identificar a individuos, incluso en escenarios complejos con información y contextos variados, como las variaciones de luz, obstrucciones en la visión, y otras dinámicas ambientales (Mrak, 2023). En particular, las redes neuronales artificiales usadas en estas tecnologías han permitido desarrollar algoritmos más sofisticados de visión computarizada, mejorando la capacidad de estos para adaptarse a ambientes dinámicos y presentar resultados más consistentes (Pulugu et al., 2023).

A pesar de su potencial, demostrado por sus resultados positivos, las condiciones existentes en la video vigilancia presentan algunos desafíos contra la precisión y eficiencia del

reconocimiento facial. Los resultados de esta tecnología pueden ser negativamente influenciados por condiciones no controladas, como movimientos de la cabeza del individuo, en la iluminación y el desenfoque de movimiento; estos factores tienen un impacto significativo en los resultados de estos sistemas. Estudios recientes resaltan la necesidad de crear sistemas más robustos y sofisticados que puedan afrontar estas dificultades, particularmente, rotaciones faciales y distorsiones geométricas (Mrak, 2023). Así mismo, el reconocimiento facial encuentra dificultades en detectar rostros que no siempre están descubiertos, como rostros con o sin máscaras, con lentes, o con otros tipos de accesorios que suelen estar en esta parte del cuerpo, y que podrían distorsionar la detección de éstos (Eker y Bal, 2022) . Además, la privacidad de los individuos es también una fuente importante de debate. Esta preocupación ha motivado el desarrollo de marcos de desidentificación que pretenden asegurar reconocimiento preciso de un individuo, y salvaguardar su privacidad (Park et al., 2024).

Para sobrellevar los desafíos que inician con la aplicación del reconocimiento facial en la video vigilancia, se aplican varias metodologías y técnicas. Por ejemplo, arquitecturas de aprendizaje profundo, como las redes neuronales convolucionales, se usan para procesar datos multidimensionales y extraer información significativa (Omarov et al., 2019). El algoritmo Fisherface también es usado para la detección y reconocimiento de rostros, el cual ofrece resultados positivos en condiciones controladas. Bajo circunstancias más específicas, como el reconocimiento de rostros enmascarados versus rostros descubiertos, el método de Circle Loss ha demostrado ser el más efectivo y preciso (Eker y Bal, 2022). Adicionalmente, la incorporación de modelos de reconocimiento de emociones ha contribuido a nuevas

dimensiones para detectar comportamientos anormales, lo cual ayuda a mejorar las capacidades de los sistemas de reconocimiento facial (Kalyta et al., 2023).

Las pautas para el futuro del reconocimiento facial en la videovigilancia deberán centrarse en solucionar las limitaciones actuales previamente mencionadas, así como mejorar los sistemas y hacerlos más robustos, especialmente en situaciones no controladas. Un área prometedora de esta tecnología es el desarrollo de modelos transparentes e interpretables, específicamente en el reconocimiento de emociones, el cual juega un papel crucial para monitorear y analizar emociones humanas (Kalyta et al., 2023). Por otro lado, las técnicas de anti-spoofing son también de alta relevancia para proteger estos sistemas de ataques físicos, particularmente en situaciones de vigilancia a larga distancia (Fang et al., 2023). Además, optimizar el procesamiento en tiempo real de estos sistemas, e integrarlos en iniciativas de ciudades inteligentes podría proveer nuevas oportunidades para mejorar la seguridad urbana. (Bouzaâchane y Guarmah, 2022).

La aplicación de la tecnología de reconocimiento facial en la videovigilancia representa un avance significativo en el campo de la seguridad y el monitoreo. Sin embargo, su efectividad depende del triunfo de esta tecnología ante los desafíos técnicos éticos a los que se enfrenta. Dicho triunfo puede alcanzarse mediante el avance científico y la innovación en este campo. La integración de tecnologías y métodos avanzados, como los algoritmos de aprendizaje profundo y modelos que se centren en preservar la privacidad de los sujetos bajo vigilancia son también clave para afrontar estos desafíos. A medida que avanzan y evolucionan los sistemas de reconocimiento facial, su potencial para mejor la seguridad, al igual que el respecto a la

privacidad del individuo, son cruciales para que esta tecnología sea exitosa y aceptada en la comunidad.

Impacto del reconocimiento Facial en Derechos Fundamentales

En el mundo se utilizan herramientas y sistemas de reconocimiento facial; las empresas comerciales las usan para obtener información de usuarios, como una mejor discriminación de precios. El campo de aplicación de la tecnología de reconocimiento facial puede dividirse en aplicaciones comerciales y aplicaciones no comerciales. En el sector público y privado, se utilizan biométricos para el control de asistencia de sus empleados.

La biometría se encarga del estudio, control y análisis de los datos biométricos para identificación. Estos datos se pueden recabar a través de: sistemas de reconocimiento de iris; reconocimiento dactilar; reconocimiento vascular y, el reconocimiento facial, que analiza las características únicas faciales de una persona.

En este contexto, los datos biométricos tienen dos características esenciales:

- Son obtenidos por tratamientos automatizados para verificar o determinar la identidad de personas a través de características fisiológicas o conductuales;

- Reconocen características fisiológicas, físicas, conductuales o psicológicas: las características fisiológicas o físicas se definen como medidas o mediciones a parte o partes del cuerpo humano (escáner al iris o huellas dactilares, patrones geométricos del rostro u orejas, reconocimiento de voz, etcétera). Por su parte, las características conductuales o psicológicas se basan en acciones derivadas directa o indirectamente de las características del cuerpo humano. (Garrido Iglesias, 2017)

En este proceso, los derechos de privacidad de los individuos se ven afectados. La Comisión Internacional de Derechos Humanos (2017) en su capítulo 4 Derecho a la privacidad y protección de datos personales, sostiene que el "funcionamiento de internet depende de la creación, almacenamiento y administración de datos personales y de otro tipo. Ello implica que una enorme cantidad de información sobre las personas pueda ser interceptada, almacenada y analizada por los Estados y por terceros" (p.81). Por tanto, es imprescindible la protección de datos en la sociedad actual, que demanda el intercambio y uso de información en la era informática.

Al respecto, en la Carta de los Derechos Fundamentales de la Unión Europea, se encuentran varios derechos fundamentales relacionados con la aplicación de tecnología: el derecho a la dignidad humana, el respeto a la vida privada y la protección de los datos personales, el derecho a la libertad de expresión, la libertad de empresa, el derecho a la protección de la propiedad intelectual, la no discriminación, la igualdad entre mujeres y hombres, la integración de las personas con discapacidad, los derechos de los trabajadores a unas condiciones de trabajo justas y equitativas.

Los sistemas de identificación biométrica en espacios públicos, que se apliquen en correspondencia con la ley, son compatibles con los derechos fundamentales, por ejemplo, vigilancia en vía pública, control de asistencia en jornadas de trabajo. En estos casos, los responsables, directivos o ejecutivos, deben evaluar el impacto del uso del sistema, en los derechos fundamentales del individuo.

En otros casos, el derecho a la privacidad, estaría en riesgo, ya que, la imagen de la cara de una persona debe ser protegida de usos ilegales o no autorizados por esa persona, en el mundo real y virtual. Sin embargo, muchas personas publican fotos de sus caras, en internet, sin darse cuenta que pueden ser utilizadas para distintos objetivos, sin que la Ley de Inteligencia Artificial, pueda detener, tampoco, se puede evitar que las personas compartan imágenes.

Ponce-Cedeño et al (2023) afirman que el derecho a la intimidad y/o privacidad, es esa posibilidad de “mantenerse alejado, de no facilitar información de carácter personal, de no formar parte de la vida colectiva, de proteger las relaciones o vínculos filiales, todo ello mediante una tutela legal”; y se evidencia el derecho al respeto que todo ser humano merece por ser persona. Concuerdan en que las herramientas tecnológicas, son útiles en el desarrollo del ser humano; sin embargo, el exceso de uso de inteligencia artificial, puede generar en las organizaciones u otras personas, rastreo o manipulación del comportamiento, si se aplica sin tutela efectiva.

Teodor y Dragos (2022) concluyeron que el uso de los datos almacenados o la recopilación de nuevos datos, podría contribuir al rediseño de los servicios que favorezcan a la persona. En este contexto, el uso de tecnología para reconocimiento facial mantiene compatibilidad con los derechos fundamentales, siempre que esté respaldada por legislación capaz de promover la protección de la privacidad de las personas. En Chile, Bravo et al. (2018) identificaron que muchos ciudadanos analizaron la utilidad del reconocimiento facial como medida de seguridad, el 50% de la percepción corresponde a las variables: las normas

sociales, la percepción de responsabilidad, el optimismo, el grado de innovación, y la percepción de inseguridad.

Ragas (2020), analizó el uso de la tecnología de vigilancia, “permite escapar de la dicotomía represión/resistencia y enfocarse en acciones insertas al interior de dichos extremos, como lo son la creación de una identidad en base al ocultamiento del rostro y la defensa pública de la privacidad” (p. 252). Al respecto, es fundamental comprender los cambios en torno a la privacidad, lo público, el uso del cuerpo y la adopción de tecnologías biométricas en un “principio aceptadas por la sociedad y luego rechazadas cuando su utilización rompe ciertos parámetros” (Ragas, 2020, pág. 253).

Burbano et al, (2021) concluyeron que, el uso de sistemas de vigilancia en Chile no se ha dado de manera causal; se ha aprovechado el constante miedo que acosa a la sociedad y deben retroalimentarse desde las nuevas dinámicas de la sociedad, porque genera una afectación que se puede medir en distintas áreas y ámbitos sociales. En Paraguay, la implementación de cámaras de vigilancia con tecnología de reconocimiento facial en espacios públicos afecta directamente al derecho a la privacidad (Penayo y Barrios Duarte, 2023). Por ello, se recomienda diagnosticar la aplicación del sistema, en cada comunidad.

En Ecuador, se protege el derecho a la intimidad, en la Carta Magna, en su artículo 66, en concordancia con el artículo 12 de la Declaración Universal de Derechos Humanos, que manifiesta que nadie puede ser objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio, ni de ataques a su honra o a su reputación, puesto que todo ser humano tiene derecho a la protección de la ley ante tales injerencias o ataques. Los autores, concluyeron que

la tecnología genera desafíos para proteger el derecho a la privacidad e intimidad, así como, el reconocimiento de nuevos derechos.

A partir de los estudios expuestos, se concluye que el reconocimiento facial es una permite identificar la identidad de una persona a partir de sus características faciales, ha generado un debate significativo en torno a su impacto sobre los derechos fundamentales, especialmente en lo que respecta a la privacidad, libertad personal, no discriminación y libertad de expresión. A continuación, se analizan algunos de los efectos más relevantes:

Derecho a la privacidad

El derecho a la privacidad es uno de los más afectados por el uso del reconocimiento facial. Esta tecnología permite la recopilación y el procesamiento de datos biométricos sin el conocimiento ni el consentimiento explícito de los individuos. Si se implementa sin regulación estricta, puede llevar a una vigilancia masiva, donde las personas se ven constantemente observadas y rastreadas. Esto puede tener un efecto disuasivo sobre la libertad de movimiento y expresión, ya que las personas pueden sentirse menos libres de participar en actividades cotidianas por temor a ser identificadas y monitorizadas.

Libertad de expresión y asociación

El reconocimiento facial puede limitar la libertad de expresión y la libertad de asociación. Si las autoridades o actores privados usan la tecnología para vigilar a personas que participan en manifestaciones, protestas o en cualquier actividad pública, esto puede crear un clima de autocensura. Las personas podrían abstenerse de expresar sus opiniones o asociarse con otros, temiendo ser identificadas y perseguidas por sus puntos de vista o actividades. En este

contexto, el derecho a la libre expresión se ve afectado, ya que la sensación de estar siendo constantemente vigilado puede inhibir el ejercicio de este derecho.

Discriminación y sesgo

El reconocimiento facial también ha sido criticado por su potencial de discriminación; ya que, pueden tener un sesgo racial, de género o de edad, mostrando una mayor tasa de error en personas de piel oscura, mujeres o personas mayores. Este sesgo puede resultar en falsas identificaciones, que pueden tener consecuencias perjudiciales para las personas afectadas, como detenciones incorrectas, exclusión de servicios o discriminación laboral. Por tanto, la implementación de esta tecnología sin una evaluación rigurosa de su imparcialidad puede violar el principio de igualdad ante la ley.

Derecho a la protección de datos personales

El uso del reconocimiento facial plantea preocupaciones sobre la protección de los datos personales. La captura de imágenes faciales puede generar enormes bases de datos biométricos, que incluyen información sensible sobre las personas. Si estos datos no son gestionados adecuadamente, existe el riesgo de que sean mal utilizados, ya sea por hackeos, filtraciones de información o abuso por parte de actores estatales o privados. Además, la falta de transparencia sobre cómo se recopilan, almacenan y usan estos datos puede violar las normas sobre protección de datos establecidas en normativas como el Reglamento General de Protección de Datos (GDPR) en Europa.

Excesiva vigilancia estatal y control social

El uso de tecnologías de reconocimiento facial por parte del Estado puede llevar a un control social excesivo. En lugares donde se emplea esta tecnología, como en el acceso a espacios públicos o en el monitoreo de vehículos, se corre el riesgo de que el Estado vigile a los ciudadanos sin una justificación legal clara o sin la debida supervisión judicial. Esto puede dar lugar a abusos de poder, especialmente si se utiliza para fines de represión política o control social.

El impacto del reconocimiento facial en los derechos fundamentales depende en gran medida de cómo se regule y utilice esta tecnología. Sin una regulación adecuada y controles estrictos, puede generar riesgos considerables para la privacidad, la no discriminación, y la libertad de las personas. Es fundamental que el uso de esta tecnología sea transparente, proporcional, y respetuoso con los derechos humanos, y que se proteja a las personas contra posibles abusos y discriminación.

Retos y Riesgos Legales de la Protección de Datos Biométricos

La protección de datos biométricos es un aspecto fundamental en la discusión sobre la seguridad pública y el respeto de la privacidad. La Ley Orgánica de Protección de Datos Personales ecuatoriana define al dato biométrico como un dato personal único, que lo convierte en un dato sensible que es objeto de protección legal.

La normativa internacional garantiza el derecho a la privacidad, entre ellas, tenemos la Declaración Universal de Derechos Humanos que, en su artículo 12, prohíbe injerencias en la vida privada. De igual manera, el Pacto Internacional de Derechos Civiles y Políticos garantiza el derecho a la privacidad en su artículo 17. En el contexto europeo, la Carta de los Derechos

Fundamentales (artículo 8) y el Convenio Europeo de Derechos Humanos (artículo 8), también proclaman el derecho a la privacidad. Este marco jurídico convierte al derecho a la privacidad en un derecho fundamental que debe ser garantizado en el procesamiento de los datos biométricos, que es un reto legal para la sociedad democrática en la era digital.

El ordenamiento jurídico de Bulgaria incluye la Directiva 95/46/CE de la Unión Europea y la Ley de Protección de Datos Personales del 2002 que garantiza que los datos sensibles deben estar protegidos con respecto a su procesamiento y uso (Deliversky y & Deliverska, 2018). A diferencia de Alemania que sus normas jurídicas de datos no protegen, de manera específica, los datos biométricos (Hornung et al., 2010).

Desde la perspectiva jurídica y de la privacidad, los sistemas biométricos han generado riesgos para la protección de datos personales, uno de los más relevantes es la obtención ilegal de datos biométricos. Sin embargo, se debe mencionar que los retos generados por los sistemas biométricos no son particulares de esta tecnología. Cada avance tecnológico genera riesgos en la sociedad de la información y del internet. En la sociedad del riesgo, la producción de riqueza, y en una sociedad contemporánea, la producción tecnológica, genera riesgo social que tiene consecuencias en la implementación de políticas estatales (Climent, 2023).

El tratamiento de los datos biométricos, que consiste en recoger información del cuerpo de una persona conlleva a graves riesgos éticos (Domaica, 2019). Los riesgos que se generan pueden afectar al respeto de la dignidad humana, por lo que el tratamiento del dato biométrico requiere ser un proceso especial al ser dato sensible.

Las discusiones por los dilemas éticos en el uso de la inteligencia artificial es un tema debatido en la actualidad. En el uso de esta tecnología, hay varios dilemas éticos a destacar: 1) Invasión de los entornos, introduciendo información falsa para que un sistema cometa errores; 2) Intimidad, la tecnología puede usarse para detectar vulnerabilidades en el sistema, y con ello, lograr publicación de información personal; 3) Seguridad, la inteligencia artificial perjudica a la seguridad política con la elaboración de perfiles basados en sesgos, y en campañas de desinformación; y, 4) Identidad, en el uso del de un examen facial para la implementación en armas autónomas (Brundage et al., 2018).En el contexto mundial, hay un caso que generó alarmas sobre los sesgos en la aplicación de una tecnología, lo que genera varios dilemas éticos. El software denominado “Rekognition” creado por Amazon, es un programa de reconocimiento facial. Sin embargo, la Unión Americana por los Derechos Civiles (ACLU) detectó que el programa tiene sesgo racional. Este programa es un ejemplo de cómo la tecnología puede generar dilemas éticos, y con ellos afectar a derechos fundamentales, como el derecho a la no discriminación.

Otro de los casos emblemáticos relacionado a la aplicación de la tecnología y el reconocimiento facial, es el caso “Bridges vs. South Wales Police”. El señor Edward Bridges, demandó a la Policía de Gales por la implementación de la tecnología de Reconocimiento Facial Automático sin su consentimiento. La Corte de Apelaciones determinó que la tecnología vulneró el artículo 8 del Convenio Europeo de Derechos Humanos.

En este contexto, el Reglamento de Inteligencia Artificial de la Unión Europea, se convierte en un documento que pionero en la regulación de la Inteligencia Artificial. En su

normativa, recoge las directrices éticas del año 2019, y determinan siete principios éticos: 1) Acción y supervisión humana; 2) Solidez técnica y seguridad; 3) Gestión de la privacidad y de los datos; 4) Transparencia; 5) Diversidad, no discriminación y equidad; 6) Bienes Social y Ambiental; y, 7) Rendición de Cuentas (Reglamento Europeo de la Inteligencia Artificial , 2024)

En el contexto ecuatoriano, nos enfrentamos el desafío de garantizar el desarrollo tecnológico y el respeto de los derechos humanos. Es importante adoptar las disposiciones del Reglamento de Inteligencia Artificial, y con ello, evitar los dilemas éticos, considerando que el Reglamento determina como riesgo inaceptable los sistemas de identificación como el reconocimiento facial. Según Hornung et al (2010), los riesgos más relevantes del tratamiento de datos biométricos, son los siguientes: a) robo de identidad, al existir captación ilegal de datos biométricos en públicos; b) tratamiento de información adicional, relacionado a enfermedades; c) seguimiento y vigilancia continua; d) recolección de datos biométricos; e) vinculación de bases de datos con información de datos biométricos; y, f) equivocación de decisiones.

Los riesgos con los datos biométricos no solo se generan en el contexto de la seguridad pública, sino también en la vida cotidiana, especialmente con el uso de las redes sociales. El uso de la inteligencia artificial, ha incrementado nuevos niveles de vulneración de derechos, desde la suplantación de identidad hasta el uso de la información para el cometimiento de delitos, lo que nos llevaría a plantearnos sobre la pérdida de la privacidad (Sánchez, 2023).

Para Soriano (2021), existen varios riesgos para la protección de los derechos en los procesos automatizados de toma de decisiones, entre ellos, se encuentra los sesgos y errores,

la discriminación y riesgos para la intimidad de las personas. Estos riesgos se generan por el uso de procesadores informáticos de datos, utilizados en la toma de decisiones de la administración pública, particularmente para la seguridad pública.

CAPÍTULO 4

Conclusiones

El uso de la videovigilancia con reconocimiento facial gana cada vez más fuerza en una sociedad ecuatoriana con altos índices de delincuencia que clama por mayor seguridad y siente que una vigilancia masiva va a prevenir e intimidar a un perpetrador en la consecución de actos delictivos. En base a nuestra muestra ejecutada en 201 personas de diferentes grupos etarios, el 84% de encuestados está de acuerdo con el uso de la video vigilancia con reconocimiento facial en el espacio público por parte de las instituciones encargadas de la seguridad ciudadana.

A pesar de, esta aceptación el objetivo general relacionado a la descripción de datos biométricos de reconocimiento facial por parte de la Policía Nacional y la vulneración de los derechos fundamental de los ciudadanos, permitió identificar que, el reconocimiento facial refleja un avance importante en la identificación de los ciudadanos, sin embargo, la implementación de la tecnología en el contexto de la seguridad pública presenta desafíos en la protección de los derechos fundamentales. En el escenario ecuatoriano, que guarda relación con las investigaciones internacionales, se evidencia que el reconocimiento facial vulnera derechos esenciales como el derecho a la privacidad, el derecho a la protección de datos personales, el derecho a la no discriminación, la libertad de expresión y de asociación. La investigación demuestra que el derecho a la privacidad es principalmente vulnerable a causa de la recopilación de datos biométricos sin que exista el conocimiento y consentimiento de los ciudadanos.

El primer objetivo específico relacionado al análisis normativo, doctrinario y crítico sobre los riesgos que implica para los ciudadanos la captura y uso de datos biométricos de reconocimiento facial por parte de la Policía Nacional, permitió que, la aplicación de la tecnología y la protección de datos biométricos representa un desafío legal en la sociedad digital y de la información. La implementación genera graves riesgos como el tratamiento ilegal de datos biométricos, el robo de identidad y la vigilancia masiva, y la vulneración de derechos fundamentales como la dignidad humana y el derecho a la privacidad. En el contexto ecuatoriano, la Ley Orgánica de Protección de Datos Personales determina el marco jurídico para la protección de datos sensibles, pero es importante establecer políticas públicas y mecanismos de protección que no permitan la vulneración de los derechos fundamentales.

El segundo objetivo específico relacionado a conocer qué datos biométricos de reconocimiento facial se capturan para no afectar los derechos fundamentales, permitió conocer que el reconocimiento facial es una herramienta que capta rasgos faciales que, en función de la forma que hayan sido captadas y cotejados los rasgos faciales permiten logar la identificación de un individuo con cierto nivel de fiabilidad. En el Ecuador, de manera general señala como funciona un sistema video vigilancia, y los métodos de analítica que se aplicará a los videos capturados, mas no se ha podido ubicar instructivos o manuales que permitan identificar las bondades del sistema que se va a adquirir o que ya han sido adquiridos para el reconocimiento facial, ni cuál es el porcentaje de falla al momento de identificar a una persona, tampoco se ha ubicado instructivos o manuales que permitan limitar la captura, el uso y

procesamiento del dato biométrico en cualquier momento de aplicación del sistema, ni el tiempo de permanencia de la información.

Recomendaciones

No es posible justificar el uso indiscriminado del Sistema de Videovigilancia con tecnología de reconocimiento facial, como una herramienta tecnológica eficaz en seguridad ciudadana, toda vez que el uso de la misma trae consigo una afectación a los derechos de las personas como son privacidad, e intimidad, y a la protección de datos personales en especial los datos biométricos en espacios públicos; a su vez puede ser empleada para la ubicación y detención de personas requeridas por la justicia, aquellas que tengan una boleta de captura vigente. Adicionalmente cualquier información recopilada sobre estas personas debe ser de uso exclusivo para su judicialización, debiendo almacenar esta información hasta que el proceso judicial finalice, debiendo, pese a la autonomía del sistema, contar con el monitoreo constante por parte de personal policial capacitado, para el manejo de este.

Nuestra Constitución establece como una garantía la protección de los datos personales, se suma a esta la Ley Orgánica de Protección de Datos Personales y su reglamento, que prohíben el tratamiento de datos sensibles, como son considerados los datos biométricos, sin que exista dentro de la normativa las reglas a seguir para un adecuado tratamiento de esta información obtenida mediante sistemas de videovigilancia, y que si bien es cierto el derecho de una persona finaliza donde empieza el de la otra, tampoco se establece el límite o límites a considerar durante el tratamiento de estos datos biométricos, o a su vez que, en la Ley Orgánica de Protección de Datos Personales de Ecuador, al igual que el

Reglamento General de Protección de Datos de la Unión Europea, debería establecer que se puede efectuar el tratamiento de datos biométricos en situaciones de cooperación judicial en materia penal, a ser tratados por el ente encargado de la seguridad ciudadana es decir Policía Nacional.

Para el tratamiento de los datos recopilados por el sistema de videovigilancia con reconocimiento facial, se debe establecer manuales, protocolos e instructivos, a fin de que este sea ético y en estricto apego de la normativa legal vigente, debiendo priorizar su uso de manera exclusiva para el fin destinado, evitando el mal uso de estos datos para la ubicación y detección de manera indiscriminada para efectos políticos, en la cual se especifique o delimite los datos biométricos a recopilar, como debe ser su almacenamiento, y las circunstancias en las cuales pueden ser utilizados, y contar con mecanismos de seguridad a fin de evitar o minimizar el robo, usurpación, o apropiación indebida de la base de datos biométricos.

Es importante poder contar con pistas de auditoría, como una herramienta esencial para la seguridad, transparencia, trazabilidad y en especial como evidenciable del cumplimiento de la normativa a ser aplicada para un adecuado tratamiento, lo que conllevaría a un control que prevenga abusos, y garantice la protección de la privacidad e integridad de estos datos biométricos.

Al existir el apoyo o la coordinación con los Gobiernos Autónomos Descentralizados Municipales, las instituciones como el ECU 911, Registro de Datos públicos, Consejo de la Judicatura, están en la obligación de suscribir convenios para el consumo de información, se deberá incluir una cláusula en la que se establezca que la actualización de la información debe

ser automatizada es decir que se actualice apenas se produzca un cambio en el sistema, para así minimizar los errores para evitar perjudicar a ciudadanos que ya hayan cumplido su pena, de esta forma se garantiza la transparencia en la gestión del manejo de datos personales y la fiabilidad del proceso.

Para la implementación de estos sistemas de videovigilancia con reconocimiento facial se debe priorizar que, mediante la Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional, se desarrolle este tipo de sistemas a fin de evitar en lo mínimo la contratación de un tercero, debiendo en el desarrollo incluir las pistas de auditoria correspondientes, lo cual coadyuva a garantizar la confidencialidad, integridad y disponibilidad de la información a ser tratada.

El Delegado Institucional vigilará que el análisis de los videos capturados por el sistema de video vigilancia, incluyendo aquellos con reconocimiento facial, sea limitado a ciertos agentes policiales especializados de los ejes investigativos e inteligencia de la Policía Nacional, que suscriban acuerdos de uso y confidencialidad de la información. Estos agentes deben tener un alto conocimiento en la protección de datos personales, así como en derechos y libertades fundamentales de los ciudadanos para evitar el uso fraudulento del sistema. Además, deberán someter a este personal a pruebas de confianza continuas, para asegurar que su intervención en el análisis de la información y datos a ser tratados no sea utilizada para intereses propios, o sea facilitada a grupos delincuenciales evitando así la revelación de secretos.

Se deberá vincular al Oficial de Seguridad de la Información y el Delegado de Protección de Datos Personales de la Policía Nacional, a fin de que brinden el asesoramiento

sobre nuevas tecnologías y su posible implementación en el sistema de video vigilancia, incluyendo aquellas con reconocimiento facial, para la actualización de los instructivos, políticas o manuales que utilizará la Policía Nacional para el tratamiento responsable de esta información, además podrán auditar estos sistemas, sus herramientas de seguridad, a fin de detectar vulnerabilidades, y recomendar su fortalecimiento, garantizando la seguridad de la información.

Para el éxito en el uso de este sistema de videovigilancia con reconocimiento facial, se debe procurar establecer mecanismos de control para su uso, herramientas de seguridad, evaluaciones periódicas de impacto, y lo más importante determinar una temporalidad en el tratamiento de la información recopilada por el mismo, procurando el respeto a los derechos fundamentales de las personas, sumado a esto la socialización para la ciudadanía donde se informe la implementación de este tipo de tecnologías, cuál será el tratamiento que se dará a la información a ser recabada.

Podríamos tomar como referencia China, el mismo que es denominado el Estado que todo lo ve, gracias a la red de videovigilancia más grande y tecnológicamente sofisticada del mundo, teniendo un aproximado de 170 millones de cámaras, de las cuales un gran número cuentan con inteligencia artificial, para reconocimiento facial, siendo posible descifrar edad, etnia y genero mediante la obtención de datos biométricos, y es así que en cuanto a la seguridad ciudadana, este sistema reconoce rostros sospechoso, enviando de inmediato una alerta a la sala de monitoreo y a la policía.

Son tantas las bondades que pone a disposición este sistema que puede relacionar el rostro obtenido con el vehículo, familiares, e incluso con personas que se ha mantenido contacto, lo cual dentro de investigaciones penales sería de mucha ayuda brindando elementos que pueden llegar a fortalecer las investigaciones. Podría considerarse un sistema de control absoluto, pero China desde 2021, se ha sumado a la tendencia mundial, la protección de los datos y la información personal, así como se desprende de la Propia Ley de Protección de Información Personal de China (PIPL), Art 26, (Cree,ers de Rogier, Grhan Websert, 2021) cualquier imagen personal o información identificable recopilada debe servir únicamente para el propósito de la seguridad pública y el uso para otros fines requiere del consentimiento explícito de los individuos

Referencias

Almeida María, R. S. (2021). *Ecuador avanza hacia la vigilancia biométrica sin protección jurídica*. Fundamedios: https://www.fundamedios.org.ec/fundamedios-pide-al-gobierno-y-a-los-municipios-abstenerse-de-implementar-el-reconocimiento-facial-en-ecuador/

Andrade, A. (2018). *Seguridad Publica.* ile:///C:/Users/cplmanabi1.audi1/Downloads/8302-Texto del artículo-38515-1-10-20231115.pdf

Arias. (2021). *Seguridad Publica.* file:///C:/Users/cplmanabi1.audi1/Downloads/8302-Texto%20del%20art%C3%ADculo-38515-1-10-20231115-2.pdf

Asamblea Nacional. (1 de 12 de 2024). *Ley de Seguridad Pública Y Del Estado*. https://www.consejodiscapacidades.gob.ec/wp-content/uploads/downloads/2016/07/LEY_DE_SEGURIDAD_P%C3%9ABLICA_Y_DEL_ESTADO.pdf

Bouzaâchane, K., & Guarmah, E. (2022). Applying Face Recognition in Video Surveillance for Security Systems. *8th International Conference on Optimization and Applications (ICOA)*, (págs. 1-5). https://doi.org/https://doi.org/10.1109/ICOA55659.2022.9934625

Bravo, C., Ramirez, P., & Arenas, J. (2018). Aceptación del Reconocimiento Facial como Medida de Vigilancia y Seguridad; Un Estudio Empírico en Chile. *Información Tecnológica*. https://doi.org/http://dx.doi.org/10.4067/S0718-07642018000200115

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., & & Amodei, D. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. *Future of Humanity Institute*. https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf

Burbano Ardilla, A., Navia López, A., & Díaz Losada, S. (2021). Sistemas de vigilancia y su efecto en el derecho a la intimidad desde el discurso de la seguridad. *Revista Latinoamericana de Derechos Humanos*, 33-51. https://doi.org/https://dx.doi.org/10.15359/rldh.33-1.2

Chipulli Arturo, y. L. (2024). Dispositivo de vigilancia electronica. Una mirada desde lo jur;idico. Uso de Dispositivos de vigilancia electrónica en materia de seguridad publica y seguridad ciudadana> Retos y perspectivas. Mexico, Mexico. https://www.researchgate.net/profile/Claudia-Rivera-Hernandez/publication/385086241_Uso_de_dispositivos_de_vigilancia_electronica_en_materia_de_seguridad_publica_y_seguridad_ciudadana_Retos_y_perspectivas/links/67150ddcd796f96b8ec38611/Uso-de-dispositivos

Climent, J. (2023). Sociedad del riesgo: producción y sostenibilidad. *Papers: Revista de Sociología*. https://doi.org/https://papers.uab.cat/article/view/v82-climent/pdf-es

Comisión de Salud Pública. (1999). *Pantallas de Visualizacion De Datos*. https://www.sanidad.gob.es/ciudadanos/saludAmbLaboral/docs/datos.pdf

Comisión Interamericana de Derechos Humanos, O. (2017). *Estándares para una internet libre, abierta e incluyente.* https://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf

Constitución de la República del Ecuador. (2008). *Constitución de la República del Ecuador.* Montecristi: Fiel Web Evolución Jurídica.

Cree,ers de Rogier, Grhan Websert. (07 de septiembre de 2021). *Dicicichina*. Universidad de Stanford: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/

Data Protecction Working Party, 2012 como lo cito Felicitas Escobar. (2021). *La Tecnolog[ia que Reconoce Rostros, pero ...Desconoce Derechos? Derecho y Nuevas tecnologias.* Buenos Aires. https://www.studocu.com/es-ar/document/universidad-de-buenos-aires/teoria-del-delito-y-sistema-de-la-pena/derecho-y-nuevas-tecnologias/70557007

Data Protection Working Party, 2012 como lo citó Felicitas Escobar. (2021). *La Tecnología que Reconoce Rostros, pero Desconoce Derechos.* Buenos Aires. https://www.studocu.com/es-ar/document/universidad-de-buenos-aires/teoria-del-delito-y-sistema-de-la-pena/derecho-y-nuevas-tecnologias/7055

Dávila Molina , Cristina Maribel. (2003). Seguridad pública en el Ecuador: https://ciencialatina.org/index.php/cienciala/article/view/8302/12501

Deliversky, J., & & Deliverska, M. (2018). Ethical and Legal Considerations in Biometric Data Usage—Bulgarian Perspective. *Frontiers in Public Health*. https://doi.org/https://doi.org/10.3389/fpubh.2018.00025

Domaica, J. (2019). Datos personales biométricos dactiloscópicos y derechos fundamentales: Nuevos retos para el legislador. https://apidspace.linhd.uned.es/server/api/core/bitstreams/56c453f1-2b82-4b27-b33f-69f57fb587d7/content

Domingo Jaramillo, C. (2021). Utilización del Sistema de Reconocimiento Facial para perservar la Seguridad Ciudadana. *Revista*. https://revistaseug.ugr.es/index.php/cridi/article/view/20899

Eker, O., & Bal, M. (2022). A comparative analysis of the face recognition methods in video surveillance scenerios. *ArXiv, abs*. https://doi.org/https://doi.org/10.48550/arXiv.2211.02952

El Universo. (2 de Enero de 2024). https://www.eluniverso.com/noticias/seguridad/el-91-de-los-crimenes-ocurridos-durante-2023-estan-bajo-investigacion-es-decir-no-han-sido-resueltos-nota/

European Union Agency for Fundamental Rights, 2019 cómo cito Felicitas Escobar. (2001). *La Tecnología que Reconoce Rostros, pero.... Desconocen Derechos? Dercho y Nuevas Tecnologías.* https://www.studocu.com/es-ar/document/universidad-de-buenos-aires/teoria-del-delito-y-sistema-de-la-pena/derecho-y-nuevas-tecnologias/70557

Europeo, P. (2024). *Reglamento Europeo de la Inteligencia Artificial .*

Fang, H., Liu, A., J., W., Escalera, S., Zhao, C., Zhang, X., . . . Lei, Z. (2023). Surveillance Face Anti-Spoofing. *IEEE Transactions on Information Forensics and Security*, 1535-1546. https://doi.org/https://doi.org/10.1109/TIFS.2023.3337970

Garrido Iglesias, R. &. (2017). La biometría en CHile y sus riesgos. *Revista Chilena de Derecho y Tecnología*, 1-25.

Goebertus Estrada, J. (17 de enero de 2025). *Ecuador necesita un enfoque diferente para combatir el crimen organizado*. Human Rights Watch: https://www.hrw.org/news/2025/01/17/ecuador-needs-different-approach-fighting-organized-crime

Herrera R. (2018). La seguridad pública en el Ecuador: Análisis de la situación actual y. Revista de la Facultad de Ciencias Jurídica.

Hornung, G., Desoi, M., & Pocs, M. (2010). Biometric Systems in Future Preventive Scenarios. *Legal Issues and Challenges*, 83-94.

INTERPOL. (2024). *INTERPOL*. Retrieved 10 de 12 de 2024, from https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Reconocimiento-facial

Kalyta, O., Barmak, O., Radiuk, P., & Krak, I. (2023). Facial Emotion Recognition for Photo and Video Surveillance Based on Machine Learning and Visual Analytics. *Applied Sciences*. https://doi.org/https://doi.org/10.3390/app13179890

Ley de Seguridad Publica y del Estado. (2017). *Estado Ecuatoriano.* https://www.flacso.edu.ec/portal/modules/umPublicacion/pndata/files/docs/sfsegdammert.pdf

Manea, T., & Dragos Lucian, I. (2022). AI Use in criminal matters as permitted under EU Law and as needed to safeguard the essence of fundamental rights. *Law in Changind*, 17-32. https://doi.org/https://doi.org/10.54934/ijlcw.v1i1.15

María Paula Romo Rodríguez Ministra del Interior y Secretaria Nacional de Gestión de la Política. (12 de 2024). *PLAN ESPECÍFICO DE SEGURIDAD PÚBLICA Y CIUDADANA*. https://www.defensa.gob.ec/wp-content/uploads/downloads/2019/07/plan-nacional-min-interior-web.pdf

Ministerio de Gobierno. (2021). *Reglamento del Sistema Informático Integrado de la Policía Nacional del Ecuador SIIPNE.* Quito: MDG.

Ministerio del Interior. (2019). *Estatuto Orgánico de Gestión Organizacional por Procesos de la Policía Nacional.* Quito: MDI.

Ministerio del Interior. (2019). *Plan Específico de Seguridad Pública y Ciudadana 2019-2030.* Quito: DCDO.

Ministerio del Interior socializa estrategias de Seguridad Pública. (1 de 12 de 2024). *Boletín N°230*. https://www.ministeriodelinterior.gob.ec/ministerio-del-interior-socializa-estrategias-de-seguridad-publica/

Mrak. (2023). Face recognition methods in video surveillance systems using machine learning. *Information and communication techonologies, electronic engineering*. https://doi.org/https://doi.org/10.23939/ictee2023.02.033

Norris, C. M. (2004). *The Growth of CCTV:A a global perspective on the international diffusion of video surveillance in publicly accesible space.* Surveillance & Society: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3369/3332

Omarov, B., Shekerbekova, S., Gusmanova, F., Oshanova, N., Sarbasova, A., Yessengaliyeva, Z., . . . Sultan, D. (2019). Applying face recognition in video surveillance security systems. En J.-M. B.-B. Manuel Mazzara, *Software Tchnology: Methods and Tools* (págs. 271-280). https://doi.org/https://doi.org/10.1007/978-3-030-29852-4_22

Park, D., Na, H., & Choi, D. (2024). Verifiable Facial De-Identification in Video Surveillance. *IEEE Access*. https://doi.org/https://doi.org/10.1109/ACCESS.2024.3399230

Penayo, O. A., & Barrios Duarte, A. (2023). Análisis de un amparo en pos de la protección de datos personales. En *Por la defensa de los datos personales en Paraguay. Compendio de ensayos de la clínica 2022 "Derecho a la privacidad y datos personales.* Tecnología & Derechos Humanos.

Personales, L. O. (26-05-2021). *Ley Organica de Protección de Datos Personales.* https://app.lexis.com.ec/sistema/visualizador-norma/PUBLICO-LEY_ORGANICA_DE_PROTECCION_DE_DATOS_PERSONALES

Polícia Nacion del Ecuador-DNTIC. (2023). *Política Tecnologíca Institucional.* Quito: S/N.

Ponce-Cedeño, A., Robles-Zambrano, G., & Diaz-Basurto, I. (2023). Inteligencia artificial y el derecho a la intimidad-privacidad. *Iustit Socialis. Revista Arbitrada de Ciencias Jurídicas*, 81-93. https://doi.org/https://doi.org/10.35381/racji.v8i1.2493

Pulugu, D., Srivastava, R., & Pal, S. (2023). Machine learning based facial recognition for video surveillance systems. *Ictact Journal on Image and Video Processing*. https://doi.org/https://doi.org/10.21917/ijivp.2023.0448

Quironprevencion. (2020). *Daños a la salud por exposición a pantallas de equipos informáticos*. https://www.quironprevencion.com/blogs/es/prevenidos/danos-salud-exposicion-pantallas-equipos-informaticos#:~:text=Trastornos%20extraoculares%3A%20cefaleas%2C%20v%C3%A9rtigos%20o,texto%20que%20se%20debe%20leer.

Ragas, J. (2020). La batalla por los rostros: el sistema de reconocimiento facial en el contexto del “estallido social” chileno. *MERIDIONAL Revista Chilena de Estudios Latinoamericanos*, 247-258. https://doi.org/DOI: 10.5354/0719-4862.57137

Ramirez 2021, como citó en Uribe, Dennisse. (2024). *El aviso de Privacidad de Datos Personales en la Era Digital de la Videovigilancia.* México, México: Montiel & Soriano S.A. de CV. https://www.researchgate.net/profile/Claudia-Rivera-Hernandez/publication/385086241_Uso_de_dispositivos_de_vigilancia_electronica_en_

materia_de_seguridad_publica_y_seguridad_ciudadana_Retos_y_perspectivas/links/67150ddcd796f96b8ec38611/Uso-de-dispositivos

Registro Oficial 435. (13-11-2023). *Reglamento de la Ley de Orgánica de Protección de Datos Personales.* https://app.lexis.com.ec/sistema/visualizador-norma/PUBLICO-REGLAMENTO_DE_LA_LEY_ORGANICA_DE_PROTECCION_DE_DATOS_PERSONALES

Registro Oficial 449. (20 de 10 de 20-10-2008). *Constitución de la República del Ecuador.* https://app.lexis.com.ec/sistema/visualizador-norma/PUBLICO-CONSTITUCION_DE_LA_REPUBLICA_DEL_ECUADOR

Registro Oficial 449. (20-10-2008). *Constitución de la República del Ecuador.* https://app.lexis.com.ec/sistema/visualizador-norma/PUBLICO-CONSTITUCION_DE_LA_REPUBLICA_DEL_ECUADOR

Registro Oficial Sumplento 114. (2022). *AGENDA DDE TRANSFORMACION DIGITAL DEL ECUADOR.* chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://esilecstorage.s3.amazonaws.com/biblioteca_silec/REGOFORIGINAL/2022/4A63B48A854B0664950175FCB177B68D0094DFCA.pdf

Registro Oficial Suplemento. (2009). *Ley de Seguridad Pública. Título IV De la seguridad ciudadana. Art;ículo 23.* https://app.lexis.com.ec/sistema/visualizador-norma/FFAA-LEY_DE_SEGURIDAD_PUBLICA_Y_DEL_ESTADO

Registro Oficial Suplemento 459. (26-05-2021). *Ley Orgánica de Protección de Datos Personales.* https://app.lexis.com.ec/sistema/visualizador-norma/PUBLICO-LEY_ORGANICA_DE_PROTECCION_DE_DATOS_PERSONALES

Registro Oficial Suplemento 557. (2024). *Decreto Ejecutivo 262. Reglamento a la Ley de Seguriidad Pública y del Estado.* blob:https://app.lexis.com.ec/9975ffcc-b624-42f9-acec-729bfff88bde

Registro Oficial Suplemento 634. (2024-09-02). *Interporalidad de los Sistemas Tecnológicos con el ECU 911.* https://app.lexis.com.ec/sistema/visualizador-norma/PUBLICO-INTEROPERABILIDAD_DE_LOS_SISTEMAS_TECNOLOGICOS_CON_EL_ECU_911

Registro Oficial Suplemento, 634. (2024). *Interporabilidad de los Sistemas Tecnológicos con el ECU 911.* https://app.lexis.com.ec/sistema/visualizador-norma/PUBLICO-INTEROPERABILIDAD_DE_LOS_SISTEMAS_TECNOLOGICOS_CON_EL_ECU_911

Romero Torres, Juan. (2023). *Seguridad pública en el Ecuador*. https://ciencialatina.org/index.php/cienciala/article/view/8302/12501

Romero Torres, Juan. (2023). *Seguridad pública en el Ecuador*. https://ciencialatina.org/index.php/cienciala/article/view/8302/12501

Sánchez, M. (2023). Detrás de la Máscara Virtual: Desvelando los peligros para tu privacidad en aplicaciones de filtros y datos biométricos. Retos y oportunidades en la participación

de las mujeres. *Revista Iberoamericana de derecho informática*, 39-46. https://revistas.fcu.com.uy/index.php/informaticayderecho/article/view/4251

Soriano, A. (2021). Decisiones automatizadas: problemas y soluciones jurídicas. Mas allá de la protección de datos. *Revista de Derecho Público: Teoría y Método*, 85-127. https://doi.org/DOI:10.37417/RPD/vol_1_2021_535

Universidad Internacional de Valencia . (2017). *Reconocimiento facial: un reto jurídico en la protección de derechos fundamentales*. https://www.universidadviu.com/es/actualidad/nuestros-expertos/reconocimiento-facial-un-reto-juridico-en-la-proteccion-de-derechos

Urvio Revista Latinoamericana. (2020). Argentina. https://www.redalyc.org/pdf/5526/552656555007.pdf